

1BitofMemory

HackTheBox Findings Report:

**Lame**

**Date: March 19th, 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)

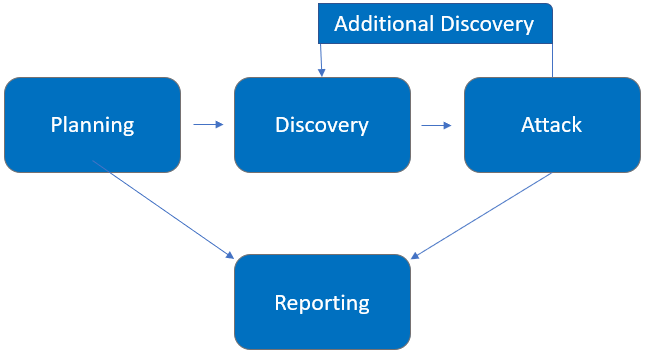
[Vulnerable Software – SMB Vulnerability (Critical) 8](#_Toc35430352)

[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 | 10.10.10.3 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 Lame’s external security posture through an external network penetration test on March 19, 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 1BitOfMemory gained internal network access, step by step:

|  |  |  |
| --- | --- | --- |
| Step | Action | Recommendation |
| 1 | Gained access to FTP server via anonymous login. | Disable anonymous login for FTP. |
| 2 | Obtained root level access by executing a publicly available exploit | Upgrade the version of samba being used. |
| 3 | Obtained user level access by executing a publicly available exploit. | Upgrade the distccd software being utilized. |

# Security Strengths

**User Access Control**

The machine did not allow non-privileged users to perform root level actions or view sensitive files.

# Security Weaknesses

## Vulnerable Software

The Samba software being utilized is easily exploited via a public exploit which leads to root access on the machine.

The distccd software being utilized is easily exploited via a public exploit which leads to user access on the machine.

# Vulnerabilities by Impact

The following chart illustrates the vulnerabilities found by impact:

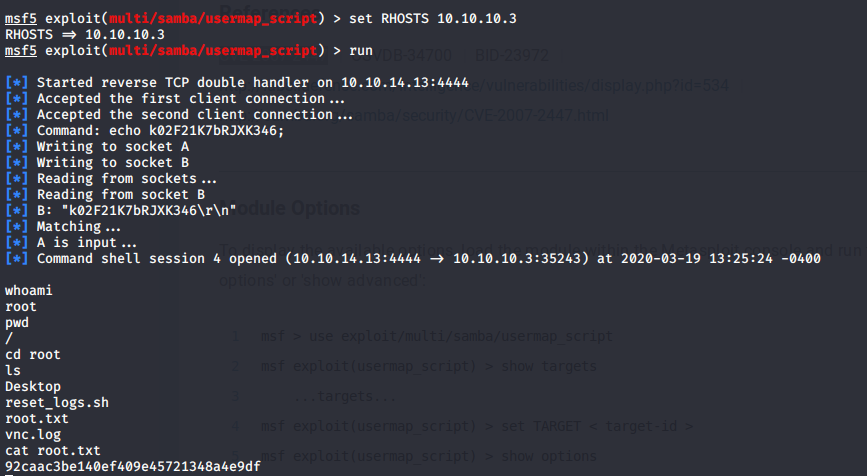
## External Penetration Test Findings

Vulnerable Software – Samba v3.0.20 (Critical)

|  |  |
| --- | --- |
| Description: | The version of SMB being utilized is susceptible to exploitation. |
| Impact: | Critical |
| System: | 10.10.10.3 |
| References: | CVE-2007-2447 |

**Exploitation Proof of Concept**

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



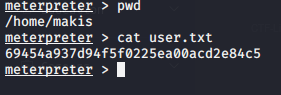
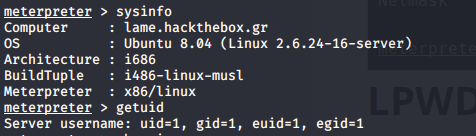
*Figure 1: Exploitation via CVE-2007-2447*

Vulnerable Software – distccd v4.2.4 (High)

|  |  |
| --- | --- |
| Description: | The version of the compiler being utilized (distccd) is susceptible to exploitation. |
| Impact: | High |
| System: | 10.10.10.3 |
| References: | CVE-2004-2687 |

**Exploitation Proof of Concept**

1BitOfMemory was able to gain user level access through the Samba vulnerability.



