Sri Lanka Institute of Information Technology

Penetration Testing Report

IE3022 - Applied Information Assurance

B.Sc. (Hons) in Information Technology

Specializing Cyber Security

- **S.A.D.H. Vishwajith**
- **IT19952376**

Executive Summary

Several standardized tools and utilities were used to examine and analyze the target system. Overall, we agree that the implementations under scrutiny have achieved an acceptable level of security, although corrective action is required owing to medium and low risk concerns. The results of the investigation showed characteristics that are well-protected against several well-known flaws.

In reconnaissance of amazon.com I found few High, medium and low-level vulnerabilities and issues including Session Cookie Not Marked as Secure, Weak Ciphers Enabled, [Possible] BREACH Attack Detected.

Company's internal network and business website were included in the framework of this

engagement. Nmap, maltego, nslookup, recon-ng, sublist3r, theHarvester, angry ip, namp, legion tool, netsparker, nikto were used in the testing.

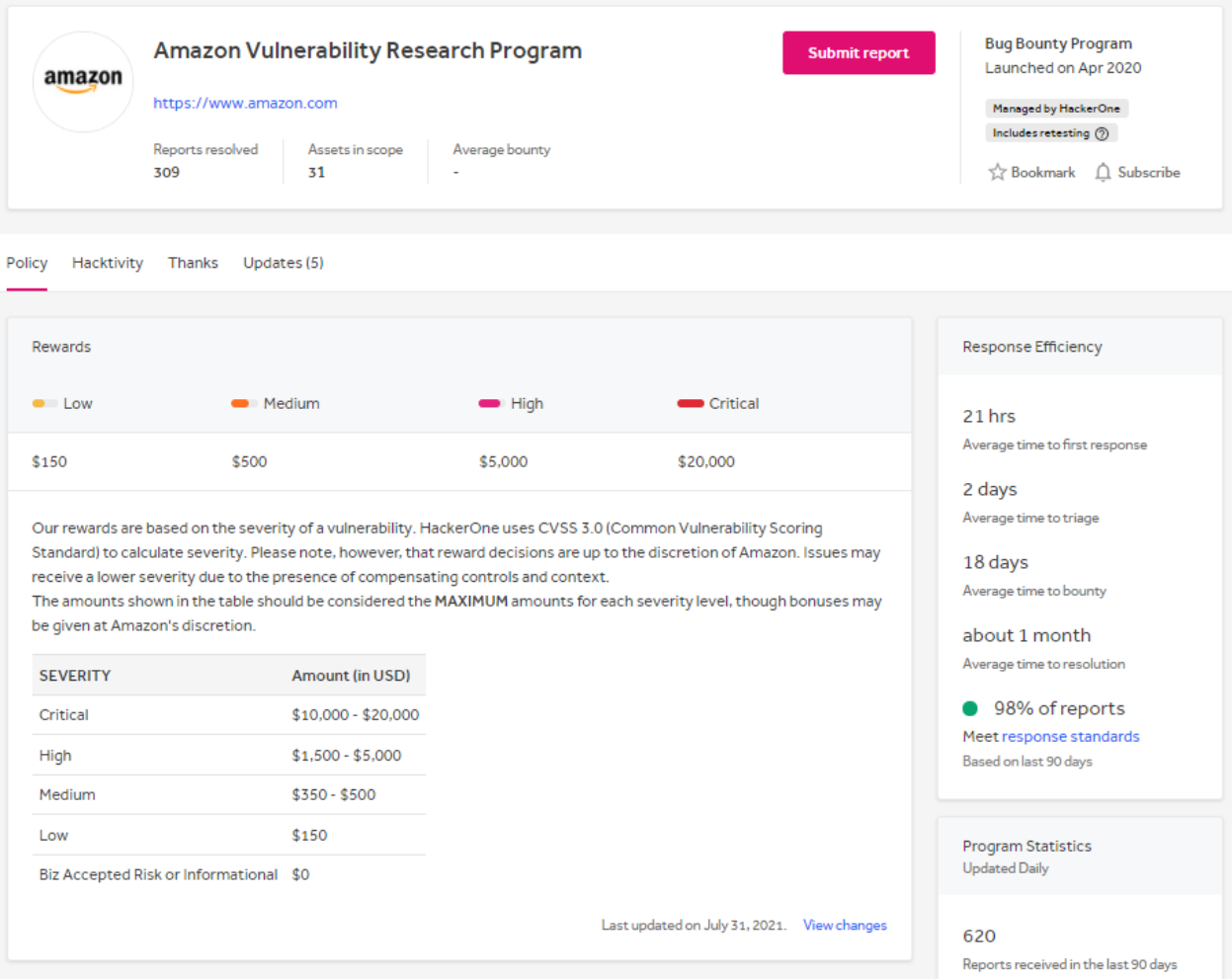
There are various stages of penetration testing listed as below,

1. Footprinting and Reconnaissance
2. Scanning
3. Enumeration
4. Analyzing Vulnerabilities

Target - www.amazon.com

Amazon.com is a vast Internet-based enterprise that sells books, music, movies, housewares, electronics, toys, and many other goods, either directly or as the middleman between other retailers and Amazon.com millions of customers.

Amazon joined with hacker one bug bounty and 300+ reports and bugs are sold and 31 assets scope only in hackerone bugbounty program.



amazon

Amazon Vulnerability Research Program

https://www.amazon.com

Submit report

Reports resolved 309 | Assets in scope 31 | Average bounty -

Bug Bounty Program
Launched on Apr 2020

Managed by HackerOne
Includes retesting

Bookmark Subscribe

Policy Hacktivity Thanks Updates (5)

Rewards

Low	Medium	High	Critical
$150	$500	$5,000	$20,000

Our rewards are based on the severity of a vulnerability. HackerOne uses CVSS 3.0 (Common Vulnerability Scoring Standard) to calculate severity. Please note, however, that reward decisions are up to the discretion of Amazon. Issues may receive a lower severity due to the presence of compensating controls and context.
The amounts shown in the table should be considered the **MAXIMUM** amounts for each severity level, though bonuses may be given at Amazon's discretion.

SEVERITY	Amount (in USD)
Critical	$10,000 - $20,000
High	$1,500 - $5,000
Medium	$350 - $500
Low	$150
Biz Accepted Risk or Informational	$0

