

CYBER SECURITY(FOOT PRINTING)

A report submitted in partial fulfillment of the requirements for the Award of Degree of

**BACHELOR OF TECHNOLOGY
in
COMPUTER SCIENCE AND ENGINEERING
by**

SAJJA SAI SREE

Y20ACS553



Department of Computer Science and Engineering

Bapatla Engineering College

(Autonomous)

Affiliated to Acharya Nagarjuna University, Guntur

Bapatla-522102

2023-24

CERTIFICATE

This is to certify that the Internship report entitled “**CYBER SECURITY(FOOT PRINTING)**” being submitted by “**SAJJA SAI SREE**” “**Y20ACS553**” “is work done by him and submitted during 2023– 2024 academic year, in partial fulfillment of the requirements for the award of the degree of **BACHELOR OF TECHNOLOGY in COMPUTER SCIENCE AND ENGINEERING**,at “**SPYPRO SECURITY SOLUTIONS Pvt. Ltd.,Vijayawada**” from **08/05/2023** and **18/06/2023**.

Department Internship Coordinator

Head of the Department

DECLARATION

I hereby declare that the dissertation entitled **CYBER SECURITY(FOOT PRINTING)** submitted for the B.Tech Degree is my work and the dissertation has not formed the basis for the award of any degree, associates, fellowship or any other similar titles.

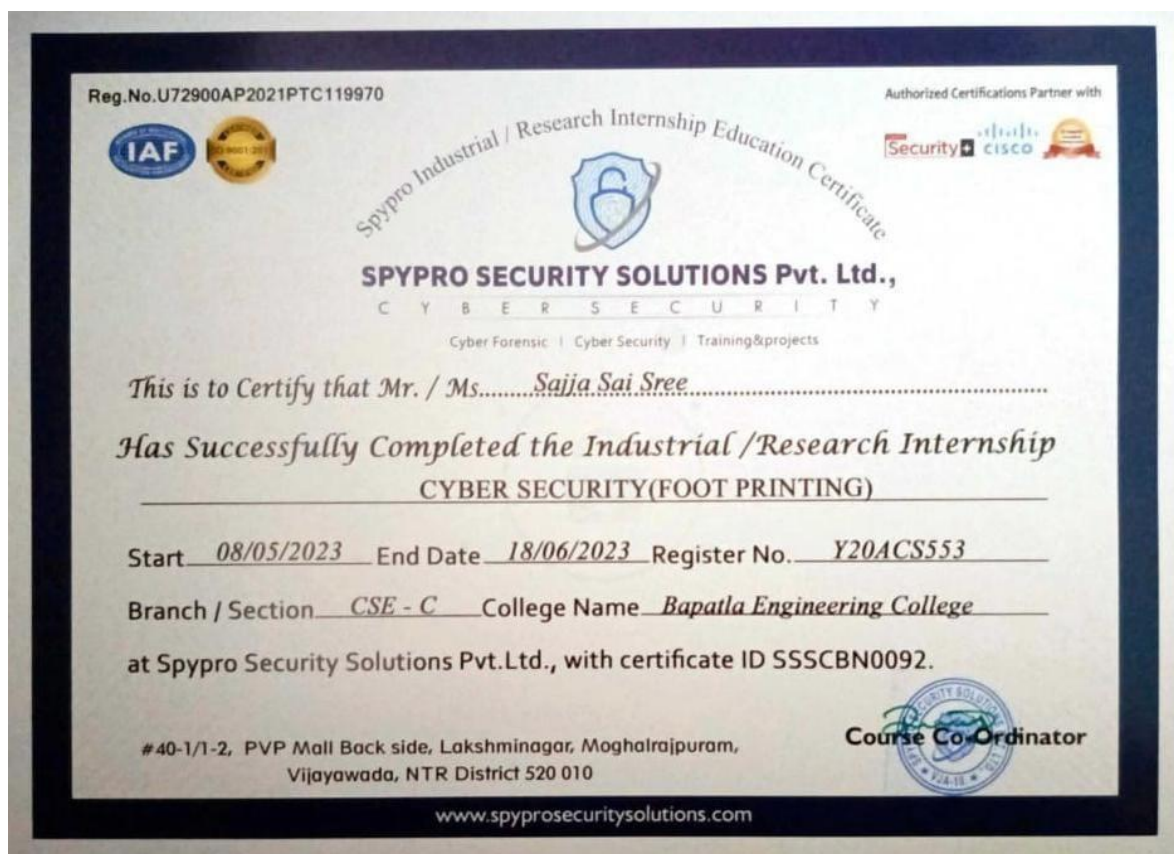
Place: Bapatla

Sajja Sai Sree

Date: 06-07-2023

Y20ACS553

INTERSHIP CERTIFICATE ISSUED BY COMPANY



COMPANY PROFILE AND EXTERNAL GUIDE DETAILS

Introduction of the Organization:

Spypro Security Solutions Private Limited is a 1 year 9 days old Private Company incorporated on 09 Nov 2021. Its registered office is in Krishna, Andhra Pradesh, India. The Company's status is Active. It's a company limited by shares having an authorized capital of Rs 10.00 lakh and a paid-up capital of Rs 1.00 lakh as per MCA. 2 Directors are associated with the organization. Veerababu Nirukonda and Naga Chaitanya Rani Nirukonda are presently associated as directors. Spypro Security Solutions Private Limited is an unlisted private company incorporated on 09 November, 2021. It is classified as a private limited company and is located in Krishna, Andhra Pradesh. Its authorized share capital is INR 10.00 lac and the total paid-up capital is INR 1.00 lac. The current status of Spypro Security Solutions Private Limited is - Active.

Chaitanya Rani .N is young Entrepreneur, Founder & CEO of Spypro Security Solutions Pvt. Ltd., . Administrator of hack you (Top hacking awareness forum in INDIA). Cyber Cops Trainer, Day to day: External/internal, web application,soc,wireless, malware, And physical assessments.

ACKNOWLEDGEMENTS

I owe a great many thanks to a great many people who helped and supported and suggested us in every step.

