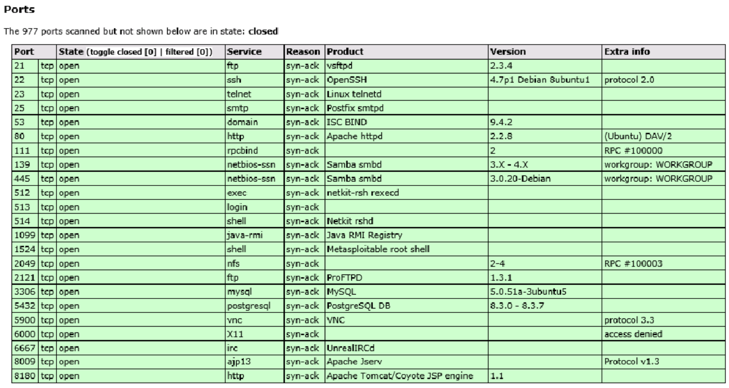
CEN4088.01 Lab 4 Due 10/21/19

Brandon Thompson 5517

October 21, 2019

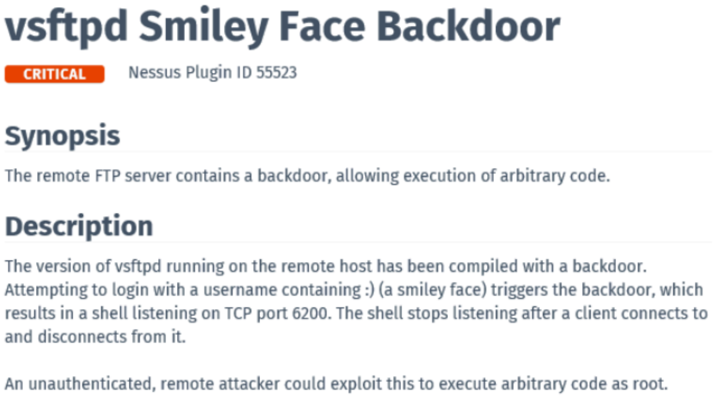


Ports

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	

Figure 1: Open ports of victim machine.



vsftpd Smiley Face Backdoor

Nessus Plugin ID 55523

Synopsis

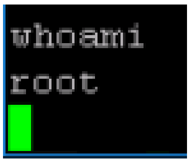
The remote FTP server contains a backdoor, allowing execution of arbitrary code.

Description

The version of vsftpd running on the remote host has been compiled with a backdoor. Attempting to login with a username containing :) (a smiley face) triggers the backdoor, which results in a shell listening on TCP port 6200. The shell stops listening after a client connects to and disconnects from it.

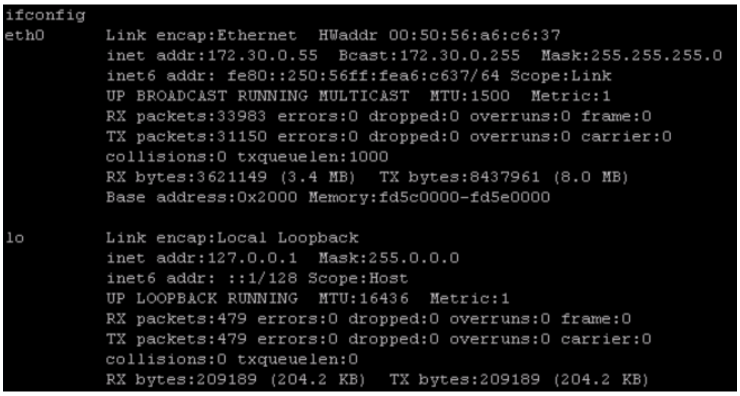
An unauthenticated, remote attacker could exploit this to execute arbitrary code as root.

Figure 2: Details of 55523 vulnerability.



```
whoami
root
```

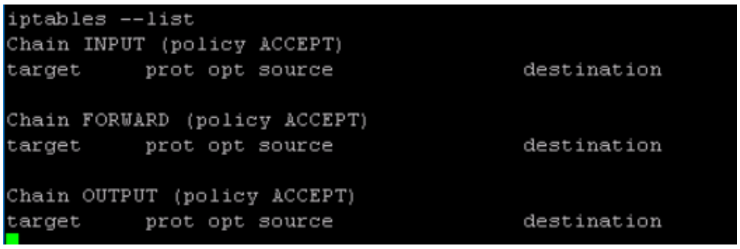
Figure 3: Result of `whoami` command after metasploit has given access to victim machine.



```
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:a6:c6:37
          inet addr:172.30.0.55  Bcast:172.30.0.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fea6:c637/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:33983 errors:0 dropped:0 overruns:0 frame:0
          TX packets:31150 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3621149 (3.4 MB)  TX bytes:8437961 (8.0 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:479 errors:0 dropped:0 overruns:0 frame:0
          TX packets:479 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:209189 (204.2 KB)  TX bytes:209189 (204.2 KB)
```

Figure 4: Result of `ifconfig` command after acquiring root access.

