KRATIKAL
SECURE FOR SURE

E-Book

Firewall Evasion

For Better Security

Securing your infrastructure with Red Teaming

Table Of Content

About Kratikal

01

Kratikal is a CERT-In-empanelled cyber security auditor. We offer comprehensive cybersecurity services to secure your IT infrastructure. In addition to assuring security through our services such as Web Application Testing, IoT Penetration Testing, Network Security Testing, and others. Our team of experts ensures to provide businesses with a variety of VAPT services as per the company's requirements. We protect businesses from online attacks and help them fix flaws, as well as comply with standard and regulatory compliances.

Kratikal is trusted by over 650+ Enterprises and SMEs worldwide. Our team of trained cybersecurity specialists offers complete security solutions to organizations of all sizes in a variety of industries. Trust Kratikal for VAPT and Compliance services to find and fix flaws before attackers exploit them. Work together with us to protect your digital assets effectively.

Introduction

02

Whether you are in a blue team or a red team, you need to know attacker tactics to prevent the latest threats and cyber attacks in cyber security. We say **"If you want to stop the hackers then you have to think like them".**

That's why we have researched and collected multiple evasion techniques attackers used to bypass them so you can better prevent those attacks on your important assets.

This E-book is a good source for all security professionals, **CISOs, CTOs,** and other decision-makers to ensure they are always one step ahead of these threat actors.

We have tried to make this e-book easy to understand so that anyone from IT can understand it and harden their IT and application security to protect them from cyber attacks.

Types of Firewall

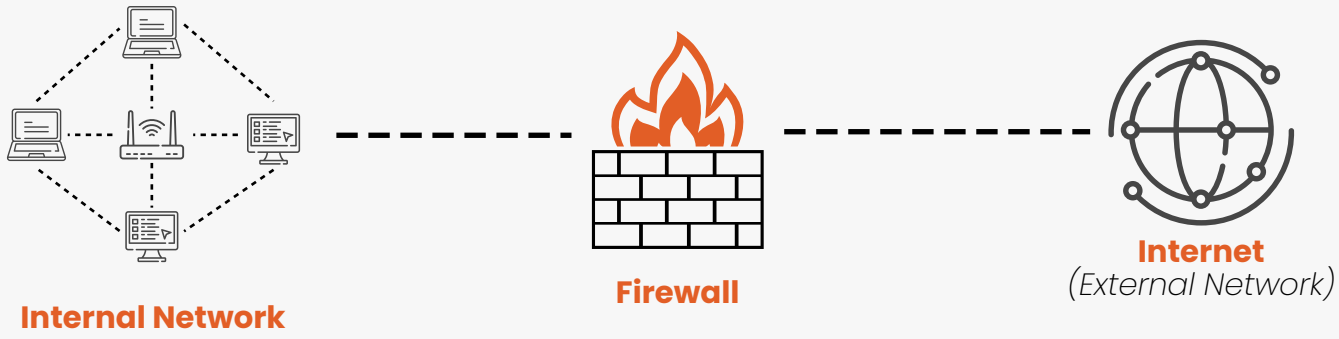
03

It is important to know what type of firewall we will discuss for evasion as there are many types of firewalls organizations use to protect their system and assets. We will first discuss the most common firewalls used by these organizations.

Type Of Firewall

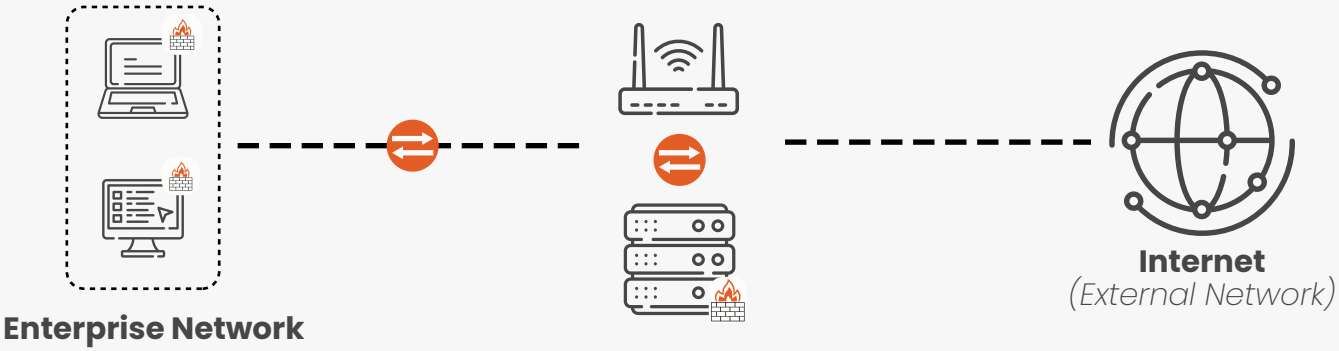
1. Network Firewall
2. Host Based Firewall
3. Web Application Firewall

Network Firewall



In a network firewall, the firewall lies between your device and the internet. All the internet traffic passes through the firewall before reaching your device. The firewall inspects the traffic and filters out any malicious packets, DDoS, or malware connections.

