🛠️ Phase 2: Scanning & Enumeration

This section details the scanning and enumeration steps to identify open ports, services, and potential vulnerabilities on the target (**Metasploitable 2**).

🔎 Phase 2: Scanning & Enumeration

2.1 Objective

The goal of this phase is to probe the target system to actively:

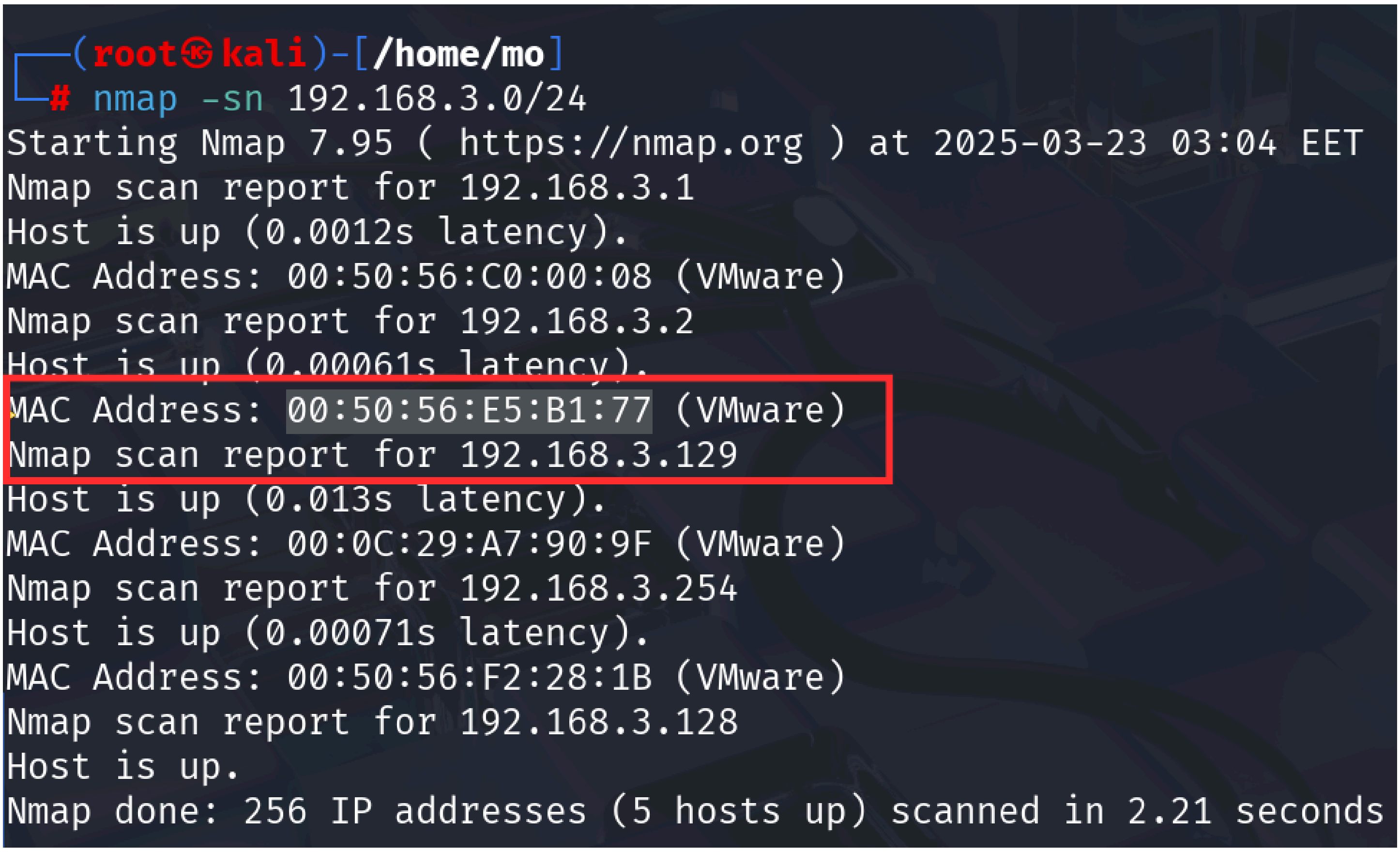
- Identify open ports and services
- Determine software versions and configurations
- Extract detailed information about vulnerable services

