Vulnerability Assessment Report

Introduction

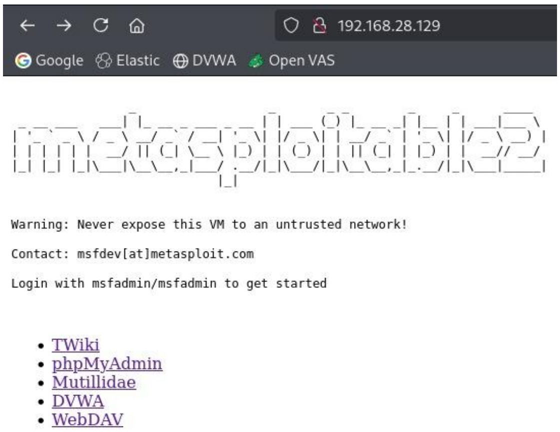
This report documents the findings of a comprehensive vulnerability assessment conducted on the Metasploitable2 virtual machine. Metasploitable2 is a intentionally vulnerable Ubuntu Linux distribution designed for security testing and training purposes. The assessment aimed to identify security vulnerabilities, misconfigurations, and potential attack vectors that could be exploited by malicious actors.

The assessment was performed using industry-standard security tools including OpenVAS vulnerability scanner and Nikto web application scanner, following established cybersecurity testing methodologies in an isolated lab environment.

Methodology

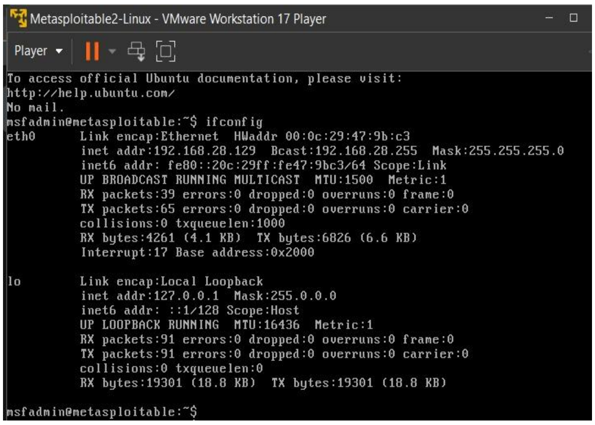
Testing Environment Setup

- ✓ **Attacker Machine:** Kali Linux
- ✓ **Target Machine:** Metasploitable2 (192.168.28.129)
- ✓ **Network Configuration:** Host-only network for isolation
- ✓ **Assessment Type:** Authenticated and unauthenticated vulnerability scanning



```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV



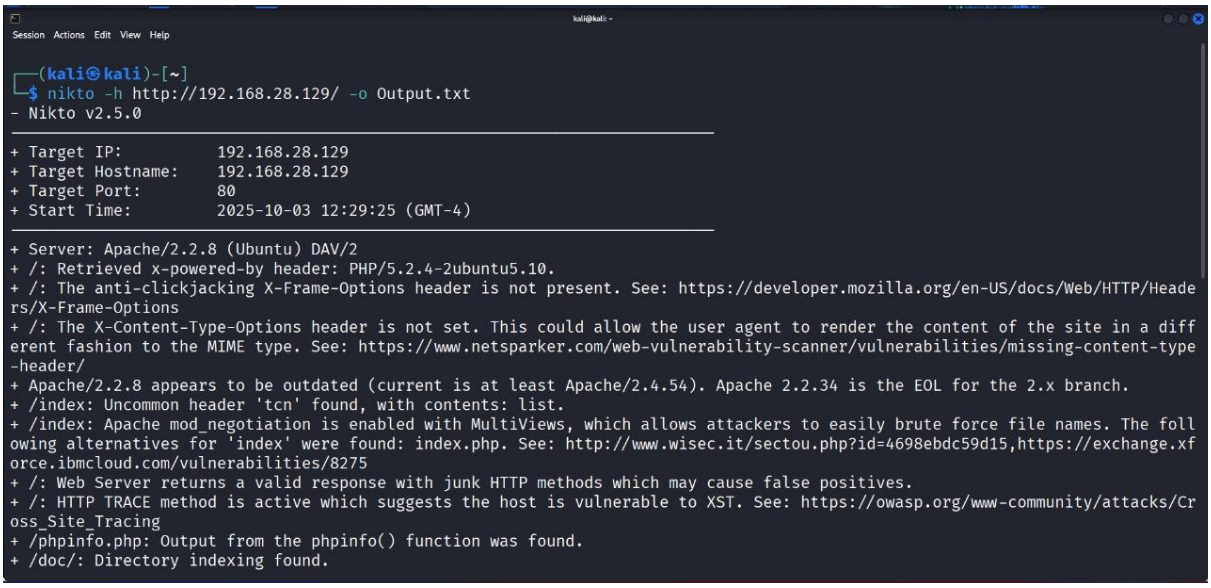
```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:47:9b:c3
          inet addr:192.168.28.129  Bcast:192.168.28.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe47:9bc3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:39 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4261 (4.1 KB)  TX bytes:6826 (6.6 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$
```

Tools Used

- ✓ **OpenVAS/Greenbone Security Assistant:** Comprehensive vulnerability scanning
- ✓ **Nikto:** Web application security scanner
- ✓ **Manual Verification:** Selective validation of critical findings

Scanning Scope

