

Footprinting

The Foundation of Information Gathering and
Vulnerability Assessment

Digital
Footprint

Lorem ipsum dolor sit amet, onsec.
Nulla vitae tincidunt dui. Phasellus elit
sit suspendisse ac nisl. Pellentesque habi-
tanti malesuada fames turis egestas.
Duis tincidunt celerisque, sevelitus
vitae tincidunt dui.

MD. RAKIBUL HASAN

Session: 2021-22

**Computer Science and Engineering
Begum Rokeya University, Rangpur**

Contents

Introduction to Footprinting	2
Types of Footprinting	2
1. Passive Footprinting:	2
2. Active Footprinting:	2
Different kind of information be gathered from Footprinting	2
Importance of Footprinting.....	2
Techniques Used in Footprinting	3
1. Passive Footprinting Techniques:	3
2. Active Footprinting Techniques:	3
Tools Used in Footprinting	4
1. Nmap:	4
2. WHOIS Lookup Tools:	4
3. Traceroute:	5
4. Maltego:	5
5. Recon-ng:	6
Ethical Considerations of Footprinting.....	6
Conclusion.....	6
Reference	7

Introduction to Footprinting

Footprinting is the first step of ethical hacking to gathering information about a target system to understand their architecture, security and system vulnerabilities. It is a most important step in ethical hacking or malicious attack that enabling attackers to figure out the entry point or backdoor before launching an attack or security testing. Footprinting can be either **passive** means there is no direct connection with system or **active** means directly connection with target system. The main purpose of Footprinting is gather most available information as possible about target system to minimize the attack process or security testing.

Types of Footprinting

Footprinting is categorized into two main types e.g. **Passive Footprinting** and **Active Footprinting**.

1. **Passive Footprinting:** Passive Footprinting means gathering information without directly interacting with target system. The information gathers through publicly available resources like search engines (<https://www.shodan.io/>), social media, public records or website. Attacker can use WHOIS lookups (<https://www.whois.com/>), DNS quires or analyzing the target IP address range.
2. **Active Footprinting:** In this case, Attacker is directly engaging with the target system to gather information. It includes various activities such as port scanning, tracerouting and sending requests to the target system to find out the open port/services and their configurations. This type of footprinting may appear notification to the target system if the system is in monitoring place.

Different kind of information be gathered from Footprinting

- The operating system (OS) of the target system.
- Firewall use in network
- IP address of target system
- Network map
- Security configuration of the target system
- Social information like email id, username, password
- Server configuration
- Browsing history and so on.

Importance of Footprinting

Footprinting is important and very critical phase in cybersecurity field because it helps attacker or security tester understand how a network operates and where the weak point of the system might be. Some key reasons are:

1. **Identifying Vulnerabilities:** By gathering information of a target network or infrastructure, an attacker or a security tester can identify the weakness of the system that can be exploited.
2. **Understanding Network Architecture:** Footprinting helps to understand a map of the network's architecture including firewalls, routers and server. It provides a detail understanding of the target system layout.

3. **Evaluating Security Posture:** This process allows an attacker or penetration tester to assess how well-protected the target is and what security mechanism are used.
4. **Palling an Attack:** Footprinting reduce the palling of the attack. It provides the strategic advantage in planning the attack, identifying the tools to use in most vulnerable points of the target.

Techniques Used in Footprinting

Various techniques are used in footprinting, they are categorized into **passive** and **active** methods.

1. Passive Footprinting Techniques:

- **WHOIS Lookup:** It provide information about domain name, domain IP addresses, contact information of domain owner and organization that owns the target domain.
- **DNS Enumeration:** It allows attacker to gather information about domain, subdomains, mail server and name server associated with the target domain.

```
Nmap: nmap -n --script "(default and *dns*)" or fcrdns or dns-srv-enum or dns-random-txid or dns-random-srport" <IP>
```

```
Subdomain Finder (sublist3r): sublist3r -d example.com
```

- **Social Engineering:** It is using techniques to gather information by interacting with employees, browsing social media profile, job profiles or using phishing emails
- **Public resources:** Searching with job postings, official announcements or technical forums for system details, software in use or vulnerabilities.

2. Active Footprinting Techniques:

- **Port Scanning:** Scans the port of target system to determine open ports and services running on the target system. Nmap is the popular tools that used for this purpose.

```
Simple scan: nmap [URL/IP]
```

```
More complex: nmap -p0- -v -A -T4 [URL/IP]
```

- **Traceroute:** It helps in identifying the path data packet take from the attacker's machine to the target machine that reveals network devices and the architecture between them.
- **Ping Sweep:** Identifying if the target system is live by sending ICMP (Internet Control Message Protocol) packets and measuring response times.

```
ping [URL/IP]
```

```
Example: ping testphp.vulnweb.com
```

```
ping 192.168.189.129
```

- **Banner Grabbing:** Gathers information about the services running on open ports including version details and software being used.