🔵 2.2 Network & Port & Vulnerability Scanning

2.2.1 Network Discovery

Using Nmap:

nmap -sn 192.168.3.0/24

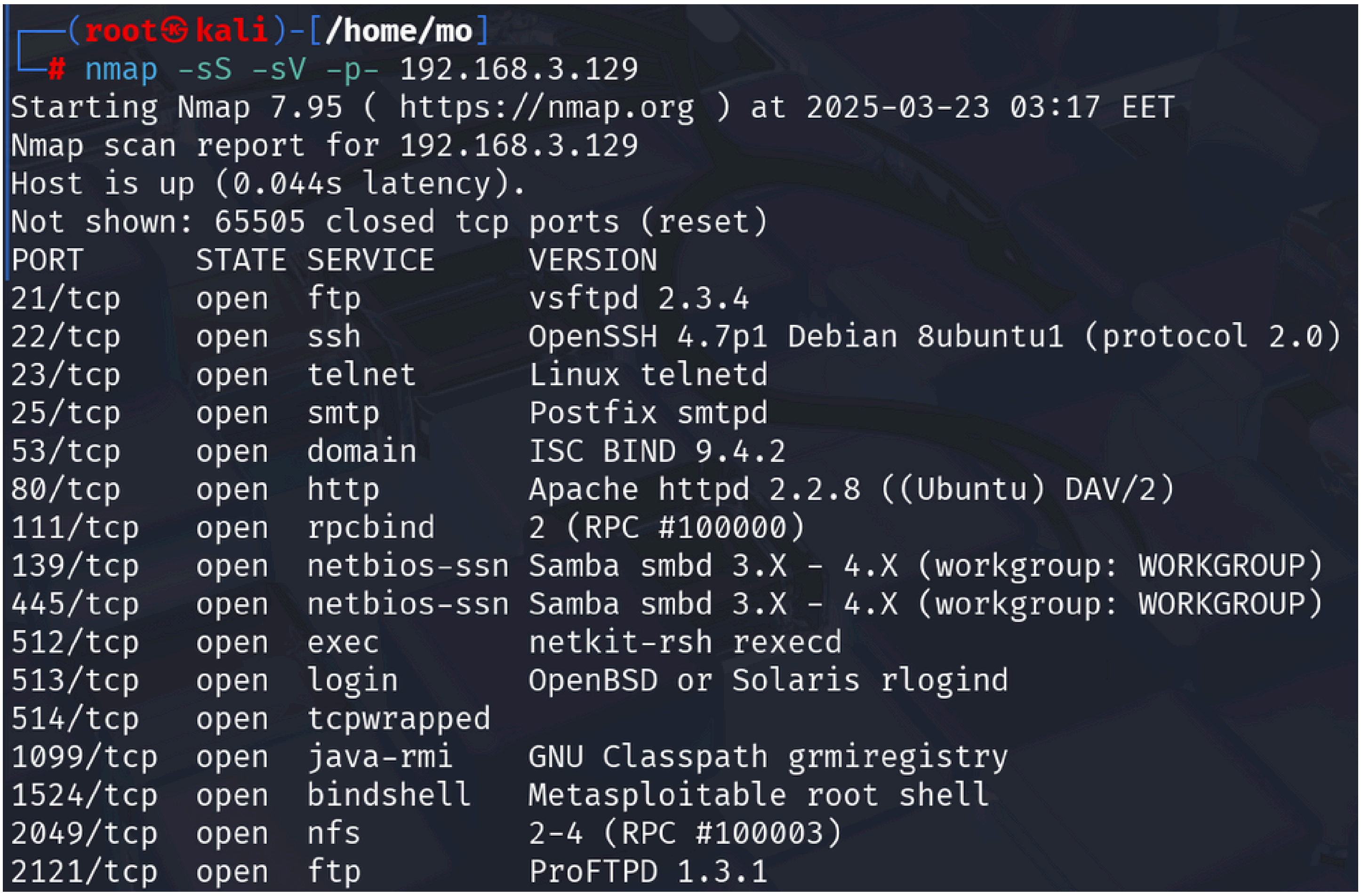


```
┌──(root㉿kali)-[/home/mo]
└─# nmap -sn 192.168.3.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-23 03:04 EET
Nmap scan report for 192.168.3.1
Host is up (0.0012s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.3.2
Host is up (0.00061s latency).
MAC Address: 00:50:56:E5:B1:77 (VMware)
Nmap scan report for 192.168.3.129
Host is up (0.013s latency).
MAC Address: 00:0C:29:A7:90:9F (VMware)
Nmap scan report for 192.168.3.254
Host is up (0.00071s latency).
MAC Address: 00:50:56:F2:28:1B (VMware)
Nmap scan report for 192.168.3.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.21 seconds
```

