Final VAPT Report

PREPARED BY: Esperanza Buitrago Díaz

Submitted To: Neuefische

Submission Date: February 2026

TABLE OF CONTENTS

EXECUTIVE SUMMARY

A comprehensive security assessment of the internal corporate network of TechShield was performed on January 20th and on. This penetration test simulated an attack from an external threat actor attempting to gain access to systems within the corporate's network.

The purpose of this assessment was to discover and identify vulnerabilities in the corporate's infrastructure and suggest methods to remediate the vulnerabilities that were found.

The assessment team identify a total of 6 vulnerabilities within the scope of engagement, which are broken down by severity in the following table:

CRITICAL	HIGH	MEDIUM	LOW
3	**2**	**1**	**0**

The hives severity vulnerabilities give potential attackers the opportunity to execute arbitrary code remotely, gain complete system control, steal sensitive credentials and maintain persistent access to critical systems. Specifically, the discovery of EternalBlue (MS17-010) vulnerability allows attackers to compromise Windows systems without user interaction, potentially leading to ransomware deployment, data exfiltration, and lateral movements throughout the network.

Additionally, unauthenticated access to SMB services and HTTP-based DoS vulnerabbilities expose the infrastructure to both data theft and service disruption attacks.

In order to ensure data confidentiality, integrity, and availability, security remediation should be implemented as described in the security assessment findings. Immediate attention should be given to patching critical vulnerabilities, particularly those affecting SMB services.

1. INTRODUCTION

TechShield, a managed IT services company requested a comprehensive vulnerability assessment and penetration test of their network infrastructure following security incidents affecting several clients. This assessment aimed to identify security weaknesses, validate exploitability of discovered vulnerabilities, and provide actionable remediation guidance to strengthen TechShield's security posture.

2. ASSESSMENT SCOPE AND OBJECTIVES

2.1 Scope

- **Target Systems:** Internal network infrastructure
- **IP Ranges:** 192.168.57.0/24
- **Primary Target:** Windows Server 2008 R2 / Windows 7 System (192.168.57.20)
- **Assessment Type:** Black-box and Gray-box testing
- **Included:** Network scanning, vulnerability exploitation, digital forensics analysis

2.2 Objectives

1. Identify and classify vulnerabilities in network infrastructure
2. Demonstrate exploitability of critical vulnerabilities
3. Conduct digital forensics analysis on compromised system image
4. Provide prioritized remediation recommendations
5. Enhance incident response capabilities

3. METHODOLOGY

3.1 Reconnaissance Phase

- Network discovery using Nmap
- Service enumeration and version detection
- Operating system fingerprinting

3.2 Vulnerability Assessment

- Automated scanning with Nmap vulnerability scripts
- Manual verification of discovered vulnerabilities
- Credentialed scanning (simulated)

3.3 Exploitation Phase

- Controlled exploitation of MS17-010 (EternalBlue)
- Post-exploitation evidence collection
- Privilege escalation demonstrations

3.4 Digital Forensics

- Analysis of compromised system image
- Timeline reconstruction of attack artifacts
- Evidence preservation and documentation

3.5 Tools Used

- Nmap 7.93
- Metasploit Framework 6.3
- TCPDump for network forensics
- Manual testing and validation

4. SUMMARY OF FINDINGS

4.1 Risk Distribution

4.2 Key Statistics

- **Systems Assessed:** 5 active hosts
- **Open Ports Identified:** 7 critical services
- **Vulnerabilities Found:** 6 (3 Critical, 2 High, 1 Medium)
- **Successful Exploitations:** 1 (MS17-010)
- **Credentials Compromised:** Administrator hashes extracted

4.3 Overall Risk Rating: CRITICAL

The assessment revealed that TechShield's network infrastructure contains multiple critical vulnerabilities that could lead to complete organizational compromise. The most severe finding (MS17-010) allows remote attackers to execute arbitrary code without authentication, potentially resulting in ransomware deployment, data theft, and service disruption.