Last updated on July 31, 2021. View changes

Response Efficiency

21 hrs
Average time to first response

2 days
Average time to triage

18 days
Average time to bounty

about 1 month
Average time to resolution

98% of reports
Meet response standards
Based on last 90 days

Program Statistics
Updated Daily

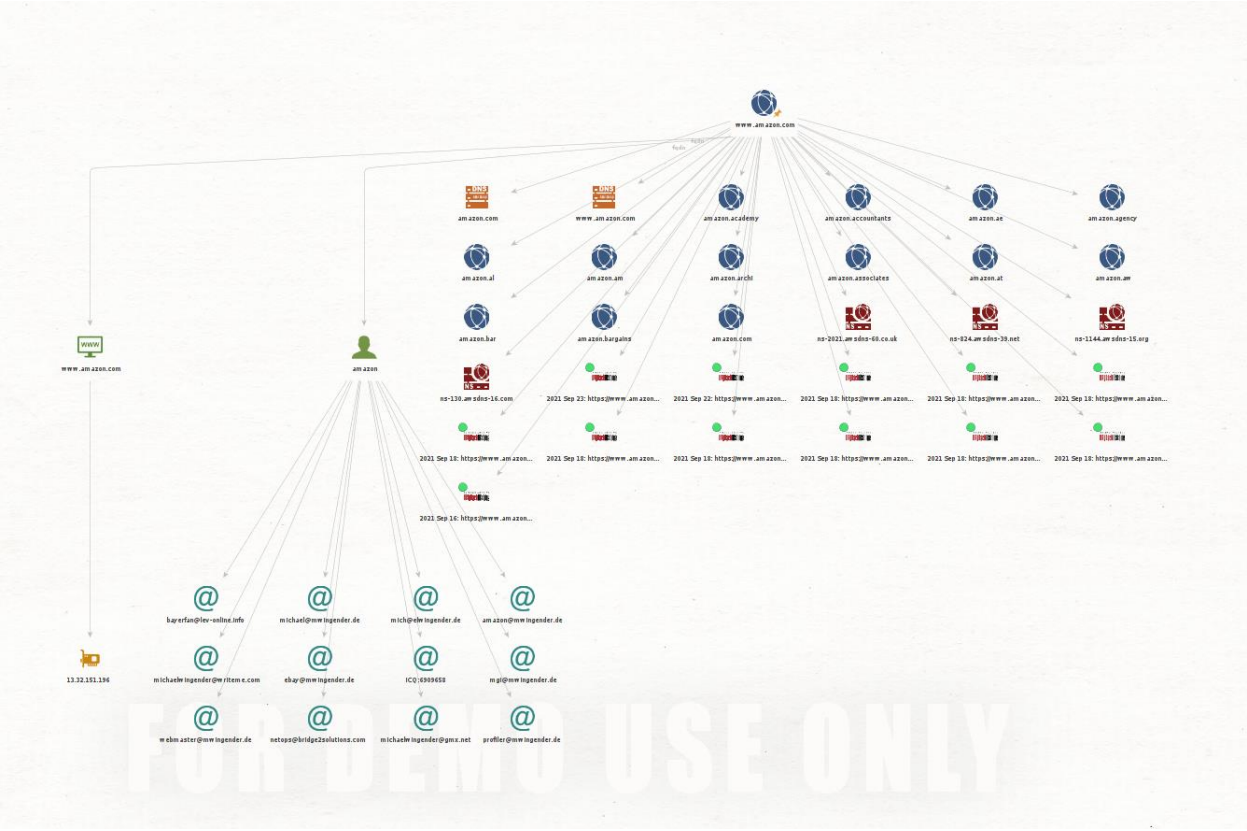
620
Reports received in the last 90 days

1. Footprinting and Reconnaissance

Footprinting is an element of the reconnaissance process that is used to acquire information about a target computer system or network. Footprinting may be both passive and active. Examining a company's website is an example of passive information collecting, whereas seeking to get access to classified information via social engineering is an example of active gathering information.

❖ Maltego

We can identify the relationships to which individuals are linked using Maltego, including their social profile, mutual friends, firms based on the details obtained, and websites.



