

FOOTPRINTING AND RECONNAISSANCE

Footprinting is one of the **most convenient ways for hackers to collect information about targets such as computer systems, devices, and networks.** Using this method, hackers can unravel information on open ports of the target system, services running, and remote access probabilities.

Since it is the initial phase of hacking it is really important to develop an accurate understanding of the entire process. The systematic footprinting of a target **enables the attacker to get a blueprint of the target's security posture.**

Here, we will get to know how malicious hackers perform footprinting on the organization or target's system, what all they can do, and how it will be harmful to businesses and individuals.

On the other hand, **white hat hackers who are well versed in footprinting will be able to improve the security of the organizations they work for.** With systematic methodology, businesses can identify their vulnerabilities so they can patch and make changes in policy accordingly.

Types of footprinting:

- **Who is footprinting**
- **Network footprinting**
 - **DNS footprinting**
 - **Competitive intelligence**
 - **Email footprinting**
 - **Website footprinting**
 - **Social Engineering**
 - **Google Hacking**

How to perform footprinting?

Footprinting is the first step, during which the **hacker gathers as much information as possible to find ways to enter a target system.** For successful footprinting, the attacker needs to first check the visibility of the target and see how to gather related information on the internet through open sources.

Through careful analysis, **the attacker can determine the scope of potential entry points**. The following information can be collected:

- **Company names**
- **Domain names**
- **Business subsidiaries**
- **IP Addresses**
- **Business emails**
- **Network phone numbers**
- **Key employees**

and so on.

In hacking terms, we can call it the **"Front Door"** of the castle on target.

The **first step of footprinting is to determine what to attack to obtain the "footprint" of the target network** which includes, but is not limited to the following:

- **Hostnames**
- **Network address ranges**
- **Exposed hosts**
- **Exposed applications**
- **OS and its versions**
- **Application and its versions**

and many more.

Apart from this, the attackers have to decide the scope of the target with regards to the entire organization or certain subsidiaries or locations. Based on the scope, they start to dig deep into the information like company web-pages, related organizations, employee details, contacts, e-mail addresses, current events, locations, news, policies, disgruntled employees, mergers, acquisitions, or events to garner some clues, opportunities, and contacts for attackers.

Methods of footprinting

1. Port Scanning

Port scanners are used to **determine live hosts on the internet and find out which Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports** are listening on each system, as well as which operating system is installed on the host. To

identify the relationship of each host and potential security mechanisms between the attacker and targets, they use traceroutes.

Tools:

- **NSLookup** - to perform DNS queries and zone transfers
- **Tracert** - to create network maps of the target.

Once port scanning and trace routing are done, attackers will create a network map that represents the target's internet footprinting.

2. Google Hacking

Despite what you may infer from the name, **this method does not involve hacking Google! This is a means by which you can collect information from the Google search engine in a smart way.**

Search engines have many features using which you can get uncommon, but very specific search results from the internet. Using these techniques, hackers and **attackers perform a search using advanced operators**, examples of which are given below.



These types of operators can uncover much sensitive information that can potentially harm the target and should therefore not be revealed.

Let's take an example.

Go to google.com and paste this- allinurl:tsweb/default.htm

You will get more than 200 websites that have tsweb/default folder. Using this, the hacker gets a chance to get into the organization's servers. This is just one example. There is plenty of such information about targets available online, which hackers can take advantage of.

3. Ping Sweep

If the attacker wants to know which are the machines on your network that are currently live, they can perform a ping sweep. Ping uses ICMP packets to send echo

requests to the target system, and waits for an echo reply. If the device is not reachable, it will show a "request time out"; but if the device is online and not restricted from responding, it will send an echo reply back. Here are some tools used to perform ping sweeps through a range of devices that determine the active devices on the target network.

- Nmap
- Angry IP scanner
- Super Scan
- Pinger etc.

4. Who is lookup

This method can be used to collect basic database queries like domain name, IP Address block, location, and much more information about the organization.

```
Domain Name: facebook.com
Registry Domain ID: 2320948_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrarsafe.com
Registrar URL: https://www.registrarsafe.com
http://www.registrarsafe.com
Updated Date: 2020-03-10T18:53:59+00:00
2020-03-10
Creation Date: 1997-03-29T05:00:00+00:00
1997-03-29
Registrar Registration Expiration Date: 2028-03-30T04:00:00+00:00
2028-03-30
Registrar: RegistrarSafe, LLC
Sponsoring Registrar IANA ID: 3237
Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
Registrar Abuse Contact Phone: 16503087004
Status:
    clientDeleteProhibited
    clientTransferProhibited
    clientUpdateProhibited
    serverDeleteProhibited
    serverTransferProhibited
    serverUpdateProhibited
Registry Registrant ID:
Registrant Name: REDACTED FOR PRIVACY (DT)
Registrant Organization: Facebook, Inc.
Registrant Street: 1601 Willow Rd
Registrant City: Menlo Park
Registrant State/Province: CA
Registrant Postal Code: 94025
Registrant Country: us
Registrant Phone: 16505434800
```