5. High level assessment overview

During the assessment, several positive security controls were observed within TechShield's network infrastructure:

1. **Network Segmentation Presence:** Multiple distinct IP ranges (192.168.57.0/24) with limited host exposure
2. **Service Hardening:** Some services showed proper access controls (NT_STATUS_ACCESS_DENIED on unauthorized SMB enumeration attempts)
3. **Limited Attack Surface:** Only essential services were exposed (7 open ports out of 65535)
4. **MAC Address Filtering:** VMware environment with controlled virtual infrastructure
5. **Workgroup Isolation:** Systems operating in WORKGROUP domain, limiting domain-wide compromise spread

Areas for Improvement

TechShield Security Assessment Team recommends TechShield takes the following actions to improve the security of the network. Implementing these recommendations will reduce the likelihood that an attacker will be able to successfully attack TechShield's information systems and/or reduce the impact of a successful attack.

Short Term Recommendations (0-30 Days)

TechShield Security Assessment Team recommends TechShield take the following actions as soon as possible to minimize business risk.

Critical Patching Priority

- **Immediate MS17-010 Remediation:** Apply Microsoft security update MS17-010 to all Windows systems
- **SMBv1 Disablement:** Disable SMBv1 protocol enterprise-wide within 24 hours
- **Emergency Isolation:** Immediately isolate vulnerable Windows 7 system (192.168.57.20) from production networks

Network Security Enhancement

- **Port Restriction:** Block unnecessary ports (135, 139, 445, 554, 2869, 5357, 10243) at network perimeter
- **Firewall Rule Review:** Implement strict ingress/egress filtering for SMB traffic
- **IDS/IPS Deployment:** Deploy intrusion detection/prevention systems to monitor for EternalBlue exploitation attempts

Long Term Recommendations (1-6 Months)

TechShield Security Assessment Team recommends the following actions be taken over the next 6 months to fix hard-to-remediate issues that do not pose an urgent risk to the business.

System Modernization

- **Operating System Upgrades:** Migrate all Windows 7/Server 2008 R2 systems to supported versions
- **Application Whitelisting:** Implement application control policies on critical systems
- **Patch Management Automation:** Establish automated vulnerability remediation processes

Security Program Development

- **Regular Assessments:** Conduct quarterly penetration tests and vulnerability assessments
- **Incident Response Planning:** Develop and test comprehensive incident response procedures
- **Security Awareness Training:** Implement ongoing security training for all technical staff

SCOPE

Project Scope

All testing was based on the scope as defined in the initial assessment requirements. The items in scope are listed below.

Network Infrastructure Assessment

- Internal Corporate Network Systems
- Windows Server Infrastructure
- SMB Services and File Sharing
- HTTP/HTTPS Services

Digital Forensics Analysis

- Compromised System Image Analysis
- Attack Timeline Reconstruction
- Evidence Preservation Procedures

Network Information

Network	Note	Host Discovered
192.168.57.0/24	TechShield Internal Lab Network	6 Active hosts

Target Systems	IP Address	Purpose
Primary assessment target	192.168.57.20	Windows 7 pro (Win7-64)
Attacker system	192.168.57.10	Kali Linux penetration testing platform
Additional Hosts	192.168.57.30 192.168.57.40 192.168.57.250	Unassesed System

	192.168.57.254	

TESTING METHODOLOGY

TechShield Security Assessment Team's testing methodology was split into three phases: Reconnaissance, Target Assessment, and Execution of Vulnerabilities. During reconnaissance, we gathered information about TechShield's network systems. **TechShield Security Assessment Team** used port scanning and other enumeration methods to refine target information and assess target values. Next, we conducted our targeted assessment. **TechShield Security Assessment Team** simulated an attacker exploiting vulnerabilities in the TechShield network. **TechShield Security Assessment Team** gathered evidence of vulnerabilities during this phase of the engagement while conducting the simulation in a manner that would not disrupt normal business operations.

Methodology Phases:

1. **Reconnaissance Phase:**
   - Network discovery using Netdiscover and Nmap
   - Host enumeration and service identification (6 active hosts identified in 192.168.57.0/24)
   - Operating system fingerprinting (Windows 7 professional 7600 confirmed)
2. **Vulnerability Assessment Phase:**
   - Automated scanning: Greenbone security assistant (OpenVAS) credentialed assessment.
   - Script-base scanning: Nmap vulnerability scripts (smb-vuln*, http-*).
   - Manual verification: Individual vulnerability validation.
   - Credential scan configuration: Windows administrative credentials configured in Greenbone.
3. **Exploitation Phase:**
   - Controlled exploitation of MS17-010 (EternalBlue) via Metasploit.
   - Post-exploitation evidence collection.
   - Privilege escalation demonstration.
4. **Forensic Analysis Phase:**

- Network traffic capture and analysis.
- System compromise timeline reconstruction.
- Evidence documentation and preservation.