❖ Recon-ng

Recon-ng is a full-featured Python Web Reconnaissance framework. With separate modules, database interaction, built-in convenience functions, interactive help, and command completion, Recon-ng provides a robust environment for doing open source web-based reconnaissance fast and comprehensively.

```
----------
AMAZON.COM
----------
[*] URL: http://searchdns.netcraft.com/?restriction=site%2Bends%2Bwith&host=amazon.com
[*] Country: None
[*] Host: www.amazon.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: smile.amazon.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: eu-west-1.console.aws.amazon.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: issues.amazon.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: w.amazon.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```

❖ Netcraft.com

Netcraft offers online security services such as cybercrime disruption and anti-phishing, application security testing, code reviews, automated penetration testing, research data, and research on a variety of internet topics.

Site report for http://www.amazon.com

Look up another site?

Share:

Background

Site title	Not Present	Date first seen	October 1995
Site rank	22	Netcraft Risk Rating	0/10
Description	Not Present	Primary language	Empty

Network

Site	http://www.amazon.com	Domain	amazon.com
Netblock Owner	Akamai Technologies, Inc.	Nameserver	dns-external-master.amazon.com
Hosting company	Akamai Technologies	Domain registrar	markmonitor.com
Hosting country	US	Nameserver organisation	whois.markmonitor.com
IPv4 address	23.72.34.17 (VirusTotal)	Organisation	Amazon Technologies, Inc., P.O. Box 8102, Reno, 89507, United States
IPv4 autonomous systems	AS16625	DNS admin	root@amazon.com
IPv6 address	Not Present	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	Not Present	DNS Security Extensions	unknown
Reverse DNS	a23-72-34-17.deploy.static.akamaitechnologies.com	Latest Performance	Performance Graph

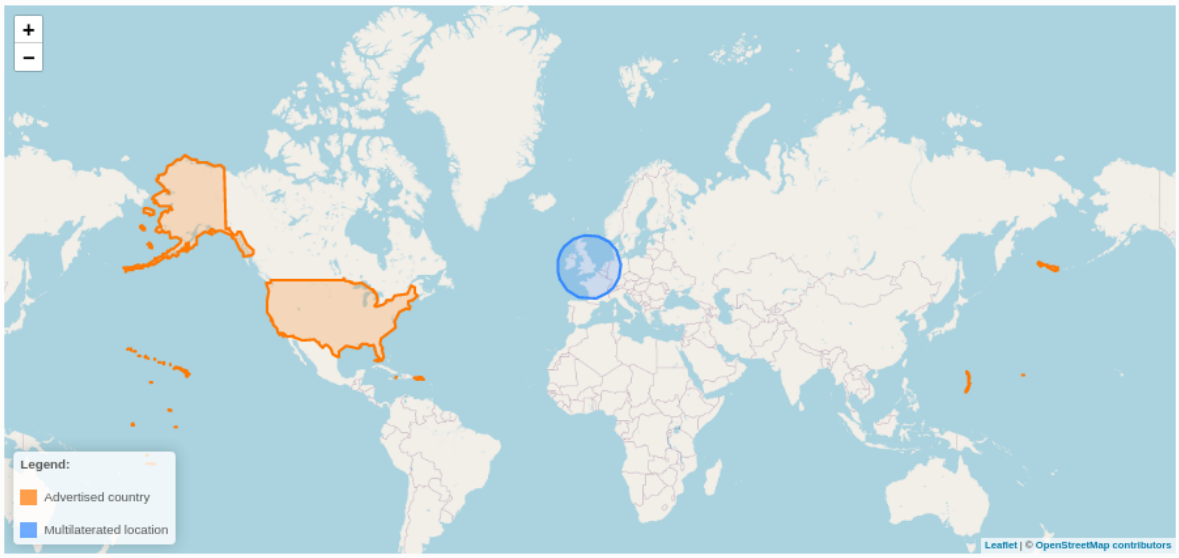
IP delegation

IPv4 address (23.72.34.17)

IP range	Country	Name	Description
0.0.0.0-255.255.255.255	N/A	IANA-BLK	The whole IPv4 address space
↳ 23.0.0.0-23.255.255.255	United States	NET23	American Registry for Internet Numbers
↳ 23.72.0.0-23.79.255.255	United States	AKAMAI	Akamai Technologies, Inc.
↳ 23.72.34.17	United States	AKAMAI	Akamai Technologies, Inc.

IP Geolocation

We use multilateration to independently determine the location of a server. Read more.



Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Amazon.com, Inc. Amazo...	162.219.225.118	unknown	Varnish	26-Sep-2021
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.40.97.56	Linux	AkamaiGHost	24-Sep-2021
Amazon.com, Inc. Amazo...	162.219.225.118	unknown	Varnish	23-Sep-2021
Akamai	88.221.17.57	Linux	AkamaiGHost	21-Sep-2021
Amazon.com, Inc. Amazo...	162.219.225.118	unknown	Varnish	20-Sep-2021
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	143.204.198.221	unknown	CloudFront	10-Sep-2021
Akamai	88.221.17.57	Linux	AkamaiGHost	9-Sep-2021
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	13.224.245.131	unknown	CloudFront	8-Sep-2021
Akamai	88.221.17.57	Linux	AkamaiGHost	7-Sep-2021
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	13.224.245.131	unknown	CloudFront	6-Sep-2021

Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of **rules**. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see **open-spf.org**.

Warning: It appears that this host does not have an SPF record. There may be an SPF record on amazon.com: Check the **site report**.

Setting up an SPF record helps prevent the delivery of forged emails from your domain. Please note that an SPF record will only protect the domain it is added to and not any **mail-enabled subdomains**. It is recommended to add an SPF record to any subdomain with an MX record.

❖ Nslookup

nslookup is a network management command-line utility that queries the Domain Name System for the mapping between a domain name and an IP address, as well as other DNS records.

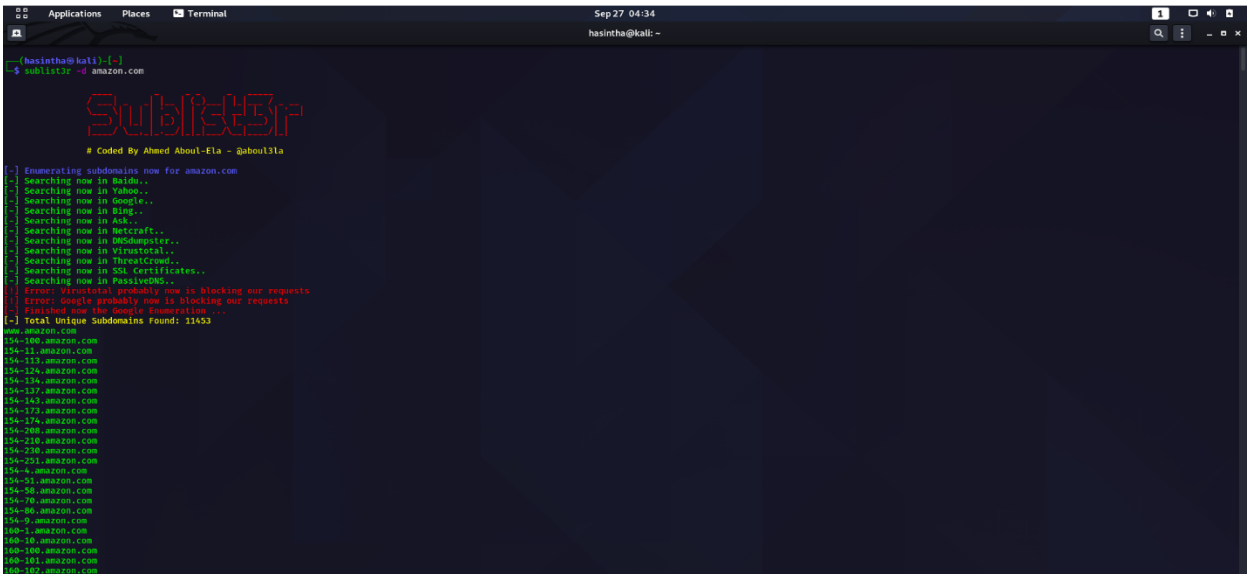
```
┌──(hasintha㉿kali)-[~]
└─$ nslookup amazon.com
Server:         192.168.8.1
Address:        192.168.8.1#53

Non-authoritative answer:
Name:   amazon.com
Address: 54.239.28.85
Name:   amazon.com
Address: 176.32.103.205
Name:   amazon.com
Address: 205.251.242.103


┌──(hasintha㉿kali)-[~]
└─$
```

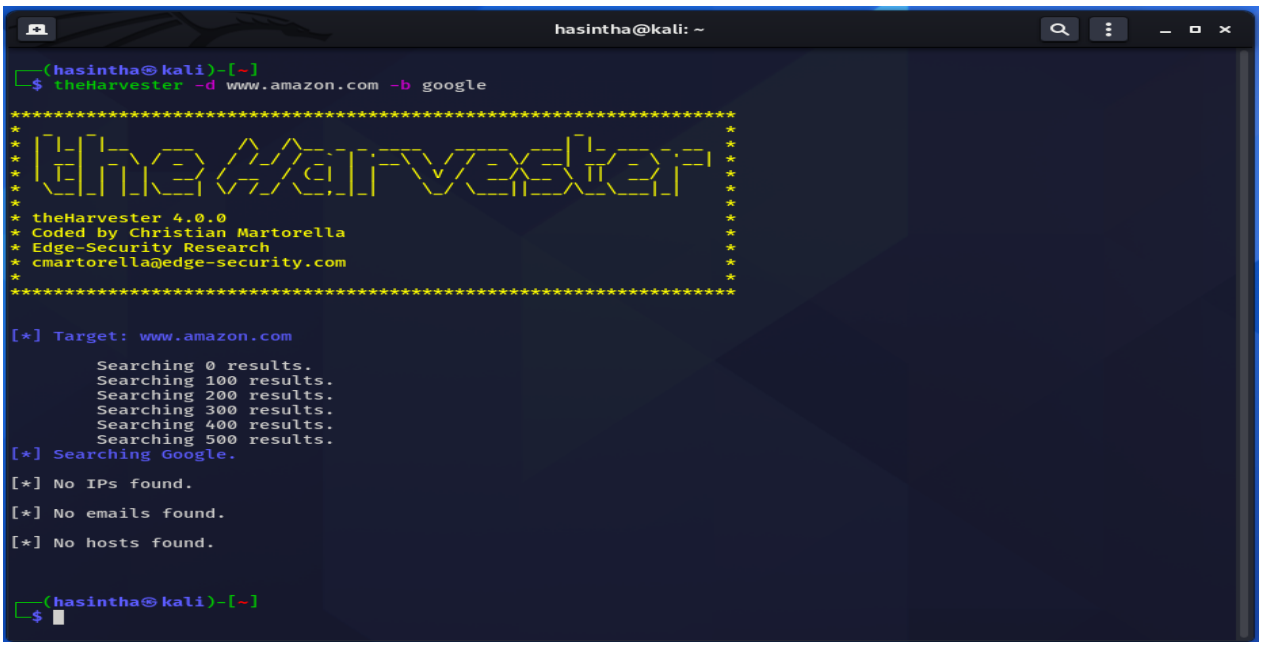
❖ Sublist3r

Sublist3r is a Python programme that uses OSINT to enumerate website subdomains. It assists penetration testers and bug hunters in collecting and gathering subdomains for the domain being targeted. Sublist3r enumerates subdomains by utilising a variety of search engines.



❖ theHarvester

The programmes' goal is to collect email, host names, employee names, subdomains, open ports, and banners from public resources such as search engines, PGP key servers, and the Shodan computer databases.



2. Scanning

❖ Nmap

Gordon Lyon invented Nmap, a free and open-source network scanner. Nmap is a network discovery tool that sends packets and analyses the replies to find hosts and services on a computer network. Nmap has several functions for probing computer networks, such as host discovery and service and os identification.

- **Using *Nmap <IP of target host>* for network scan.**

