

1BitofMemory

HackTheBox Findings Report:

**Legacy**

**Date: March 18th, 2020**

# Table of Contents

[Table of Contents 2](#_Toc35430336)

[Assessment Overview 3](#_Toc35430337)

[Assessment Components 3](#_Toc35430338)

[External Penetration Test 3](#_Toc35430339)

[Finding Severity Ratings 4](#_Toc35430340)

[Scope 5](#_Toc35430341)

[Scope Exclusions 5](#_Toc35430342)

[Client Allowances 5](#_Toc35430343)

[Executive Summary 6](#_Toc35430344)

[Attack Summary 6](#_Toc35430345)

[Security Strengths 6](#_Toc35430346)

[SMB Access Control 6](#_Toc35430347)

[Security Weaknesses 6](#_Toc35430348)

[Vulnerable Software 6](#_Toc35430349)

[Vulnerabilities by Impact 7](#_Toc35430350)

[External Penetration Test Findings 8](#_Toc35430351)

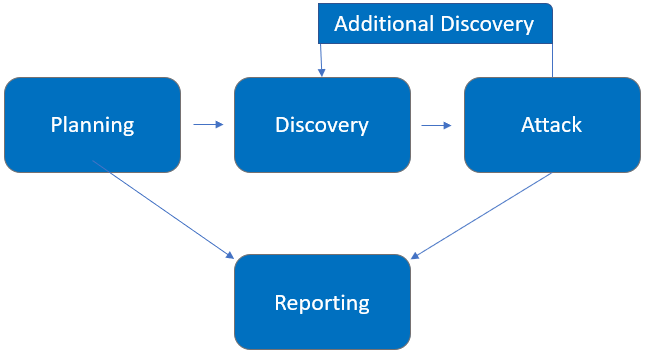
[Vulnerable Software – SMB Vulnerability (Critical) 8](#_Toc35430352)

[Additional Reports and Scans (Informational) 10](#_Toc35430353)

# Assessment Overview

Phases of penetration testing activities include the following:

* Discovery – Scanning and enumeration of given machine to gather information and identify vulnerabilities.
* Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
* Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



# Assessment Components

## External Penetration Test

An external penetration test emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge. Independent penetration tester 1BitOfMemory performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

# 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. |

# Scope

|  |  |
| --- | --- |
| Assessment | Details |
| External Penetration Test | 10.10.10.4 via VPN |

## Scope Exclusions

Per HackTheBox request, 1BitOfMemory does not perform any Denial of Service attacks during testing.

## Client Allowances

HackTheBox did not provide any allowances to assist the testing.

# Executive Summary

1BitOfMemory evaluated Legacy’s external security posture through an external network penetration test on March 18, 2020. By leveraging a series of attacks, 1BitOfMemory found critical level vulnerabilities that allowed full machine access. It is highly recommended that Legacy addresses these vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort.

## Attack Summary

The following table describes how TCMS gained internal network access, step by step:

|  |  |  |
| --- | --- | --- |
| Step | Action | Recommendation |
| 1 | Obtained full machine action by executing a publicly available exploit. | Upgrade the operating system immediately. |
|  |  |  |
|  |  |  |

# Security Strengths

**SMB Access Control**

The machine did not allow for easy access via a null session attack (unauthenticated access to data).

# Security Weaknesses

## Vulnerable Software

The software is severely out of date and allows easy exploitation leading to full system compromise.

# Vulnerabilities by Impact

The following chart illustrates the vulnerabilities found by impact:

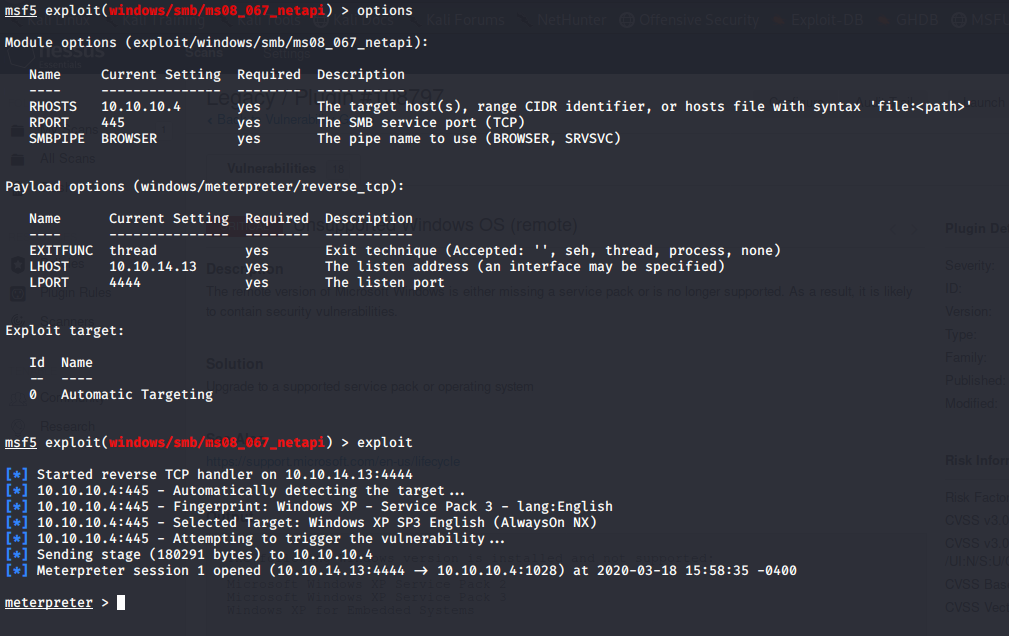
## External Penetration Test Findings

Vulnerable Software – SMB Vulnerability (Critical)

|  |  |
| --- | --- |
| Description: | The version of SMB being utilized is susceptible to exploitation. |
| Impact: | Critical |
| System: | 10.10.10.4 |
| References: | MS08-067 |

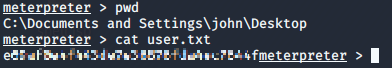
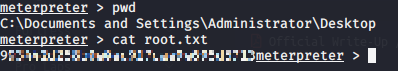
**Exploitation Proof of Concept**

1BitOfMemory was able to gain full system access through the SMB vulnerability.



*Figure 1: Exploitation via MS08-067*

1BitOfMemory was able to access critical data after exploitation.