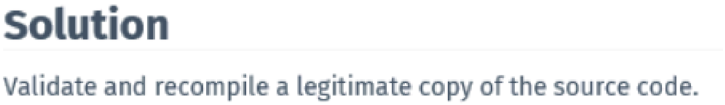


```
iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

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

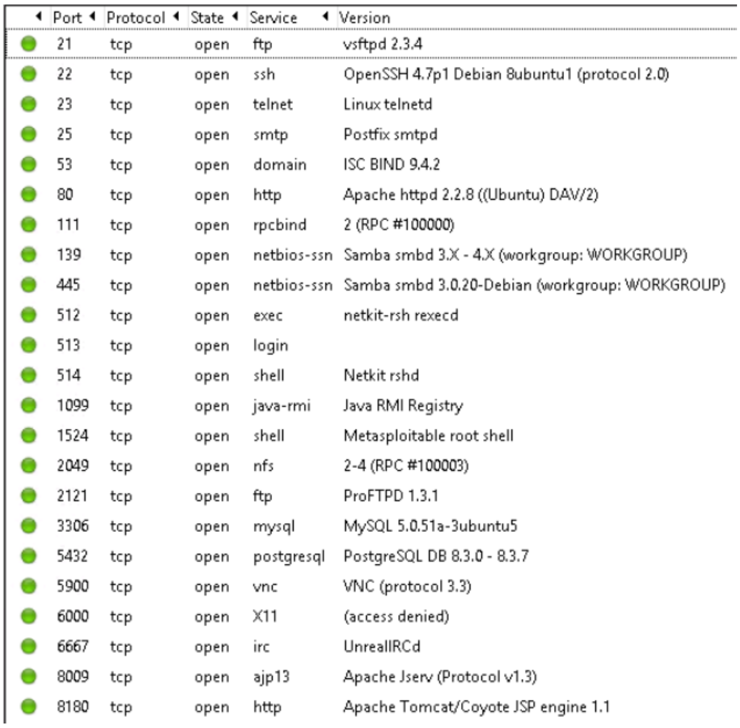
Figure 5: List of ip tables and rules after acquiring root access.



Solution

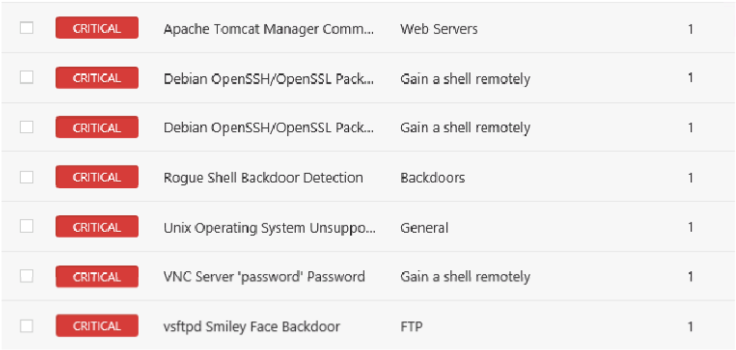
Validate and recompile a legitimate copy of the source code.

Figure 6: Solution to the `vstftpd` vulnerability.



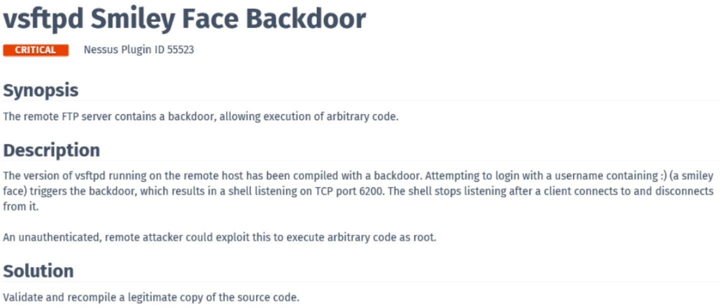
	Port	Protocol	State	Service	Version
●	21	tcp	open	ftp	vsftpd 2.3.4
●	22	tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
●	23	tcp	open	telnet	Linux telnetd
●	25	tcp	open	smtp	Postfix smtpd
●	53	tcp	open	domain	ISC BIND 9.4.2
●	80	tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
●	111	tcp	open	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

Figure 7: List of open ports given from the Zenmap tool.



□	CRITICAL	Apache Tomcat Manager Comm...	Web Servers	1
□	CRITICAL	Debian OpenSSH/OpenSSL Pack...	Gain a shell remotely	1
□	CRITICAL	Debian OpenSSH/OpenSSL Pack...	Gain a shell remotely	1
□	CRITICAL	Rogue Shell Backdoor Detection	Backdoors	1
□	CRITICAL	Unix Operating System Unsuppo...	General	1
□	CRITICAL	VNC Server 'password' Password	Gain a shell remotely	1
□	CRITICAL	vsftpd Smiley Face Backdoor	FTP	1

Figure 8: List of critical vulnerabilities given by Nessus web client.



vsftpd Smiley Face Backdoor

CRITICAL Nessus Plugin ID 55523

Synopsis

The remote FTP server contains a backdoor, allowing execution of arbitrary code.

Description

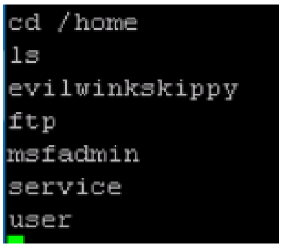
The version of vsftpd running on the remote host has been compiled with a backdoor. Attempting to login with a username containing :) (a smiley face) triggers the backdoor, which results in a shell listening on TCP port 6200. The shell stops listening after a client connects to and disconnects from it.

An unauthenticated, remote attacker could exploit this to execute arbitrary code as root.

Solution

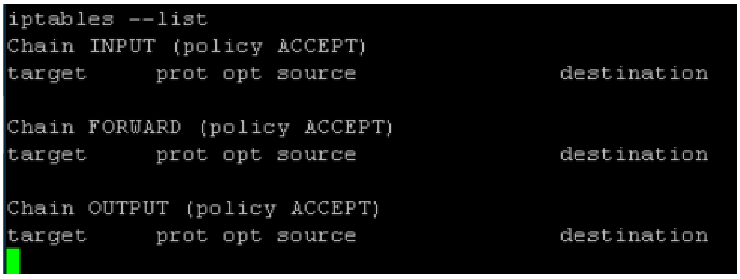
Validate and recompile a legitimate copy of the source code.

Figure 9: Details of 55523 vulnerability given by Nessus web client.



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

Figure 10: Contents of `/home` of Metasploitable machine.

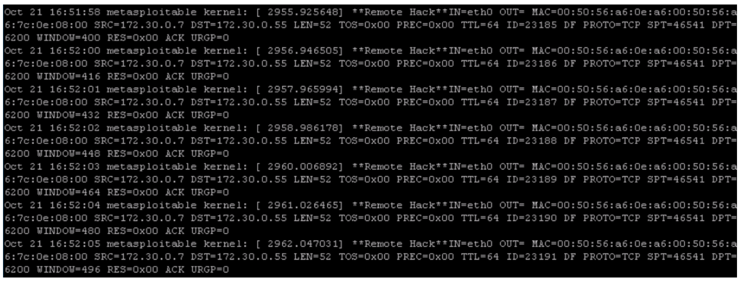