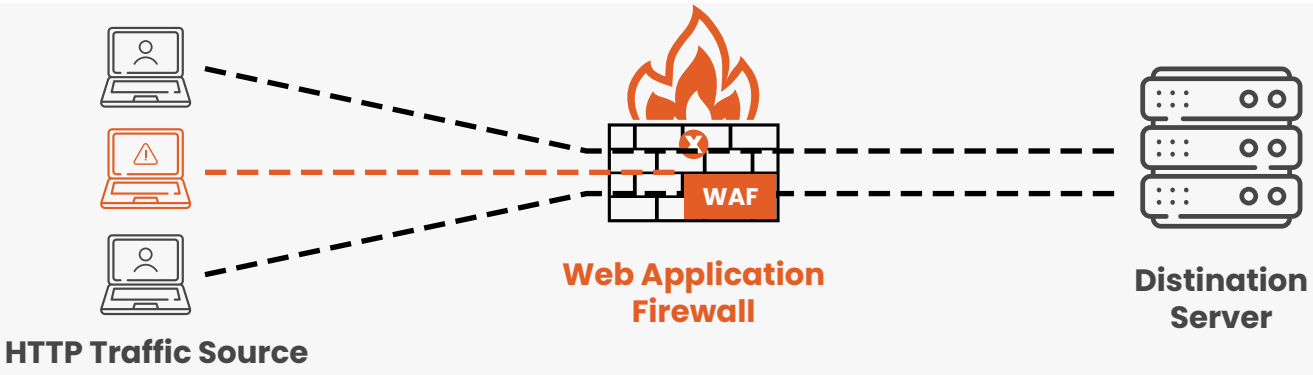
Host Based Firewall



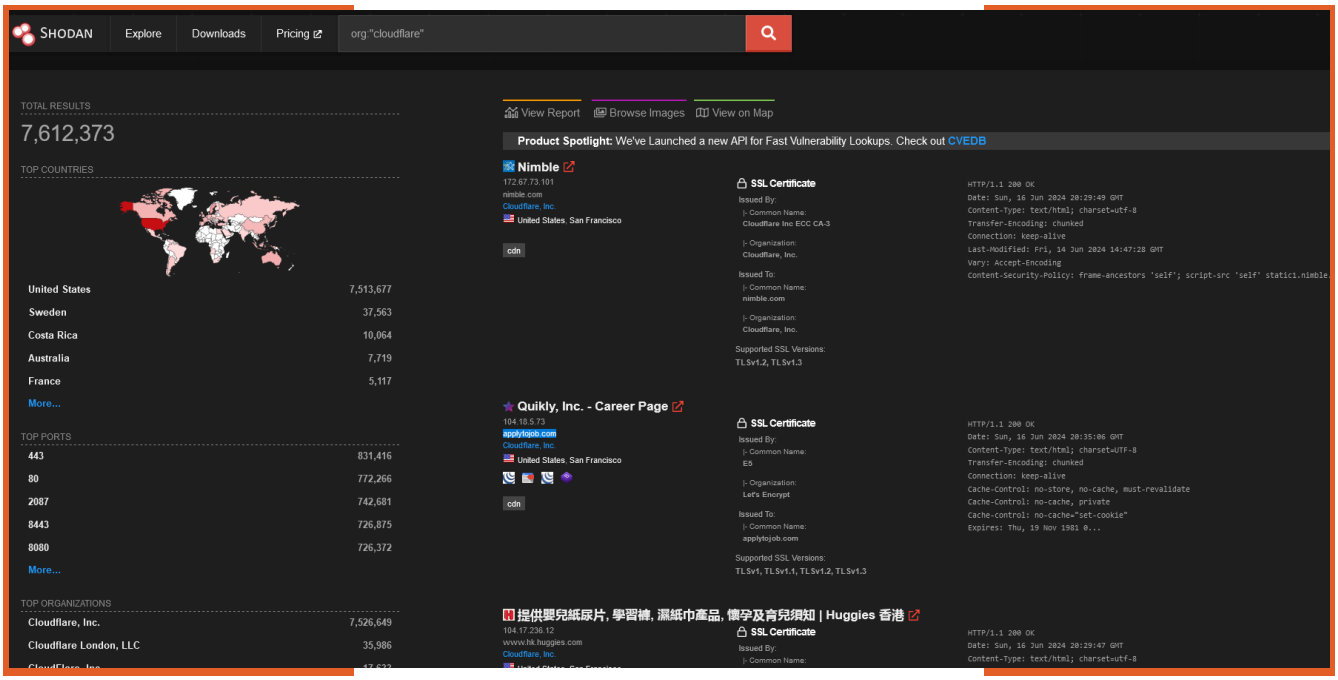
In Host-based firewalls, the firewall is installed on the device, for example in Linux IP Tables, firewall, or Windows firewall in the Windows operating system. These firewalls can be configured from the device and add extra layers to security with an added network firewall. This also prevents any malware from establishing any communication with servers.