I am glad to the **SPYPRO SECURITY SOLUTIONS PVT. LTD.**, for the internship provided and also great support of **Ms. Chaitanya Rani mam**, my internal guide for helping me in the completion of my internship till end.

I am glad for having the support of our principal Dr. Nazeer Shaik who inspired us with his words filled with dedication and discipline towards work.

I express our gratitude towards **Dr. P.Pardhasaradhi, Professor & HOD of CSE Department** for extending his support through training classes which had been the major source to carry out our project.

I am very much thankful to **K.Siva Kumar , Asst Professor**, Guide of our project for guiding and correcting various documents of ours with attention and care. He has taken pain to go through the project and make necessary corrections as and when needed.

Finally, I thank one and all who directly and indirectly helped us to complete our project successfully.

Project Associate

Sajja Sai Sree

Y20ACS553

ABSTRACT

This paper discusses the often overlooked issues and key vulnerabilities evident in Web facing technologies. The process of uncovering these issues and vulnerabilities is known as footprinting. As the part of internship, I choose a random website for my project “FOOTPRINTING”. We can only perform hacking only the website having loop holes or vulnerabilities. Through the process of checking for the website having open ports, I got the restaurant website of WEEBLY ONLINE SHOPPING COMPANY. To find vulnerabilities we use Sam Spade, nslookup, traceroute, Nmap and neotrace tools

Keywords:

Reconnaissance, Whois, Nmap, Sam Spade, Scanning, Trace route

Table of contents:

SNO	CONTENTS	PAGE NO
1.	Introduction	1-2
2.	Software Requirement Analysis	3
3.	Existing and Proposed Systems	4-7
4.	Software Design	8
5.	Basic commands	9-10
6.	Screenshots and Results	11-17
7.	Conclusion	18
8.	References	19

Introduction:

Problem Statement:

Knowing the security posture of the target(Person,Website,IP Address,Server,Machine,etc) which reduce the focus area to identify vulnerabilities.

FootPrinting:

Footprinting (also known as reconnaissance) is the technique used for gathering information about computer systems and the entities they belong to.

To get this information, a hacker might use various tools and technologies.

Objectives of Foot Printing:

Footprinting can be used to gather information about

- The domain name of an organization
- IP Address of servers
- Operating System of the server
- Applications used on the server
- Location of the servers
- Employee details of the organization
- Email ID,contact number & social network profiles of key employees etc.

TARGET: WEEBLY ONLINE SHOPPING COMPANY

Name of the TARGET ----- weebly.com

IP Address----- 74.115.50.109

IP Location-----United States – California – San Francisco – Weebly Inc.

Types:

There are two types of Footprinting that can be used:

1. Active Footprinting
2. Passive Footprinting

Passive footprinting: Gathering information from publicly available sources such as websites, news articles, and company profiles

Active footprinting: Using more intrusive methods to access sensitive data, such as hacking into systems or applying social engineering technique.

Whois Footprinting is an ethical hacking practice that collects data about targets and their condition. This is the pre-attack phase and the activities performed will be stealthed and best efforts will be made to prevent the target from tracking you.

Network Footprinting information gathering about network like IP Address, Port Scanning

Website Footprinting refers to monitoring and analyzing the target organization's website for information.

DNS Footprinting is a technique that is used by an attacker to gather DNS information about the target system.

Social engineering is the act of manipulating people into giving up private or confidential information by appearing to be a likely insiders.

Email footprinting is a method in which a hacker can trace an email and get information from it. Email footprinting gives us information regarding the sender's email, name, location, IP address, etc

Google hacking, also named Google dorking, is a hacker technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites are using.

Software requirement Analysis:

Functional Requirements:

Ethical hacker:

To gather as much as data possible about a specific targeted computer system, an infrastructure and networks to identify opportunities to penetrate them.

Non-Functional Requirements:

Performance and scalability:

How fast does the system return results? How much will this performance change with higher workloads?

Portability and compatibility:

Which hardware, operating systems, and browsers, along with their versions does the software run on? Does it conflict with other applications and processes within these environments?

Reliability, maintainability, availability:

How often does the system experience critical failures? How much time does it take to fix the issue when it arises? And how is user availability time compared to downtime?

Security:

How well are the system and its data protected against attacks?

Localization:

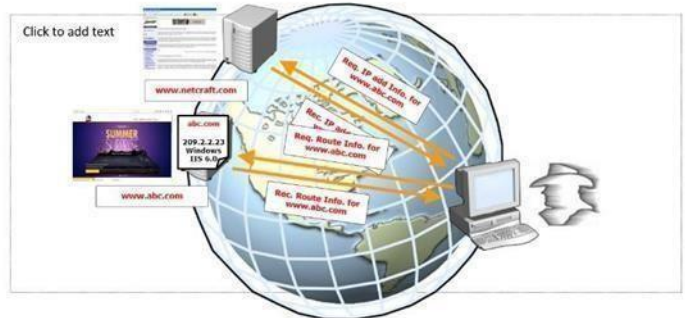
Is the system compatible with local specifics?

Existing Systems:

Footprinting websites:

- google.com
- netcraft.com
- whois.net
- technicalinfo.net
- archive.org
- networktools.com
- mailtracking.com
- whoreadme.com

How Foot Printing Works



Search Engines:

Search engines like Google, Bing, and others can be used to gather information about the target by searching for publicly available data such as company websites, employee profiles, news articles, and other online resources.

Social Media Platforms:

Social media platforms like Facebook, Twitter, LinkedIn, and Instagram can provide valuable insights about an organization or individual. Footprinting can involve analyzing public posts, profiles, connections, and other shared information.

WHOIS Databases:

WHOIS databases maintain records of domain registrations, including information about domain owners, registrars, and contact details. By querying WHOIS databases, footprinters can uncover information about the target's domains and related entities.

DNS Enumeration:

Footprinters can use tools like DNS lookup or Zone Transfer to gather information about a target's DNS records, such as subdomains, mail servers, and associated IP addresses.

