Lab1A: Reconnaissance Lab Report

Scanning Manifest

Penetration Tester	Gregory Kukanich
Scanning periods	2/2/2021 6:30 PM – 2/3/2021 8:30 PM
Tools	Nmap, OpenVAS
Scope	Identifying network vulnerabilities in clients computer system with the IP of "10.0.2.4".
Description	Identifying vulnerabilities in the clients computer systems so that they can be patched to ensure proper security of the system.

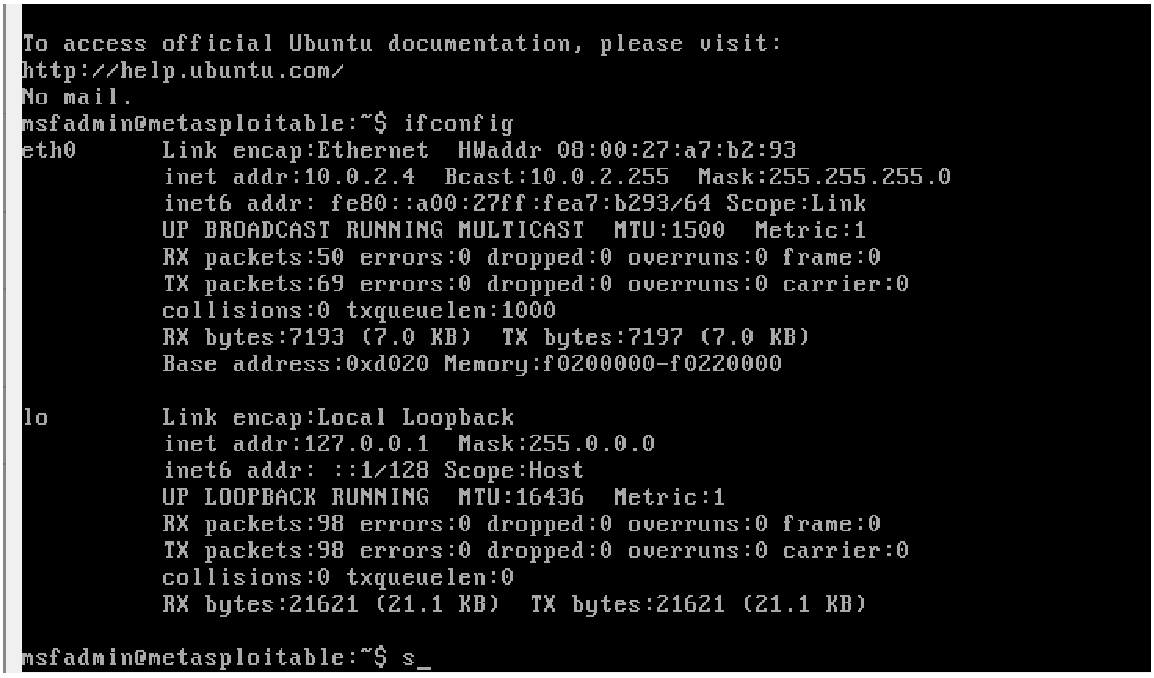
Executive Summary

Scope:

The scans conducted were an attempt to identify possible vulnerabilities in the client's computer system. Vulnerabilities that are left unchecked can cause huge issues for companies. They can allow for attackers to gain access to the systems or be able to disrupt the systems. The hope of today's scan is to identify all the issues so that they can all be fixed to improve the security of the system.

Approach:

First I identified the target system that the client wanted us to check. Using the "ifconfig" command on the target system I was able to get the IP address of the system which was "10.0.2.4".