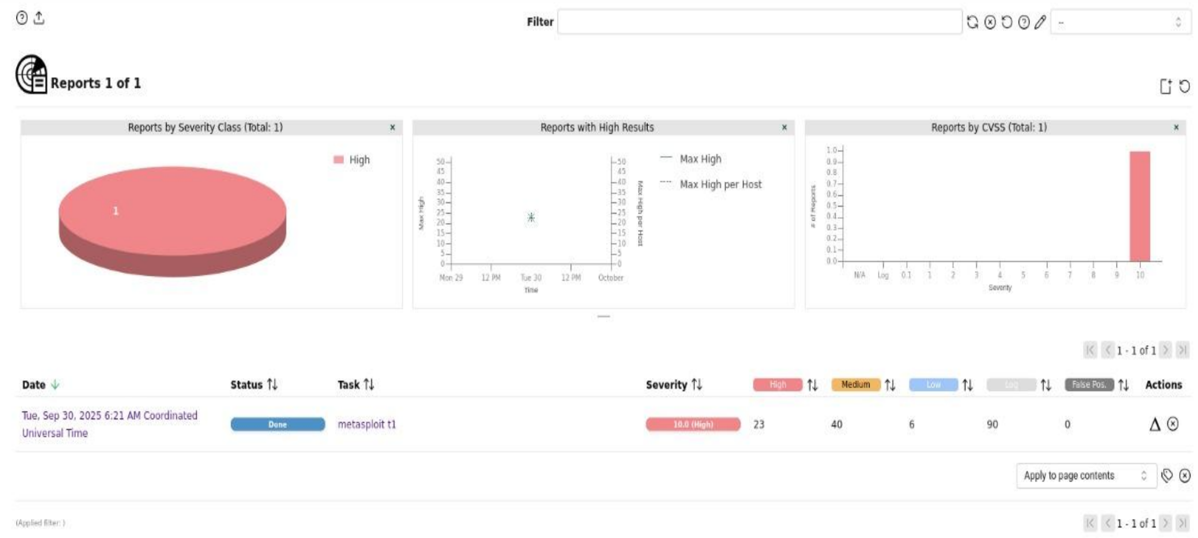
- ✓ **Network Range:** 192.168.28.129
- ✓ **Port Range:** Full TCP port scan
- ✓ **Scan Type:** Comprehensive vulnerability assessment
- ✓ **Web Applications:** Multiple web services and applications



```
┌──(kali㉿kali)-[~]
└─$ nikto -h http://192.168.28.129/ -o Output.txt
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.28.129
+ Target Hostname:    192.168.28.129
+ Target Port:        80
+ Start Time:         2025-10-03 12:29:25 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Heade
rs/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 diff
erent fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type
-header/
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The foll
owing alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xf
orce.ibmcloud.com/vulnerabilities/8275
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cr
oss_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
```

Executive Summary

The vulnerability assessment revealed **multiple critical security vulnerabilities** that pose significant risks to the target system. The most severe findings include:



Date ↓	Status ⇅	Task ⇅	Severity ⇅	High ⇅	Medium ⇅	Low ⇅	Log ⇅	False Pos. ⇅	Actions
Tue, Sep 30, 2025 6:21 AM Coordinated Universal Time	Done	metasploit t1	10.0 (High)	23	40	6	90	0	Δ ⊗

Key Findings:

- ✓ 15 Critical Vulnerabilities (CVSS 9.0-10.0)
- ✓ 12 High Severity Vulnerabilities (CVSS 7.0-8.9)
- ✓ Multiple Medium and Low severity issues
- ✓ System-wide security misconfigurations
- ✓ Outdated and end-of-life software components

Overall Risk Level: CRITICAL

The target system requires immediate remediation actions, particularly for the critical remote code execution vulnerabilities and backdoor services.