Web Application Firewall

This is the firewall attackers usually target. These firewalls lie between your web server and the traffic coming from the internet. This allows web apps to block malicious traffic before reaching the server.



We will show how hackers bypass the **Cloudflare** firewall as this is the most used WAF (Web Application Firewall) by organizations. Cloudflare works as a **CDN (Content Delivery Network)** and a firewall; this makes it a perfect choice for most companies.



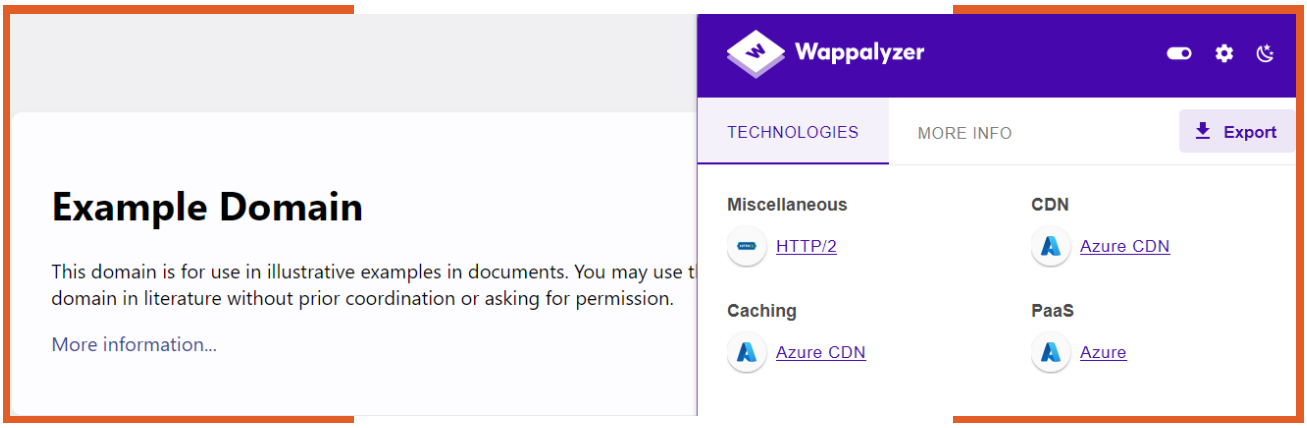
Finding Details About the Firewall

04

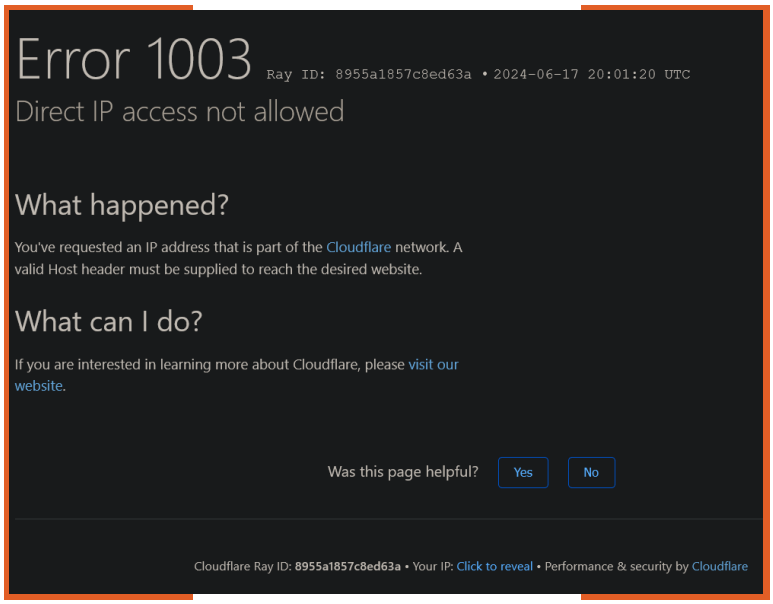
Identifying the server firewall is straightforward as the target has used many ways to detect the WAF.