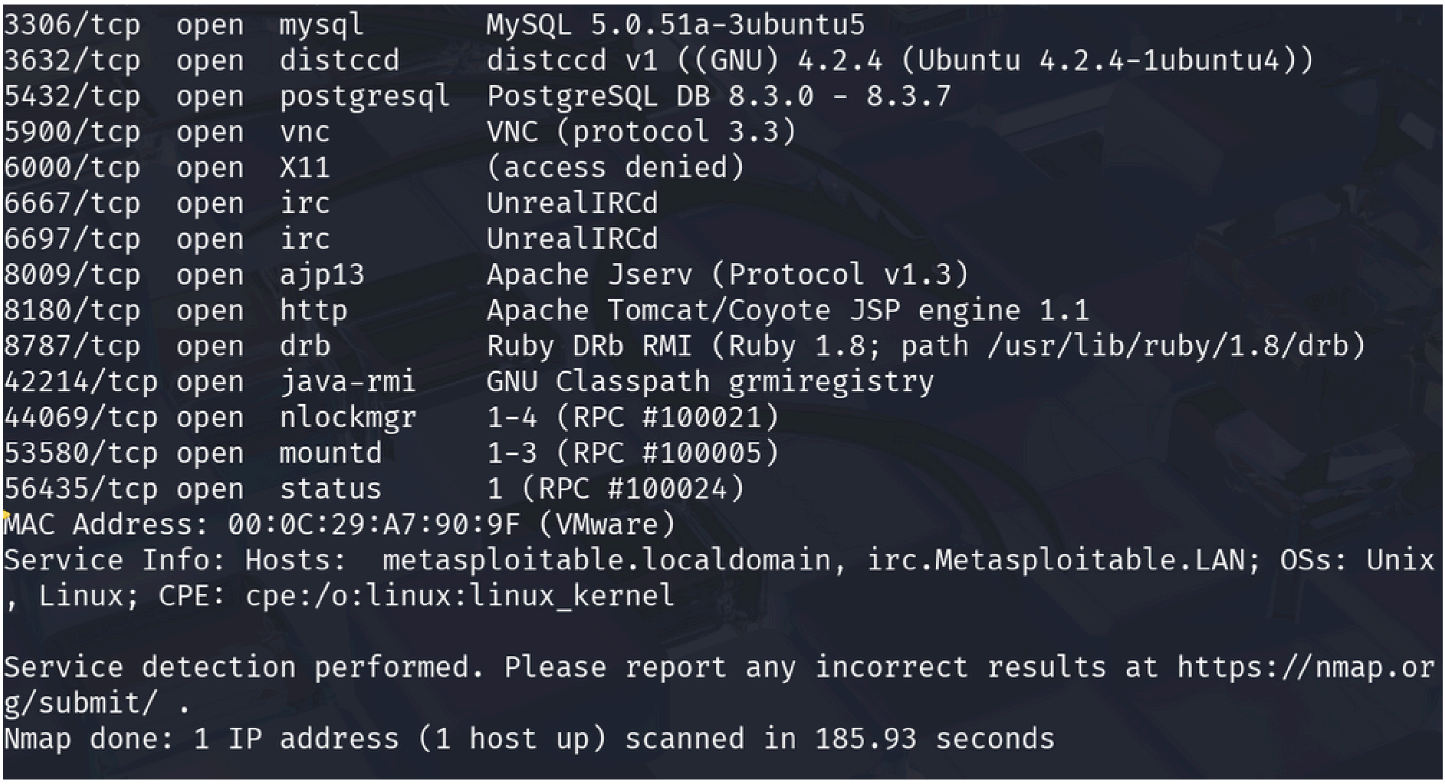
2.2.2 Full Port Scan & 2.2.3 Service & Version Detection

Using Nmap:

nmap -sS -sV -p- 192.168.3.129



```
┌──(root㉿kali)-[/home/mo]
└─# nmap -sS -sV -p- 192.168.3.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-23 03:17 EET
Nmap scan report for 192.168.3.129
Host is up (0.044s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
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)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login       OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
```

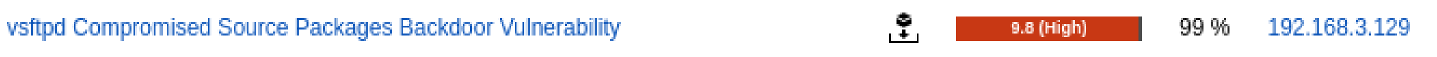


```
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
42214/tcp open  java-rmi    GNU Classpath grmiregistry
44069/tcp open  nlockmgr    1-4 (RPC #100021)
53580/tcp open  mountd      1-3 (RPC #100005)
56435/tcp open  status      1 (RPC #100024)
MAC Address: 00:0C:29:A7:90:9F (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix
, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.or
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 185.93 seconds
```

2.2.3 vuln scan

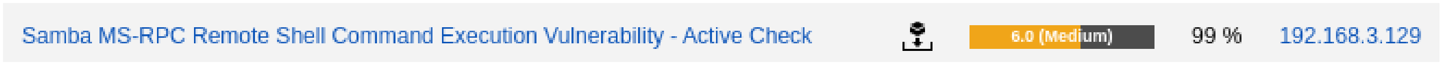
Using OpenVAS & Nmap :