Web Archive Services:

Services like the Wayback Machine allow footprinters to view historical snapshots of websites, providing insights into the target's past web presence, changes, and potentially outdated information that could be exploited.

Tools and Techniques:

Tools:

Sam Spade

Nslookup

Traceroute

Nmap

Neotrace

Techniques:

DNS queries

Network enumeration

Network queries

Operating system identification

WHOIS

WHOIS is a web application used to get information about the target website, such as the administrator's e-mail address and details about the registration. WHOIS is a very large database and contains information of approximately all clearnet websites. It can be searched by domain name.

Nmap:

This tool is used for the gathering of the outputs, ports and hosts, tropology, host details of there spective website of the website.

Sam Spade:

It is a windows software tool designed to assist in tracking down sources of e-mail spam.

Proposed System:

Open-Source Intelligence (OSINT) Tools:

Various OSINT tools are available that automate the process of gathering information from diverse sources, including search engines, social media, and other public databases. These tools help streamline and accelerate the footprinting process.

Passive Information Gathering:

Proposed systems might involve passive information gathering techniques that focus on collecting data without directly interacting with the target. This can include monitoring network traffic, analyzing public data breaches, and leveraging online forums and discussion boards for insights.

Dark Web Monitoring:

Proposed systems could include monitoring the dark web for any information related to the target organization, such as leaked credentials, vulnerabilities, or discussions about potential exploits.

Machine Learning and Data Analytics:

Advanced techniques like machine learning and data analytics can be employed to process and analyze large volumes of data gathered during the footprinting process. These systems can help identify patterns, detect potential vulnerabilities, and assist in generating actionable intelligence.

It's important to note that footprinting should be conducted ethically and within legal boundaries. Organizations and individuals should follow relevant laws, regulations, and ethical guidelines when gathering information about systems and networks.

Steps in Footprinting:

Several steps need to be followed during footprinting to collect all relevant information.

1. Identifying Targets

The first step is to identify which systems or organizations to footprint by scanning networks for open ports or performing reconnaissance using Google searches and tools like Shodan.

2. Gathering Information

After the target has been identified, the next step is to gather as much information about it as possible using tools like Nmap, Netcat, and Whois to identify open ports and services, usernames and passwords, web server information, and more.

3. Analyzing Results

After all relevant data has been collected, it needs to be analyzed to determine the most vulnerable points. This is done by identifying common weaknesses across multiple systems or comparing results against known exploits.

4.Planning Attacks

The final step is to use the information gathered during footprinting to plan a successful attack against the target's systems, networks, and devices. This may involve developing custom exploits or choosing a suitable attack vector based on the data collected.

What Information Is Collected in Footprinting?

Network topology:

Collecting this type of information involves identifying the IP addresses and hostnames of all systems on the network and mapping out the connections among them.

Operating systems and applications:

Information about the target's operating system and applications can be used to identify potential security vulnerabilities. For example, if a company uses an outdated version of Windows, it may be vulnerable to specific attacks that are not possible against newer versions.

User accounts:

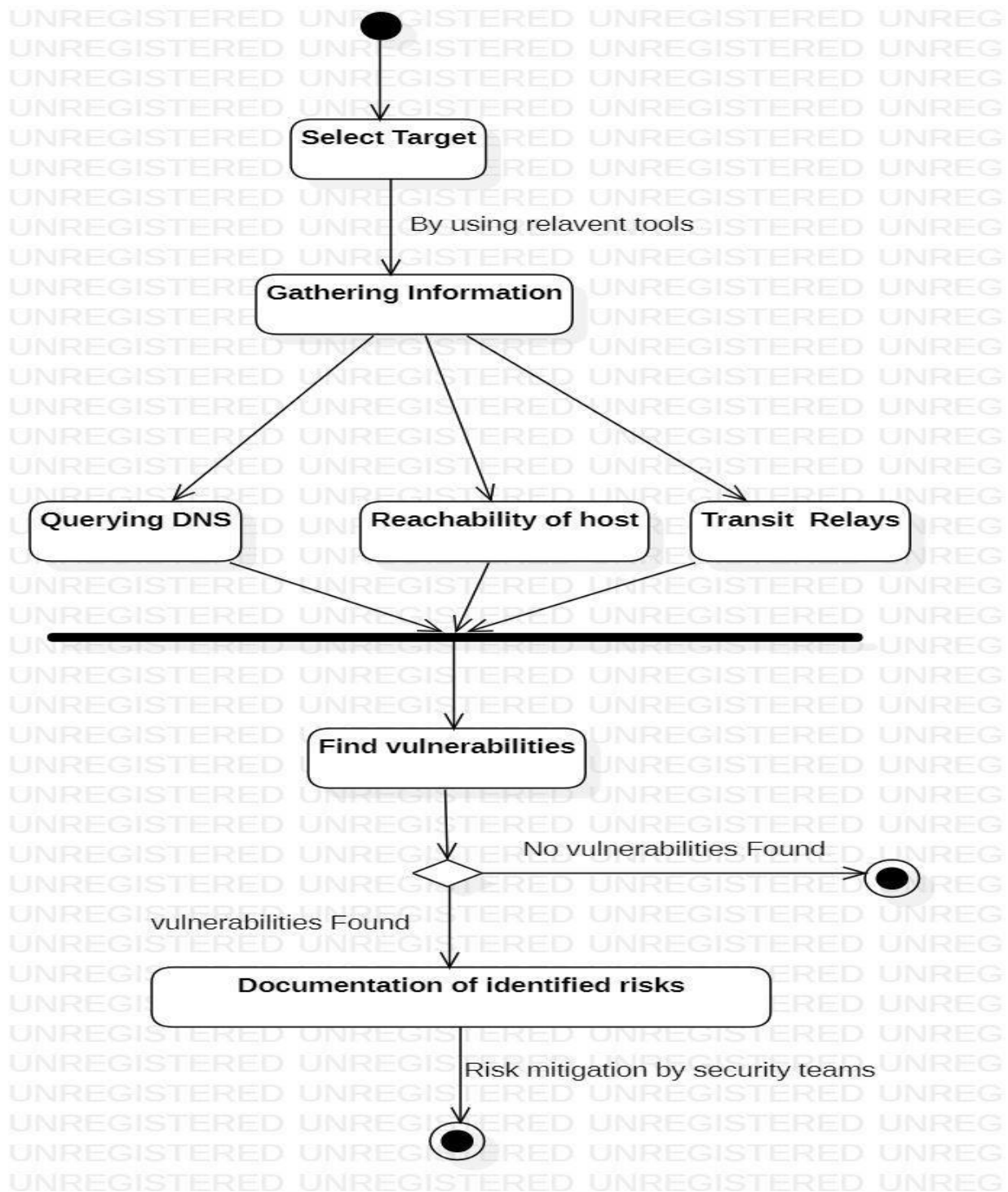
Footprinting can reveal usernames and passwords for user accounts on the target system, which can be helpful in the later stages of an attack.