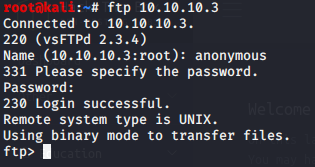
*Figure 2: Exploitation via CVE-2004-2687*

Misconfigured Software – vsFTPD v2.3.4 (Moderate)

|  |  |
| --- | --- |
| Description: | The FTP server allows for anonymous login. |
| Impact: | Moderate |
| System: | 10.10.10.3 |
| References: | http://www.networksolutions.com/support/what-is-anonymous-ftp-and-how-to-use-it/ |

**Exploitation Proof of Concept**

Anyone can log in to the FTP server without credentials. Files being hosted are publicly available.

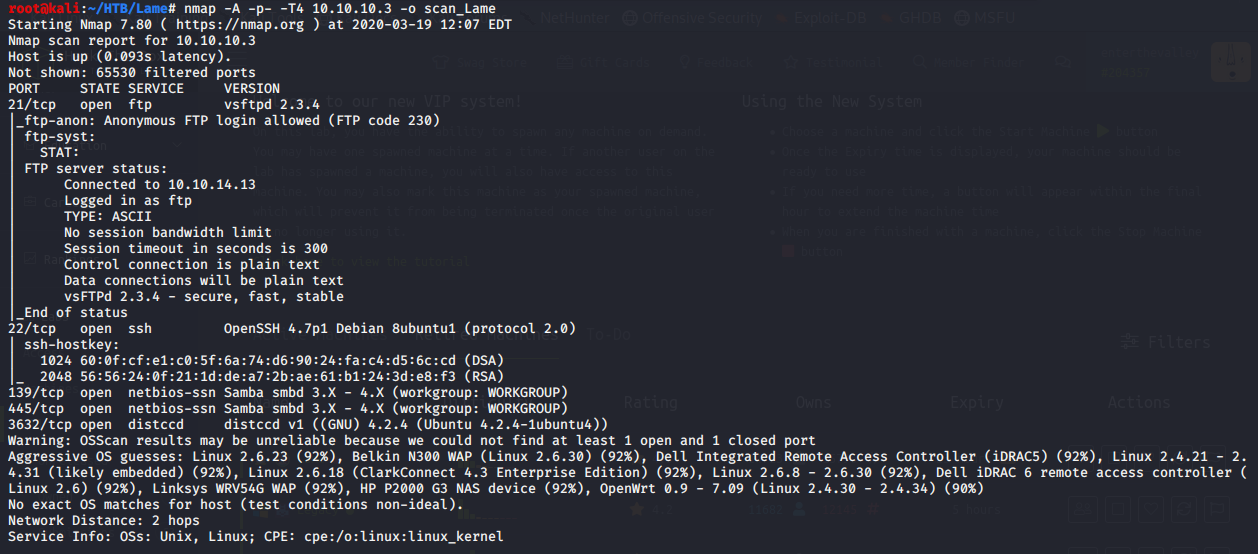
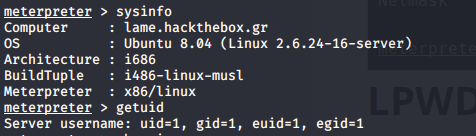


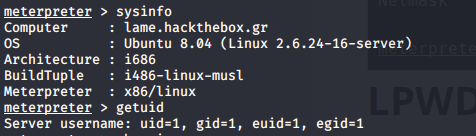
*Figure 3: Anonymous login to the FTP server*