CVE-2011-2523



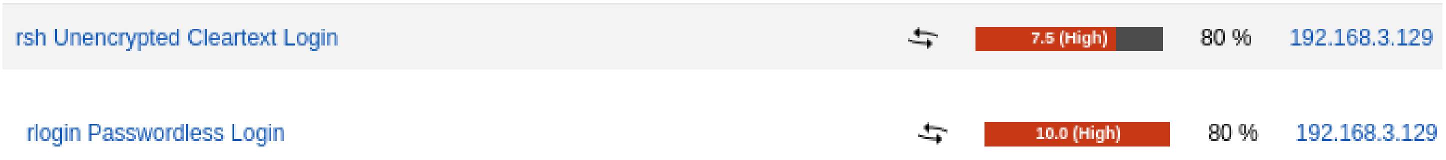
vsftpd Compromised Source Packages Backdoor Vulnerability	9.8 (High)	99 %	192.168.3.129

CVE-2007-2447



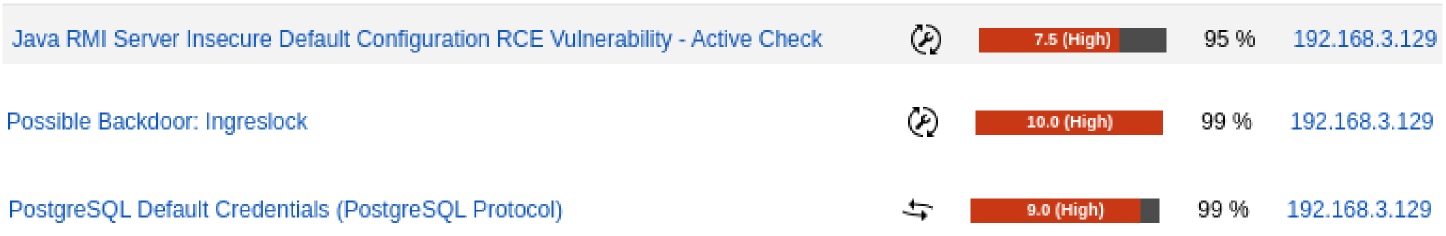
Samba MS-RPC Remote Shell Command Execution Vulnerability - Active Check	6.0 (Medium)	99 %	192.168.3.129

CVE-1999-0651



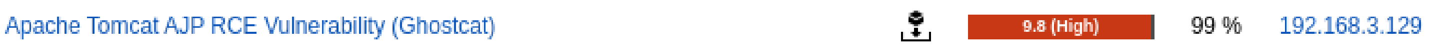
rsh Unencrypted Cleartext Login	7.5 (High)	80 %	192.168.3.129
rlogin Passwordless Login	10.0 (High)	80 %	192.168.3.129

CVE-2011-3556



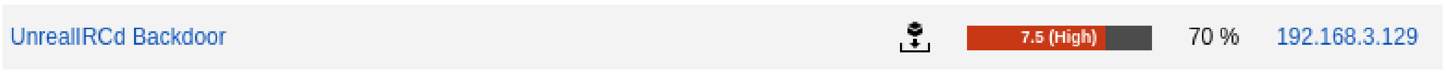
Java RMI Server Insecure Default Configuration RCE Vulnerability - Active Check	7.5 (High)	95 %	192.168.3.129
Possible Backdoor: Ingreslock	10.0 (High)	99 %	192.168.3.129
PostgreSQL Default Credentials (PostgreSQL Protocol)	9.0 (High)	99 %	192.168.3.129