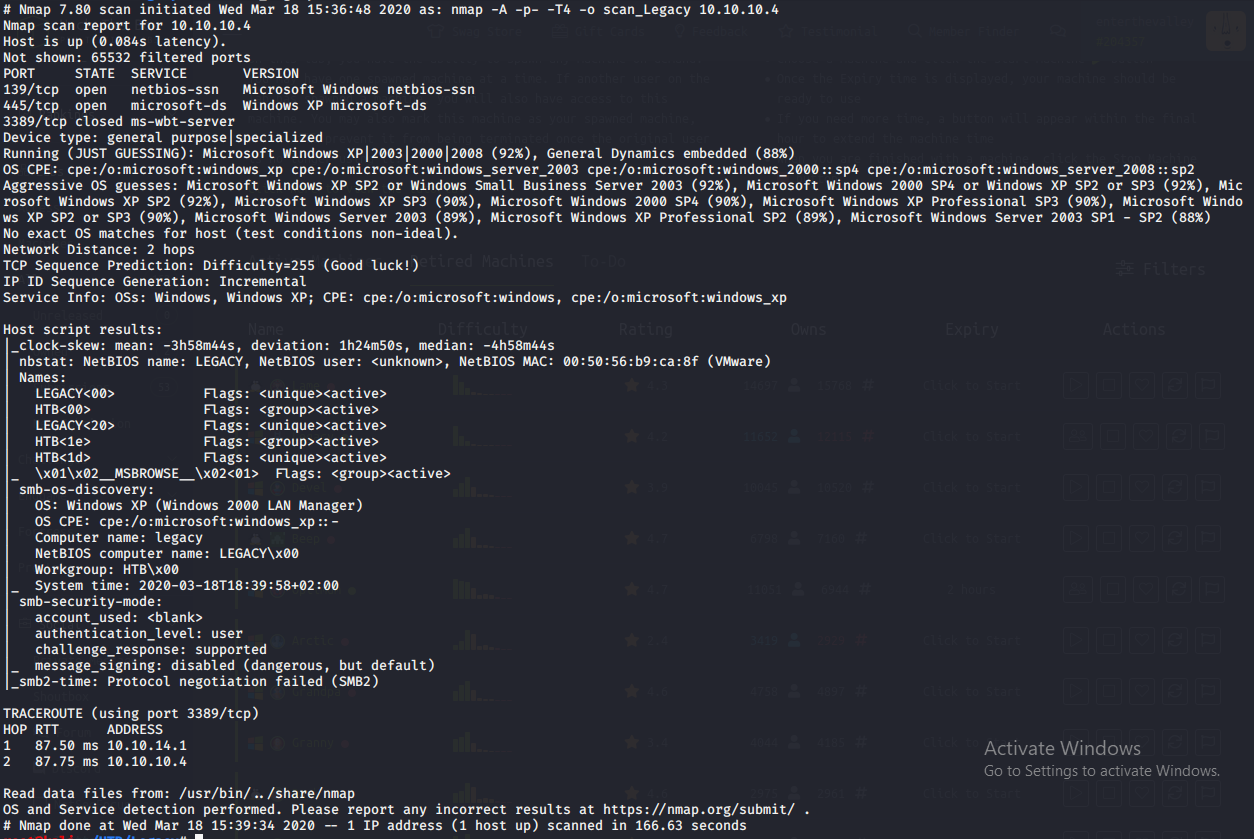


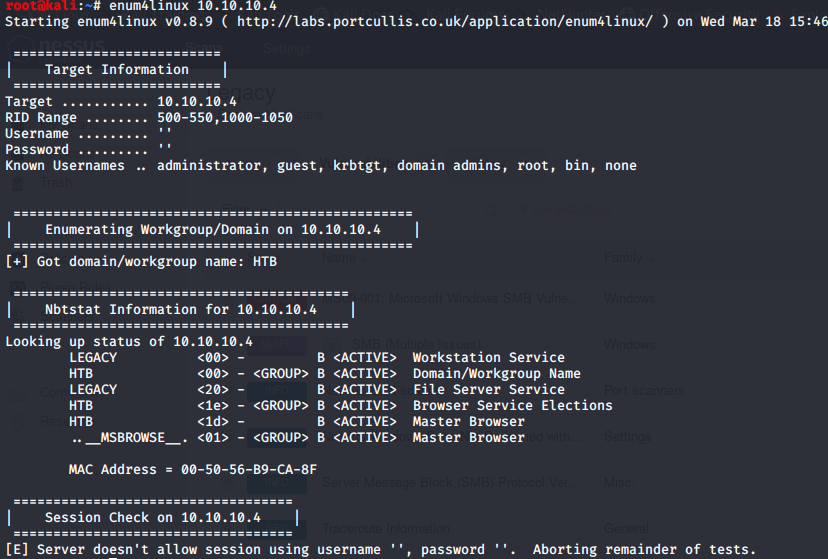
*Figure 2: The root and user flags were located*

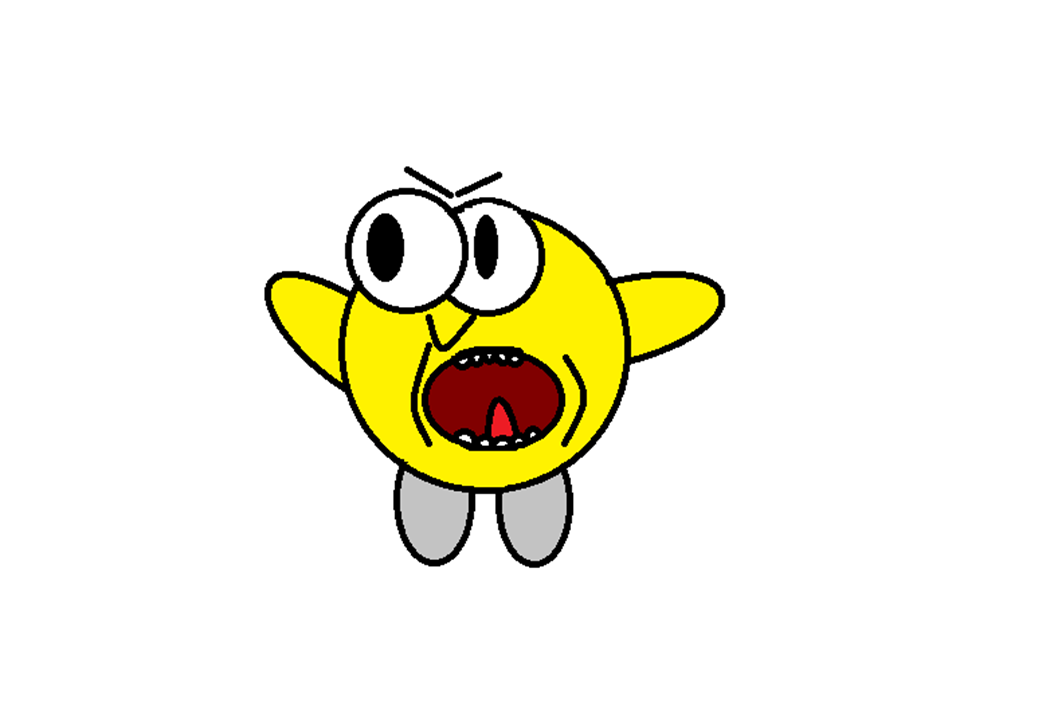
**Remediation**

|  |  |
| --- | --- |
| Who: | IT Team |
| Vector: | Remote |
| Action: | Item 1: It is critical to update the operating system and the SMB software being utilized. The system is highly vulnerable because of outdated software. |

Additional Reports and Scans (Informational)







Last Page