Web servers:

This includes the servers' software versions, installed modules, and enabled features.

Software Design:

Activity Diagram:



Basic Commands:

Z:\>ping 74.115.50.109

Pinging 74.115.50.109 with 32 bytes of data:

Reply from 74.115.50.109: bytes=32 time=235ms TTL=49

Reply from 74.115.50.109: bytes=32 time=234ms TTL=49

Reply from 74.115.50.109: bytes=32 time=239ms TTL=49

Reply from 74.115.50.109: bytes=32 time=234ms TTL=49

Ping statistics for 74.115.50.109:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 234ms, Maximum = 239ms, Average = 235ms

Z:\>tracert www.weebly.com

Tracing route to weebly.com [74.115.50.110]

over a maximum of 30 hops:

```
1  <1 ms  <1 ms  <1 ms 172.16.0.1
2   1 ms   1 ms   1 ms 117.239.150.74
3  11 ms  11 ms  12 ms 117.216.207.214
4   *      *      *   Request timed out.
5 248 ms 248 ms 256 ms xe-4-4-3-0.a04.lsanca07.us.bb.gin.ntt.net [168.143.105.232]
6   *      *      *   Request timed out.
7 270 ms 257 ms 255 ms ae-3.r24.snjsca04.us.bb.gin.ntt.net [129.250.4.150]
8 258 ms 258 ms 258 ms ae-3.r05.plalca01.us.bb.gin.ntt.net [129.250.4.43]
9 228 ms 228 ms 228 ms xe-0-1-0-2-7.r05.plalca01.us.ce.gin.ntt.net [129.250.197.218]
10 228 ms 228 ms 228 ms core1-a-edge1-a.sf2p.weebly.net [74.115.50.158]
11 231 ms 231 ms 231 ms www.weebly.com [74.115.50.110]
```

Trace complete.

Z:\>nslookup

Default Server: win2012.win2k18.local

Address: 10.2.2.22

> set type=a

> www.weebly.com

Server: win2012.win2k18.local

Address: 10.2.2.22

Non-authoritative answer:

Name: weebly.com



Addresses: 74.115.50.110

74.115.50.109

Aliases: www.weebly.com

> exit

WHOIS



 **DomainTools** [PROFILE](#) [CONNECT](#) [MONITOR](#) [SUPPORT](#) 

[Home](#) > [Whois Lookup](#) > [Weebly.com](#)


Whois Record for Weebly.com

— Domain Profile

Registrant	Data protected, not disclosed
Registrant Country	us
Registrar	Safenames Ltd SafeNames Ltd. IANA ID: 447 URL: http://www.safenames.net Whois Server: whois.safenames.net abuse@safenames.net (p) 441908200022
Registrar Status	clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited
Dates	6,107 days old Created on 2006-03-29 Expires on 2023-03-28 Updated on 2022-03-29
Name Servers	DNS1.P01.NSONE.NET (has 2,779,893 domains) DNS2.P01.NSONE.NET (has 2,779,893 domains) DNS3.P01.NSONE.NET (has 2,779,893 domains) NS-123.AWSDNS-15.COM (has 36,437 domains) NS-1500.AWSDNS-59.ORG (has 47,675 domains) NS-646.AWSDNS-16.NET (has 29 domains)

Tech Contact	International Domain Tech Safenames House, Sunrise Parkway, Milton Keynes, Bucks, MK14 6LS, gb hostmaster@safenames.net (p) 441908200022 (f) 441908325192
IP Address	74.115.50.109 - 278 other sites hosted on this server
IP Location	 - California - San Francisco - Weebly Inc.
ASN	 AS27647 WEEBLY, US (registered Feb 12, 2009)
Domain Status	Registered And No Website
IP History	18 changes on 18 unique IP addresses over 16 years
Hosting History	9 changes on 7 unique name servers over 15 years

— Website

Website Title	 500 SSL negotiation failed:
Response Code	500

Whois Record (last updated on 2022-12-17)

```

Domain Name: WEEBLY.COM
Registry Domain ID: 393059299_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.safenames.net
Registrar URL: http://www.safenames.net
Updated Date: 2022-03-29T00:54:20Z
Creation Date: 2006-03-29T00:25:07Z
Registrar Registration Expiration Date: 2023-03-28T23:25:07Z
Registrar: Safenames Ltd
Registrar IANA ID: 447
Registrar Abuse Contact Email: abuse@safenames.net
Registrar Abuse Contact Phone: +44.1908200022
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Data protected, not disclosed
Registrant Organisation: Weebly, Inc.
Registrant Street: Data protected, not disclosed
Registrant Street: Data protected, not disclosed
Registrant City: Data protected, not disclosed
Registrant State/Province: Data protected, not disclosed
Registrant Postal Code: Data protected, not disclosed
Registrant Country: US
Registrant Phone: Data protected, not disclosed
Registrant Fax: Data protected, not disclosed
Registrant Email: info@weebly.com
Registry Admin ID: Not Available From Registry
Admin Name: International Domain Administrator
Admin Organisation: Safenames Ltd
Admin Street: Safenames House, Sunrise Parkway
Admin Street: Linford Wood
Admin City: Milton Keynes
Admin State/Province: Bucks
Admin Postal Code: MK14 6LS
Admin Country: UK
Admin Phone: +44.1908200022
Admin Fax: +44.1908325192
Admin Email: hostmaster@safenames.net
Registry Tech ID: Not Available From Registry
Tech Name: International Domain Tech
Tech Organisation: Safenames Ltd
Tech Street: Safenames House, Sunrise Parkway
Tech Street: Linford Wood
Tech City: Milton Keynes
Tech State/Province: Bucks
Tech Postal Code: MK14 6LS
Tech Country: UK
Tech Phone: +44.1908200022
Tech Fax: +44.1908325192
Tech Email: hostmaster@safenames.net
Name Server: dns1.p01.nsone.net
Name Server: dns2.p01.nsone.net
Name Server: dns3.p01.nsone.net
Name Server: ns-123.awsdns-15.com
Name Server: ns-1500.awsdns-59.org
Name Server: ns-646.awsdns-16.net
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

"For more information on Whois status codes, please visit https://icann.org/epp"