```
┌──(hasintha㉿kali)-[~]
└─$ nmap amazon.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-27 12:59 +0530
Nmap scan report for amazon.com (176.32.103.205)
Host is up (0.27s latency).
Other addresses for amazon.com (not scanned): 54.239.28.85 205.251.242.103
Not shown: 997 filtered ports
PORT     STATE SERVICE
25/tcp   open  smtp
80/tcp   open  http
443/tcp  open  https

Nmap done: 1 IP address (1 host up) scanned in 18.23 seconds
```

- **Using *Nmap –sV <IP of target host>* for an aggressive scan.**

```
┌──(hasintha㉿kali)-[~]
└─$ nmap -sV 176.32.103.205
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-27 13:00 +0530
Nmap scan report for 176.32.103.205
Host is up (0.27s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE    VERSION
25/tcp  open  tcpwrapped
80/tcp  open  http       Server
443/tcp open  ssl/https  Server
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.91%I=7%D=9/27%Time=6151734B%P=x86_64-pc-linux-gnu%r(GetR
SF:equest,165,"HTTP/1\.1\x20301\x20Moved\x20Permanently\r\nServer:\x20Serv
SF:er\r\nDate:\x20Mon,\x2027\x20Sep\x202021\x2007:31:22\x20GMT\r\nContent-
SF:Type:\x20text/html\r\nContent-Length:\x20179\r\nConnection:\x20keep-ali
SF:ve\r\nLocation:\x20https:///\r\n\r\n<html>\r\n<head><title>301\x20Moved
SF:\x20Permanently</title></head>\r\n<body\x20bgcolor=\"white\">\r\n<cente
SF:r><h1>301\x20Moved\x20Permanently</h1></center>\r\n<hr><center>Server</
SF:center>\r\n</body>\r\n</html>\r\n")%r(HTTPOptions,165,"HTTP/1\.1\x20301
SF:\x20Moved\x20Permanently\r\nServer:\x20Server\r\nDate:\x20Mon,\x2027\x2
SF:0Sep\x202021\x2007:31:23\x20GMT\r\nContent-Type:\x20text/html\r\nConten
SF:t-Length:\x20179\r\nConnection:\x20keep-alive\r\nLocation:\x20https:///
SF:\r\n\r\n<html>\r\n<head><title>301\x20Moved\x20Permanently</title></hea
SF:d>\r\n<body\x20bgcolor=\"white\">\r\n<center><h1>301\x20Moved\x20Perman
SF:ently</h1></center>\r\n<hr><center>Server</center>\r\n</body>\r\n</html
SF:>\r\n")%r(FourOhFourRequest,188,"HTTP/1\.1\x20301\x20Moved\x20Permanent
SF:ly\r\nServer:\x20Server\r\nDate:\x20Mon,\x2027\x20Sep\x202021\x2007:31:
SF:29\x20GMT\r\nContent-Type:\x20text/html\r\nContent-Length:\x20179\r\nCo
SF:nnection:\x20keep-alive\r\nLocation:\x20https:///nice%20ports%2C/Tri%6E
SF:ity\.txt%2ebak\r\n\r\n<html>\r\n<head><title>301\x20Moved\x20Permanentl
SF:y</title></head>\r\n<body\x20bgcolor=\"white\">\r\n<center><h1>301\x20M
SF:oved\x20Permanently</h1></center>\r\n<hr><center>Server</center>\r\n</b
SF:ody>\r\n</html>\r\n")%r(SIPOptions,139,"HTTP/1\.1\x20400\x20Bad\x20Requ
SF:est\r\nServer:\x20Server\r\nDate:\x20Mon,\x2027\x20Sep\x202021\x2007:32
SF::01\x20GMT\r\nContent-Type:\x20text/html\r\nContent-Length:\x20167\r\nC
SF:neonction:\x20close\r\n\r\n<html>\r\n<head><title>400\x20Bad\x20Request
SF:</title></head>\r\n<body\x20bgcolor=\"white\">\r\n<center><h1>400\x20Ba
SF:d\x20Request</h1></center>\r\n<hr><center>Server</center>\r\n</body>\r\
SF:n</html>\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port443-TCP:V=7.91%T=SSL%I=7%D=9/27%Time=61517352%P=x86_64-pc-linux-gnu
SF:%r(GetRequest,ED,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nServer:\x20Serv
SF:er\r\nDate:\x20Mon,\x2027\x20Sep\x202021\x2007:31:30\x20GMT\r\nContent-
SF:Type:\x20text/html\r\nContent-Length:\x2071\r\nConnection:\x20close\r\n
SF:ETag:\x20\"614331e6-47\"\r\n\r\n<!DOCTYPE\x20html><html><head><title>x<
SF:/title></head><body></body></html>\n")%r(HTTPOptions,ED,"HTTP/1\.1\x204
SF:00\x20Bad\x20Request\r\nServer:\x20Server\r\nDate:\x20Mon,\x2027\x20Sep
SF:\x202021\x2007:31:31\x20GMT\r\nContent-Type:\x20text/html\r\nContent-Le
SF:ngth:\x2071\r\nConnection:\x20close\r\nETag:\x20\"614331e6-47\"\r\n\r\n
SF:<!DOCTYPE\x20html><html><head><title>x</title></head><body></body></htm
SF:l>\n")%r(FourOhFourRequest,ED,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nSe
SF:rver:\x20Server\r\nDate:\x20Mon,\x2027\x20Sep\x202021\x2007:31:32\x20GM
SF:T\r\nContent-Type:\x20text/html\r\nContent-Length:\x2071\r\nConnection:
SF:\x20close\r\nETag:\x20\"614331e6-47\"\r\n\r\n<!DOCTYPE\x20html><html><h
SF:ead><title>x</title></head><body></body></html>\n")%r(tor-versions,157,
SF:"HTTP/1\.1\x20500\x20Internal\x20Server\x20Error\r\nServer:\x20Server\r
SF:\nDate:\x20Mon,\x2027\x20Sep\x202021\x2007:31:33\x20GMT\r\nContent-Type
SF::\x20text/html\r\nContent-Length:\x20187\r\nConnection:\x20close\r\n\r\
SF:n<html>\r\n<head><title>500\x20Internal\x20Server\x20Error</title></hea
```

- ***UsingNmap –p <port_number> <IP_of_target_host>*** **to scan a specific port number and** ***Nmap –p <range of port numbers> <IP_of_target_host>*** **to scan a specific port range.**

```
┌──(hasintha㉿kali)-[~]
└─$ nmap -p 20 176.32.103.205
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-27 13:24 +0530
Nmap scan report for 176.32.103.205
Host is up (0.31s latency).