Service Check

By checking the services running on the target system we can detect if any firewall or CDN is running on the target system. To do this attackers can use **wappalyzer.com** to detect and tell them all the services installed on the target server.



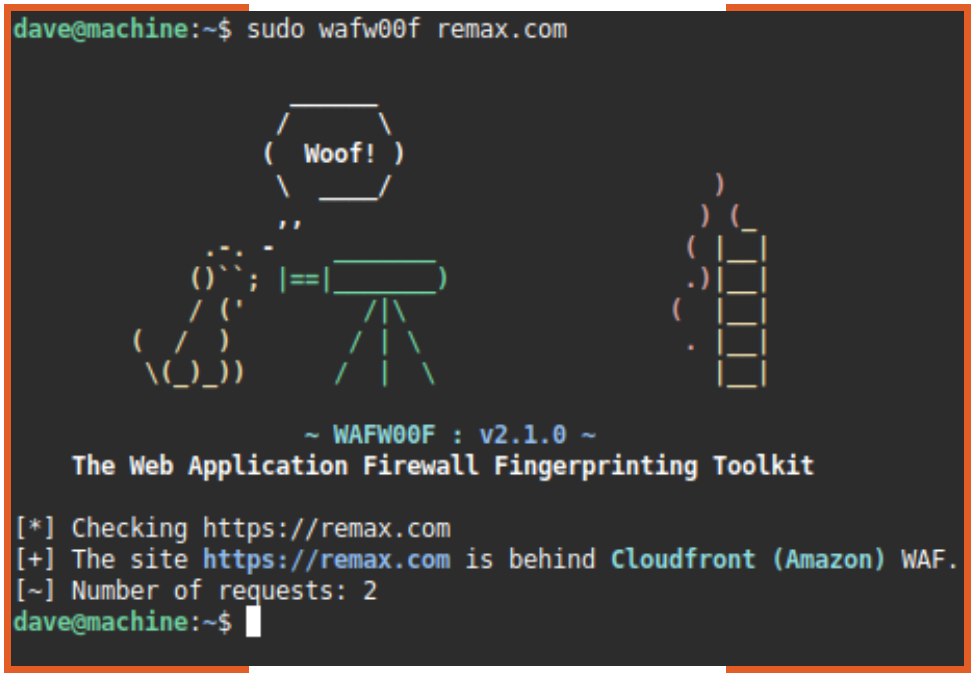
Ping Check



If we are talking about Cloudflare, they don't allow direct IP access so if the attacker pings the domain and tries to connect the website directly through the IP address he will get an alert from Cloudflare that "**Direct IP access not allowed".**