```

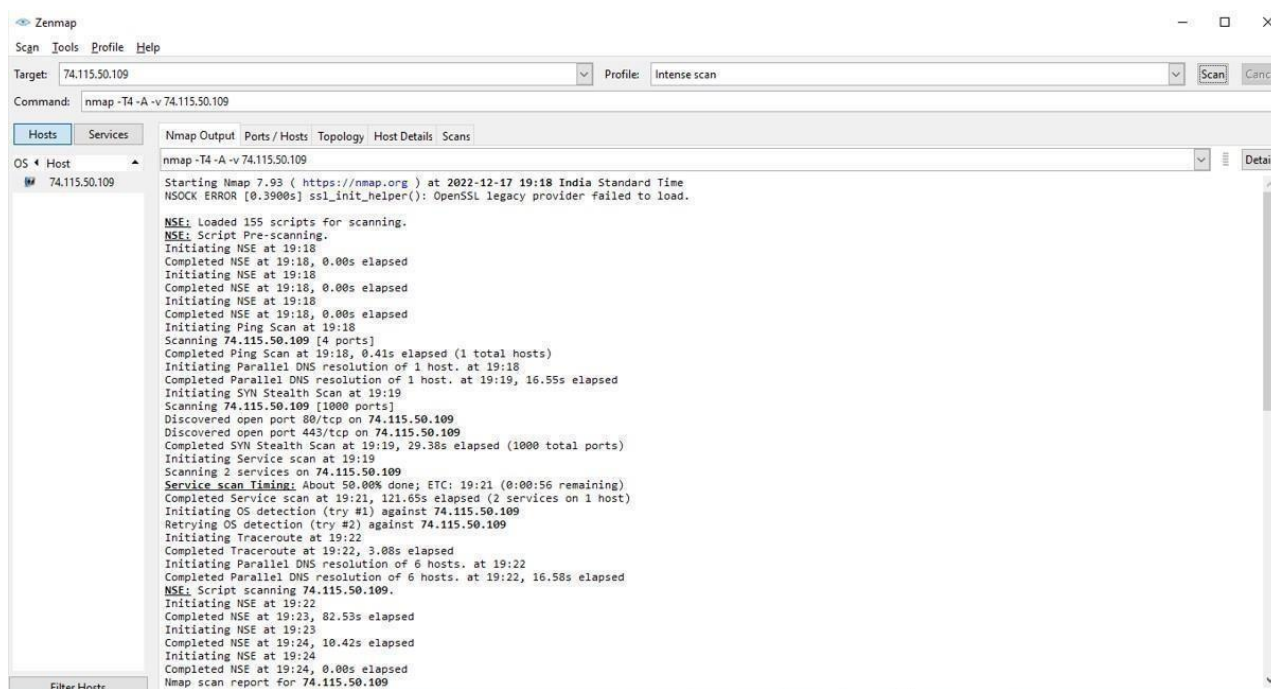
PROCESS:

Firstly, select the website which is going to perform hacking by the ethical hacker. there are many tools in the internet for finding Ip-address to the selected website. After getting the Ip-address of the selected website “ping” the Ip-address to get the “TTL” values of the operating system. By knowing the “TTL” values of an operating system, Hacker can know the which type of operating system it is. After knowing the “TTL” values of the system of the website, it is much easier for preparing the algorithm. After this, tracing the Ip servers of the website.

After all the process of ping, Trace, TTL values and now, the Ip-address of the website is pasted in a tool for knowing the ports that are open, ports and Hosts and tropology, Host details. Therefore, the details of the website are gathered for initializing the hacking methods.

NMAP

Output:

