Service and OS Discovery

@mmar

CONCEPT

Service Discovery

- Identify Open Ports
- Identify Services Running on the ports

OS Discovery

- Identify running OS on target system

Service Discovery

Nmap

- Nmap is the go to tool for identifying open ports and services running on these ports

```
>nmap –sS –sV 192.168.18.1/24
```

sS	-	TCP Stealth scan
sV	-	Version Enumeration

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -sV 192.168.18.110
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-10 08:11 EDT
Nmap scan report for 192.168.18.110
Host is up (0.0022s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
```

Hping

- Hping is another very useful tool to identify ports and services

```
hping3 -S 192.168.18.110 -p 80 -c 5
```

S	-	TCP Stealth scan
P 80	-	Scan for port 80

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -S 192.168.18.110 -p 80 -c 5
HPING 192.168.18.110 (eth0 192.168.18.110): S set, 40 headers + 0 data bytes
len=46 ip=192.168.18.110 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=5840 rtt=7.2 ms
len=46 ip=192.168.18.110 ttl=64 DF id=0 sport=80 flags=SA seq=1 win=5840 rtt=3.4 ms
len=46 ip=192.168.18.110 ttl=64 DF id=0 sport=80 flags=SA seq=2 win=5840 rtt=5.1 ms
len=46 ip=192.168.18.110 ttl=64 DF id=0 sport=80 flags=SA seq=3 win=5840 rtt=8.0 ms
len=46 ip=192.168.18.110 ttl=64 DF id=0 sport=80 flags=SA seq=4 win=5840 rtt=3.4 ms
```

OS Discovery

Nmap

- OS discovery with nmap is very simple. Use the following command to determine the target system

```
>nmap –sS –O 192.168.18.1
```

```
MAC Address: 00:0C:29:71:62:0D (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

Nmap

- Nmap also has an inbuilt script to identify the OS but it needs smb service running on the system

```
sudo nmap --script smb-os-discovery.nse 192.168.18.110
```

```
Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-06-10T08:23:15-04:00
```

Manual Banner Grabbing

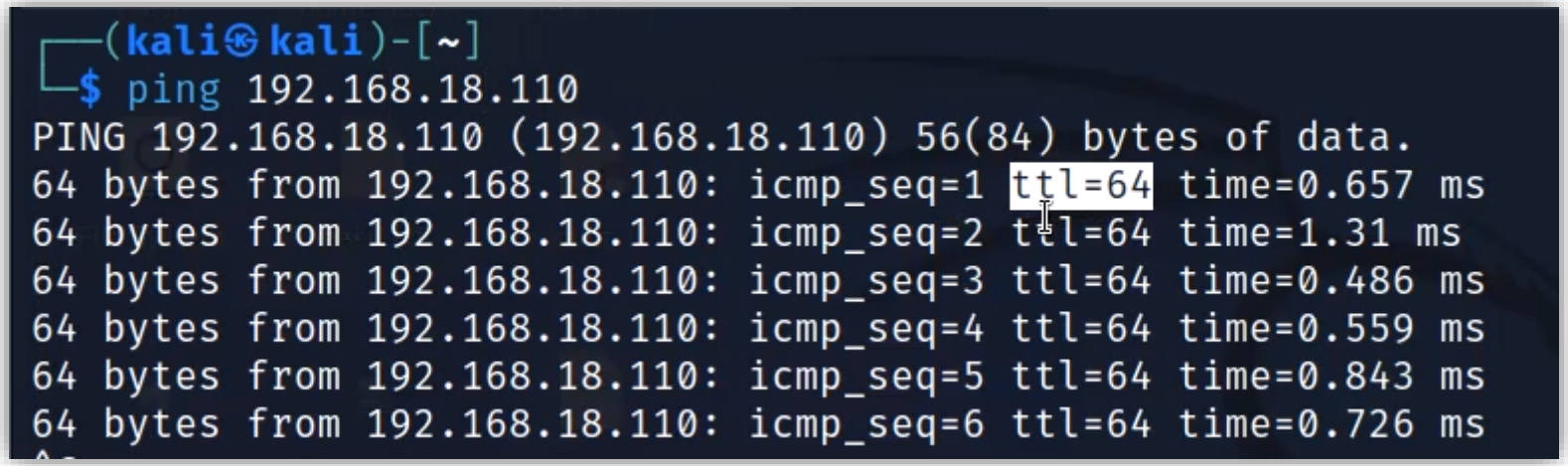
Parameters such as TTL and TCP window size in the IP header of the first packet in a TCP session plays an important role in identifying the OS running on the target machine. The TTL field determines the maximum time a packet can remain in a network, and the TCP window size determines the length of the packet reported. These values differ for different OSes: you can refer to the following table to learn the TTL values and TCP window size associated with various OSes.

Operating System	Time To Live	TCP Window Size
Linux	64	5840
FreeBSD	64	65535
OpenBSD	255	16384
Windows	128	65,535 bytes to 1 Gigabyte
Cisco Routers	255	4128
Solaris	255	8760
AIX	255	16384

Manual Banner Grabbing

- So, just ping your target and infer the OS from the response received

```
>ping 192.168.18.110
```



Comprehensive Scan

Nmap

- We can use the following one-liner on most of the targets to gather a lot of useful information like OS detection, version detection, script scanning, and traceroute

```
>sudo nmap –sS –p 445 –A 192.168.18.1
```

THANKS