PORT   STATE    SERVICE
20/tcp filtered ftp-data

Nmap done: 1 IP address (1 host up) scanned in 3.44 seconds

┌──(hasintha㉿kali)-[~]
└─$ nmap -p 20-30 176.32.103.205
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-27 13:25 +0530
Nmap scan report for 176.32.103.205
Host is up (0.25s latency).

PORT   STATE    SERVICE
20/tcp filtered ftp-data
21/tcp filtered ftp
22/tcp filtered ssh
23/tcp filtered telnet
24/tcp filtered priv-mail
25/tcp open     smtp
26/tcp filtered rsftp
27/tcp filtered nsw-fe
28/tcp filtered unknown
29/tcp filtered msg-icp
30/tcp filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 3.99 seconds

┌──(hasintha㉿kali)-[~]
└─$
```

- **Using** ***Nmap –O <IP of target host>*** **for check Operating system.**

```
┌──(root💀kali)-[/home/hasintha]
└─# nmap -o 20 176.32.103.205

Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-27 13:27 +0530
Warning: 176.32.103.205 giving up on port because retransmission cap hit (10).
Nmap scan report for 176.32.103.205
Host is up (0.00027s latency).
Not shown: 551 closed ports, 446 filtered ports
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 8201.32 seconds
```

- **Using *sudo Nmap --traceroute < IP of target host >***

```
┌──(root💀kali)-[/home/hasintha]
└─# sudo nmap --traceroute 176.32.103.205
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-27 13:29 +0530
Warning: 176.32.103.205 giving up on port because retransmission cap hit (10).
Nmap scan report for 176.32.103.205
Host is up (0.00047s latency).
Not shown: 676 filtered ports, 321 closed ports
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.16 ms 10.0.2.2
2   0.24 ms 176.32.103.205

Nmap done: 1 IP address (1 host up) scanned in 11058.00 seconds
```

- **Using *Nmap -oN < IP of target host >***

```
┌──(hasintha㉿kali)-[~]
└─$ nmap -oN amazon.txt 176.32.103.205
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-27 13:30 +0530
Nmap scan report for 176.32.103.205
Host is up (0.28s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 17.57 seconds

┌──(hasintha㉿kali)-[~]
└─$
```

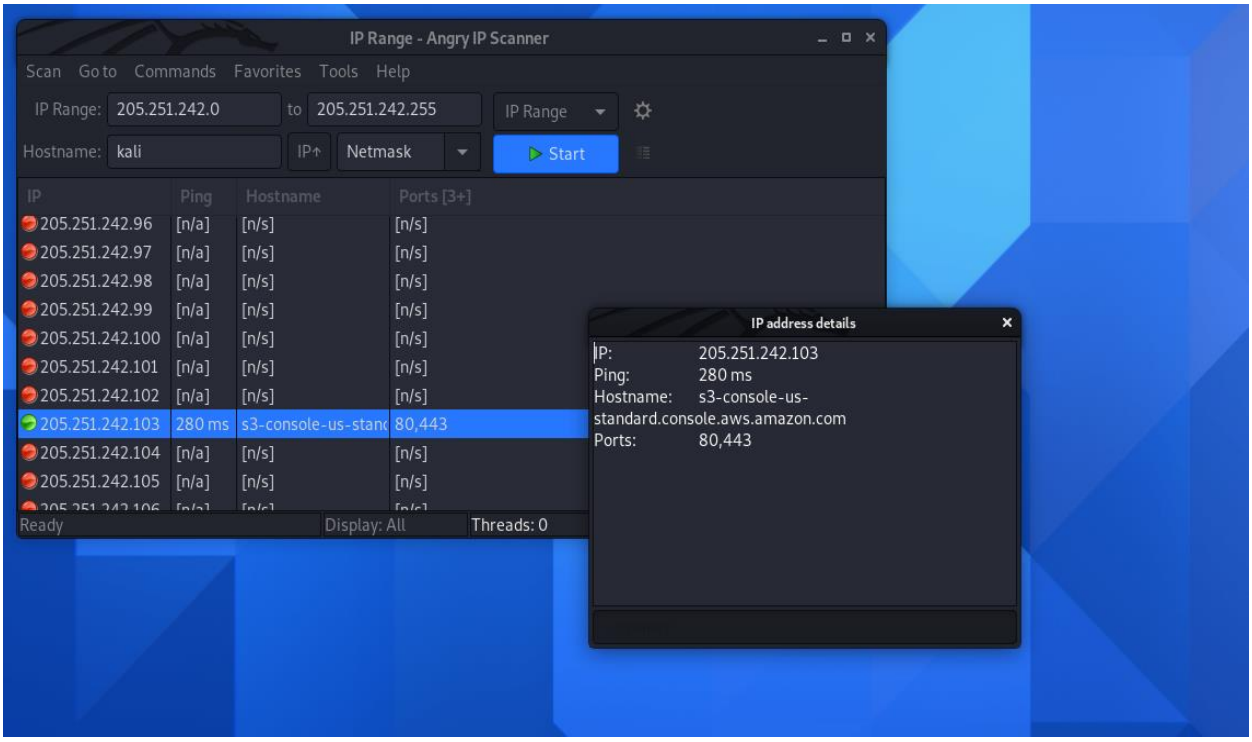
- **Using *Nmap -A < IP of target host >***

```
┌──(hasintha㉿kali)-[~]
└─$ nmap -A 176.32.103.205
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-27 13:03 +0530
Nmap scan report for 176.32.103.205
Host is up (0.29s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE    VERSION
25/tcp  open  tcpwrapped
|_smtp-commands: Couldn't establish connection on port 25
80/tcp  open  http       Server
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 301 Moved Permanently
|     Server: Server
|     Date: Mon, 27 Sep 2021 07:34:06 GMT
|     Content-Type: text/html
|     Content-Length: 179
|     Connection: keep-alive
|     Location: https:///nice%20ports%2C/Tri%6Eity.txt%2ebak
|     <html>
|     <head><title>301 Moved Permanently</title></head>
|     <body bgcolor="white">
|     <center><h1>301 Moved Permanently</h1></center>
|     <hr><center>Server</center>
|     </body>
|     </html>
|   GetRequest:
|     HTTP/1.1 301 Moved Permanently
|     Server: Server
|     Date: Mon, 27 Sep 2021 07:33:59 GMT
|     Content-Type: text/html
|     Content-Length: 179
|     Connection: keep-alive
|     Location: https:///
|     <html>
|     <head><title>301 Moved Permanently</title></head>
|     <body bgcolor="white">
|     <center><h1>301 Moved Permanently</h1></center>
|     <hr><center>Server</center>
|     </body>
|     </html>
|   HTTPOptions:
|     HTTP/1.1 301 Moved Permanently
|     Server: Server
|     Date: Mon, 27 Sep 2021 07:34:00 GMT
|     Content-Type: text/html
|     Content-Length: 179
|     Connection: keep-alive
|     Location: https:///
|     <html>
|     <head><title>301 Moved Permanently</title></head>
|     <body bgcolor="white">
|     <center><h1>301 Moved Permanently</h1></center>
|     <hr><center>Server</center>
|     </body>
|     </html>
|   SIPOptions:
|     HTTP/1.1 400 Bad Request
|     Server: Server
|     Date: Mon, 27 Sep 2021 07:34:38 GMT
```

