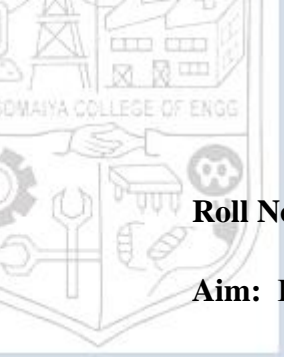




Experiment No. 8

Title: Implementing Active Reconnaissance

**Roll No.: 16010420075****Experiments No.: 8****Aim:** Implementing Active Reconnaissance

Resources: virtual box

Theory:

Active reconnaissance is a type of computer attack in which an intruder engages with the targeted system to gather information about vulnerabilities.

The word reconnaissance is borrowed from its military use, where it refers to a mission into enemy territory to obtain information. In a computer security context, reconnaissance is usually a preliminary step toward a further attack seeking to exploit the target system. The attacker often uses port scanning, for example, to discover any vulnerable ports. After a port scan, an attacker usually exploits known vulnerabilities of services associated with open ports that were detected.

Somewhat confusingly, active and passive reconnaissance are both sometimes referred to as passive attacks because they are just seeking information rather than actively exploiting the targets, as active attacks do.

Both active and passive reconnaissance are also used for ethical hacking, in which white hat hackers use attack methods to determine system vulnerabilities so that problems can be taken care of before the system falls prey to a real attack.

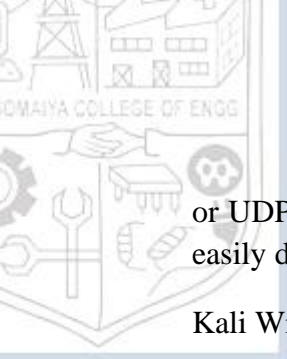
The simplest way to prevent most port scan attacks or reconnaissance attacks is to use a good firewall and intrusion prevention system (IPS). The firewall controls which ports are exposed and to whom they are visible. The IPS can detect port scans in progress and shut them down before the attacker can gain a full map of your network.

IMPLEMENTATION AND RESULTS:

Netcat:

We connect the client to the host using metasploitable and then extract data. netcat is a computer networking utility for reading from and writing to network connections using TCP

(A Constituent College of Somaiya Vidyavihar University)



or UDP. The command is designed to be a dependable back-end that can be used directly or easily driven by other programs and scripts.

Kali Window:

```
(kali@kali)-[~]  
$ sudo -i  
[sudo] password for kali:  
(root@kali)-[~]  
# nc -lp 3565  
hi  
hello  
i am client  
i am server  
ok  
yep  
bye
```

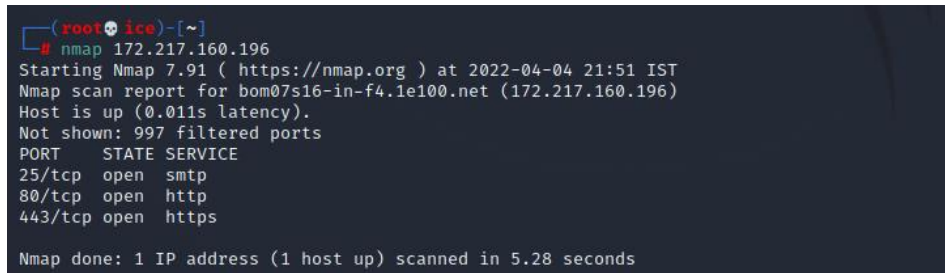
Metasploitable Window:

```
RX packets:24790 errors:0 dropped:0 overruns:0 frame:0  
TX packets:372 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:2437600 (2.3 MB) TX bytes:32143 (31.3 KB)  
Base address:0xd020 Memory:f0200000-f0220000  
  
lo Link encap:Local Loopback  
inet addr:127.0.0.1 Mask:255.0.0.0  
inet6 addr: ::1/128 Scope:Host  
UP LOOPBACK RUNNING MTU:16436 Metric:1  
RX packets:320 errors:0 dropped:0 overruns:0 frame:0  
TX packets:320 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0  
RX bytes:70008 (68.3 KB) TX bytes:70008 (68.3 KB)  
  
msfadmin@metasploitable:~$ sudo nc 10.0.2.15 3565  
hi  
hello  
i am client  
i am server  
ok  
yep  
bye  
  
msfadmin@metasploitable:~$
```

Nmap:

Nmap is a network mapper that has emerged as one of the most popular, free network discovery tools on the market. Nmap is now one of the core tools used by network administrators to map their networks. The program can be used to find live hosts on a network, perform port scanning, ping sweeps, OS detection, and version detection.

A number of recent cyberattacks have re-focused attention on the type of network auditing that Nmap provides. Analysts have pointed out that the recent Capital One hack, for instance, could have been detected sooner if system administrators had been monitoring connected devices.



```
(root@ice)-[~]
# nmap 172.217.160.196
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-04 21:51 IST
Nmap scan report for bom07s16-in-f4.1e100.net (172.217.160.196)
Host is up (0.011s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https
Nmap done: 1 IP address (1 host up) scanned in 5.28 seconds
```

Outcomes: Successfully explored active recon tools

Conclusion: (Conclusion to be based on the objectives and outcomes achieved)

Active reconnaissance was successfully implemented.

Grade: AA / AB / BB / BC / CC / CD /DD

Signature of faculty in-charge with date

REFERENCES:

- <https://nmap.org/book/man-briefoptions.html>
- <https://hostinger.in/tutorials/how-to-use-the-dig-command-in-linux/>
- <https://www.kali.org/tools/theharvester/>
- <https://www.computerhope.com/unix/unslooku.html>
- <https://www.computerhope.com/unix/uwhois.html>

(A Constituent College of Somaiya Vidyavihar University)