PENETRATION TEST REPORT

Scope:
The assessment includes the internal Metasploitable 2 lab VM and the external website PL Kutak (plkutak.com) as part of the web testing scope.
The Metasploitable 2 VM was fully tested in an isolated lab environment, while PL Kutak was not actively exploited, as only preliminary reconnaissance and scope identification were performed.

PLKUTAK.COM SCAN REPORT

1. Scope

Target: plkutak.com
Assessment Type: Non-intrusive vulnerability assessment
Method: Nmap scanning & configuration analysis

2. Findings

Finding 1 – **Open SSH Port (22)**
Severity: **Medium**
Description: SSH service is publicly accessible.
Risk: Possible brute-force attacks if password authentication is enabled.
Recommendation: Use key-based authentication and restrict SSH via firewall.

Finding 2 – **Missing Security Headers**
Severity: **Low**
Description: Security headers such as HSTS and CSP are not implemented.
Risk: Increased exposure to clickjacking and content injection.
Recommendation: Implement recommended HTTP security headers.

Finding 3 – **TLS Configuration**
Severity: **Informational**
Description: TLS 1.2 and TLS 1.3 enabled with strong ciphers.

Risk: Low
Recommendation: Maintain current configuration.

3. Vulnerability Script Scan Results

Nmap vulnerability scripts were executed against exposed services (SSH, HTTP, HTTPS).
No publicly known vulnerabilities were detected during the automated assessment. This indicates that the server software appears to be up to date and not affected by commonly exploitable CVEs detectable via standard NSE scripts.

INTERNAL VULNERABILITY ASSESSMENT REPORT

Target: Windows 10 Host (Internal Network Lab)
Testing Machine: Kali Linux
Testing Type: Internal Network Assessment
Date: 21.02.2026
Tester: Hasan Duraković

1. Executive Summary

An internal vulnerability assessment was conducted against a Windows 10 host within an isolated lab environment. The objective of the test was to identify exposed services and evaluate potential security misconfigurations.

The assessment identified the SMB service (port 445) exposed internally. However, no legacy or critical vulnerabilities were detected. The system appears to be properly configured with modern SMB protocols enabled and insecure legacy protocols disabled.

Overall Risk Rating: **Low**

2. Scope of Testing

Target: Single Windows 10 machine
Network Type: Internal (Hyper-V virtual network)
IP Address: 192.168.100.10
Testing Methodology: Non-intrusive enumeration and service analysis

No exploitation attempts or brute-force attacks were performed.

3. Methodology

The following tools were used during the assessment:

Nmap (service discovery and SMB enumeration)
SMB script scanning (smb-os-discovery, smb-security-mode, smb-protocols)

Commands executed:

nmap -sS -sV <target-ip>
nmap --script smb-os-discovery -p 445 <target-ip>

nmap --script smb-security-mode -p 445 <target-ip>
nmap --script smb-protocols -p 445 <target-ip>

4. Findings

Finding 1: SMB Service Exposure (Port 445)

Severity: Low

Description

The target system exposes the SMB (Server Message Block) service on TCP port 445 within the internal network.

Open Ports Identified:

135/tcp – MSRPC
139/tcp – NetBIOS
445/tcp – SMB (Microsoft-DS)

SMB dialects detected:

2.0.2
2.1.0
3.0.0
3.0.2
3.1.1

SMBv1 was not detected.

Risk Analysis

Although SMB is commonly required for file sharing and system operations in Windows environments, exposing SMB internally may increase the attack surface.

If additional weaknesses such as:

Weak credentials
Disabled SMB signing
Poor network segmentation

exist within a real enterprise environment, attackers could leverage SMB for lateral movement.

However, in this case:

No legacy SMBv1 protocol detected
Modern SMB dialects in use
No critical vulnerabilities identified

Risk level is considered LOW in this lab environment.

