Ethical Hacking - Fingerprinting

The term OS fingerprinting in Ethical Hacking refers to any method used to determine what operating system is running on a remote computer. This could be −

- **Active Fingerprinting** − Active fingerprinting is accomplished by sending specially crafted packets to a target machine and then noting down its response and analyzing the gathered information to determine the target OS. In the following section, we have given an example to explain how you can use NMAP tool to detect the OS of a target domain.
- **Passive Fingerprinting** − Passive fingerprinting is based on sniffer traces from the remote system. Based on the sniffer traces (such as Wireshark) of the packets, you can determine the operating system of the remote host.

We have the following four important elements that we will look at to determine the operating system −

- **TTL** − What the operating system sets the **Time-To-Live** on the outbound packet.
- **Window Size** − What the operating system sets the Window Size at.
- **DF** − Does the operating system set the **Don't Fragment** bit.
- **TOS** − Does the operating system set the **Type of Service**, and if so, at what.

By analyzing these factors of a packet, you may be able to determine the remote operating system. This system is not 100% accurate, and works better for some operating systems than others.

Basic Steps

Before attacking a system, it is required that you know what operating system is hosting a website. Once a target OS is known, then it becomes easy to determine which vulnerabilities might be present to exploit the target system.

Below is a simple **nmap** command which can be used to identify the operating system serving a website and all the opened ports associated with the domain name, i.e., the IP address.

```
$nmap -O -v tutorialspoint.com
```

It will show you the following sensitive information about the given domain name or IP address −

```
Starting Nmap 5.51 ( http://nmap.org ) at 2015-10-04 09:57 CDT
Initiating Parallel DNS resolution of 1 host. at 09:57
Completed Parallel DNS resolution of 1 host. at 09:57, 0.00s elapsed
Initiating SYN Stealth Scan at 09:57
Scanning tutorialspoint.com (66.135.33.172) [1000 ports]
Discovered open port 22/tcp on 66.135.33.172
Discovered open port 3306/tcp on 66.135.33.172
Discovered open port 80/tcp on 66.135.33.172
Discovered open port 443/tcp on 66.135.33.172
Completed SYN Stealth Scan at 09:57, 0.04s elapsed (1000 total ports)
Initiating OS detection (try #1) against tutorialspoint.com (66.135.33.172)
Retrying OS detection (try #2) against tutorialspoint.com (66.135.33.172)
Retrying OS detection (try #3) against tutorialspoint.com (66.135.33.172)
Retrying OS detection (try #4) against tutorialspoint.com (66.135.33.172)
Retrying OS detection (try #5) against tutorialspoint.com (66.135.33.172)
Nmap scan report for tutorialspoint.com (66.135.33.172)
Host is up (0.000038s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql

TCP/IP fingerprint:
OS:SCAN(V=5.51%D=10/4%OT=22%CT=1%CU=40379%PV=N%DS=0%DC=L%G=Y%TM=56113E6D%P=
OS:x86_64-redhat-linux-gnu)SEQ(SP=106%GCD=1%ISR=109%TI=Z%CI=Z%II=I%TS=A)OPS
OS:(O1=MFFD7ST11NW7%O2=MFFD7ST11NW7%O3=MFFD7NNT11NW7%O4=MFFD7ST11NW7%O5=MFF
OS:D7ST11NW7%O6=MFFD7ST11)WIN(W1=FFCB%W2=FFCB%W3=FFCB%W4=FFCB%W5=FFCB%W6=FF
OS:CB)ECN(R=Y%DF=Y%T=40%W=FFD7%O=MFFD7NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A
OS:=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%
OS:Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=
OS:A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=
OS:Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%
OS:T=40%CD=S)
```

If you do not have **nmap** command installed on your Linux system, then you can install it using the following **yum** command −

```
$yum install nmap
```

You can go through **nmap** command in detail to check and understand the different features associated with a system and secure it against malicious attacks.

Quick Fix

You can hide your main system behind a secure proxy server or a VPN so that your complete identity is safe and ultimately your main system remains safe.

Port Scanning

We have just seen information given by **nmap** command. This command lists down all the open ports on a given server.

```
PORT       STATE   SERVICE
22/tcp     open    ssh
80/tcp     open    http
443/tcp    open    https
3306/tcp   open    mysql
```

You can also check if a particular port is opened or not using the following command −

```
$nmap -sT -p 443 tutorialspoint.com
```

It will produce the following result −

```
Starting Nmap 5.51 ( http://nmap.org ) at 2015-10-04 10:19 CDT
Nmap scan report for tutorialspoint.com (66.135.33.172)
Host is up (0.000067s latency).
PORT    STATE SERVICE
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
```

Once a hacker knows about open ports, then he can plan different attack techniques through the open ports.

Quick Fix

It is always recommended to check and close all the unwanted ports to safeguard the system from malicious attacks.

Ping Sweep

A ping sweep is a network scanning technique that you can use to determine which IP address from a range of IP addresses map to live hosts. Ping Sweep is also known as **ICMP sweep**.

You can use **fping** command for ping sweep. This command is a ping-like program which uses the Internet Control Message Protocol (ICMP) echo request to determine if a host is up.

fping is different from **ping** in that you can specify any number of hosts on the command line, or specify a file containing the lists of hosts to ping. If a host does not respond within a certain time limit and/or retry limit, it will be considered unreachable.

Quick Fix

To disable ping sweeps on a network, you can block ICMP ECHO requests from outside sources. This can be done using the following command which will create a firewall rule in **iptable**.

```
$iptables -A OUTPUT -p icmp --icmp-type echo-request -j DROP
```

DNS Enumeration

Domain Name Server (DNS) is like a map or an address book. In fact, it is like a distributed database which is used to translate an IP address 192.111.1.120 to a name www.example.com and vice versa.

DNS enumeration is the process of locating all the DNS servers and their corresponding records for an organization. The idea is to gather as much interesting details as possible about your target before initiating an attack.

You can use **nslookup** command available on Linux to get DNS and host-related information. In addition, you can use the following **DNSenum** script to get detailed information about a domain −

DNSenum.pl

DNSenum script can perform the following important operations −

- Get the host's addresses
- Get the nameservers
- Get the MX record
- Perform **axfr** queries on nameservers
- Get extra names and subdomains via **Google scraping**
- Brute force subdomains from file can also perform recursion on subdomain that has NS records
- Calculate C class domain network ranges and perform **whois** queries on them
- Perform **reverse lookups** on **netranges**

Quick Fix

DNS Enumeration does not have a quick fix and it is really beyond the scope of this tutorial. Preventing DNS Enumeration is a big challenge.

If your DNS is not configured in a secure way, it is possible that lots of sensitive information about the network and organization can go outside and an untrusted Internet user can perform a DNS zone transfer.