```
|     </html>
|   SIPOptions:
|     HTTP/1.1 400 Bad Request
|     Server: Server
|     Date: Mon, 27 Sep 2021 07:34:38 GMT
|     Content-Type: text/html
|     Content-Length: 167
|     Cneonction: close
|     <html>
|     <head><title>400 Bad Request</title></head>
|     <body bgcolor="white">
|     <center><h1>400 Bad Request</h1></center>
|     <hr><center>Server</center>
|     </body>
|     </html>
|_http-server-header: Server
|_http-title: Did not follow redirect to https://176.32.103.205/
443/tcp open  ssl/https  Server
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 400 Bad Request
|     Server: Server
|     Date: Mon, 27 Sep 2021 07:34:08 GMT
|     Content-Type: text/html
|     Content-Length: 71
|     Connection: close
|     ETag: "614331e6-47"
|     <!DOCTYPE html><html><head><title>x</title></head><body></body></html>
|   GetRequest:
|     HTTP/1.1 400 Bad Request
|     Server: Server
|     Date: Mon, 27 Sep 2021 07:34:06 GMT
|     Content-Type: text/html
|     Content-Length: 71
|     Connection: close
|     ETag: "614331e6-47"
|     <!DOCTYPE html><html><head><title>x</title></head><body></body></html>
|   HTTPOptions:
|     HTTP/1.1 400 Bad Request
|     Server: Server
|     Date: Mon, 27 Sep 2021 07:34:07 GMT
|     Content-Type: text/html
|     Content-Length: 71
|     Connection: close
|     ETag: "614331e6-47"
|     <!DOCTYPE html><html><head><title>x</title></head><body></body></html>
|   RPCCheck:
|     HTTP/1.1 500 Internal Server Error
|     Server: Server
|     Date: Mon, 27 Sep 2021 07:34:17 GMT
|     Content-Type: text/html
|     Content-Length: 187
|     Connection: close
|     <html>
|     <head><title>500 Internal Server Error</title></head>
|     <body bgcolor="white">
|     <center><h1>500 Internal Server Error</h1></center>
|     <hr><center>Server</center>
|     </body>
|     </html>
|   RTSPRequest:
```

❖ Angry ip

Angry IP Scanner is a cross-platform, open-source network scanner that is quick and easy to use. It checks IP addresses and ports and has a slew of additional capabilities. It is extensively used by network administrators and ordinary users all over the world, including major and small businesses, banks, and government organizations. It operates on Linux, Windows, and Mac OS X, and it may support additional platforms in the future.

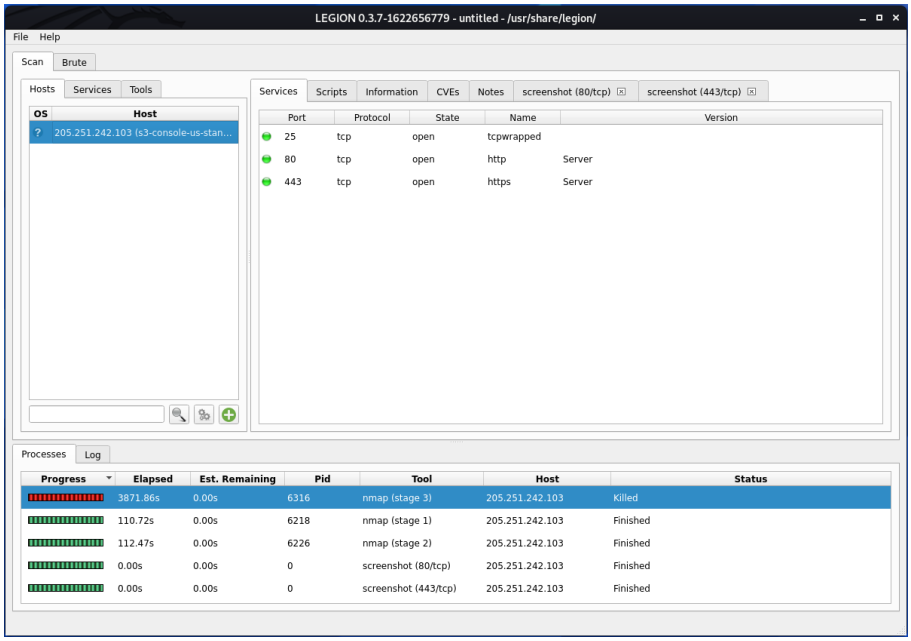


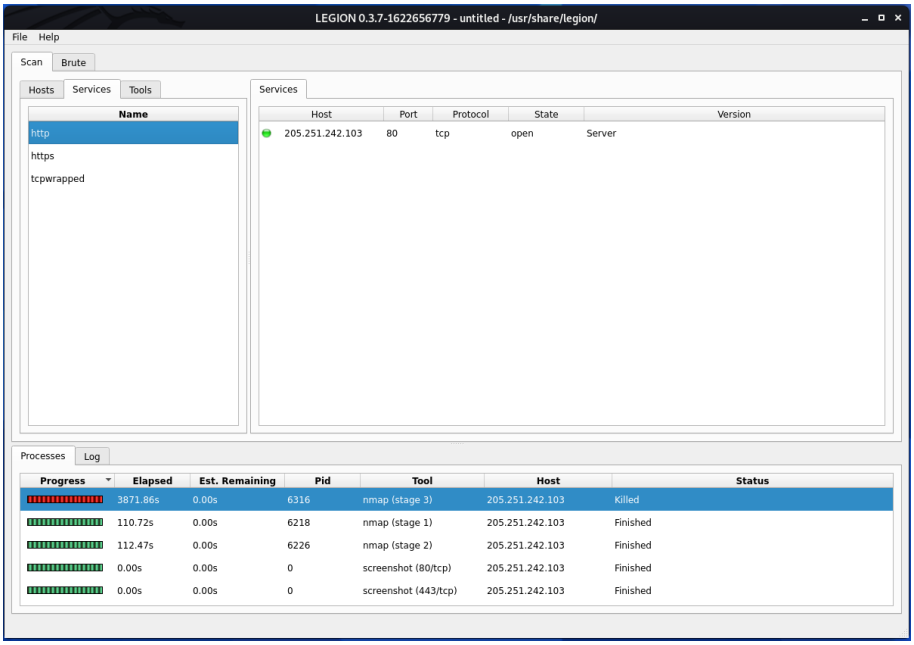
3. Enumeration

Enumerating target is a method that discovers and gathers information about the ports, os, and services of the victim machine. This technique is frequently used once we have established that the target machines are reachable.

❖ Legion Tool

Legion tool is a moderately penetration testing platform. Legion is extremely straightforward to run. Features of Legion Tool: GUI with panels and a broad number of settings that allow pentesters to swiftly discover and exploit attack routes on hosts.





❖ Host command

In a Linux system, the host command is used to do DNS (Domain Name System) lookups. In layman's terms, this command is used to discover the IP address of a specific domain name, or if you want to find the domain name of a specific IP address, the host command comes in useful.

- **public ip and mail servers**