Recommendation

Ensure SMB signing is enforced
Restrict SMB access using firewall rules
Disable SMB where not required
Apply strong password policies
Maintain regular system patching

5. Conclusion

The Windows 10 host was found to expose standard Windows services internally. No critical vulnerabilities or insecure legacy protocols were identified during testing.

The system appears to follow modern security configurations.

Further testing involving authentication testing and credential auditing would be required to fully evaluate internal attack surface.

6. Final Risk Rating

LOW RISK

PENETRATION TEST REPORT

Internal Network Security Assessment – Metasploitable 2

1. Executive Summary

An internal penetration test was conducted against a vulnerable lab environment (Metasploitable 2). The objective was to identify security weaknesses that could allow unauthorized access, privilege escalation, and lateral movement.

The system was fully compromised through exposed services, weak credential storage, and insecure configurations.

Overall Risk Rating: CRITICAL

2. Scope

Target System:

Metasploitable 2 (Linux-based vulnerable VM)
Internal IP: 192.168.100.11

Testing Environment:

Kali Linux (attacker machine)

Testing Type:

Internal network penetration test

3. Methodology

The assessment followed industry-standard penetration testing methodology aligned with:

OWASP Testing Guide
PTES (Penetration Testing Execution Standard)
Offensive Security penetration testing practices

Testing phases included:

1. Reconnaissance
2. Service Enumeration

3. Exploitation
4. Post-Exploitation
5. Credential Dumping
6. Password Cracking
7. Lateral Movement

4. Findings

4.1 Remote Code Execution via Backdoor Service

Severity: Critical
Port: 6200
Service: Unauthenticated shell access

An open service running on TCP port 6200 provided direct shell access without authentication.

Exploit method:

nc 192.168.100.11 6200

Result:

Immediate interactive shell access to the target system.

Impact:

Full remote command execution
Complete system compromise
Ability to access sensitive files

4.2 Credential Dumping

Severity: High

After obtaining shell access, sensitive credential data was extracted from system files.

Example:
cat /etc/shadow

Password hashes for multiple users were obtained.

Impact:
Exposure of all local user password hashes
Enables offline password cracking attacks

4.3 Password Cracking

Severity: High

Extracted hashes were cracked using an offline password cracking tool.

The hash format identified:

md5crypt

Multiple user passwords were successfully recovered.

Impact:

Compromise of legitimate user accounts
Ability to authenticate via SSH
Increased attack surface

4.4 Lateral Movement via SSH

Severity: High

Using cracked credentials, SSH access was attempted:

ssh msfadmin@192.168.100.11

Initial SSH negotiation errors related to deprecated algorithms were resolved by adjusting client-side SSH options.

Result:

Successful authenticated SSH session.

Impact:

Legitimate user-level access
Ability to pivot within the system
Foundation for privilege escalation

5. Risk Assessment Summary

Vulnerability	Severity	Impact
Unauthenticated Backdoor (Port 6200)	Critical	Full system compromise
Weak Password Hashing (md5crypt)	High	Credential exposure
Weak SSH Configuration	Medium	Facilitates lateral movement

Overall Risk Level: **CRITICAL**

6. Technical Impact

An attacker on the internal network can:

Gain remote shell access without credentials
Extract password hashes
Crack weak passwords offline
Log in via SSH as legitimate users
Fully compromise the system

The attack requires minimal sophistication and no zero-day vulnerabilities.

7. Recommendations

1. Remove and disable unauthorized or backdoor services (close port 6200).
2. Upgrade password hashing algorithms to modern standards (bcrypt, Argon2).
3. Enforce strong password policies.
4. Restrict SSH to key-based authentication only.
5. Disable deprecated SSH algorithms.
6. Implement network segmentation and firewall rules.
7. Apply regular patching and system hardening.

8. Conclusion

The Metasploitable 2 system was fully compromised through:

- Exposed unauthenticated services
- Weak credential storage mechanisms
- Insecure service configurations

The findings demonstrate the critical importance of secure configuration management, strong authentication mechanisms, and service exposure control.

The system in its current state should not be deployed in any production environment.