Comprehensive Report

Comprehensive Exploitation Report

Target: 192.168.1.50

Generated: 2025-09-02 13:56:35

Executive Summary

- **Total Exploits Found**: 0
- **Successful Services**: 0
- **Services Tested**: 0

Risk Summary

Severity	Confirmed	Potential
Critical	0	0
High	0	4

Severity	Confirmed	Potential
Medium	0	3
Low	0	0

Services & Scan Overview

Service	Ports	Recon	Exploit	Post-Exploitation
AJP13	8009/tcp	-	-	-
BAKBONENETVAULT	20031/udp	-	-	-
BINDSHELL	1524/tcp	-	-	-
DHCPC	68/udp	-	-	-
DISTCCD	3632/tcp	-	-	-
DLS-MONITOR	2048/udp	-	-	-
DOMAIN	53/udp	-	-	-
DRB	8787/tcp	-	-	-
EXEC-	512/tcp	-	-	-
FTP (Port 21)	-	Yes	-	-
H225GATEDISC	1718/udp	-	-	-
HTTP Web Server (Port 80)	-	Yes	-	-

Service	Ports	Recon	Exploit	Post-Exploitation
HTTPS	443/udp	-	-	-
IAD1	1030/udp	-	-	-
IRC (Port 6667)	-	Yes	-	-
JAVA-RMI	1099/tcp	-	-	-
LOGIN	513/tcp	-	-	-
MOUNTD	47917/tcp	-	-	-
MSANTIPIRACY	2222/udp	-	-	-
MySQL (Port 3306)	3306/tcp	Yes	-	-
NETBIOS-NS	137/udp	-	-	-
NETBIOS-SSN	139/tcp	-	-	-
NFS (Port 2049)	-	Yes	-	-
NLOCKMGR	44654/tcp	-	-	-
PostgreSQL (Port 5432)	5432/tcp	Yes	-	-
RETROSPECT	497/udp	-	-	-
RPCBIND	111/tcp	-	-	-
SMTP (Port 25)	-	Yes	-	-
SSH (Port 22)	-	Yes	-	-
STATUS	39086/tcp	-	-	-

Service	Ports	Recon	Exploit	Post-Exploitation
TCPWRAPPED	514/tcp	-	-	-
Telnet (Port 23)	23/tcp	-	-	-
TFTP	69/udp	-	-	-
UNKNOWN	49152/udp	-	-	-
VNC (Port 5900)	-	Yes	-	-
X11	6000/tcp	-	-	-

Confirmed Vulnerabilities

The following vulnerabilities were actively exploited and confirmed on the target system.

Vulnerability	Risk	Impact

Potential Vulnerabilities

The following vulnerabilities were identified but not actively exploited during the engagement.

Vulnerability	Risk	Impact
Apache/2.2.8	High	Outdated software can be exploited by attackers to gain unauthorized access or execute malicious code.

Vulnerability	Risk	Impact
PHP/5.2.4-2ubuntu5.10.	High	Outdated software can be exploited by attackers to gain unauthorized access or execute malicious code.
Apache/2.4.54).	High	Outdated software can be exploited by attackers to gain unauthorized access or execute malicious code.
mod_negotiation + MultiViews Enabled (Brute-force Files)	Medium	Security misconfigurations can expose sensitive data or functionality, potentially leading to unauthorized access.
HTTP TRACE Method Enabled (XST Attack)	Medium	Security misconfigurations can expose sensitive data or functionality, potentially leading to unauthorized access.
ETag Information Leak (Inode Leakage)	Medium	Security misconfigurations can expose sensitive data or functionality, potentially leading to unauthorized access.

Prioritized Remediation Plan

Immediate Actions Required (Critical & High Risk):

Secondary Actions (Medium & Low Risk):

Reconnaissance

IRC (Port 6667)

Field	Value
Target	192.168.1.50

- **Irc Raw Banner**: :irc.Metasploitable.LAN NOTICE AUTH : **Looking up your hostname... :irc.Metasploitable.LAN NOTICE AUTH :** Found your hostname (cached)
- **Msf Exploit Cves**:
- none
- **Msf Exploit Found**: no
- **Msf Exploit Mods**:
- none
- **Nmap Irc Banner**: Starting Nmap 7.95 (https://nmap.org) at 2025-09-02 13:25 +01 Nmap scan report for 192.168.1.50 (192.168.1.50) Host is up (0.00023s latency).