5. **Tools Used**
    - Greenbone security assistant 22.4: comprehensive vulnerability management.
    - Nmap 76.93: Network discovery and vulnerability scanning.
    - Metasploit framework: Exploitation and post-exploitation.
    - Netdiscover: ARP-based network discovery.
    - TCPDump: Network traffic capture.

CLASSIFICATION DEFINITIONS

Risk Classifications

Level	Score	Description
Critical	10	The vulnerability poses an immediate threat to the organization. Successful exploitation may permanently affect the organization. Remediation should be immediately performed.
High	7-9	The vulnerability poses an urgent threat to the organization, and remediation should be prioritized.
Medium	4-6	Successful exploitation is possible and may result in notable disruption of business functionality. This vulnerability should be remediated when feasible.
Low	1-3	The vulnerability poses a negligible/minimal threat to the organization. The presence of this vulnerability should be noted and remediated if possible.
Informational	0	These findings have no clear threat to the organization, but may cause business processes to function differently than desired or reveal sensitive information about the company.

Exploitation Likelihood Classifications

Likelihood	Description

Likely	Exploitation methods are well-known and can be performed using publicly available tools. Low-skilled attackers and automated tools could successfully exploit the vulnerability with minimal difficulty.
Possible	Exploitation methods are well-known, may be performed using public tools, but require configuration. Understanding of the underlying system is required for successful exploitation.
Unlikely	Exploitation requires deep understanding of the underlying systems or advanced technical skills. Precise conditions may be required for successful exploitation.

Business Impact Classifications

Impact	Description
Major	Successful exploitation may result in large disruptions of critical business functions across the organization and significant financial damage.
Moderate	Successful exploitation may cause significant disruptions to non-critical business functions.
Minor	Successful exploitation may affect few users, without causing much disruption to routine business functions.

Remediation Difficulty Classifications

Difficulty	Description
Hard	Remediation may require extensive reconfiguration of underlying systems that is time consuming. Remediation may require disruption of normal business functions.
Moderate	Remediation may require minor reconfigurations or additions that may be time-intensive or expensive.
Easy	Remediation can be accomplished in a short amount of time, with

	little difficulty.

ASSESSMENT FINDINGS

#	Finding	Risk Score	Risk	Exploitation Likelihood	Detection source
1	MS17-010 EternalBlue SMB Remote Code Execution	**10**	**Critical**	**Likely**	**Nmap, greenbone, manual exploitation**
2	Unpatched Windows 7 Operating System (EOL)	**9**	**High**	**Likely**	**Nmap, greenbone**
3	Slowloris HTTP Denial of Service Vulnerability	**8**	**High**	**Likely**	**Nmap OS detection, greenbone**
4	Unrestricted NetBIOS/SMB Service Exposure	**7**	**High**	**Possible**	**Nmap greenbone**
5	Microsoft RPC Service Exposure	**6**	**Medium**	**Possible**	**Nmap**
6	Legacy RTSP Service Exposure	**5**	**Medium**	**Unlikely**	**Nmap**
7	HTTPAPI Services with Default Configurations	**4**	**Medium**	**Possible**	**Nmap, greenbone**

6. DETAILED VULNERABILITY FINDINGS

Finding 1: MS17-010 EternalBlue SMB Remote Code Execution

- **Risk Score:** 10/10 (Critical)
- **Affected System:** 192.168.57.20 (WIN7-64)
- **CVE:** CVE-2017-0143
- **Port/Service:** 445/tcp (SMB)

Evidence:

```
Host script results:
smb-vuln-ms17-010:
  VULNERABLE:
  Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
  State: VULNERABLE
  IDs: CVE:CVE-2017-0143
  Risk factor: HIGH
```

Successful Exploitation:

```
[*] 192.168.57.20:445 - Target is vulnerable to MS17-010!
[*] 192.168.57.20:445 - Exploiting target...
[*] Meterpreter session 1 opened (192.168.57.10:4444 -> 192.168.57.20:49247)
```

Impact: Complete system compromise with SYSTEM privileges, credential theft capability, lateral movement potential, ransomware deployment risk.