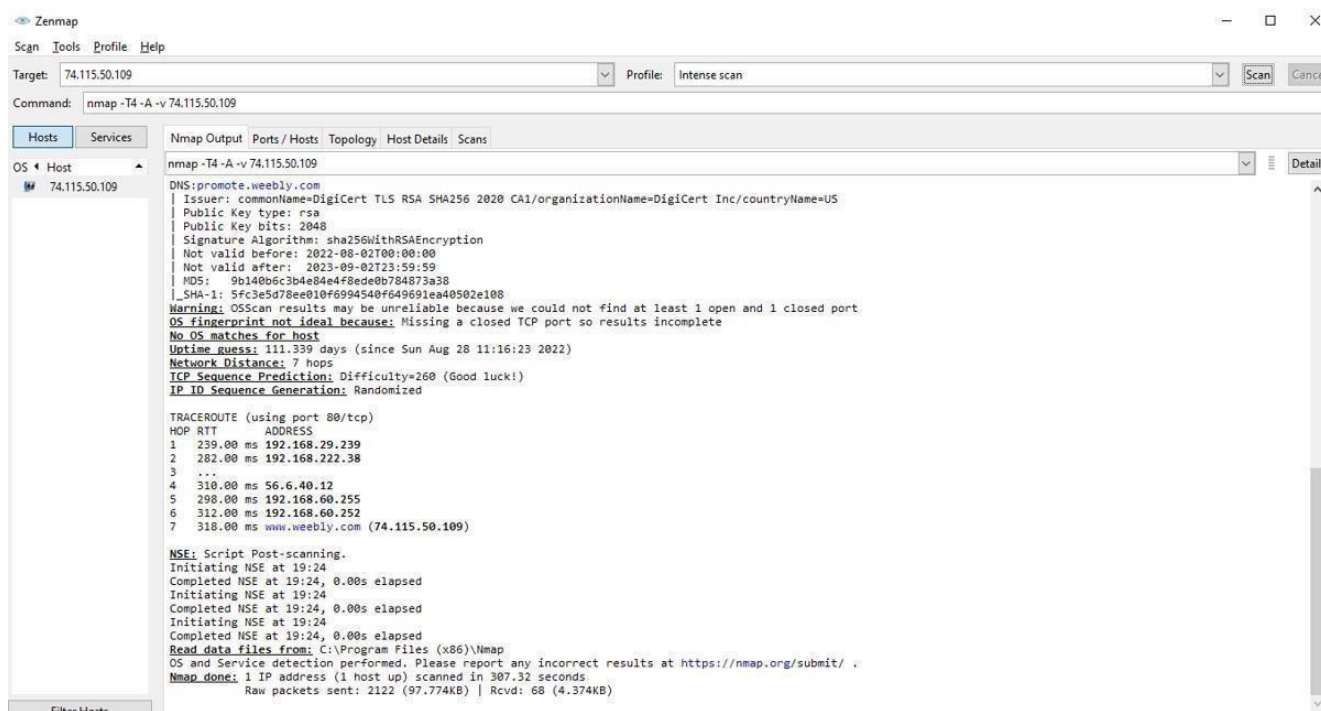


The screenshot shows the Zenmap application window. The 'Target' field is set to '74.115.50.109' and the 'Profile' is 'Intense scan'. The 'Command' field shows 'nmap -T4 -A -v 74.115.50.109'. The 'Nmap Output' tab is selected, displaying the following text:

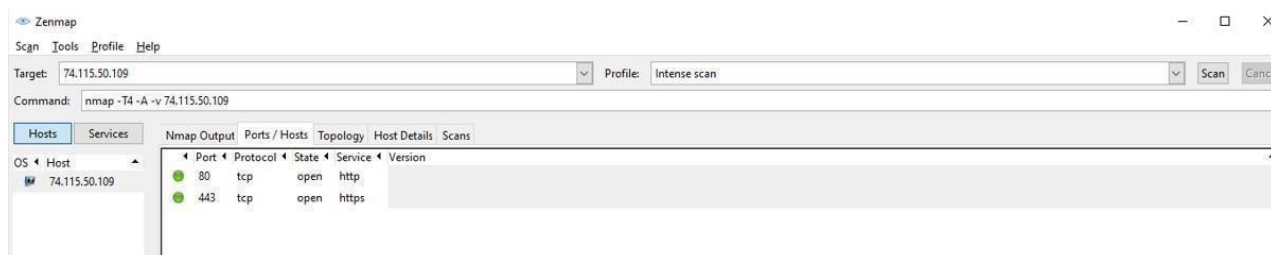
```
nmap -T4 -A -v 74.115.50.109
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-17 19:18 India Standard Time
NSOCK ERROR [0.3900s] ssl_init_helper(): OpenSSL legacy provider failed to load.
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 19:18
Completed NSE at 19:18, 0.00s elapsed
Initiating NSE at 19:18
Completed NSE at 19:18, 0.00s elapsed
Initiating NSE at 19:18
Completed NSE at 19:18, 0.00s elapsed
Initiating Ping Scan at 19:18
Scanning 74.115.50.109 [4 ports]
Completed Ping Scan at 19:18, 0.41s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:18
Completed Parallel DNS resolution of 1 host. at 19:19, 16.55s elapsed
Initiating SYN Stealth Scan at 19:19
Scanning 74.115.50.109 [1000 ports]
Discovered open port 80/tcp on 74.115.50.109
Discovered open port 443/tcp on 74.115.50.109
Completed SYN Stealth Scan at 19:19, 29.38s elapsed (1000 total ports)
Initiating Service scan at 19:19
Scanning 2 services on 74.115.50.109
Service scan Timing: About 50.00% done; ETC: 19:21 (0:00:56 remaining)
Completed Service scan at 19:21, 121.65s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 74.115.50.109
Retrying OS detection (try #2) against 74.115.50.109
Initiating Traceroute at 19:22
Completed Traceroute at 19:22, 3.08s elapsed
Initiating Parallel DNS resolution of 6 hosts. at 19:22
Completed Parallel DNS resolution of 6 hosts. at 19:22, 16.58s elapsed
NSE: Script scanning 74.115.50.109.
Initiating NSE at 19:22
Completed NSE at 19:23, 82.53s elapsed
Initiating NSE at 19:23
Completed NSE at 19:24, 10.42s elapsed
Initiating NSE at 19:24
Completed NSE at 19:24, 0.00s elapsed
Nmap scan report for 74.115.50.109
```

Here, there is a Ip-address targeted by the tool “Nmap” and this Ip-address is applied to the many tools like Sam spade, DNS domain view and visual route. The process of applying the Nmap tool to the Ip-address is to get the open TCPs of the respective website that have being selected by the ethical hacker. by using the data given by the Nmap tool, of different data like open TCPs, ports and hosts, tropology, host details.