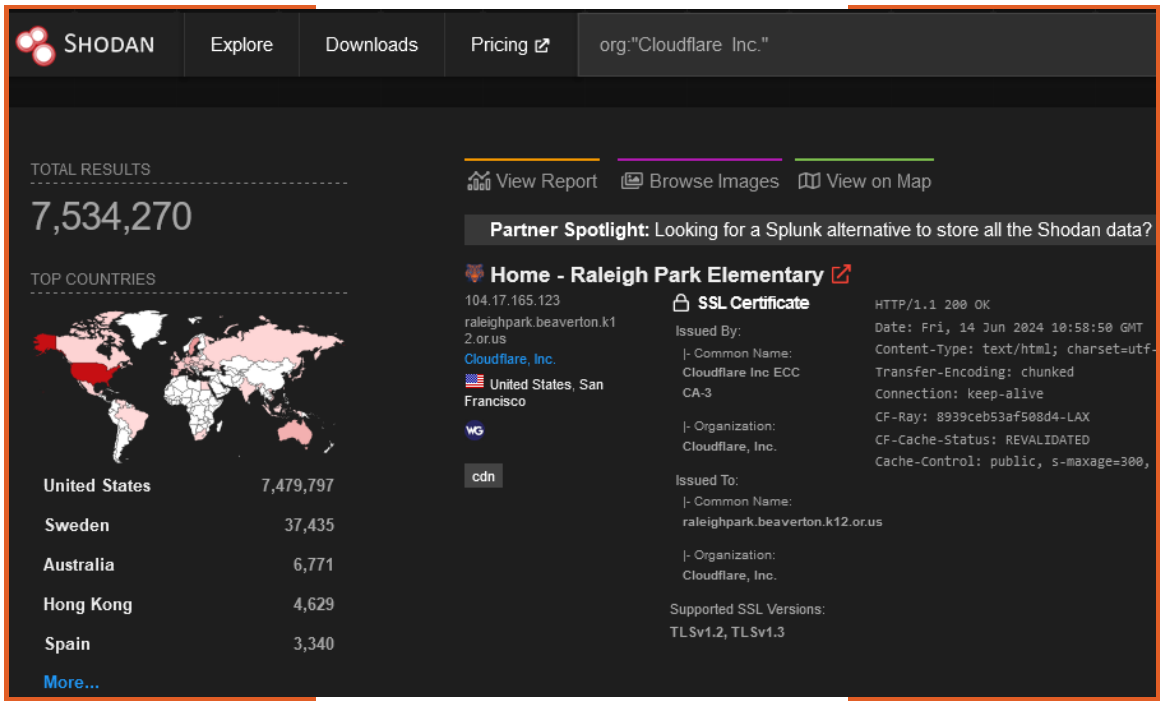
Wafw00f

Wafw00f is a go-to recon tool for your recon activity. Threat actors just need to set the target domain and it will fetch the running application firewall on the server side.



05 Why Attackers Target Cloudflare WAF?

The reason we are talking about Cloudflare bypass is that most organizations use it to protect their website from various attacks. If we look at Shodan, it will give us approximate data about how many websites use Cloudflare and that's approximately 7 lakh websites worldwide.



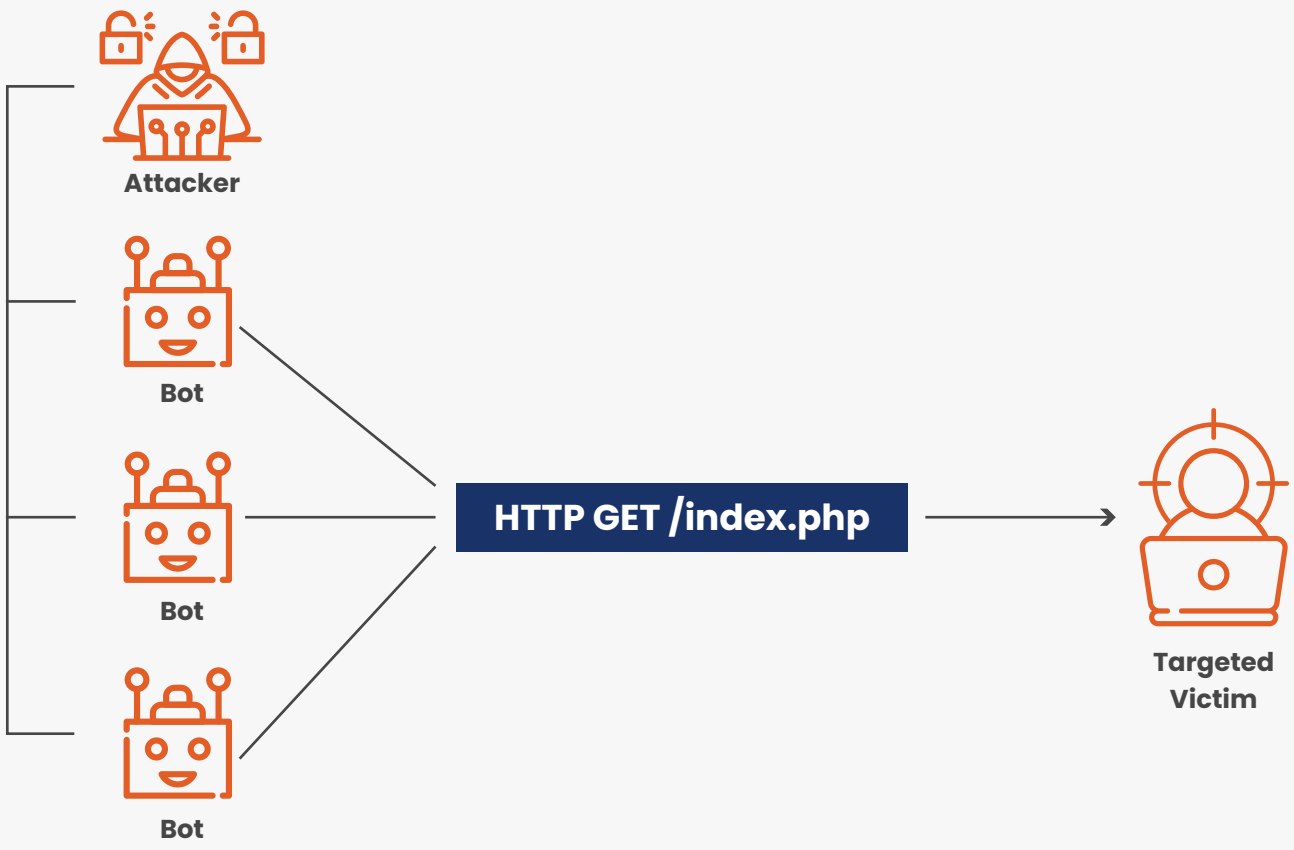
What after WAF Bypass?