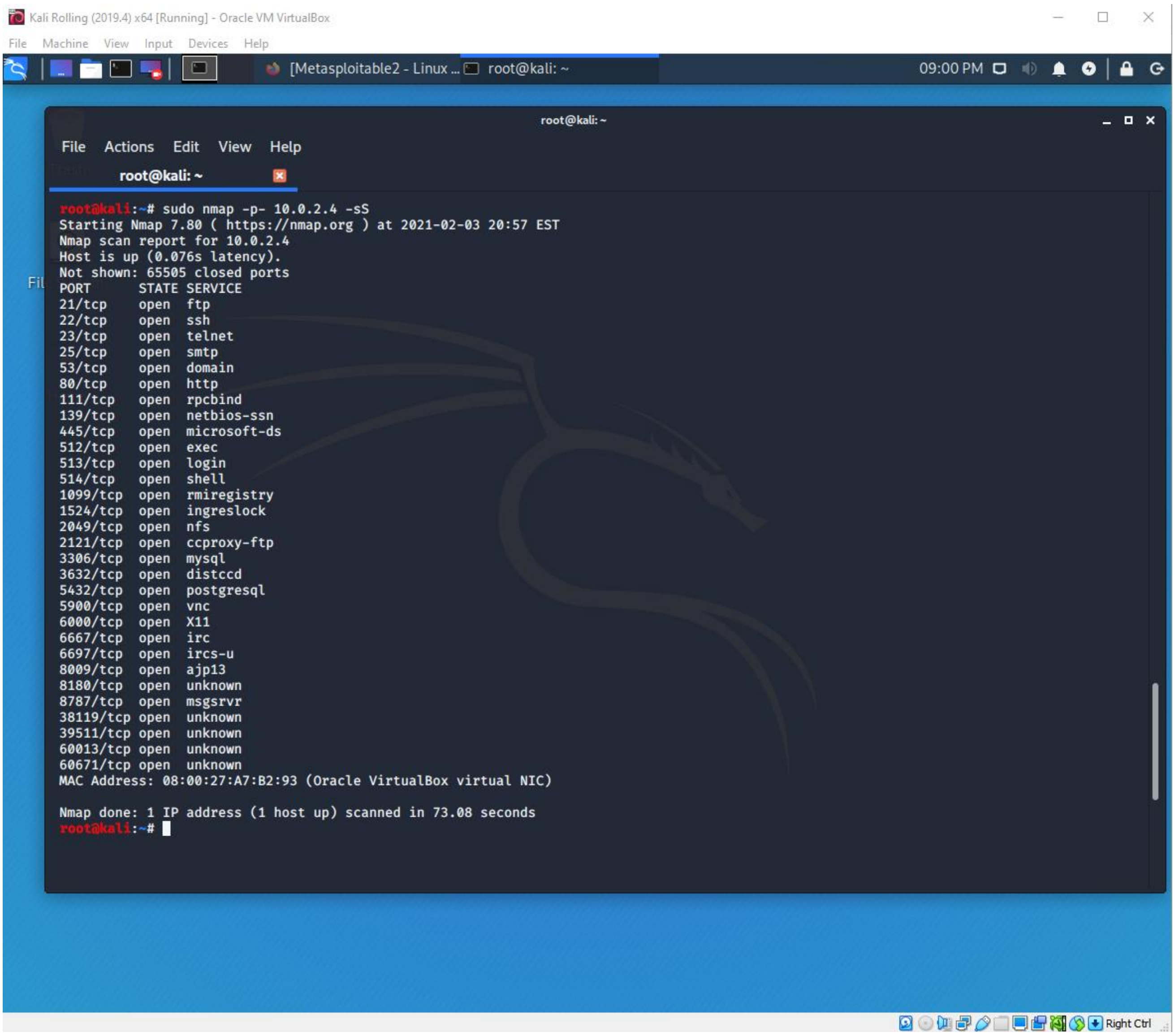


```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a7:b2:93
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea7:b293/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:50 errors:0 dropped:0 overruns:0 frame:0
          TX packets:69 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7193 (7.0 KB)  TX bytes:7197 (7.0 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:98 errors:0 dropped:0 overruns:0 frame:0
          TX packets:98 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21621 (21.1 KB)  TX bytes:21621 (21.1 KB)

msfadmin@metasploitable:~$ s_
```

After Identifying the target systems IP address, I can now move forward with scanning the system for vulnerabilities. I next used the Nmap SYN scan to look for all the open/filtered/closed TCP ports. To do this I used “nmap -p- 10.0.2.4 -sS”. The “-p-” specifies to scan all TCP ports and the “-sS” specifies to use a SYN scan.