```
iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

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

Figure 11: List of iptables and rules of Metasploitable machine.



```
Oct 21 16:51:58 metasploitable kernel: [ 2955.925648] **Remote Hack**IN=eth0 OUT= MAC=00:50:56:a6:0e:a6:00:50:56:a
6:7c:0e:08:00 SRC=172.30.0.7 DST=172.30.0.55 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=23185 DF PROTO=TCP SPT=46541 DPT=
6200 WINDOW=400 RES=0x00 ACK URGP=0
Oct 21 16:52:00 metasploitable kernel: [ 2956.946505] **Remote Hack**IN=eth0 OUT= MAC=00:50:56:a6:0e:a6:00:50:56:a
6:7c:0e:08:00 SRC=172.30.0.7 DST=172.30.0.55 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=23186 DF PROTO=TCP SPT=46541 DPT=
6200 WINDOW=416 RES=0x00 ACK URGP=0
Oct 21 16:52:01 metasploitable kernel: [ 2957.965994] **Remote Hack**IN=eth0 OUT= MAC=00:50:56:a6:0e:a6:00:50:56:a
6:7c:0e:08:00 SRC=172.30.0.7 DST=172.30.0.55 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=23187 DF PROTO=TCP SPT=46541 DPT=
6200 WINDOW=432 RES=0x00 ACK URGP=0
Oct 21 16:52:02 metasploitable kernel: [ 2958.986178] **Remote Hack**IN=eth0 OUT= MAC=00:50:56:a6:0e:a6:00:50:56:a
6:7c:0e:08:00 SRC=172.30.0.7 DST=172.30.0.55 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=23188 DF PROTO=TCP SPT=46541 DPT=
6200 WINDOW=448 RES=0x00 ACK URGP=0
Oct 21 16:52:03 metasploitable kernel: [ 2960.006892] **Remote Hack**IN=eth0 OUT= MAC=00:50:56:a6:0e:a6:00:50:56:a
6:7c:0e:08:00 SRC=172.30.0.7 DST=172.30.0.55 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=23189 DF PROTO=TCP SPT=46541 DPT=
6200 WINDOW=464 RES=0x00 ACK URGP=0
Oct 21 16:52:04 metasploitable kernel: [ 2961.026465] **Remote Hack**IN=eth0 OUT= MAC=00:50:56:a6:0e:a6:00:50:56:a
6:7c:0e:08:00 SRC=172.30.0.7 DST=172.30.0.55 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=23190 DF PROTO=TCP SPT=46541 DPT=
6200 WINDOW=480 RES=0x00 ACK URGP=0
Oct 21 16:52:05 metasploitable kernel: [ 2962.047031] **Remote Hack**IN=eth0 OUT= MAC=00:50:56:a6:0e:a6:00:50:56:a
6:7c:0e:08:00 SRC=172.30.0.7 DST=172.30.0.55 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=23191 DF PROTO=TCP SPT=46541 DPT=
6200 WINDOW=496 RES=0x00 ACK URGP=0
```

Figure 12: **Remote Hack** message in log file of Metasploitable machine.