Example of Footprinting

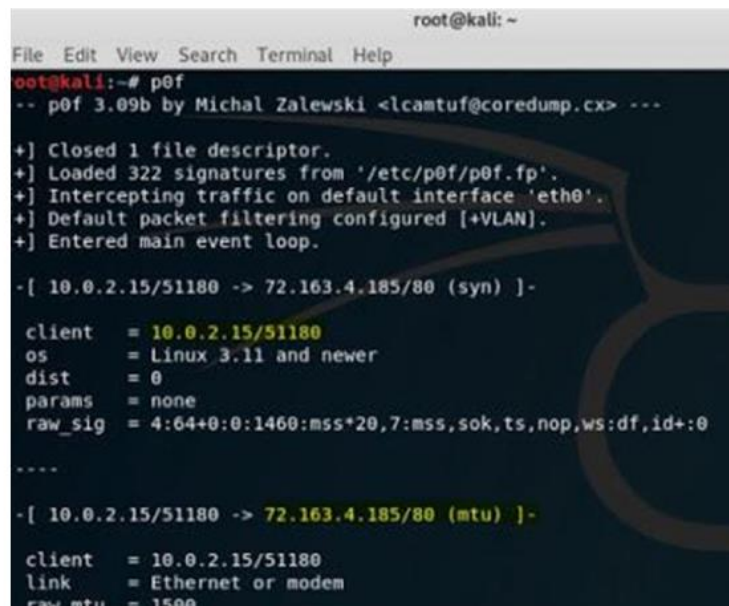
Let's see an example of footprinting using the **Linux tool p0f**.

p0f is a passive TCP/IP stack fingerprinting tool to identify the system running on machines that send network traffic to the box it is running on, or to a machine that shares a medium with the machine on which it is running. p0f can also assist in analyzing other aspects of the remote system.

Basically, it is a tool used to perform a forensic investigation of a system that has been compromised or is under attack. Using this tool, you can analyze the structure of TCP/IP packets to determine OS and other configurations of the target host. Let's check how to do this.

- **step 1 - Open Linux Terminal and type p0f**
- **Step 2 - Explore your target host using any browser**

Once the connection is established with the target host, the client will start to interact with the server.



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# p0f
-- p0f 3.09b by Michal Zalewski <lcamtuf@coredump.cx> ---

+] Closed 1 file descriptor.
+] Loaded 322 signatures from '/etc/p0f/p0f.fp'.
+] Intercepting traffic on default interface 'eth0'.
+] Default packet filtering configured [+VLAN].
+] Entered main event loop.

-[ 10.0.2.15/51180 -> 72.163.4.185/80 (syn) ]-

client  = 10.0.2.15/51180
os      = Linux 3.11 and newer
dist    = 0
params  = none
raw_sig = 4:64+0:0:1460:mss+20,7:mss,sok,ts,nop,ws:df,id+:0
----