CVE-2020-1938

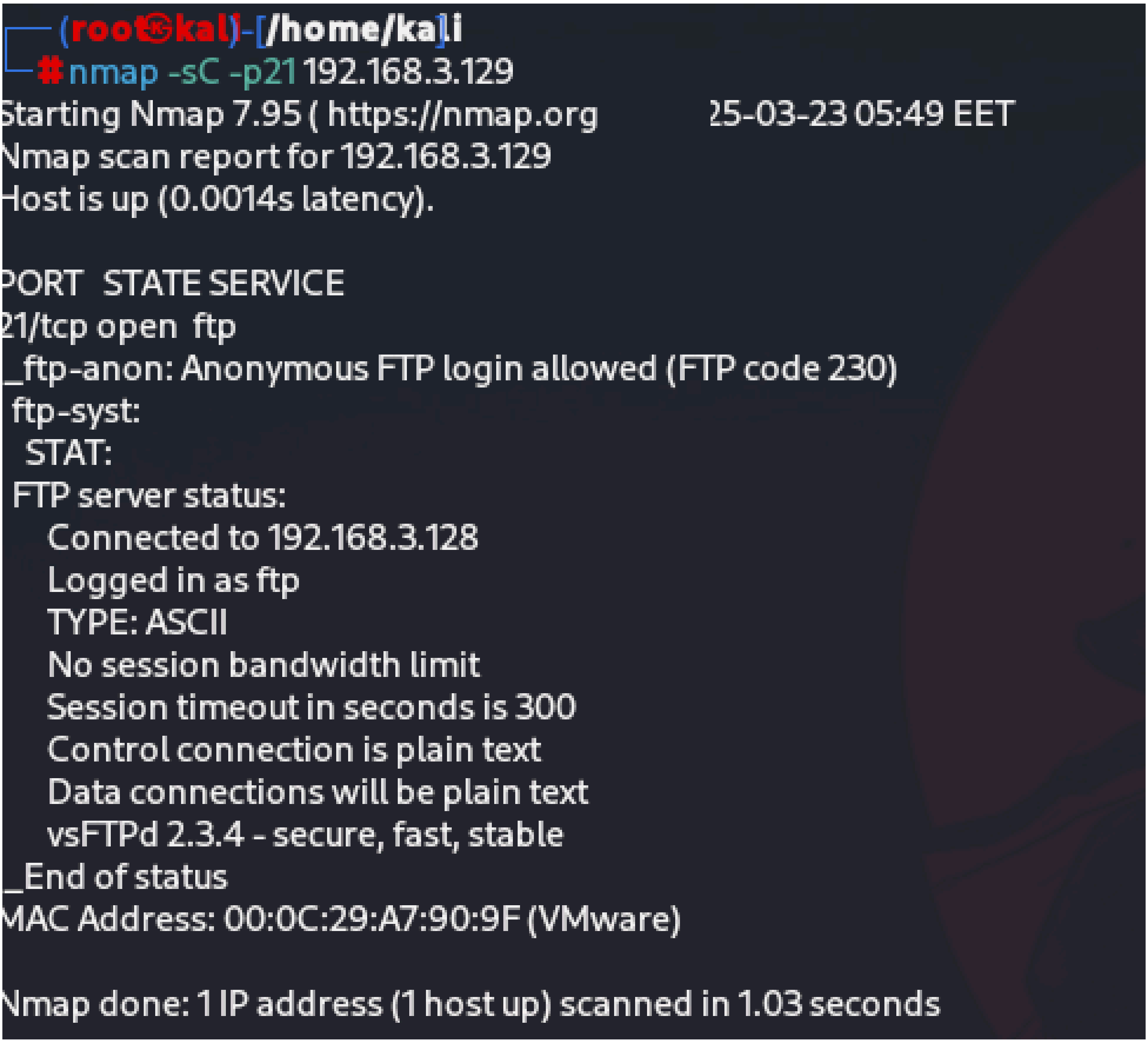


Apache Tomcat AJP RCE Vulnerability (Ghostcat)	9.8 (High)	99 %	192.168.3.129

CVE-2010-2075



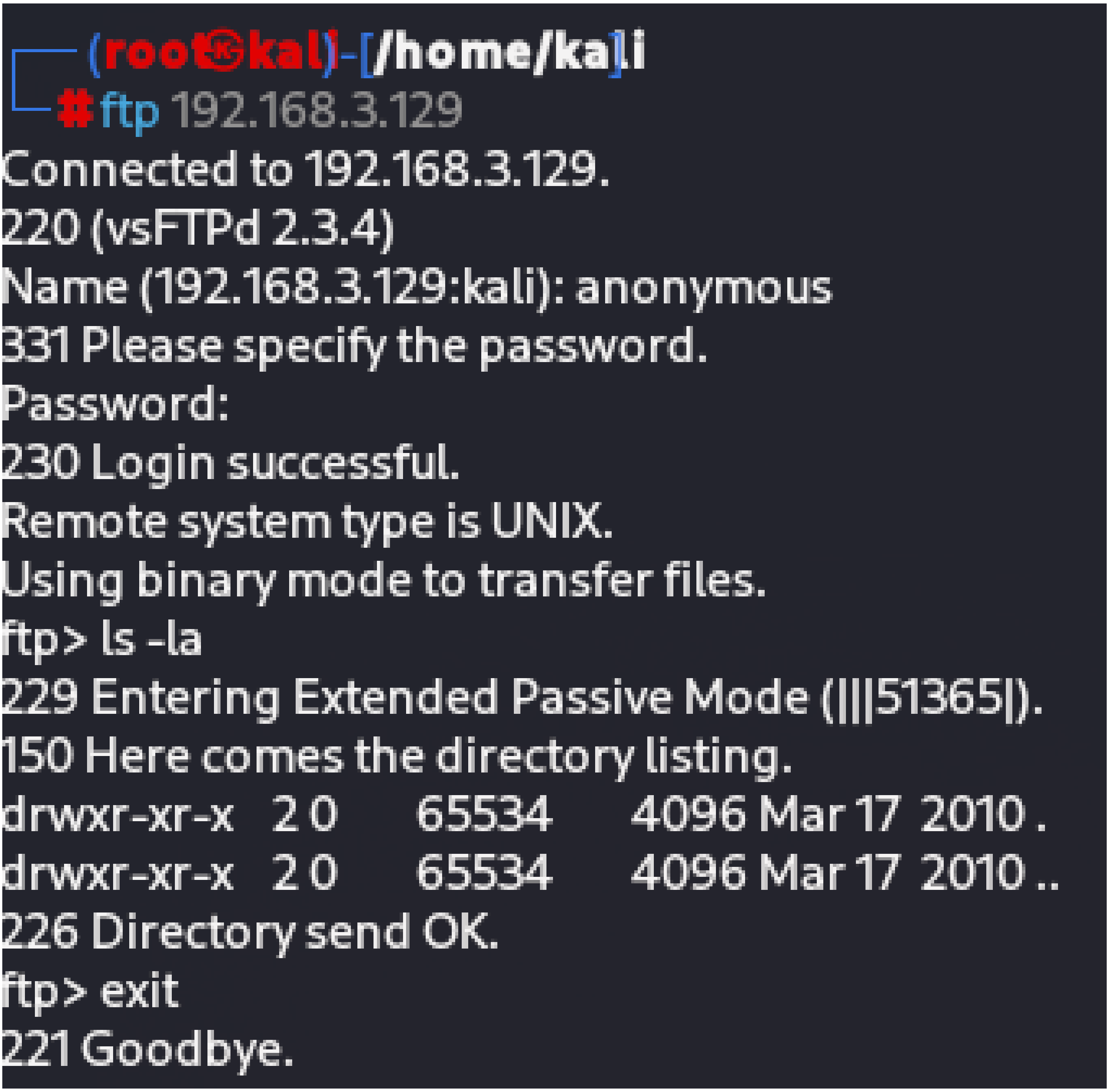
UnrealIRCd Backdoor	7.5 (High)	70 %	192.168.3.129