```
┌──(hasintha㉿kali)-[~]
└─$ host amazon.com
amazon.com has address 176.32.103.205
amazon.com has address 205.251.242.103
amazon.com has address 54.239.28.85
amazon.com mail is handled by 5 amazon-smtp.amazon.com.
```

- **Name servers**

```
┌──(hasintha㉿kali)-[~]
└─$ host -t ns amazon.com
amazon.com name server ns4.p31.dynect.net.
amazon.com name server pdns1.ultradns.net.
amazon.com name server pdns6.ultradns.co.uk.
amazon.com name server ns1.p31.dynect.net.
amazon.com name server ns2.p31.dynect.net.
amazon.com name server ns3.p31.dynect.net.
```

- **Mail servers**

```
┌──(hasintha㉿kali)-[~]
└─$ host -t mx amazon.com
amazon.com mail is handled by 5 amazon-smtp.amazon.com.
```

❖ Dig command

dig is a network management command-line program that searches the Domain Name System. Dig is handy for troubleshooting as well as education. It may run in batch mode by reading requests from an operating system file, or it can operate depending on command line option and flag arguments.

```
┌──(hasintha㉿kali)-[~]
└─$ dig amazon.com

; <<>> DiG 9.16.15-Debian <<>> amazon.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64239
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;amazon.com.                    IN      A

;; ANSWER SECTION:
amazon.com.             27      IN      A       54.239.28.85
amazon.com.             27      IN      A       176.32.103.205
amazon.com.             27      IN      A       205.251.242.103

;; Query time: 0 msec
;; SERVER: 192.168.8.1#53(192.168.8.1)
;; WHEN: Mon Sep 27 17:31:05 +0530 2021
;; MSG SIZE  rcvd: 87
```

- **Mail Servers**

```
┌──(hasintha㉿kali)-[~]
└─$ dig amazon.com mx

; <<>> DiG 9.16.15-Debian <<>> amazon.com mx
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33470
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;amazon.com.                    IN      MX

;; ANSWER SECTION:
amazon.com.             900     IN      MX      5 amazon-smtp.amazon.com.

;; Query time: 83 msec
;; SERVER: 192.168.8.1#53(192.168.8.1)
;; WHEN: Mon Sep 27 17:31:25 +0530 2021
;; MSG SIZE  rcvd: 67
```

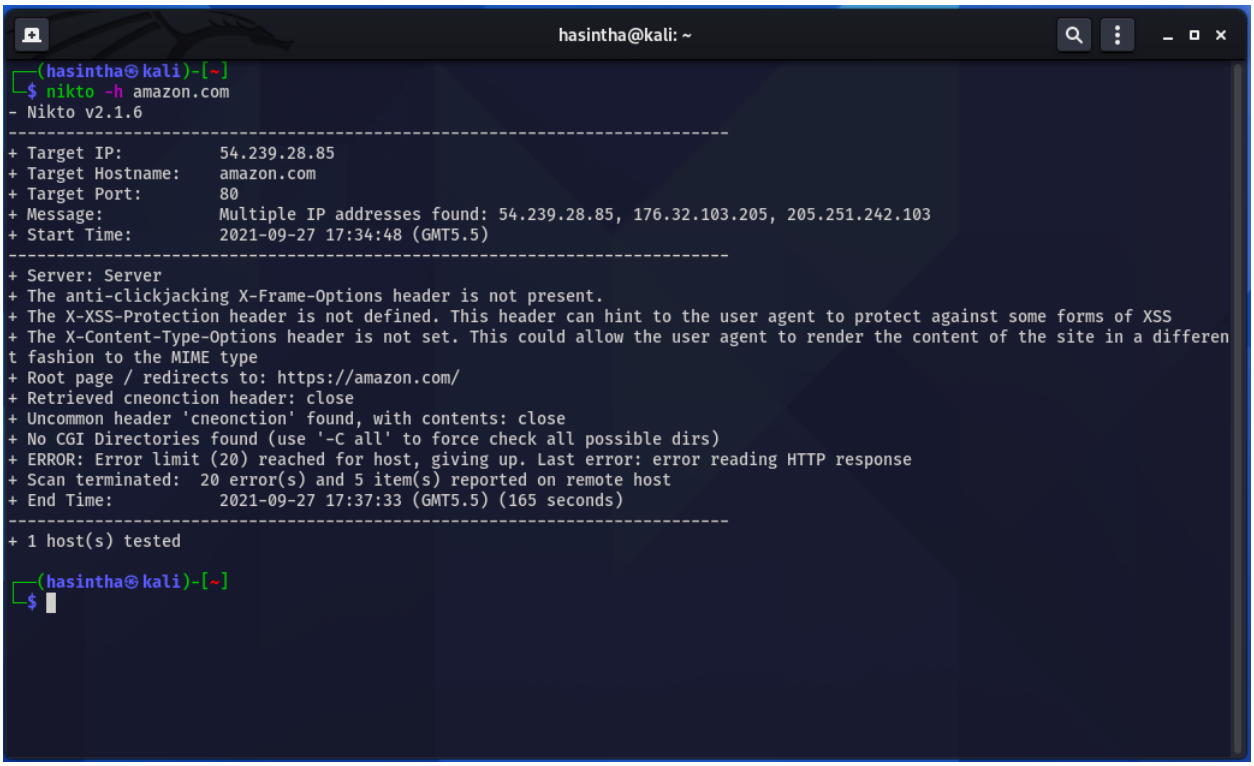
- **Name Servers**