If organizations are using Cloudflare then they may already have an idea of what could go wrong if hackers get access to their website IP.

But since this ebook targets every IT professional, let's discuss what happens if threat actors bypass Cloudflare.

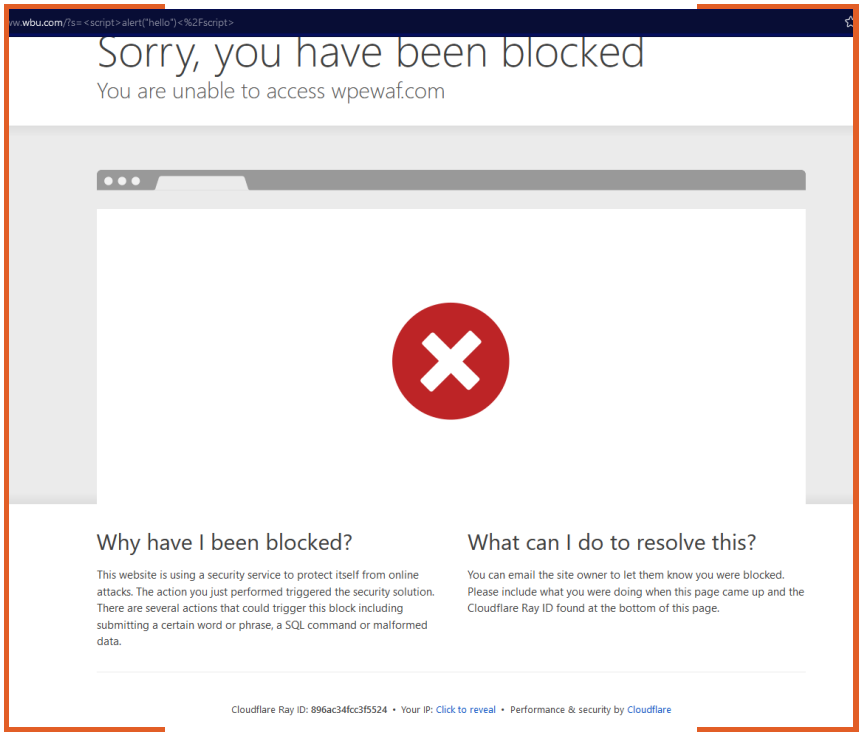
1. Nothing to protect against malicious traffic

Once hackers get access to the website's IP there's nothing to protect against any malicious traffic, especially DDoS attacks which can take down the website and create huge financial and reputational loss.



2. No protection from web attacks

Attackers are constantly learning new methods and ways to get inside the server, deface the site, and gain access to sensitive information and they get access to website without any firewall. For example, the screenshot below shows what happens when an attacker tries to insert malicious code in a website protected by a web app firewall, the WAF immediately blocks it.



So overall firewall (in this case **Cloudflare**) protects you from multiple attacks and threats coming from the internet to the website.

Bypass Cloudflare

06

This Cloudflare bypass helps attackers get direct access to the server and as we talked about this earlier there is nothing to protect against attacks. Please note this bypass method will not discuss XSS or other injection attack payload.

Subdomain Enumeration

When a website is protected by Cloudflare, the publicly visible IP address may not be the true IP address of the origin server. To reveal the actual IP address, you can perform subdomain enumeration, which involves identifying and enumerating all the subdomains associated with the target domain. Using Knockpy for Subdomain Enumeration.

One tool that can be used for this purpose is **Knockpy,** an open-source subdomain enumeration tool. To use Knockpy, simply run the command knockpy target.com (replacing target.com with the domain you want to

investigate). This will provide you with a list of subdomains associated with the target domain, along with the IP addresses where those subdomains are hosted. By analyzing the IP addresses revealed through the subdomain enumeration process, you can identify the true IP address of the origin server, which is typically concealed by Cloudflare's proxy services.