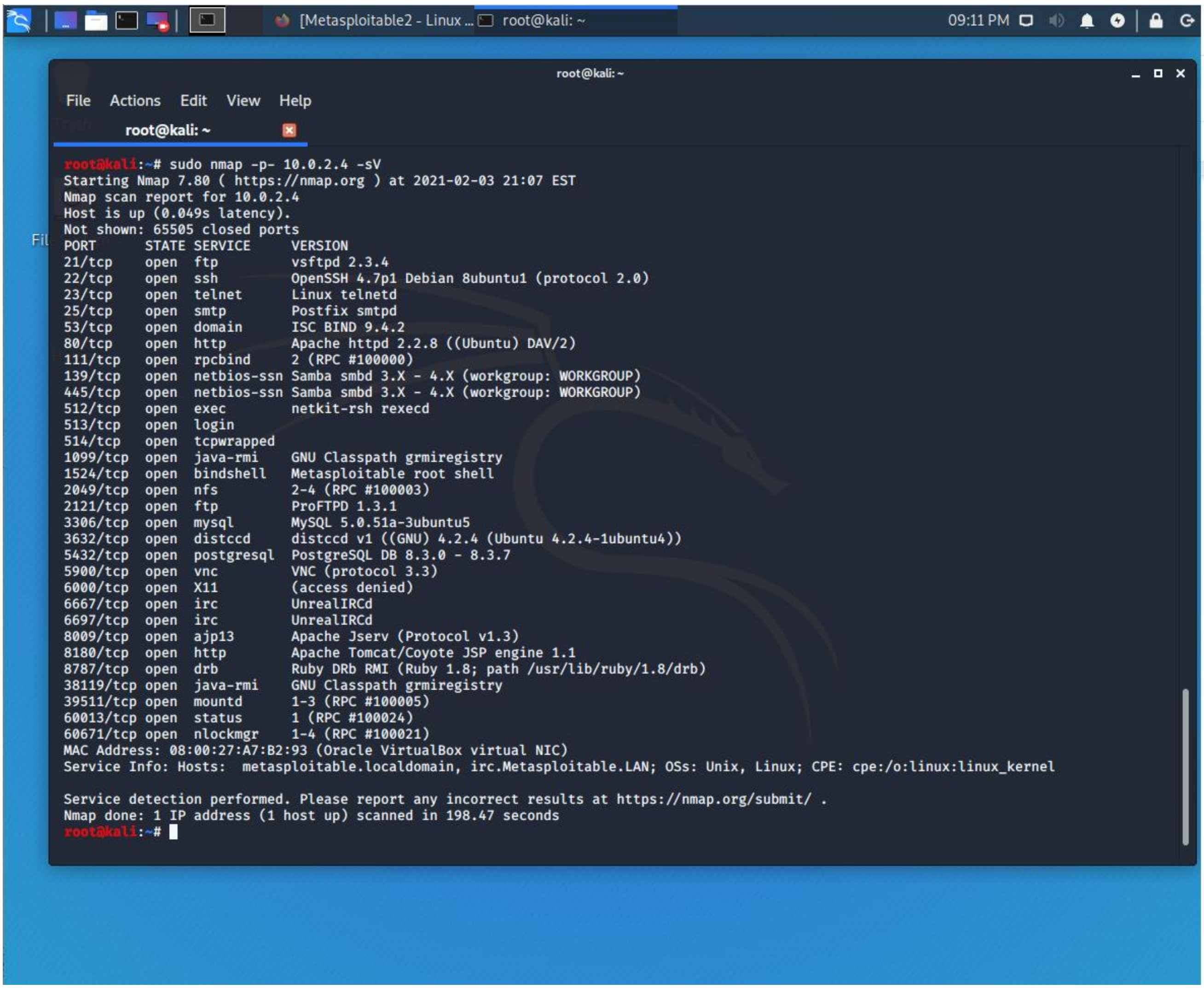

Kali Rolling (2019.4) x64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[Metasploitable2 - Linux ...
root@kali: ~
09:00 PM
root@kali: ~
File Actions Edit View Help
root@kali: ~
Right Ctrl

```
root@kali:~# sudo nmap -p- 10.0.2.4 -sS
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-03 20:57 EST
Nmap scan report for 10.0.2.4
Host is up (0.076s latency).
Not shown: 65505 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
38119/tcp open  unknown
39511/tcp open  unknown
60013/tcp open  unknown
60671/tcp open  unknown
MAC Address: 08:00:27:A7:B2:93 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 73.08 seconds
root@kali:~# 
```

As you can see lots of ports were scanned and the results show that most of the ports are closed. But there is a group of some that are open. These open ports could be used as an access point by an attacker.

After doing that scan, I wanted some more information about what the OS was and what services were running. So, I used “nmap -p- 10.0.2.4 -sV” the “-sV” specifies to search and find service/version information about the system.

