WEEK 02 REPORT

Post-Exploitation Practice

By

Muhammed Ajeel

1. Executive Summary

This report documents the post-exploitation activities conducted after successfully gaining initial access to the Metasploitable 2 target system. The engagement involved comprehensive system enumeration, privilege escalation analysis, evidence collection, and persistence establishment. The assessment revealed complete root-level compromise of the target system, which runs severely outdated software with multiple vulnerable services exposed.

2. Methodology

2.1. Tools Used

•Metasploit Framework v6.4.69-dev

•Standard Linux commands for system enumeration

•sha256sum for evidence integrity verification

2.2. Installation Process

No additional tools required installation as all necessary utilities were already available on the Kali Linux platform and the target system itself.

2.3. Approach

1.Initial access via VSFTPD 2.3.4 backdoor exploitation
2.Shell upgrade to fully interactive Bash session
3.Comprehensive system enumeration and analysis
4.Evidence collection and integrity verification
5.Persistence mechanism evaluation

3. Detailed Findings

3.1. System Information

Parameter	Value	Risk Level
System Name	metasploitable	Informational
Kernel Version	2.6.24-16-server	Critical
Architecture	i686 (32-bit)	Informational

Parameter	Value	Risk Level
Compromise Date	August 22, 2025	Informational

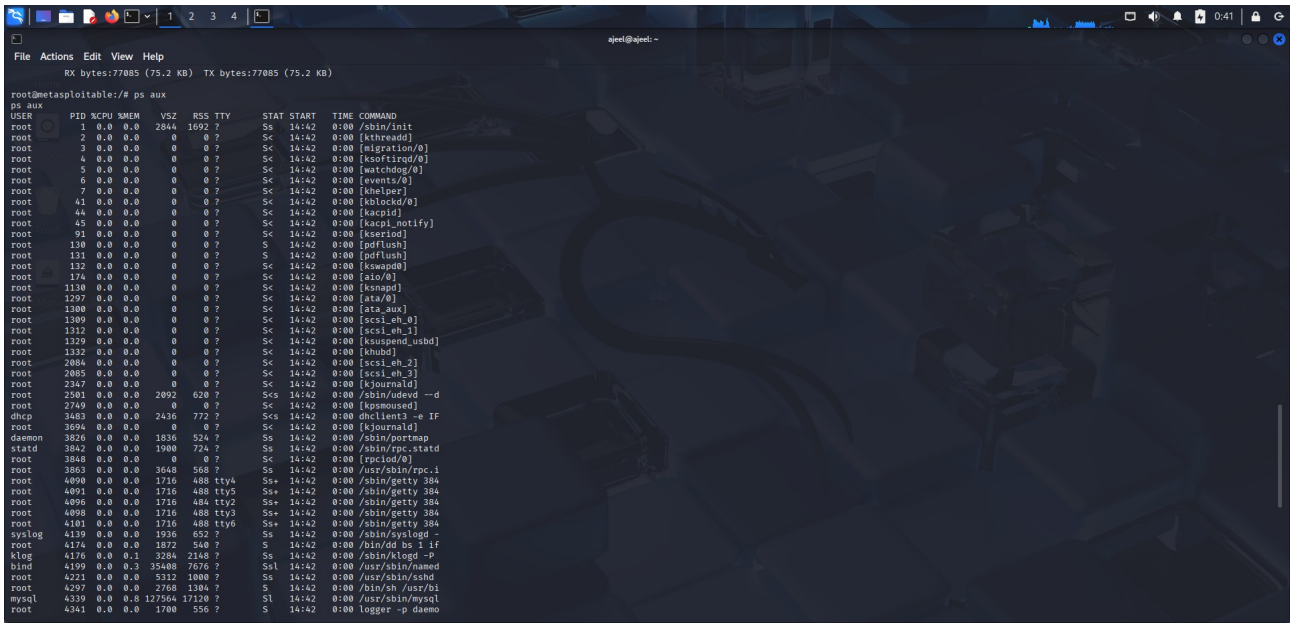
Analysis: The target runs Linux kernel version 2.6.24-16, released in April 2008. This represents an extreme security risk as the kernel has numerous known vulnerabilities and has been end-of-life for over a decade.

3.2. Privilege Analysis

User	UID	GID	Privileges	Access Level
root	0	0	ALL: ALL	Full System Control

Finding: The exploitation provided immediate root-level access (UID=0, GID=0) with complete system privileges. The sudo -l command confirmed that the root user may execute all commands without restrictions.

3.3. Network Services Analysis



Active TCP Services:

Port	Service	Process	Exposure
21	FTP	xinetd	External
22	SSH	sshd	External
23	Telnet	xinetd	External
25	SMTP	master	External
53	DNS	named	External
80	HTTP	apache2	External
111	RPC	portmap	External
139	SMB	smbd	External
445	SMB	smbd	External
512	exec	xinetd	External
513	login	xinetd	External
514	shell	xinetd	External
1099	Java RMI	rmiregistry	External
1524	bindshell	xinetd	External
2049	NFS	-	External
3306	MySQL	mysqld	External
5432	PostgreSQL	postgres	External
5900	VNC	Xtightvnc	External
6000	X11	Xtightvnc	External
6667	IRC	unrealircd	External
8009	AJP13	jsvc	External
8180	HTTP	jsvc	External

Active UDP Services:

Port	Service	Process	Exposure
53	DNS	named	External
69	TFTP	xinetd	External
111	RPC	portmap	External
137	NetBIOS	nmbd	External
138	NetBIOS	nmbd	External