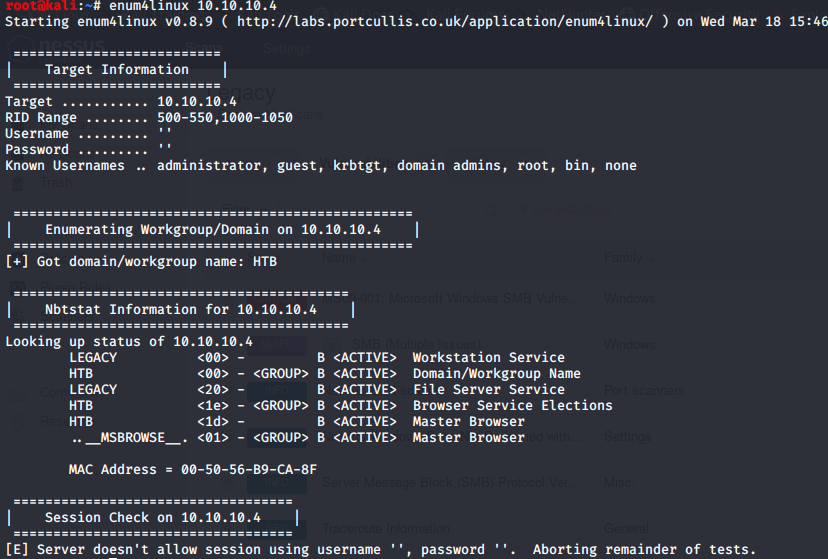
**Remediation**

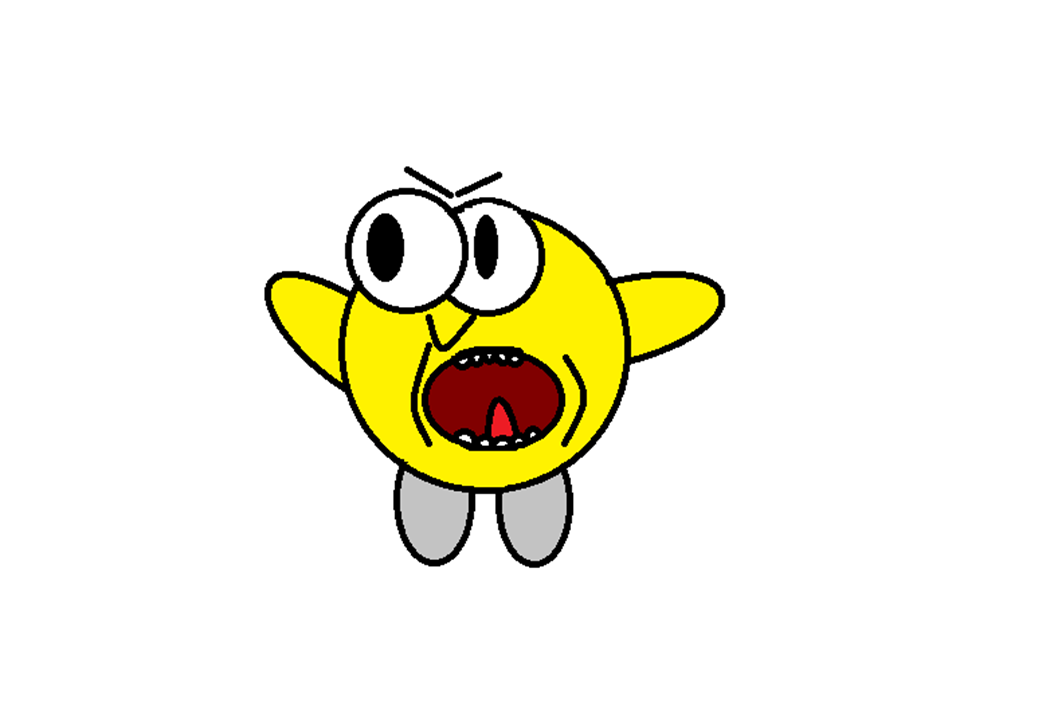
|  |  |
| --- | --- |
| Who: | IT Team |
| Vector: | Remote |
| Action: | Item 1: It is critical to update the Samba software being utilized as the current version is exploitable and allows root level privileges.  Item 2: It is critical to update the version of distccd being utilized as the current version is exploitable and allows user level privileges.  Item 3: It is important to configure the FTP server to not allow anonymous login. Anyone can view hosted files and upload to the server in the current configuration. |

Additional Reports and Scans (Informational)









Last Page