PORT STATE SERVICE VERSION 6667/tcp open irc UnrealIRCd MAC Address: 08:00:27:58:9E:87 (PCS Systemtechnik/Oracle VirtualBox virtual NIC) Service Info: Host: irc.Metasploitable.LAN

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds

FTP (Port 21)

Field	Value
Target	192.168.1.50
Port	2121

- **Anonymous Login Allowed**: no
- **Anonymous Upload Allowed**: no
- **Backdoor Detected**: no
- **Exploitdb Cves**:
- none
- **Exploitdb Mods**:
- none
- **Ftp Syst**:
- **Msf Cves**:
- none
- **Msf Mods**:
- none
- **Server**: ProFTPD
- **Version**: 1.3.1

SMTP (Port 25)

Field	Value
Target	192.168.1.50

- **Open Relay**: yes
- **Smtp Banner**: Starting Nmap 7.95 (https://nmap.org) at 2025-09-02 13:35 +01
- **Smtp Exploit Cves**:
- none
- **Smtp Exploit Found**: no
- **Smtp Exploit Mods**:
- none
- **Smtp Open**: yes
- **Users Valid**: 0

SSH (Port 22)

Field	Value
Target	192.168.1.50
Port	22

- **Allows Password Auth**: False
- **Audit**:
- **Auth Methods**:
-
- **Exploitdb Cves**:
- none

- **Exploitdb Mods**:
- OpenSSH 2.3 < 7.7 - Username Enumeration (PoC) (linux/remote/45210.py
- OpenSSH 2.3 < 7.7 - Username Enumeration (linux/remote/45233.py
- OpenSSH < 6.6 SFTP (x64) - Command Execution (linux_x86-64/remote/45000.c
- OpenSSH < 6.6 SFTP - Command Execution (linux/remote/45001.py
- OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain So (linux/local/40962.txt
- OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading (linux/remote/40963.txt
- OpenSSH < 7.7 - User Enumeration (2) (linux/remote/45939.py
- **Msf Cves**:
- none
- **Msf Mods**:
- none
- **Server**: OpenSSH
- **Version**: 4.7p1

VNC (Port 5900)

Field	Value
Target	192.168.1.50

- **Msf Exploit Cves**:
- none
- **Msf Exploit Found**: no
- **Msf Exploit Mods**:
- none
- **Nmap Vnc Banner**: Starting Nmap 7.95 (https://nmap.org) at 2025-09-02 13:43 +01 Nmap scan report for 192.168.1.50 (192.168.1.50) Host is up (0.00038s latency).

PORT STATE SERVICE VERSION 5900/tcp open vnc VNC (protocol 3.3) MAC Address: 08:00:27:58:9E:87 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 0.88 seconds - **Raw Vnc Banner**: RFB 003.003

HTTP Web Server (Port 80)

Field	Value
Target	192.168.1.50
OS Fingerprint	Linux 2.6.9 - 2.6.33
HTTP Banner	Apache/2.2.8 (Ubuntu) DAV/2
HTTPS Banner	unknown
Discovered Endpoints	28
Vulnerable Endpoint Categories	lfi, sql_injection

Discovered Endpoints (top 25)

URL	Type	Params
http://192.168.1.50/.htpasswd.bak	sensitive_file	file, path, include
http://192.168.1.50/phpMyAdmin	admin_panel	username, password, user (+4)
http://192.168.1.50/.htpasswd.txt	general_endpoint	id, file, page (+2)
http://192.168.1.50/server-status	general_endpoint	id, file, page (+2)

URL	Type	Params
http://192.168.1.50/.htaccess	general_endpoint	id, file, page (+2)
http://192.168.1.50/.htaccess.php	dynamic_file	id, file, page (+6)
http://192.168.1.50/cgi-bin/	general_endpoint	id, file, page (+2)
http://192.168.1.50/.htaccess.config	sensitive_file	file, path, include
http://192.168.1.50/.hta.txt	general_endpoint	id, file, page (+2)
http://192.168.1.50/.htaccess.bak	sensitive_file	file, path, include
http://192.168.1.50/index.php	dynamic_file	id, file, page (+6)
http://192.168.1.50/.htpasswd	general_endpoint	id, file, page (+2)
http://192.168.1.50/.htpasswd.config	sensitive_file	file, path, include
http://192.168.1.50/phpinfo	general_endpoint	id, file, page (+2)
http://192.168.1.50/.hta.php	dynamic_file	id, file, page (+6)
http://192.168.1.50/.htpasswd.php	dynamic_file	id, file, page (+6)
http://192.168.1.50/.htaccess.zip	general_endpoint	id, file, page (+2)
http://192.168.1.50/test	general_endpoint	id, file, page (+2)
http://192.168.1.50/.htaccess.txt	general_endpoint	id, file, page (+2)
http://192.168.1.50/twiki	general_endpoint	id, file, page (+2)
http://192.168.1.50/.hta.bak	sensitive_file	file, path, include

URL	Type	Params
http://192.168.1.50/.hta.config	sensitive_file	file, path, include
http://192.168.1.50/phpinfo.php	dynamic_file	id, file, page (+6)
http://192.168.1.50/.hta.zip	general_endpoint	id, file, page (+2)
http://192.168.1.50/index	general_endpoint	id, file, page (+2)
... and 3 more endpoints		