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sC -p21 192.168.3.129
Starting Nmap 7.95 ( https://nmap.org          25-03-23 05:49 EET
Nmap scan report for 192.168.3.129
Host is up (0.0014s latency).

PORT   STATE SERVICE
21/tcp open  ftp
_ftp-anon: Anonymous FTP login allowed (FTP code 230)
 ftp-syst:
   STAT:
 FTP server status:
      Connected to 192.168.3.128
      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
MAC Address: 00:0C:29:A7:90:9F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.03 seconds
```

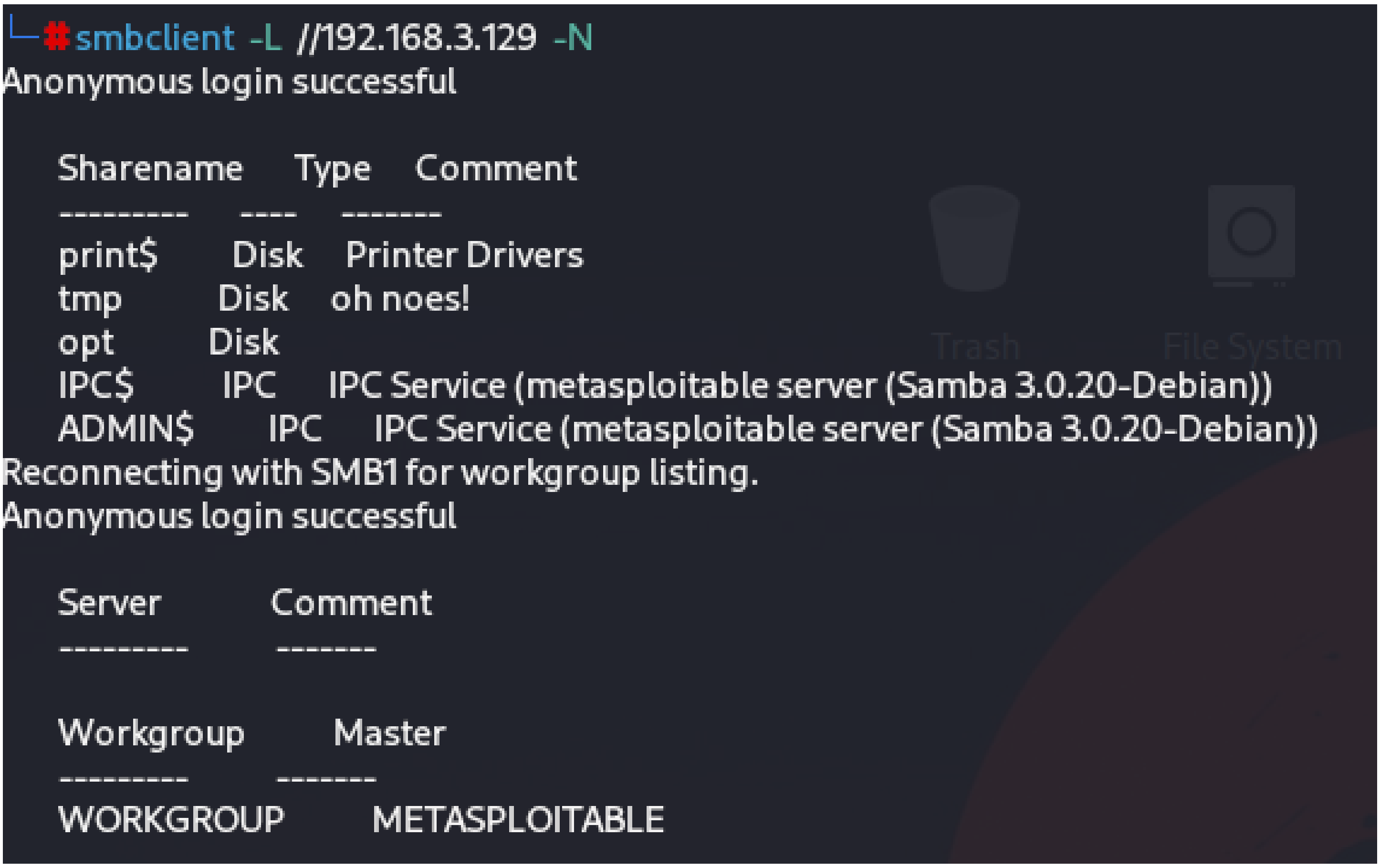
🔴 2.3 Enumeration (Detailed Service Probing)

🔹 2.3.1 FTP (Port 21) - VSFTPD 2.3.4



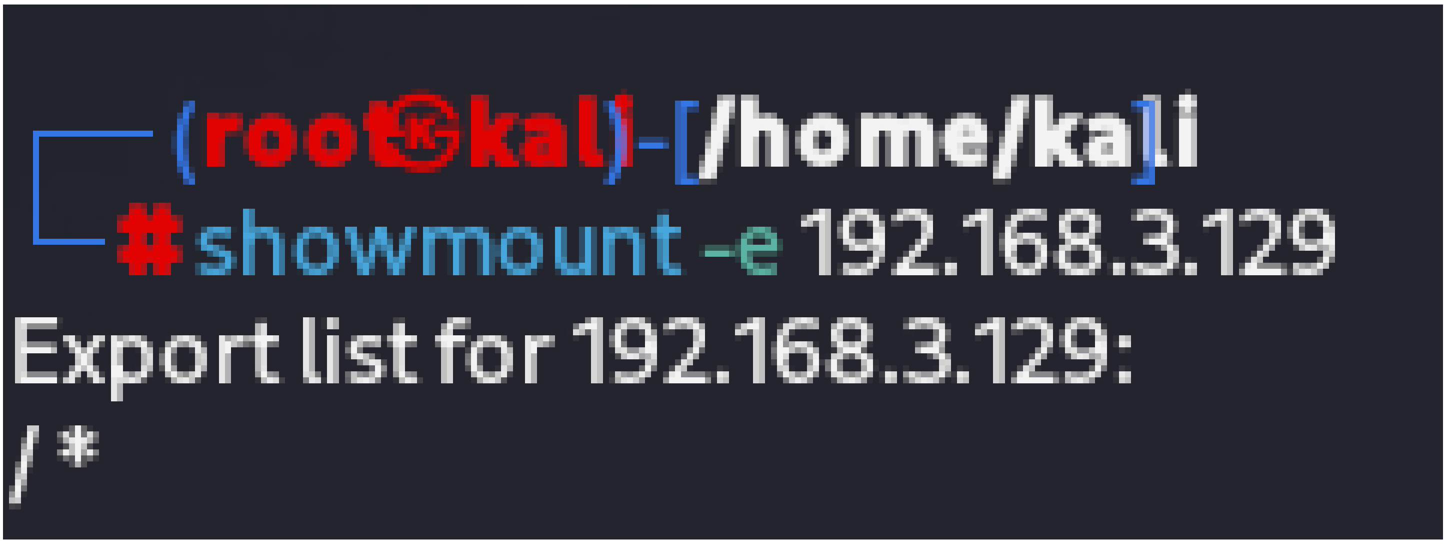