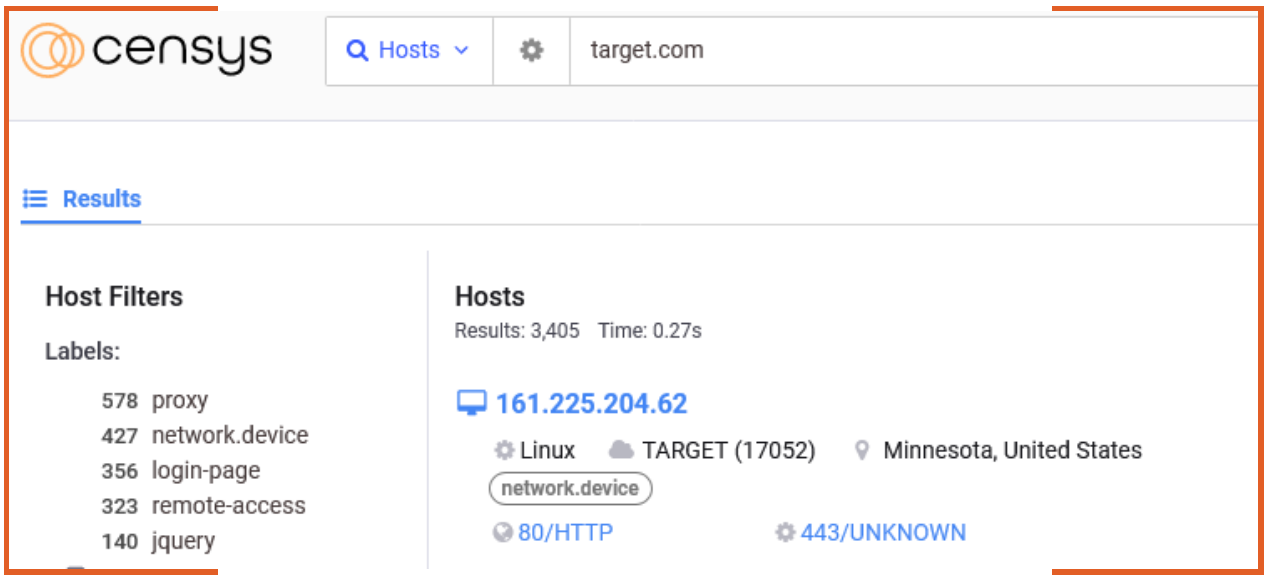
```
 _ __                  _
| |/ /                | |   v5.1.0
| ' / _ __   ___   __| | ___ __  _   _
|  < | '_ \ / _ \ / _| |/ / '_ \| | | |
| . \| | | | (_) | (__|   <| |_) | |_| |
|_|\_\_| |_|\___/ \___|_|\_\ .__/ \__, |
                           | |     __/ |
                           |_|    |___/

local: 2019 | google: 0 | duckduckgo: 5 | virustotal: 0

Wordlist: 2024 | Target: test.com | Ip: 67.225.146.248

10:20:17

Ip address      Code Subdomain                Server                   Real hostname
--------------- ---- ----------------------- ----------------------- -----------------------
69.167.164.199       01.test.com
69.167.164.199       02.test.com
69.167.164.199       03.test.com
69.167.164.199       1.test.com
69.167.164.199       10.test.com
```

This information can be valuable for further investigation or potential exploitation, depending on the context and your authorized access.

The screenshot demonstrates a technique for bypassing a WAF by enumerating subdomains that do not resolve to actual websites but return a 200 status code from servers not associated with Cloudflare. The attacker checks for subdomains meeting these criteria to potentially bypass the WAF's protections and access the origin server directly.

Certificate Search

Attackers use certificate search to bypass Cloudflare protection. Certificate details contain the unique identity of the website which threat actors use to gain information about the target website and get the real IP address of the server.

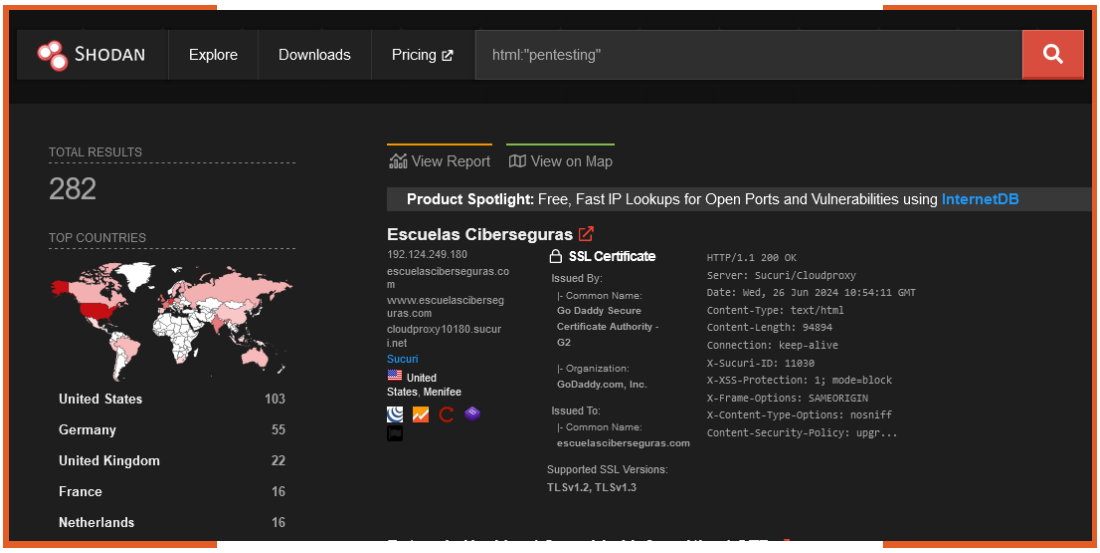


An example search shows how **Censys** check for certificate details and provide you the list of IP addresses.