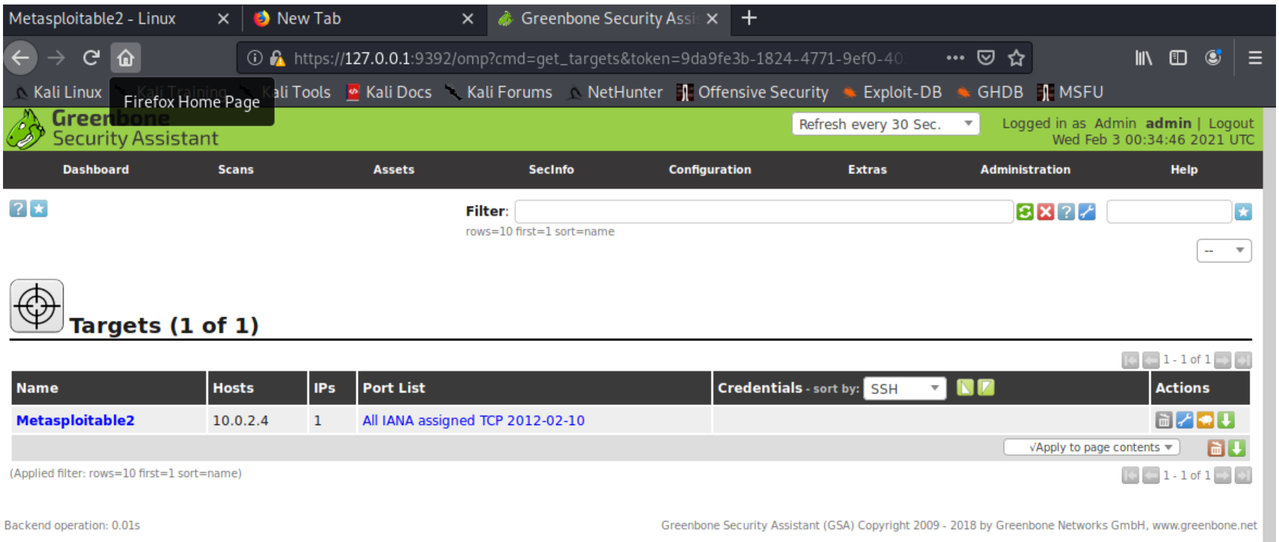


```
root@kali:~# sudo nmap -p- 10.0.2.4 -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-03 21:07 EST
Nmap scan report for 10.0.2.4
Host is up (0.049s latency).
Not shown: 65505 closed ports
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
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)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
38119/tcp open  java-rmi    GNU Classpath grmiregistry
39511/tcp open  mountd      1-3 (RPC #100005)
60013/tcp open  status      1 (RPC #100024)
60671/tcp open  nlockmgr    1-4 (RPC #100021)
MAC Address: 08:00:27:A7:B2:93 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; 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 198.47 seconds
root@kali:~# 
```

As you can see the scan was successful it informed me of the Host OS as well as the services running on the open ports. Some of the services seen such as SMTPD on port 25, Apache on port 80, and PostgreSQL on port 5432, these services correspond with a mail server, a web server, and an SQL database, respectively. Leaving ports like this open and vulnerable can have consequences.

After this I decided to run an OpenVAS scan to look for specific vulnerabilities on the system. As you can see the targets IP address “10.0.2.4” that was gathered earlier is set as the host target. The results of this scan will be attached detailing all of the vulnerabilities that were discovered.



Name	Hosts	IPs	Port List	Credentials - sort by: SSH	Actions
Metasploitable2	10.0.2.4	1	All IANA assigned TCP 2012-02-10		

Findings:

There were a large number of vulnerabilities discovered on the system all of which will be attached in a report that goes into more detail. These vulnerabilities make the clients computer system extremely insecure and easily attackable. I recommend the IT department reviews both my report and the attached report of all the vulnerabilities to quickly fix and resolve them to ensure system security.

I want to specifically address one of the vulnerabilities that was found due to its extreme nature. During the OpenVAS scan a vulnerability on port 80 was discovered that is considered to be an extreme threat to the system. The system is running an outdated version “TWiki” on port 80. This outdated version is open to Cross-Site Scripting and Command Execution Vulnerabilities. If an attacker were to exploit this vulnerability, they could execute scripts or commands that could harm the system. The fix for this vulnerability is simple, the IT department needs to update “TWiki” to version 4.2.4 or later as the vendor fixed the vulnerability in their software.