Final VAPT Report

PREPARED BY: Esperanza Buitrago Díaz

Submitted To: Neuefische

Submission Date: February 2026

TABLE OF CONTENTS

EXECUTIVE SUMMARY

A targeted security assessment focusing on credential security and password cracking was conducted on February 2nd, 2026. This assessment simulated an attacker who had already gained initial access via the EternalBlue vulnerability (MS17-010) and aimed to escalate privileges, enumerator users, and crack weak passwords via SMB brute-force attacks.

The purpose of this assessments was the evaluate the strength of password policies, demonstrate the ease of credentials compromise, and provide actionable recommendation to strengthen authentication security.

The assessment successfully compromised 2 user accounts via weak passwords, extracted password hashes from the SAM database, and demonstrated the risk of credentials reuse and weak passwords policies.

2. ASSESSMENT SCOPE AND OBJECTIVES

2.1 Scope

- **Target Application:** Windows 7 Professional (192.168.57.20)
- **IP Address:** 192.168.57.10
- **Assessment Type:** Post-exploitation credential testing
- **Included:**
    - User enumeration
    - Custom wordlist creation
    - SMB bruce-force attacks
    - Hash extractions and cracking

2.2 Objectives

1. Exploit Windows systems via EternalBlue and establish Meterpreter sessions.
2. Enumerator local users and extract credential hashes.
3. Perform SMB brute-force attacks using Hydra with custom wordlists.
4. Demonstrated successful credential compromise.
5. Recommend password policy and authentication hardening measures.

3. METHODOLOGY

3.1 Initial Exploitation

- EternalBlue exploitation via Metasploit (exploit/windows/smb/ms17_010_eternalblue)
- Meterpreter session establishment with SYSTEM privileges.

3.2 User Enumeration

- Local user enumeration via net users and Meterpreter modules.
- Hash extraction via hashdump and post/windows/gather/hasdump.

3.3 Wordlist Creation

- Custom wordlist compiled with 10 command passwords.

3.4 Bruce-force attack

- SMB brute-force using Hydra with enumerated usernames and custom wordlist.

3.5 Credential validation

- Successful authentication via smbclient and crackmapexec.

3.6 Tools used

- Metasploit Framework

- Hydra
- Hashcat (for hash cracking demonstration)
- Custom scripts for enumeration and validation

4. SUMMARY OF FINDINGS

4.1 Risk Distribution

- Critical: 1
- High: 2
- Medium: 1
- Low: 0

4.2 Key Statistics

- **Systems compromised:** 1 (Windows 7)
- **Users enumerated:** 3 (Administrator, Guest, student)
- **Passwords cracked:** 2 (Administrator, student)
- **Hashes extracted:** 4 NTLM hashes

4.3 Overall Risk Rating: CRITICAL

5. DETAILED VULNERABILITY FINDINGS

Finding 1: MS17-010 EternalBlue Exploitation (Critical)

- **Risk Score:** 10/10 (Critical)
- **Affected System:** 192.168.57.20 (Windows Professional)
- **Evidence:**
    - Successful exploitation via Metasploit

```
[*] 192.168.57.20:445 - Target is vulnerable to MS17-010!
[*] Meterpreter session 1 opened (192.168.57.10:4445 -> 192.168.57.20:49247)
```

  - SYSTEM-level access confirmed:

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

  - System information gathered:

```
Computer : WIN7-64
OS : Windows 7 (6.1 Build 7600)
```

- **Impact:** Complete system compromise, credential theft, persistent access.
- **Recommendation:** Apply MS17-010 patch immediately, disable SMBv1, isolate vulnerable systems.

Finding 2: Weak password Policy and SMB Brute-force Vulnerability (High)

- **Risk Score:** 8/10 (High)
- **Affected Service:** SMB (Port 445)

Evidence:

- Custom wordlist creation with 10 common passwords.
- User enumeration file created (smb_users_eternalblue.txt)

```
Administrator
Guest
student
```

- Hydra SMB brute-force successful:

```
[DATA] attacking smb://192.168.57.20/
[DATA] attack: 192.168.57.20 login: Administrator password: Password
[DATA] attack: 192.168.57.20 login: student password: Password
3 target successfully completed, 2 valid passwords found
```

- Credential validation smbclient.

```
smbclient -L //192.168.57.20/ -U "Administrator%Password"
```

Impact: Unauthorized access, lateral movement, privilege escalation

Recommendation: Implement strong password policy (min 12 characters, complexity, age, etc.), account lockout policies, MFA.

Finding 3: SAM Database Hash Extractions (High)

- **Risk Score:** 7/10
- **Affected Module:** Windows security account manager (SAM)

Evidence:

- Hashdump via Meterpreter

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
student:1000:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser:1002:aad3b435b51404eeaad3b435b51404ee:498ce8b42f5e4b06b16a432f0d3a473d:::
```

- Password hint extraction:

```
[*] Dumping password hints...
student:"standard"
```

Impact: Credential theft, pass-the-hash attacks, persistent access.

Recommendation: Implementation credential guard, restrict SAM access, use LAPS for local admin passwords.

Finding 4: Insecure default and common passwords (Medium)

- **Risk Score:** 6/10
- **Affected Module:**Administrator, student.

Evidence:

- Both accounts used password: P@ssw0rd.

Impact: Easy credential guessing, automated attacks successful.

Recommendation: Enforce password complexity, regular passwords rotations, user security training.

ASSESSMENT FINDINGS

#	Finding	Risk Score	Risk	Exploitation Likelihood	Business impact	Remediation difficulty
1	MS17-010 EternalBlue Exploitation	**10**	**Critical**	**Likely**	**Major**	**Easy**
2	Weak Password Policy & SMB Brute-Force	**8**	**High**	**Likely**	**Major**	**Moderate**
3	SAM Database Hash Extraction	**7**	**High**	**Possible**	**Major**	**Hard**
4	Insecure Default & Common Passwords	**6**	**Medium**	**Likely**	**Moderate**	**Easy**

6. FORENSIC EVIDENCE SUMMARY

- Eternal exploitation: Meterpreter session screenshots and command outputs.
- User enumeration: net users output showing successful compromises.
- Hash extraction: Complete SAM database dump with NTLM hashes.
- Brute-force results: Hydra output showing successful compromises.
- Credentials validation: smbclient and crackmapexec successful connections.

6. RECOMMENDATIONS

6.1 Immediate Actions (0-7 days)

1. Change compromised passwords: Immediately reset passwords for Administrator and student accounts.
2. Enable account lockout: Implement lockout after 5 failed attempts.
3. Disable SMBv1: Enterprise-wise disablements of SMBv1 protocol.
4. Isolate vulnerable system: Remote 192.168.57.20 from production network.

6.2. Short term (7-30 days)

1. Password policy enforcement:
    a. Minimum 12 characteres.
    b. Complexity requirements (upper letter, lower letter, number, special character).
2. Implement LAPS: Local Administrator Password Solution for automated password management.
3. Enable Windows defender credential guard.
4. Network segmentation: Restrict SMB traffic to necessarily hosts only.

6.3 Long term (1-6 months)

1. Multifactor Authentication (MFA): Implement for all administrative accounts.
2. Regular credential auditing: Quarterly password strength and hash audits.

3. Security awareness training: Focus on password hygiene and phishing resistance.
4. Privileges access management (PAM): Implement just-in-access controls.

Conclusion

The assessment demonstrated critical weaknesses in password security and authentication controls. The combination of an unpatched EternalBlue vulnerability and weak passwords allowed rapid system compromises and credential theft. Immediate remediation is required, with a focus on patching, password policy enforcement, and credential protection mechanisms.