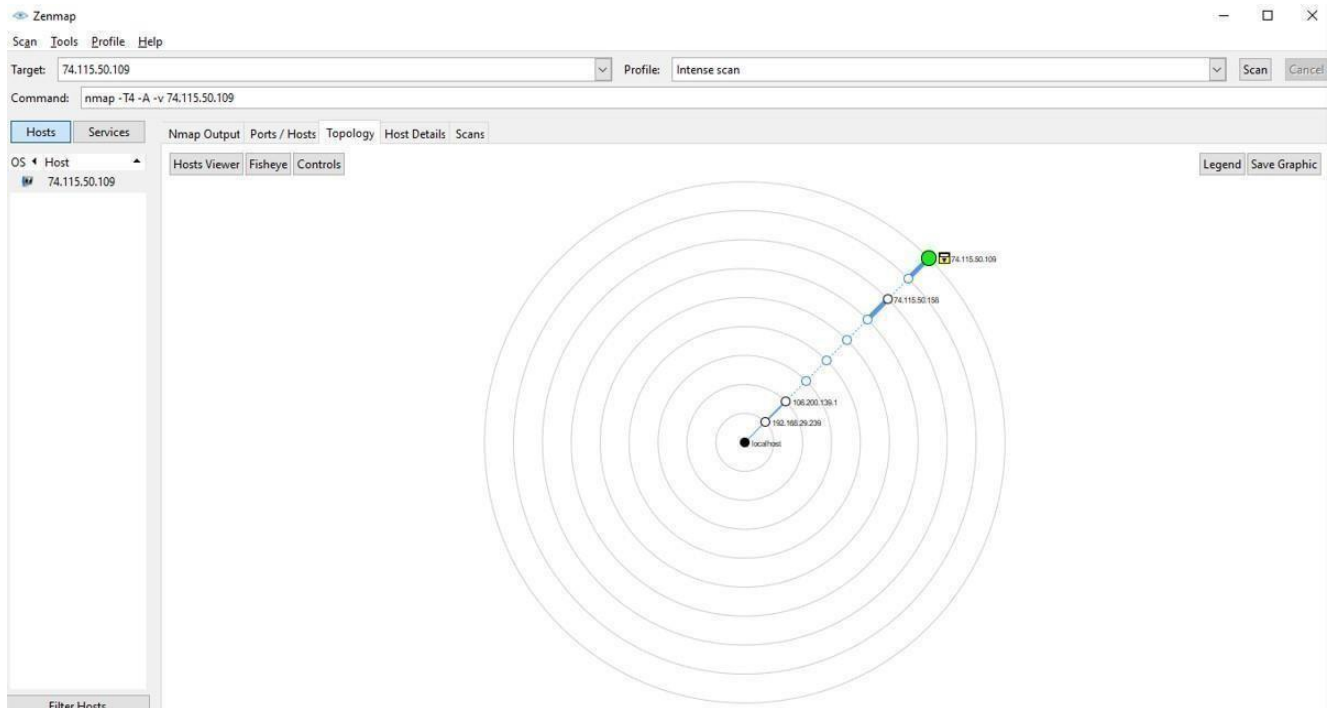
The above picture shows the open TCPs of respective website, through the open TCPs it is easy to start a hacking on the website. here, the open TCP helps the hacker that which type of version is that Ip-address. the total open ports of that Ip-address (104.21.67.175) has „3“ ports.



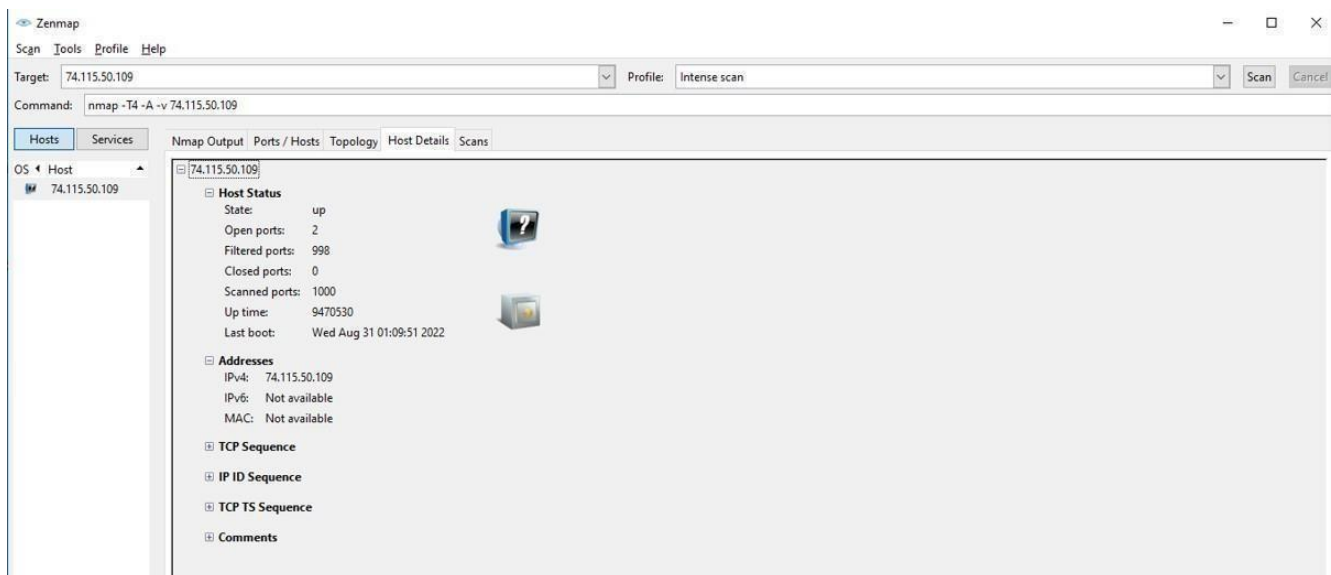
Ports/Hosts:



Topology:



Host Details:



Therefore, by using different tools the hacker will find the ping for TTL value, Ip tracing, ports and hosts, topology, host details. The information of the website is gathered for ethical hacking. and for building the security for a website, to understand the un-ethical hacker hacking techniques and how ethical hacker is going to protect the website. It is the half quarter process for the ethical hacking.