-[ 10.0.2.15/51180 -> 72.163.4.185/80 (mtu) ]-

client  = 10.0.2.15/51180
link    = Ethernet or modem
raw_mtu = 1500
```

You can see that my client IP 10.0.2.15 has established a connection with the target web server 72.163.4.185 using port 80.

How to prevent Footprinting?

Your every move, each activity, or data available on the internet is a potential footprint that can open layers of information for attackers.

Now let's discuss preventive steps to avoid threats and reduce the security risk of the organization and individual.

1. Delete or De-activate old accounts

Once your account is assigned online, it can be shared anywhere with your full name, email address, pictures, location, and other information. Official email accounts provided to the employees are also available online. Once the employee has left the organization, the email account must be deleted to avoid fraudulent transactions using the same.

2. Unsubscribe from unwanted mails

All of us keep subscribing to newsletters, events registrations, offers and to many other mail lists. While some of these lists may be useful, most of them result in unnecessary clutter in our mailbox. Unsubscribe to all unnecessary emails so that you can reduce your digital footprinting on the internet.

3. Use stealth mode

There are many browsers which help you to surf with privacy. This is how you can search online with ease and avoid websites from tracking your interests, location, etc. Using browsers like TOR, Duck Duck Go with some advance settings in your regular browser can restrict the sharing of your information online.

4. Use a VPN

There are many VPNs, or Virtual Private Networks, available that you can use for privacy. A VPN provides you with an extra layer of security to protect your privacy over the internet. This will prevent others from tracking your web activity and being able to collect data by watching your surfing patterns.

5. SEO

Prevent search engines from crawling through your cached webpages and user anonymous registration details, and minimize unwanted footprints.

6. Configure Web servers

Configure your web servers to avoid information leakage and block all unwanted protocols to prevent any unethical external scans. Use TCP/IP and IPSec Protocols. Always maintain a separation between the internal and external DNS.

7. Do it yourself

Perform footprinting techniques as we have discussed above and do a check to see whether any sensitive or unwanted information of yours is available on the internet. Use the OSINT framework to delve deeper, and remove posted/ shared data that reveals any kind of sensitive information which can be a potential threat. Share tips and tricks to avoid fraud calls and social engineering.

What is Reconnaissance

Reconnaissance is a very important stage in the initial hacking process. In this stage, attackers gather information, much like a detective does! This process involves gathering information about the target flaws, vulnerabilities that can be used in penetration testing, and the beginning of any data breaches.

Any information gathered about the target may be a crucial piece of the jigsaw, needed to reveal the critical vulnerabilities of the target.

What critical information can be revealed in the reconnaissance phase?

1) Network Information

- IP addresses
- subnet mask
- network topology
- domain names

2) Host Information

- user- names
- group names
- architecture type
- operating system family and version
- TCP and UDP services running with versions

3) Security Policies

- password complexity requirements
- password change frequency
 - expired/disabled account retention
- physical security (e.g. access badges, door locks, etc.)
- firewalls and intrusion detection systems

4) Personnel details

- designations
- telephone number
- social hangouts
- computer skills

There are two types of reconnaissance.

1. Passive reconnaissance

This is when the **attacker gathers information about the target through openly available sources.** There are multiple sources available free on the internet which may provide a blueprint of the organization or individual.

2. Active reconnaissance

Here, **the attacker directly interacts with the target's computer system to gain information using scanning, eavesdropping, and packet capturing techniques.** The advantage of active reconnaissance is that the **collected information is quite accurate and relevant;** however, there is a risk of getting detected.

Netcat, Nmap are the best tools for this.

What is Enumeration?

Once an attacker creates an active connection with the target, they are able to perform directed queries to gain more information. For example,

- Usernames
- hostnames
- IP address
- Passwords (or strength)
- configuration

The information gathered about the target can be used to identify vulnerabilities in the target system. Once an attacker gains this information, they can steal private data and sometimes, even worse, change the configuration.

Types of Enumeration

There are multiple types of enumeration. Let's take a look at one example.

DNS Enumeration

DNS enumeration is the technique employed to find all the DNS servers and their corresponding records for an organization. A list of DNS records provides an overview of database records.

DNS zone transfer will allow replication of DNS data or DNS files. The user will perform a DNS zone transfer query from the name server. If the name server allows transfer by any other unauthorized user than all DNS names and IP addresses hosted by the name server will return in ASCII Text.

Some of the tools that can be for this include nslookup, maltego, dnenum, dnsrecon, etc.

Here is an example that uses nslookup.

NSlookup queries DNS servers for machine names and addresses.

For example, if we want to find the IP address of Google's web server by entering nslookup, we will enter the below command.

```
nslookup www.google.com
```

and then the output will be like this.

```
C:\>nslookup www.google.com
```

```
Server: dnsr1.sbcglobal.net
```

```
Address: 68.94.156.1
```

```
Non-authoritative answer:
```

```
Name: www.1.google.com
```

```
Addresses: 64.233.187.99, 64.233.187.104
```

```
Aliases: www.google.com
```

The first two lines of output tell us which DNS servers are being queried. In this case, it's dnsr1.sbcglobal.net in Texas. The non-authoritative answer lists two IP addresses for the Google web servers.

Responses from non-authoritative servers do not contain copies of any domains. They have a cache file that is constructed from all the DNS lookups it has performed in the past, for which it has received an authoritative response.



In the interactive mode, the user will be given a prompt of >; at which point, the user can enter a variety of options, including attempts to perform a zone transfer.

The hackers can enumerate other information like network resources and sharing, routing tables, machine names, applications and banners, users, and groups, etc.

There are other types of enumeration.

- Windows enumeration
- Linux enumeration
- LDAP enumeration
- NetBios enumeration
- SNMP enumeration
- NTP enumeration etc.

Steps to prevent enumeration.

1. Use centralized network administration contact details in the **NIC (Network Information Center)** database to prevent social engineering against IT departments.
2. Configure Name servers to disable DNS zone transfer for untrusted hosts. Configure web servers to prevent indexing of directories without index files and avoid keeping sensitive files and documents on publicly accessible hosts like FTP, HTTP, etc.
3. Configure **SMTP servers** to ignore emails from unknown recipients.
4. Disable SMB 
5. Use NTLM or basic authentication to limit access for authorized users only. Implement the group policy security option named "access restrictions for anonymous connections." 

Isisreviving.weebly.com