Tools Used in Footprinting

1. Nmap:

Nmap or Network Mapper is a free and open-source tools for network scanning and security auditing. It provides detailed information about open ports, activated services, operating system (OS) with their version, what type of firewall are used in network. It designed for scanning large networks, but it works fine against single hosts. The GUI version of nmap is Zenmap.

```
root@rakib: ~  
root@rakib:~# nmap 192.168.88.131  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-09 09:28 EDT  
Nmap scan report for 192.168.88.131  
Host is up (0.0010s latency).  
Not shown: 978 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
80/tcp    open  http  
111/tcp   open  rpcbind  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
512/tcp   open  exec  
513/tcp   open  login  
514/tcp   open  shell  
1099/tcp  open  rmiregistry  
1524/tcp  open  ingreslock  
2049/tcp  open  nfs  
2121/tcp  open  ccproxy-ftp  
3306/tcp  open  mysql  
5432/tcp  open  postgresql  
5900/tcp  open  vnc  
6000/tcp  open  X11  
6667/tcp  open  irc  
8009/tcp  open  ajp13  
8180/tcp  open  unknown  
MAC Address: 00:0C:29:20:AA:03 (VMware)  
Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

2. WHOIS Lookup Tools:

Tools like Whois.net or command line tools whois, nslookup, nmap, dnsrecon, host are used for gathering all Domain registration information.

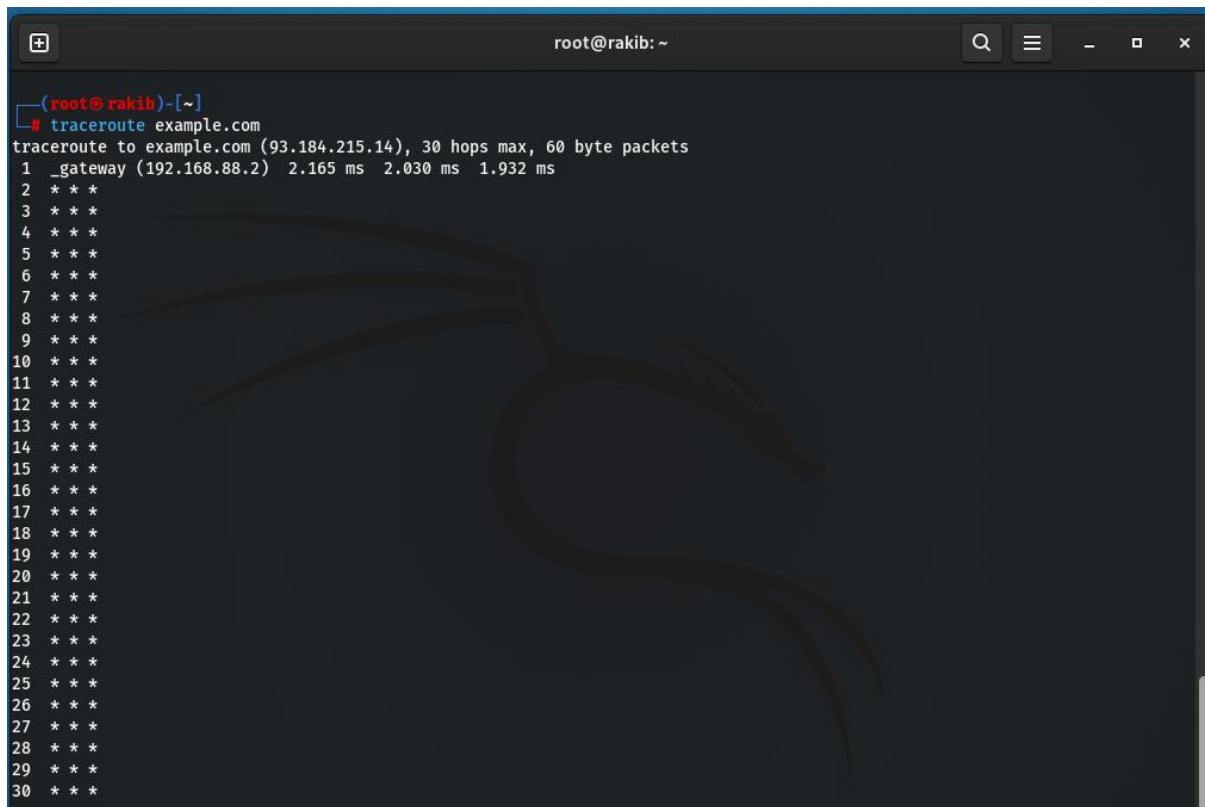
- whois example.com
- nslookup example.com
- dnsrecon -d example.com
- host -a example.com