Detailed Findings

Critical Vulnerabilities (CVSS 9.0-10.0)

System-Level Critical Issues

Vulnerability	CVSS	Port	Impact	Remediation Priority
Operating System EOL	10.0	N/A	Complete system compromise	Immediate
Ingreslock Backdoor	10.0	1524	Root command execution	Immediate
rlogin Passwordless Root	10.0	513	Unauthenticated root access	Immediate
Distributed Ruby RCE	10.0	8787	Arbitrary command execution	Immediate

Service-Specific Critical Issues

Service	CVSS	Port	CVE	Description
vsftpd	9.8	21, 6200	CVE-2011-2523	Backdoor installation
MySQL	9.8	3306	Multiple	Default empty root password
PHP CGI	9.8	80	CVE-2012-1823	Remote code execution
Apache Tomcat	9.8	8009	CVE-2020-1938	Ghostcat file read/RCE

High Severity Vulnerabilities (CVSS 7.0-8.9)

Web Application Vulnerabilities:

✓ Apache Tomcat Ghostcat (Port 8009)

- CVSS: 9.8
- CVE: CVE-2020-1938
- Impact: File read and potential RCE via AJP connector

✓ TWiki XSS and Command Execution (Port 80)

- CVSS: 10.0
- CVE: CVE-2008-5304, CVE-2008-5305

Service Vulnerabilities:

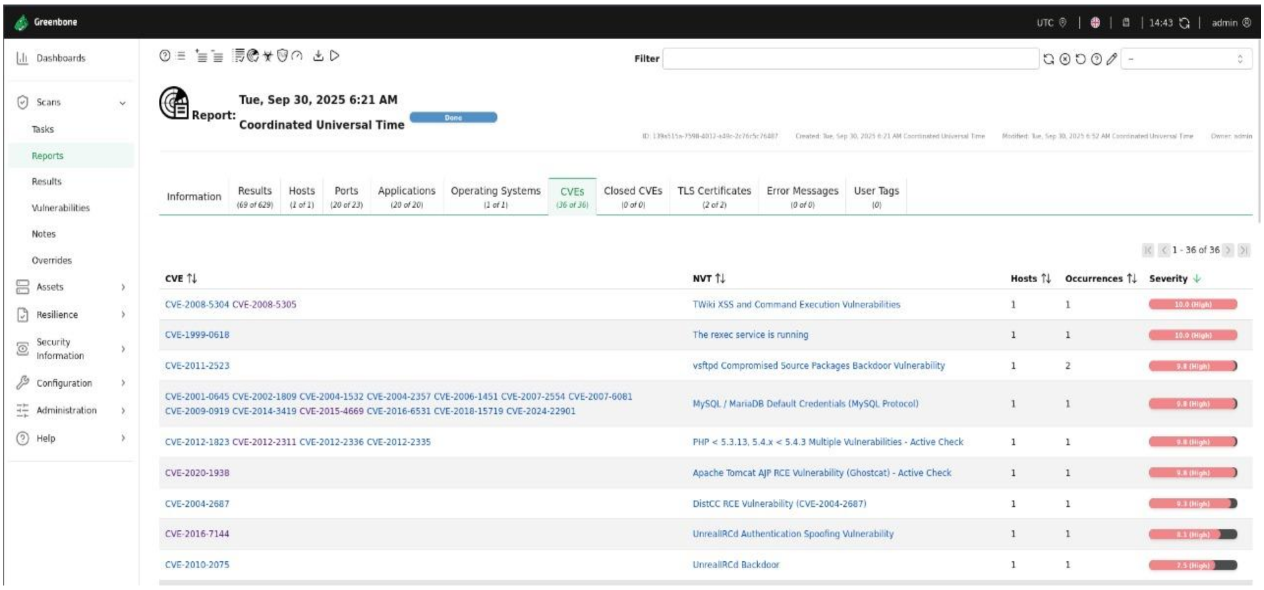
✓ UnrealIRCd Backdoor (Port 6697)

- CVSS: 7.5
- CVE: CVE-2010-2075

✓ Java RMI Insecure Configuration (Port 1099)

- CVSS: 7.5
- CVE: CVE-2011-3556

Screenshots:



Report: Tue, Sep 30, 2025 6:21 AM Coordinated Universal Time Done

ID: 139a515a-7598-4012-a49c-2c76c5c76487 Created: Tue, Sep 30, 2025 6:21 AM Coordinated Universal Time Modified: Tue, Sep 30, 2025 6:52 AM Coordinated Universal Time Owner: admin

CVE ↑↓	NVT ↑↓	Hosts ↑↓	Occurrences ↑↓	Severity ↓
CVE-2008-5304 CVE-2008-5305	TWiki XSS and Command Execution Vulnerabilities	1	1	10.0 (High)
CVE-1999-0618	The rexec service is running	1	1	10.0 (High)