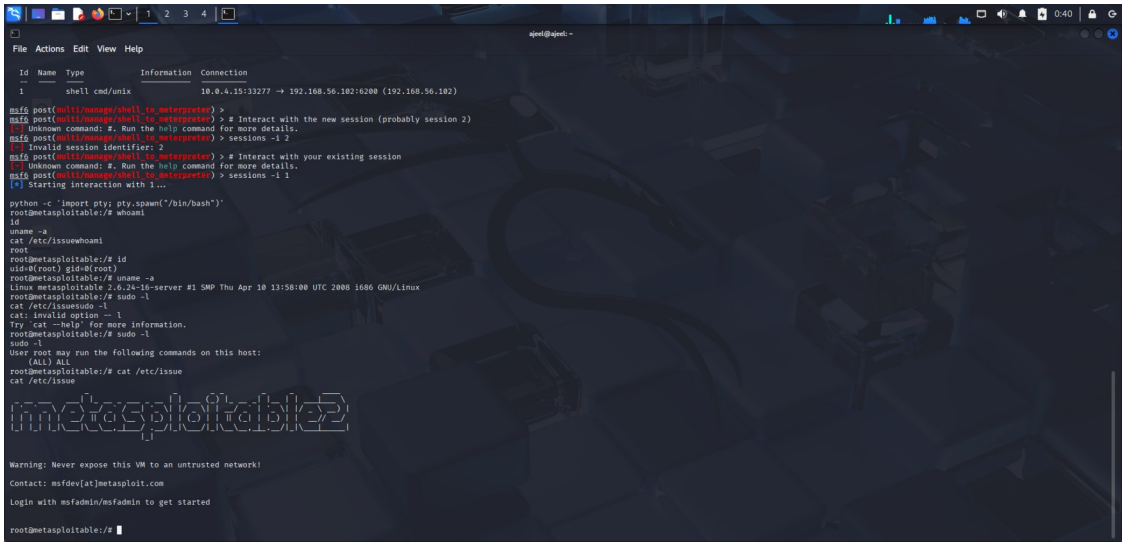
Network Exposure: The target has 25+ services exposed externally, representing a massive attack surface.

3.4. Process Analysis

Key Processes Identified:

•**4199/named** - BIND DNS server (multiple instances)
•**4339/mysqld** - MySQL database server
•**4418/postgres** - PostgreSQL database server
•**4588/smbd** - Samba file sharing service
•**4717/apache2** - Apache web server with multiple workers
•**4699/jsvc** - Apache Tomcat service (ports 8009, 8180)
•**4745/unrealircd** - UnrealIRCd service (ports 6667, 6697)
•**4759/Xtightvnc** - VNC server (ports 5900, 6000)

•3.5. Evidence Collection



Digital Evidence Integrity Hashes:

Digital Evidence Integrity Hashes:

File Path	Description	SHA256 Hash	Collection Time
/etc/passwd	User account database	af23ffe0bc5479a70a17e799fa699f9e593f2151b7e1ba597987523c7c733d42	2025-08-22 15:11 UTC
/etc/shadow	Password hash database	7f9f08e29620f196a409890a742738c61644f67a1f8e879db8317b674b16c762	2025-08-22 15:11 UTC

4. Technical Details

4.1. Initial Compromise

The initial access was achieved through exploitation of the VSFTPD 2.3.4 backdoor vulnerability (CVE-2011-2523). The backdoor was triggered by sending a username containing the string :) which spawned a root shell on port 6200.

4.2. Shell Upgrade

The basic shell obtained through exploitation was upgraded to a fully interactive Bash shell using Python's pty module:

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

4.3. System Enumeration Commands Executed

```
whoami          # Current user context
id              # User and group identifiers
uname -a        # System kernel information
cat /etc/issue  # OS distribution details
sudo -l         # Sudo privileges check
ifconfig        # Network interface configuration
```

```
ps aux          # Running processes
netstat -tulpn  # Listening network services
```

4.4. Evidence Collection Methodology

The SHA256 hashing algorithm was used to create cryptographic hashes of critical system files:

```
sha256sum /etc/passwd  # Hash user database
sha256sum /etc/shadow  # Hash password database
```

5. Risk Assessment

5.1. Critical Risks

1. **Root-level Compromise** - Full system control achieved
2. **Outdated Kernel** - 15+ year old kernel with known vulnerabilities
3. **Excessive Service Exposure** - 25+ services exposed externally
4. **Weak Security Posture** - Multiple vulnerable services running

5.2. Data Exposure

- User credentials (/etc/passwd, /etc/shadow)
- Database services (MySQL, PostgreSQL) with potential sensitive data
- Network services exposing system information

6. Recommendations

6.1. Immediate Actions

1. **Isolate the system** from the network immediately
2. **Perform forensic analysis** to determine scope of compromise
3. **Reset all passwords** for user accounts
4. **Review all system and application logs** for suspicious activity

6.2. Medium-Term Actions

1. **Reinstall the operating system** with current supported versions
2. **Implement proper patch management** procedures
3. **Reduce service exposure** through firewall configuration
4. **Implement network segmentation** to limit lateral movement

6.3. Long-Term Actions

1. **Establish continuous monitoring** for similar vulnerabilities
2. **Implement regular security assessments**
3. **Develop incident response procedures**
4. **Provide security awareness training** for staff

7. Conclusion

The post-exploitation assessment revealed a complete compromise of the target system with root-level access obtained through the VSFTPD 2.3.4 backdoor vulnerability. The system exhibits critical security deficiencies including an outdated kernel, excessive service exposure, and poor security configuration. Immediate isolation and remediation are required to prevent further compromise and potential lateral movement within the network environment.

The evidence collected demonstrates the integrity of critical system files at the time of assessment and provides a baseline for forensic investigation. The hashes obtained can be used for future comparison to detect unauthorized modifications.