```
┌──(root㉿kali)-[/home/kali]
└─# ftp 192.168.3.129
Connected to 192.168.3.129.
220 (vsFTPd 2.3.4)
Name (192.168.3.129:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||51365|).
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.
```

2.3.7 SMB (Port 139, 445)



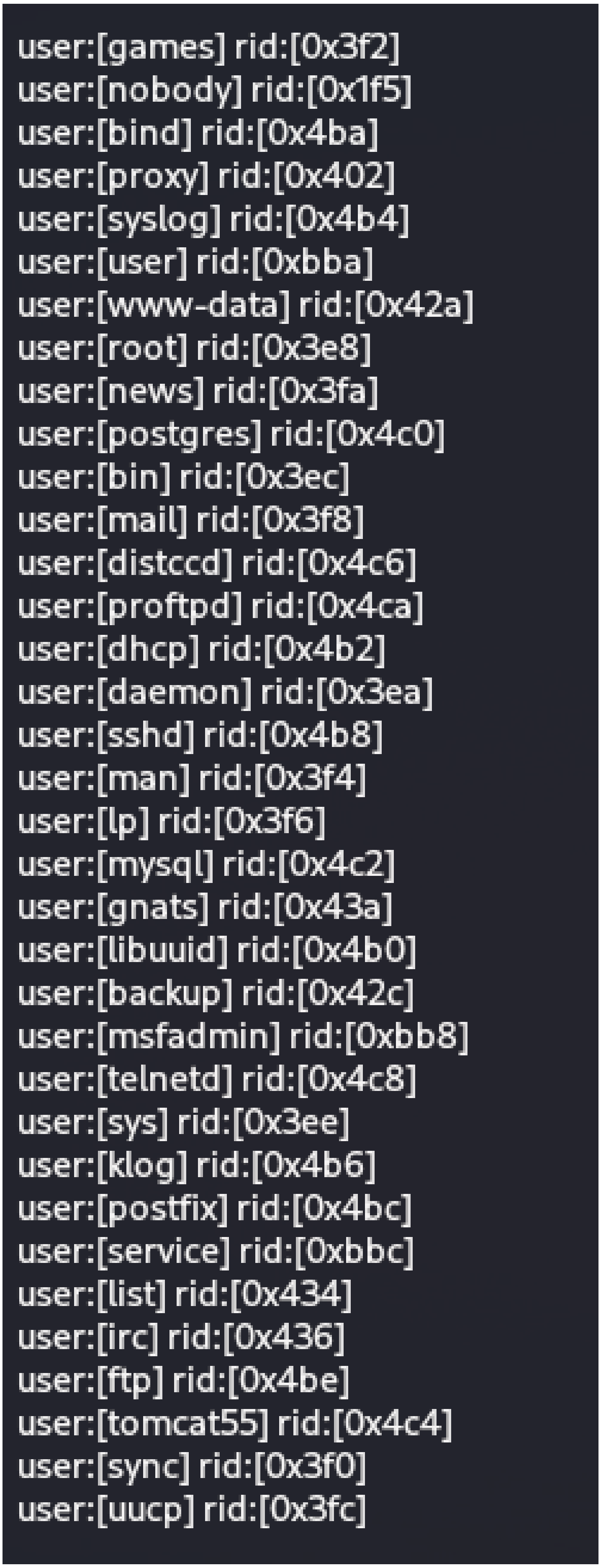
```
└─# smbclient -L //192.168.3.129 -N
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        tmp             Disk      oh noes!
        opt             Disk
        IPC$            IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
        ADMIN$          IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            METASPLOITABLE
```

2.3.8 NFS (Port 2049)