```
┌──(hasintha㉿kali)-[~]
└─$ dig amazon.com -t ns +short
ns3.p31.dynect.net.
ns2.p31.dynect.net.
pdns6.ultradns.co.uk.
ns4.p31.dynect.net.
ns1.p31.dynect.net.
pdns1.ultradns.net.
```

4. Analyzing Vulnerabilities

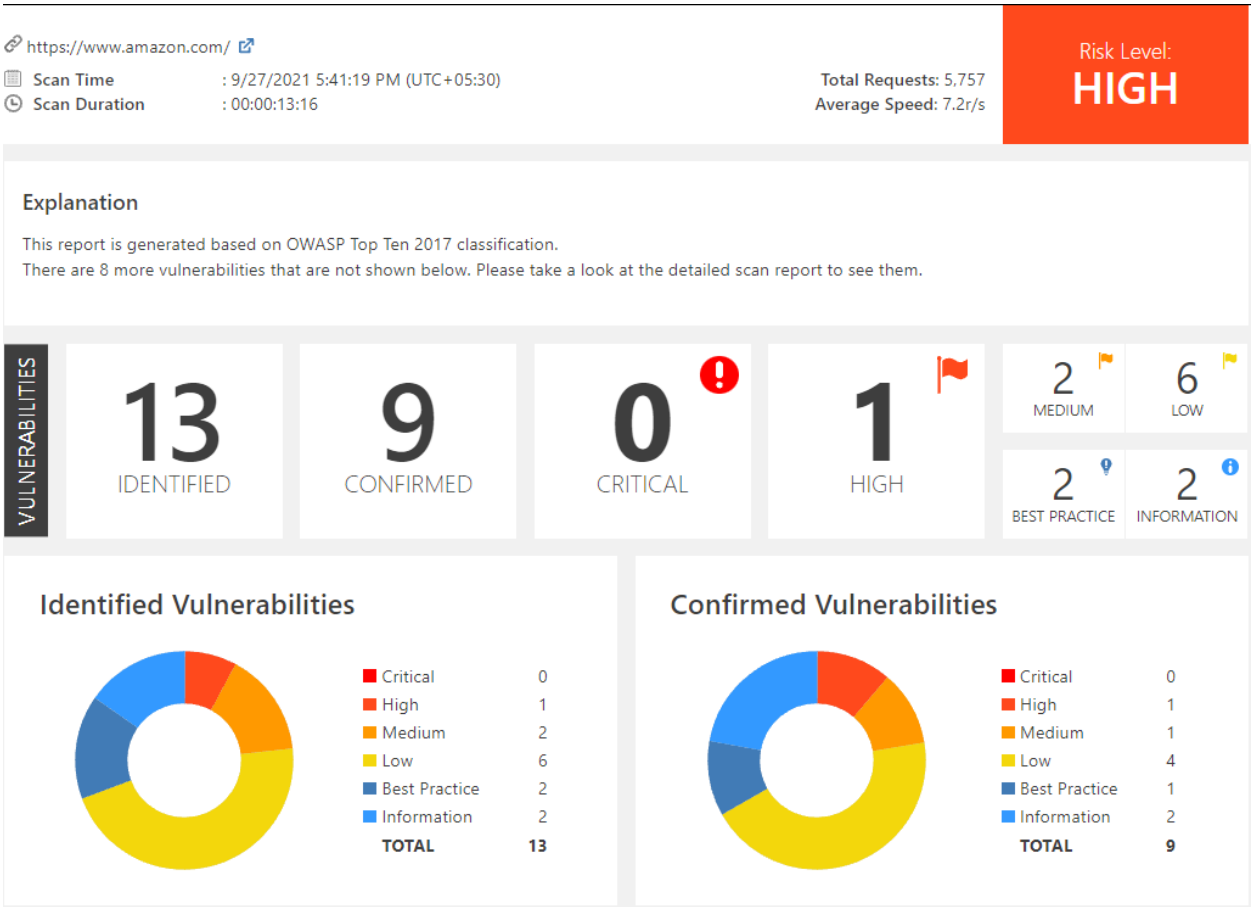
❖ Nikto scan

Nikto is a free command-line vulnerability scanner that looks for hazardous files/CGIs, obsolete server software, and other issues on webservers.



❖ Netsparker

Netsparker is an automatic, yet completely configurable, online application security scanner that allows you to scan and discover security issues in websites, web applications, and web services. Netsparker can scan all sorts of online applications, independent of platform or programming language.



Vulnerabilities Found

1. Session Cookie Not Marked as Secure

Impact

- Level - **HIGH**
- This cookie will be transmitted over a HTTP connection; therefore, an attacker might intercept it and hijack a victim's session. If the attacker can carry out a man-in-the-middle attack, he/she can force the victim to make an HTTP request to your website in order to steal the cookie.

Action to Take

- See the remedy for solution.
- Mark all cookies used within the application as secure.

Remedy

- Mark all cookies used within the application as secure.

2. Weak Ciphers Enabled

Impact

- Level - **MEDIUM**
- Attackers might decrypt SSL traffic between your server and your visitors.

Actions to Take

- For Apache, you should modify the SSLCipherSuite directive in the httpd.conf.
  SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4

- Lighttpd:
  ssl.honor-cipher-order = "enable"
  ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"

- For Microsoft IIS, you should make some changes to the system registry. Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.

Remedy

- Configure your web server to disallow using weak ciphers.

3. [Possible] BREACH Attack Detected

Impact

- Level – **MEDIUM**
- Even if you use an SSL/TLS protected connection, an attacker can still view the victim's encrypted traffic and cause the victim to send HTTP requests to the vulnerable web server (by using invisible frames). Following these steps, an attacker could steal information from the website and do the following:
  - Inject partial plaintext they have uncovered into a victim's requests
  - Measure the size of encrypted traffic

Remedy

- If possible, disable HTTP level compression
- Separate sensitive information from user input
- Protect vulnerable pages with CSRF token. The Same Site Cookie attribute will mitigate this issue, because to exploit this issue an attacker forces the victim to visit a target website using invisible frames. With the Same Site cookie attribute added, cookies that belong to the target won't be sent with a request that does not include top level navigation.
- Hide the length of the traffic by adding a random number of bytes to the responses.
- Add in a rate limit, so that the page maximum is reached five times per minute.

4. Insecure Frame (External)

Impact

- Level – **LOW**
- IFrame sandboxing enables a set of additional restrictions for the content within a frame in order to restrict its potentially malicious code from causing harm to the web page that embeds it.

Remedy

- Apply sandboxing in inline frame
  <iframe sandbox src="framed-page-url"></iframe>

- For untrusted content, avoid the usage of seamlessattribute and allow-top-navigation, allow-popupsand allow-scriptsin sandbox attribute.

5. Insecure Transportation Security Protocol Supported (TLS 1.0)

Impact

- Level – **LOW**
- Attackers can perform man-in-the-middle attacks and observe the encryption traffic between your website and its visitors.

Actions to Take

- We recommended to disable TLS 1.0 and replace it with TLS 1.2 or higher. See Remedy section for more details.

Remedy

- For Apache, adjust the SSLProtocol directive provided by the mod_ssl module. This directive can be set either at the server level or in a virtual host configuration.
  SSLProtocol +TLSv1.2

- For Nginx, locate any use of the directive ssl_protocols in the nginx.conffile and remove TLSv1.
  ssl_protocols TLSv1.2;

- For Microsoft IIS, you should make some changes on the system registry. Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.
  i. Click on Start and then Run, type regedt32or regedit, and then click OK.
  ii. In Registry Editor, locate the following registry key or create if it does not exist:
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0
  iii. Locate a key named Serveror create if it doesn't exist.
  iv. Under the Serverkey, locate a DWORD value named Enabledor create if it doesn't exist and set its value to "0".

6. Cookie Not Marked as HttpOnly

Impact

- Level – LOW
- During a cross-site scripting attack, an attacker might easily access cookies and hijack the victim's session

Actions to Take

- Consider marking all of the cookies used by the application as HTTPOnly. (After these changes javascript code will not be able to read cookies.)

Remedy

- Mark the cookie as HTTPOnly. This will be an extra layer of defense against XSS. However, this is not a silver bullet and will not protect the system against cross-site scripting attacks. An attacker can use a tool such as XSS Tunnelto bypass HTTPOnly protection.

Conclusion

Following the evaluation, it was discovered that the application's fundamental security was not properly designed and implemented, except for a few loose ends. Overall, the web application's dependability and trustworthiness are well-structured thanks to the use of security techniques and protocols.