```
root@rakib: ~  
root@rakib:~# whois example.com  
Domain Name: EXAMPLE.COM  
Registry Domain ID: 2336799_DOMAIN_COM-VRSN  
Registrar WHOIS Server: whois.iana.org  
Registrar URL: http://res-dom.iana.org  
Updated Date: 2024-08-14T07:01:34Z  
Creation Date: 1995-08-14T04:00:00Z  
Registry Expiry Date: 2025-08-13T04:00:00Z  
Registrar: RESERVED-Internet Assigned Numbers Authority  
Registrar IANA ID: 376  
Registrar Abuse Contact Email:  
Registrar Abuse Contact Phone:  
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: A.IANA-SERVERS.NET  
Name Server: B.IANA-SERVERS.NET  
DNSSEC: signedDelegation  
DNSSEC DS Data: 370 13 2 BE74359954660069D5C63D200C39F5603827D7DD02B56F120EE9F3A86764247C  
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/  
>>> Last update of whois database: 2024-10-09T13:38:31Z <<<
```


3. Traceroute:

It is a commonly used tool to gather information about network paths. It helps trace the route packets take from target system to a specified destination.

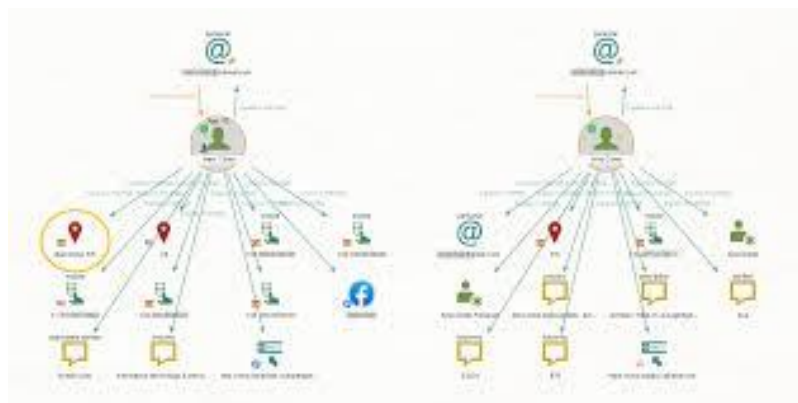
```
traceroute [URL]
Example: traceroute example.com
```



```
(root@rakib)-[~]
# traceroute example.com
traceroute to example.com (93.184.215.14), 30 hops max, 60 byte packets
1 _gateway (192.168.88.2) 2.165 ms 2.030 ms 1.932 ms
2 * * *
3 * * *
4 * * *
5 * * *
6 * * *
7 * * *
8 * * *
9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
```

4. Maltego:

Maltego is a powerful tool for information gathering. It used for both getting information of a person, a domain or a system. It help to visualizing relationship between people, organizations and network or system.



5. Recon-ng:

Recon-ng is a full-featured Web Reconnaissance framework written in Python. Complete with independent modules, database interaction, built in convenience functions, interactive help and command completion. Recon-ng provides a powerful environment in which open-source web-based reconnaissance can be conducted quickly and thoroughly.

Ethical Considerations of Footprinting

When an attacker done Footprinting for ethical hacking or penetration testing, must be conducted with explicit permission form the target organization. Engaging in footprinting without any permission can be illegal and classified as cybercrime or unauthorized access. Ethical hacker always ensure that they are within the legal frameworks and have signed contracts outlining their scope of work.

Conclusion

Footprinting is an important process both offensive and defensive cybersecurity practices. By gathering as much as information of a target, security analyst can better understand the potential risk of system while attacker can use this information to exploit vulnerabilities. However, it must be ensured that footprinting performed lawfully and responsibly. As the first step in a cybersecurity assessment, footprinting sets the stage for more in-depth testing or attacks and its critical role in the cybersecurity lifecycle.

Reference

1. <https://www.kali.org/tools/recon-ng/>
2. <https://nmap.org/book/man.html>
3. <https://www.geeksforgeeks.org/ethical-hacking-footprinting/>
4. <https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/footprinting-steps-penetration-testing/>
5. <https://medium.com/@prem112/footprinting-4a4d36164607>