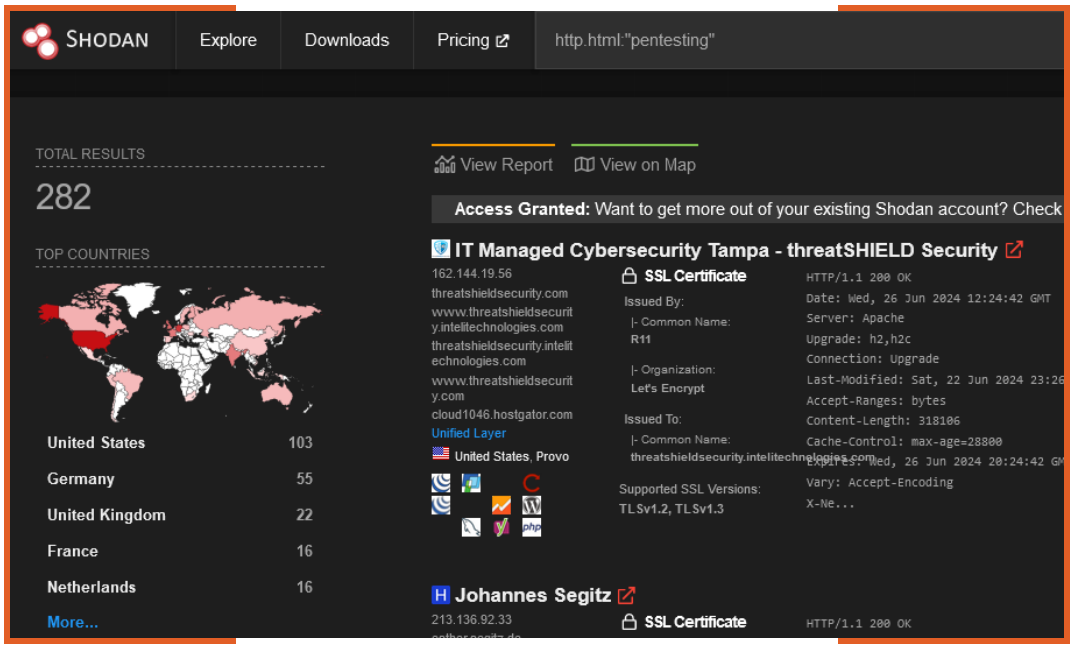
Shodan Search

Shodan can help you find the original server of a website. There are so many different search queries available on Shodan.

Start with html tag; just type the organization name in html and this should return the target website IP address.



The attacker can also find the real IP of the web server by using a **"unique string"** on the website. For example, if the target website is example.com and there's a word on the website that says **"advance pentesting"** then the attacker can search on Shodan using the query **http.html:"pentesting"** to get the real IP of the website.



Conclusion

07

Getting access to your real IP doesn't mean it will get hacked but that means now there is no one to protect from any kind of attack attempt by the threat actor. By properly configuring your firewall, installing a detection system, and following proper compliance you can prevent attackers from gaining unauthorized access to your system. However, Kratikal recommends frequent security assessments for better and improved security.

Kratikal's Red teaming solutions can be effective in protecting organizations from various types of cyber attacks, including those aimed at security bypass by using tools and techniques such as vulnerability assessments, penetration testing, and security audits organziations can prevent themselves from recent attacks.

Shaquib Izhar
Kratikal Security Research

KRATIKAL
SECURE FOR SURE

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

650+ Enterprises & SMEs

25k IT Infra Devices Tested & Delivered

100m+ Lines of Code Tested

4.1k+ Weeks Pentesting Experience

Our Services

VAPT Services

- Web Application Security Testing
- Mobile Application Security Testing
- Network Penetration Testing
- Cloud Penetration Testing
- IoT Security Testing
- Secure Code Review
- Medical Device Security Testing
- Threat Modeling
- Root Cause Analysis (RCA)

Compliance Services

Standard Compliance

- IS0/IEC 27001 Compliance
- SOC 2 Compliance
- GDPR Compliance
- HIPAA Compliance
- PCI DSS Compliance
- ISO 27701 PIMS
- ISO 27018 Certification
- ISO/IEC 27017 Certification
- Cyber Crisis Management Plan
- SDLC GAP Analysis

Regulatory Compliance

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