Vulnerable Endpoints

Type	URL	Parameter	Evidence
Sql Injection	http://192.168.1.50/phpinfo	id	-
Sql Injection	http://192.168.1.50/phpinfo	file	-
Sql Injection	http://192.168.1.50/phpinfo	page	-
Sql Injection	http://192.168.1.50/phpinfo	param	-
Sql Injection	http://192.168.1.50/phpinfo	action	-
Sql Injection	http://192.168.1.50/phpinfo.php	id	-
Sql Injection	http://192.168.1.50/phpinfo.php	file	-

Type	URL	Parameter	Evidence
Sql Injection	http://192.168.1.50/phpinfo.php	page	-
Sql Injection	http://192.168.1.50/phpinfo.php	include	-
Sql Injection	http://192.168.1.50/phpinfo.php	path	-
Sql Injection	http://192.168.1.50/phpinfo.php	cmd	-
Sql Injection	http://192.168.1.50/phpinfo.php	exec	-
Sql Injection	http://192.168.1.50/phpinfo.php	param	-
Sql Injection	http://192.168.1.50/phpinfo.php	action	-
Lfi	http://192.168.1.50/phpinfo	file	-
Lfi	http://192.168.1.50/phpinfo	page	-
Lfi	http://192.168.1.50/phpinfo.php	file	-
Lfi	http://192.168.1.50/phpinfo.php	page	-
Lfi	http://192.168.1.50/phpinfo.php	include	-

Type	URL	Parameter	Evidence
Lfi	http://192.168.1.50/phpinfo.php	path	-
... more vulnerable endpoints omitted for brevity			

- **Auth Bypass Opportunities**:
- HTTP TRACE Method
- **Burp Runner**:
- **Burp Summary**:
- **Default Files**:
- /index
- /phpMyAdmin/changelog.php
- **Exploitable Versions**:
- **Exposed Directories**:
- /phpMyAdmin/changelog.php
- /phpMyAdmin/ChangeLog
- /phpMyAdmin/
- /phpMyAdmin/Documentation.html
- /phpMyAdmin/README
- **Http Exploit Cves**:
- none
- **Http Exploit Found**: no
- **Http Exploit Mods**:
- none
- **Https Exploit Cves**:
- none

• **Https Exploit Found**: no

• **Https Exploit Mods**:

• none

• **Joomla Findings**:

• **Version**: unknown

• **Login Form Sql Injection**:

• **Success**: False

• **Misconfigurations**:

• mod_negotiation + MultiViews Enabled (Brute-force Files

• HTTP TRACE Method Enabled (XST Attack

• ETag Information Leak (Inode Leakage

• **Os Exploit Cves**:

• CVE-2006-2502

• CVE-2009-2692

• CVE-2010-3904

• CVE-2021-22555

• **Os Exploit Found**: yes

• **Os Exploit Mods**:

• exploit/linux/http/dreambox_openpli_shell

• exploit/linux/local/netfilter_xtables_heap_oob_write_priv_esc

• exploit/linux/local/rds_rds_page_copy_user_priv_esc

• exploit/linux/local/sock_sendpage

• exploit/linux/pop3/cyrus_pop3d_popsubfolders

• **Outdated Software**:

• Apache/2.2.8

• PHP/5.2.4-2ubuntu5.10

• Apache/2.4.54

- **Sqlmap Findings**:
- **Database Type**: unknown
- **Technique**: unknown
- **Technologies**:
- **Web Server**:
  - Apache
- **Programming Language**:
  - PHP
- **Wordpress Findings**:
- **Version**: unknown

PostgreSQL (Port 5432)

Field	Value
Target	192.168.1.50
Port	5432

- **Error**: Footprint error: [Errno 32] Broken pipe
- **Protocol**: tcp

NFS (Port 2049)

Field	Value
Target	192.168.1.50

- **Exploits Found**: yes
- **Metasploit Modules**:

- exploit/multi/http/atlassian_confluence_namespace_ognl_injection
- exploit/multi/http/atlassian_confluence_rce_cve_2024_21683
- exploit/multi/http/atlassian_confluence_unauth_backup
- exploit/multi/http/atlassian_confluence_webwork_ognl_injection
- exploit/netware/sunrpc/pkernel_callit
- exploit/osx/local/nfs_mount_root
- exploit/windows/ftp/labf_nfsaxe
- exploit/windows/ftp/xlink_client
- exploit/windows/ftp/xlink_server
- exploit/windows/nfs/xlink_nfsd
- **Nfs Exports**:
- none
- **Nfs Exports Count**: 0
- **Nfs Version**: nfs
- **Rpc Services Count**: 23

MySQL (Port 3306)

Field	Value
Target	192.168.1.50
Port	3306

- **Error**: Decoding error: 'utf-8' codec can't decode byte 0xaa in position 36: invalid start byte
- **Protocol**: tcp

Exploitation

Post-Exploitation