CVE-2011-2523	vsftpd Compromised Source Packages Backdoor Vulnerability	1	2	9.8 (High)
CVE-2001-0645 CVE-2002-1809 CVE-2004-1532 CVE-2004-2357 CVE-2006-1451 CVE-2007-2554 CVE-2007-6081 CVE-2009-0919 CVE-2014-3419 CVE-2015-4669 CVE-2016-6531 CVE-2018-15719 CVE-2024-22901	MySQL / MariaDB Default Credentials (MySQL Protocol)	1	1	9.8 (High)
CVE-2012-1823 CVE-2012-2311 CVE-2012-2336 CVE-2012-2335	PHP < 5.3.13, 5.4.x < 5.4.3 Multiple Vulnerabilities - Active Check	1	1	9.8 (High)
CVE-2020-1938	Apache Tomcat AJP RCE Vulnerability (Ghostcat) - Active Check	1	1	9.8 (High)
CVE-2004-2687	DistCC RCE Vulnerability (CVE-2004-2687)	1	1	9.3 (High)
CVE-2016-7144	UnrealIRCd Authentication Spoofing Vulnerability	1	1	8.1 (High)
CVE-2010-2075	UnrealIRCd Backdoor	1	1	7.5 (High)

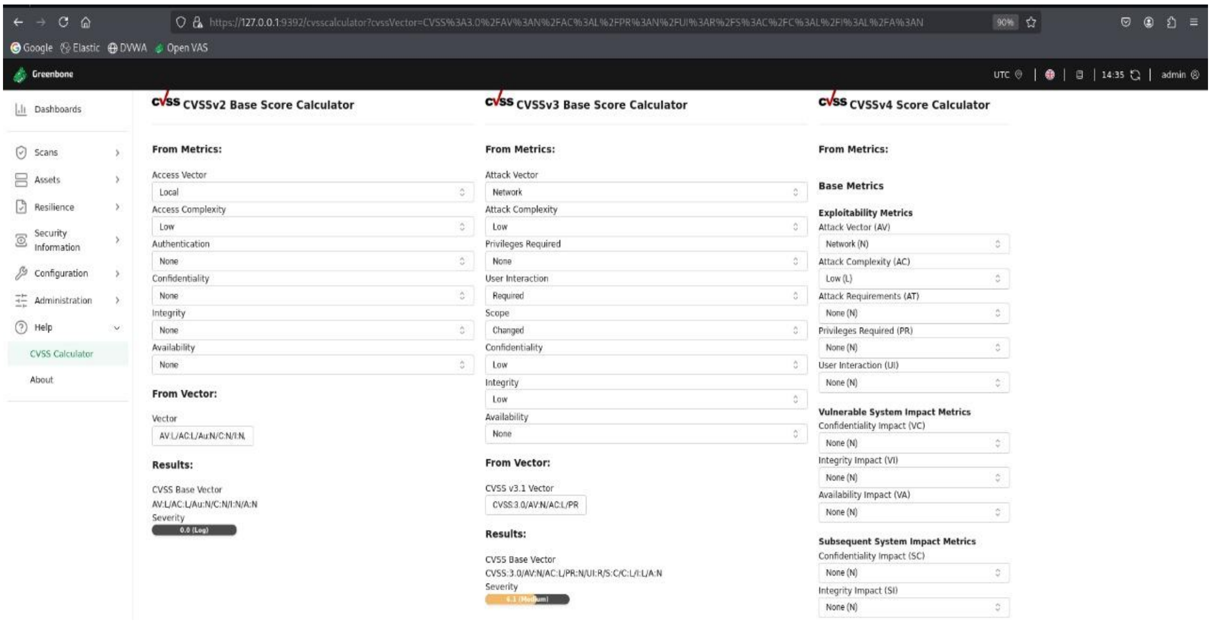
Web Application Vulnerabilities

- ✓ TWiki XSS & Command Injection (CVSS: 10.0)
- ✓ UnrealIRCd Backdoor (CVSS: 7.5, CVE-2010-2075)
- ✓ Java RMI Insecure Configuration (CVSS: 7.5, CVE-2011-3556)

Risk Prioritization Matrix

	Low Impact	Medium Impact	High Impact
High Likelihood		**FTP Weak Creds** **SSL Issues**	**CRITICAL** **• Backdoors** **• RCE Vulns** **• Auth Bypasses**
Medium Likelihood	**Info Disclosure**	**Web App XSS** **CSRF Vulns**	**Service Misconfigs** **Database Issues**
Low Likelihood	**TCP Timestamps**	**SSL Renegotiation**	**Crypto Weakness**

Screenshots:



https://127.0.0.1:9392/cvsscalculator?cvssVector=CVSS%3A3.0%2FAV%3AN%2FAC%3AL%2FPR%3AN%2FUI%3AR%2FS%3AC%2FC%3AL%2FI%3AL%2FA%3AN

CVSSv2 Base Score Calculator

From Metrics:

Access Vector: Local
Access Complexity: Low
Authentication: None
Confidentiality: None
Integrity: None
Availability: None

From Vector:

Vector: AV:L/AC:L/Au:N/C:N/I:N,

Results:

CVSS Base Vector
AV:L/AC:L/Au:N/C:N/I:N/A:N
Severity
0.0 (Log)

CVSSv3 Base Score Calculator

From Metrics:

Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required
Scope: Changed
Confidentiality: Low
Integrity: Low
Availability: None

From Vector:

CVSS v3.1 Vector: CVSS:3.0/AV:N/AC:L/PR

Results:

CVSS Base Vector
CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Severity
6.1 (Medium)

CVSSv4 Score Calculator

From Metrics:

Base Metrics

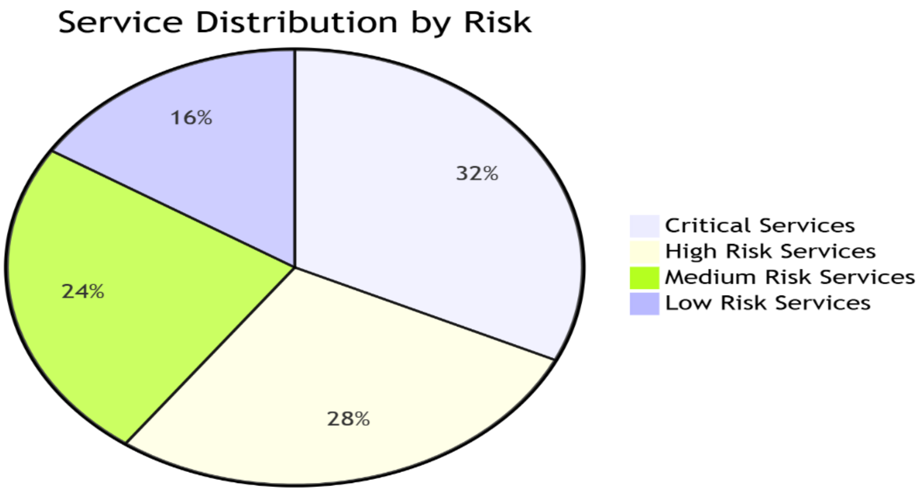
Exploitability Metrics
Attack Vector (AV): Network (N)
Attack Complexity (AC): Low (L)
Attack Requirements (AT): None (N)
Privileges Required (PR): None (N)
User Interaction (UI): None (N)

Vulnerable System Impact Metrics
Confidentiality Impact (VC): None (N)
Integrity Impact (VI): None (N)
Availability Impact (VA): None (N)

Subsequent System Impact Metrics
Confidentiality Impact (SC): None (N)
Integrity Impact (SI): None (N)

TECHNICAL ANALYSIS

Attack Surface Mapping:



Most Exploitable Services

- ✓ **vsftpd backdoor** - Immediate system compromise
- ✓ **Ingreslock backdoor** - Root access available
- ✓ **PHP CGI RCE** - Web-level system compromise
- ✓ **DistCC RCE** - Developer tool exploitation
- ✓ **Default credentials** - Multiple services affected

Attack Surface Analysis

- ✓ **Network Services:** 25+ services exposed
- ✓ **Web Applications:** 5+ vulnerable web apps
- ✓ **Authentication:** Widespread weak/default credentials
- ✓ **Encryption:** Outdated SSL/TLS configurations

Remediation Recommendations

Immediate Actions (Critical)

- ✓ **Isolate System** from production networks
- ✓ **Reinstall Operating System** with current supported version

