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