Recommendation: Apply MS17-010 patch immediately. Disable SMBv1 protocol. Isolate affected systems.

Finding 2: Unpatched Windows 7 Operating System (End of Life)

- **Risk Score:** 9/10 (High)
- **Affected System:** 192.168.57.20
- **OS Details:** Windows 7 Professional 7600

Evidence:

```
OS: Windows 7 Professional 7600 (Windows 7 Professional 6.1)
Computer name: win7-64
Workgroup: WORKGROUP
```

Impact: No security updates available, exposure to multiple unpatched vulnerabilities, compliance violations.

Recommendation: Upgrade to supported Windows version or implement strict application control.

Finding 3: Slowloris HTTP Denial of Service Vulnerability

- **Risk Score:** 8/10 (High)
- **Affected System:** 192.168.57.20
- **CVE:** CVE-2007-6750
- **Ports:** 2869/tcp, 5357/tcp, 10243/tcp

Evidence:

```
http-slowloris-check:
  VULNERABLE:
  Slowloris DOS attack
  State: LIKELY VULNERABLE
```

Impact: Service disruption, potential downtime for client-facing services.

Recommendation: Apply HTTPAPI updates, implement connection limiting, deploy DoS protection.

Finding 4: Unrestricted NetBIOS/SMB Service Exposure

- **Risk Score:** 7/10 (High)
- **Affected System:** 192.168.57.20
- **Ports:** 139/tcp, 445/tcp

Evidence:

```
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
```

Impact: Network reconnaissance, brute-force attacks, credential harvesting.

Recommendation: Restrict SMB access, implement strong authentication, disable NetBIOS where possible.

Finding 5: Microsoft RPC Service Exposure

- **Risk Score:** 6/10 (Medium)
- **Affected System:** 192.168.57.20
- **Port:** 135/tcp

Evidence:

```
135/tcp open  msrpc    Microsoft Windows RPC
```

Impact: Service enumeration, potential RPC-based exploits, DoS attack vector.

Recommendation: Restrict RPC access through firewall, apply security updates.

Finding 6: Legacy RTSP Service Exposure

- **Risk Score:** 5/10 (Medium)
- **Affected System:** 192.168.57.20
- **Port:** 554/tcp

Evidence:

```
554/tcp open  rtsps
```

Impact: Service information disclosure, potential buffer overflow attacks.

Recommendation: Disable RTSP if not required, restrict access to authorized clients.

Finding 7: HTTPAPI Services with Default Configurations

- **Risk Score:** 4/10 (Medium)
- **Affected System:** 192.168.57.20
- **Ports:** 2869/tcp, 5357/tcp, 10243/tcp

Evidence:

```
2869/tcp  open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```

Impact: Information disclosure, potential service-specific vulnerabilities.

Recommendation: Harden HTTPAPI configurations, implement access controls.

DIGITAL FORENSICS SUMMARY

Evidence Collected:

1. **Network Traffic Capture:** Complete packet capture during exploitation
2. **System Compromise Evidence:** Screenshots of Meterpreter session
3. **Timeline Reconstruction:** Detailed attack timeline from initial scan to system compromise
4. **Credential Evidence:** Hash extraction results (where applicable)
5. **Artifact Documentation:** System changes and persistence mechanisms

Forensic Findings:

- **Attack Duration:** Initial scan to full compromise: < 15 minutes
- **Exploitation Method:** MS17-010 EternalBlue via Metasploit
- **Privilege Level Achieved:** NT AUTHORITY\SYSTEM
- **Data Access:** Full system access demonstrated
- **Persistence:** Capability for persistent access confirmed

APPENDIX A - TOOLS USED

TOOL	DESCRIPTION
Nmap	Network discovery and vulnerability scanning.
Metasploit Framework	Exploitation and post-exploitation.
Netdiscover	ARP-based network discovery.
TCPDump	Network traffic capture.
Python XML Parcer	Results analysis and reporting.

Table A.1: *Tools used during assessment*

APPENDIX B - Risk Calculation methodology

All risks scores were calculated using CVSS v3.1 methodology, considering:

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Changed
Confidentiality, integrity, availability impact	High