YOUNGDEV INTERNS

01 MONTH INTERNSHIP **HAMZA ZAHID**

INTERMEDIATE TASKS

TASK 01 :

PERFORM A BASIC VULNERABILITY SCAN

In this task we see a basic vulnerability scan by using Nmap

We use two virtual box machines

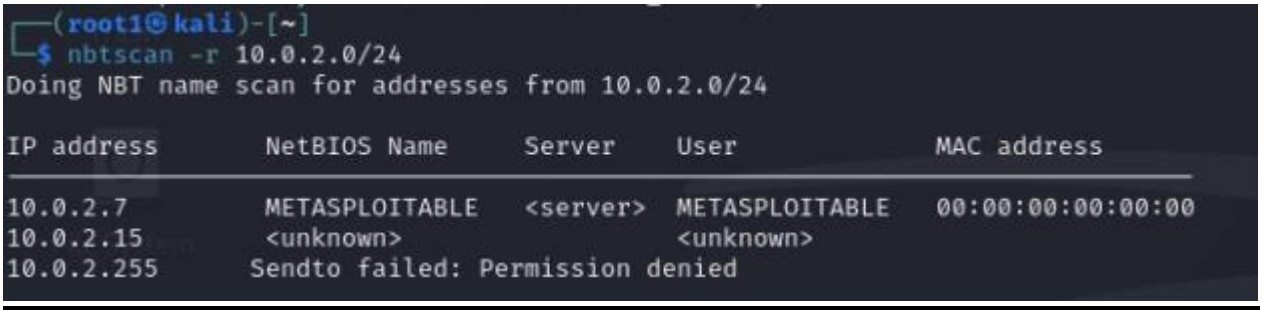
First is Linux which is an attacker machine

Second is Metasploitable which is target machine

These two virtual box machines are connected on the same subnet

Must three steps we follow

STEP 01



1 – In this step we use nbtscan -r <ip address>

2- this command finds all the ip address of the target machine that are connected

On the same network.

3-the target machine ip address is 10.0.2.7

4- the attacker machine ip address is 10.0.2.15

STEP : 02

```
┌──(root1㉿kali)-[~]
└─$ ping 10.0.2.7
PING 10.0.2.7 (10.0.2.7) 56(84) bytes of data.
64 bytes from 10.0.2.7: icmp_seq=1 ttl=64 time=20.7 ms
64 bytes from 10.0.2.7: icmp_seq=2 ttl=64 time=2.62 ms
64 bytes from 10.0.2.7: icmp_seq=3 ttl=64 time=8.90 ms
64 bytes from 10.0.2.7: icmp_seq=4 ttl=64 time=14.3 ms
64 bytes from 10.0.2.7: icmp_seq=5 ttl=64 time=5.96 ms
^C
── 10.0.2.7 ping statistics ──
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 2.619/10.509/20.730/6.397 ms
```

1- **In this step command we use the ping command to check the connectivity Of target machine**

STEP : 03

```
┌──(root1㉿kali)-[~]
└─$ nmap -sT  -sV  -F 10.0.2.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-13 02:45 EDT
Nmap scan report for 10.0.2.7
Host is up (0.033s latency).
Not shown: 85 closed tcp ports (conn-refused)
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
25/tcp   open  smtp?
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 169.60 seconds
```

1- **In this step we use the nmap command to to check the vulnerabilities of target machine**

   1 -sT to check all the tcp open ports

   2 -sV to find the services and version info of open ports

   3 -F is the fast mode it scan all the ports fastly within seconds .