SamSpade

WHOIS :

```
Spade - [whois http://www.weebly.com, finished]
File Edit View Window Basics Tools Help
http://www.weebly.com 10 Magic
12/17/22 19:24:33 whois http://www.weebly.com
.com is a domain of USA & International Commercial
Searches for .com can be run at http://www.crsnic.net/

whois -h whois.crsnic.net weebly.com ...
Domain Name: WEEBLY.COM
Registry Domain ID: 393059299_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.safenames.net
Registrar URL: http://www.safenames.net
Updated Date: 2022-03-28T23:54:33Z
Creation Date: 2006-03-29T00:25:07Z
Registry Expiry Date: 2023-03-28T23:25:07Z
Registrar: SafeNames Ltd.
Registrar IANA ID: 447
Registrar Abuse Contact Email: abuse@safenames.net
Registrar Abuse Contact Phone: +44.1908200022
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: DNS1.P01.NSONE.NET
Name Server: DNS2.P01.NSONE.NET
Name Server: DNS3.P01.NSONE.NET
Name Server: NS-123.AWSDNS-15.COM
Name Server: NS-1500.AWSDNS-59.ORG
Name Server: NS-646.AWSDNS-16.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-12-17T13:54:21Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
http://www.weebly.
For Help, press F1
```

```
Spade - [whois http://www.weebly.com, finished]
File Edit View Window Basics Tools Help
http://www.weebly.com 10 Magic
NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability. VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
http://www.weebly.
For Help, press F1
```


Ping , Trace , DNS:

```
Spade - [ping http://www.weebly.com, finished]
File Edit View Window Basics Tools Help
http://www.weebly.com 10 Magic
12/17/22 19:26:03 ping http://www.weebly.com
Ping http://www.weebly.com (74.115.50.110) ...
1 Addr:74.115.50.110, RTT: 537ms, TTL: 45
2 failed
3 failed
4 Addr:74.115.50.110, RTT: 416ms, TTL: 45
5 failed
6 Addr:74.115.50.110, RTT: 721ms, TTL: 45
7 failed
8 Addr:74.115.50.110, RTT: 526ms, TTL: 45
9 Addr:74.115.50.110, RTT: 332ms, TTL: 45
10 failed
```

```
Spade - [Fast traceroute http://www.weebly.com, finished]
File Edit View Window Basics Tools Help
http://www.weebly.com 10 Magic
12/17/22 19:26:25 Fast traceroute http://www.weebly.com
Trace http://www.weebly.com (74.115.50.110) ...
1 192.168.29.239 226ms 106ms 174ms TTL: 64 (No rDNS)
2 192.168.222.38 111ms 5ms 69ms TTL: 63 (No rDNS)
3 No Response * * *
4 56.6.40.12 85ms 116ms 141ms TTL:252 (No rDNS)
5 192.168.60.251 75ms 181ms * TTL:251 (No rDNS)
6 192.168.60.248 136ms 127ms * TTL:250 (No rDNS)
7 172.26.77.72 142ms 57ms 285ms TTL:122 (No rDNS)
8 172.26.77.50 59ms 70ms 184ms TTL:248 (No rDNS)
9 192.168.60.228 46ms 58ms 75ms TTL:247 (No rDNS)
10 No Response * * *
11 No Response * * *
12 103.198.140.174 117ms 71ms 86ms TTL:245 (No rDNS)
13 103.198.140.56 167ms 177ms 186ms TTL:243 (No rDNS)
14 103.198.140.107 175ms 214ms 233ms TTL:244 (No rDNS)
15 149.14.125.1 178ms 293ms 164ms TTL:243 (hu0-0-0-9.ccr31.mrs02.atlas.cogentco.com bogus rDNS: host not found [authoritative])
16 62.115.11.140 * 204ms 210ms TTL:242 (mei-b5-link.ip.twelve99.net bogus rDNS: host not found [authoritative])
17 62.115.124.54 * 203ms 194ms TTL:236 (prs-bb1-link.ip.twelve99.net bogus rDNS: host not found [authoritative])
18 62.115.135.24 269ms 398ms 205ms TTL:236 (ldn-bb1-link.ip.twelve99.net bogus rDNS: host not found [authoritative])
19 62.115.113.20 258ms 394ms 255ms TTL:234 (nyk-bb2-link.ip.twelve99.net bogus rDNS: host not found [authoritative])
20 62.115.122.36 355ms 385ms 319ms TTL:231 (palo-b24-link.ip.twelve99.net bogus rDNS: host not found [authoritative])
21 213.248.96.255 332ms 356ms 340ms TTL:235 (internationalbandwidth-ic338995-palo-b1.ip.twelve99-cust.net bogus rDNS: host not found [authoritative])
22 74.115.50.162 * 336ms 334ms TTL: 47 (core1-b-edgel-b.sf2p.weebly.net ok)
23 74.115.50.110 * 329ms TTL: 45 (www.weebly.com ok)
24 74.115.50.110 558ms 590ms TTL: 45 (www.weebly.com ok)
```

```
Spade - [dns http://www.weebly.com, finished]
12/17/22 19:29:52 dns http://www.weebly.com
Canonical name: weebly.com
Aliases:
www.weebly.com
Addresses:
74.115.50.110
74.115.50.109
```

CONCLUSION

In conclusion, footprinting is an important process in cybersecurity that involves gathering information about a target system or network. It helps assess vulnerabilities, identify potential attack surfaces.

During the footprinting process, we use search engines, social media platforms, WHOIS databases, DNS enumeration, and web archive services to gather information about the target. These systems provide valuable insights and publicly available data that can be analyzed to understand the target's digital footprint.

Presenting the report containing the footprint analysis to the appropriate stakeholders, such as management or security teams, to guide decision-making and risk mitigation strategies is the ending of footprinting tasks .And it is important to note that footprinting should always be conducted ethically and legally.

REFERENCES:

1. GeeksforGeeks. (2021, October 20). Ethical hacking | Footprinting.
<https://www.geeksforgeeks.org/ethical-hacking-footprinting/>
2. Ghahrai, A. (2019, July 9). Footprinting and reconnaissance. DevQA.
<https://devqa.io/footprinting-overview/>
3. Gupta, A. (2022, February 3). Determining the appropriate penetration testing method. Forbes.
<https://www.forbes.com/sites/forbestechcouncil/2022/02/03/determining-the-appropriate-penetration-testing-method/>