✓ **Remove Backdoor Services:**

- Reinstall vsftpd from trusted sources
- Remove Ingreslock service
- Recompile DistCC with security patches

Service Hardening

✓ **Disable Unnecessary Services:**

rlogin, rsh, rexec, telnet

✓ **Implement Strong Authentication:**

- Change all default credentials
- Implement SSH key-based authentication
- Disable password-based VNC access

✓ **Web Application Security:**

- Update PHP to supported version
- Patch or remove vulnerable web applications
- Implement Web Application Firewall

Network Security

✓ **Firewall Configuration:**

- Restrict services to required networks only
- Implement default deny policies
- Monitor for suspicious connections

✓ **SSL/TLS Hardening:**

- Disable SSLv2/SSLv3
- Implement TLS 1.2+
- Remove weak cipher suites

Conclusion

The Metasploitable2 system exhibits numerous critical security vulnerabilities that would allow complete system compromise in a production environment. The presence of multiple backdoors, remote code execution vulnerabilities, and widespread authentication weaknesses make this system highly vulnerable to attack.

Key Security Lessons:

- Regular system updates and patch management are critical
- Default credentials pose significant security risks
- Unnecessary services expand the attack surface
- End-of-life systems cannot be secured effectively

References

✓ Kali Linux: https://www.kali.org/

✓ OpenVAS: https://www.openvas.org/

✓ Nikto: https://github.com/sullo/nikto

✓ Metasploitable2: https://docs.rapid7.com/metasploit/metasploitable-2/

✓ NVD CVSS Calculator: https://nvd.nist.gov/vuln-metrics/cvss

✓ CVE Databases: https://cve.mitre.org/