```
┌──(root㉿kali)-[/home/kali]
└─# showmount -e 192.168.3.129
Export list for 192.168.3.129:
/ *
```

Use Enum4linux:



```
user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[user] rid:[0xbba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[postgres] rid:[0x4c0]
user:[bin] rid:[0x3ec]
user:[mail] rid:[0x3f8]
user:[distccd] rid:[0x4c6]
user:[proftpd] rid:[0x4ca]
user:[dhcp] rid:[0x4b2]
user:[daemon] rid:[0x3ea]
user:[sshd] rid:[0x4b8]
user:[man] rid:[0x3f4]
user:[lp] rid:[0x3f6]
user:[mysql] rid:[0x4c2]
user:[gnats] rid:[0x43a]
user:[libuuid] rid:[0x4b0]
user:[backup] rid:[0x42c]
user:[msfadmin] rid:[0xbb8]
user:[telnetd] rid:[0x4c8]
user:[sys] rid:[0x3ee]
user:[klog] rid:[0x4b6]
user:[postfix] rid:[0x4bc]
user:[service] rid:[0xbbc]
user:[list] rid:[0x434]
user:[irc] rid:[0x436]
user:[ftp] rid:[0x4be]
user:[tomcat55] rid:[0x4c4]
user:[sync] rid:[0x3f0]
user:[uucp] rid:[0x3fc]
```

📌 2.4 Summary of Findings

Service: FTP

Port: 21

Version: vsftpd 2.3.4

CVE: CVE-2011-2523

Service: SMB

Port: 445

Version: samba 3.0.20-Debian

CVE: CVE-2007-2447

Service: http

Port: 8180

Version: Apache Tomcat/coyote JSP engine 1.1

CVE: CVE-2020-1938

Service: Jave-rmi

Port: 1099

Version: GNU classpath grmiregistry

CVE: CVE-2011-3556

Service: exec

Port: 512

Version: netkit-rsh

CVE: CVE-1999-0651

Service: irc

Port: 6697

Version: UnrealIRCd

CVE: CVE-2010-2075

Service: postgrespl

Port: 5432

Version: DB 8.3.0 -8.3.7

vuln: Default credentials

Service: nfs

Port: 2049

vuln: no_root_squash(Misconfiguration)