NETWORK MAPPER(NMAP)

Vulnerability Scanning Report
Date: Saturday, July 19, 2025

Methodology

Tool Used: Nmap (Network Mapper)

Version: 7.94SVN

Target Network: 192.168.180.1/24 and specific host 192.168.180.133

Scan Types:

Network scan for hosts and open ports (nmap 192.168.180.1/24)

Found out the ip address of the target is 192.168.180.133.

TCP SYN scan(nmap -sS 192.168.180.133)

Probe open ports to determine service/version info(nmap -sV 192.168.180.133)

Enable OS detection, version detection, script scanning, and traceroute(nmap -A 192.168.180.133)

Objectives: Identify live hosts, open ports, and services; gather service versions for vulnerability assessment.

Key Findings

1. Open Ports & Services

Multiple ports are open on host 192.168.180.133, with many associated with well-known, frequently exploited services:

21/tcp – FTP (vsftpd 2.3.4): Known to have backdoors and allows anonymous login.

22/tcp – SSH (OpenSSH 4.7p1): Outdated, possibly vulnerable to several exploits.

23/tcp – Telnet: Exposes data in plaintext, high security risk.

25/tcp – SMTP: Can be abused for spam/relaying if unsecured.

53/tcp – DNS (ISC BIND 9.4.2): Multiple historic vulnerabilities.

80/tcp – HTTP (Apache 2.2.8): Known for old vulnerabilities and misconfigurations.

139/tcp, 445/tcp – Samba/NetBIOS: Historically vulnerable to exploits like EternalBlue.

3306/tcp – MySQL (5.0.51a): Outdated version, has remote code execution and privilege escalation issues.

5432/tcp – PostgreSQL: Outdated; may contain vulnerabilities.

5900/tcp – VNC: Outdated protocol, often weak or no authentication.

6667/tcp – IRC (UnrealIRCd): Past backdoors in specific versions.

Several other ports: Including RPCBind, Java RMI, and backdoor shells, which represent serious security risks.

2. Service Version Disclosure

Many services provided detailed version info, making it easier for attackers to search for public exploits against these specific versions.

3. SSL/TLS Weaknesses

SSLv2 Supported: Detected weak ciphers and protocols (e.g., SSL2_RC2, SSL2_RC4, SSL2_DES), which are deprecated due to major vulnerabilities.

Expired/Invalid Certificates: Certificates detected are long expired and not valid for current use.

4. Other Weaknesses

Anonymous FTP Login: Allows unrestricted access.

Exposed Management Interfaces: HTTP, Telnet, SSH, VNC, and Java RMI accessible remotely without clear authentication hardening.

Screenshots

Nmap command execution and scan results for both network and host discovery (see appended screenshots for step-by-step setup and findings).

Recommended Actions

Disable/Restrict Unused Services: Shut down unnecessary and insecure services (Telnet, anonymous FTP, outdated web, RPC, and shell interfaces).

Update Software: Patch or upgrade all services to currently supported, secure versions.

Implement Access Controls: Restrict SSH, Telnet, VNC, and management services to trusted IPs only; disable anonymous logins.

Harden Authentication: Enforce strong passwords, use public/private key authentication for SSH, and implement multi-factor authentication where possible.

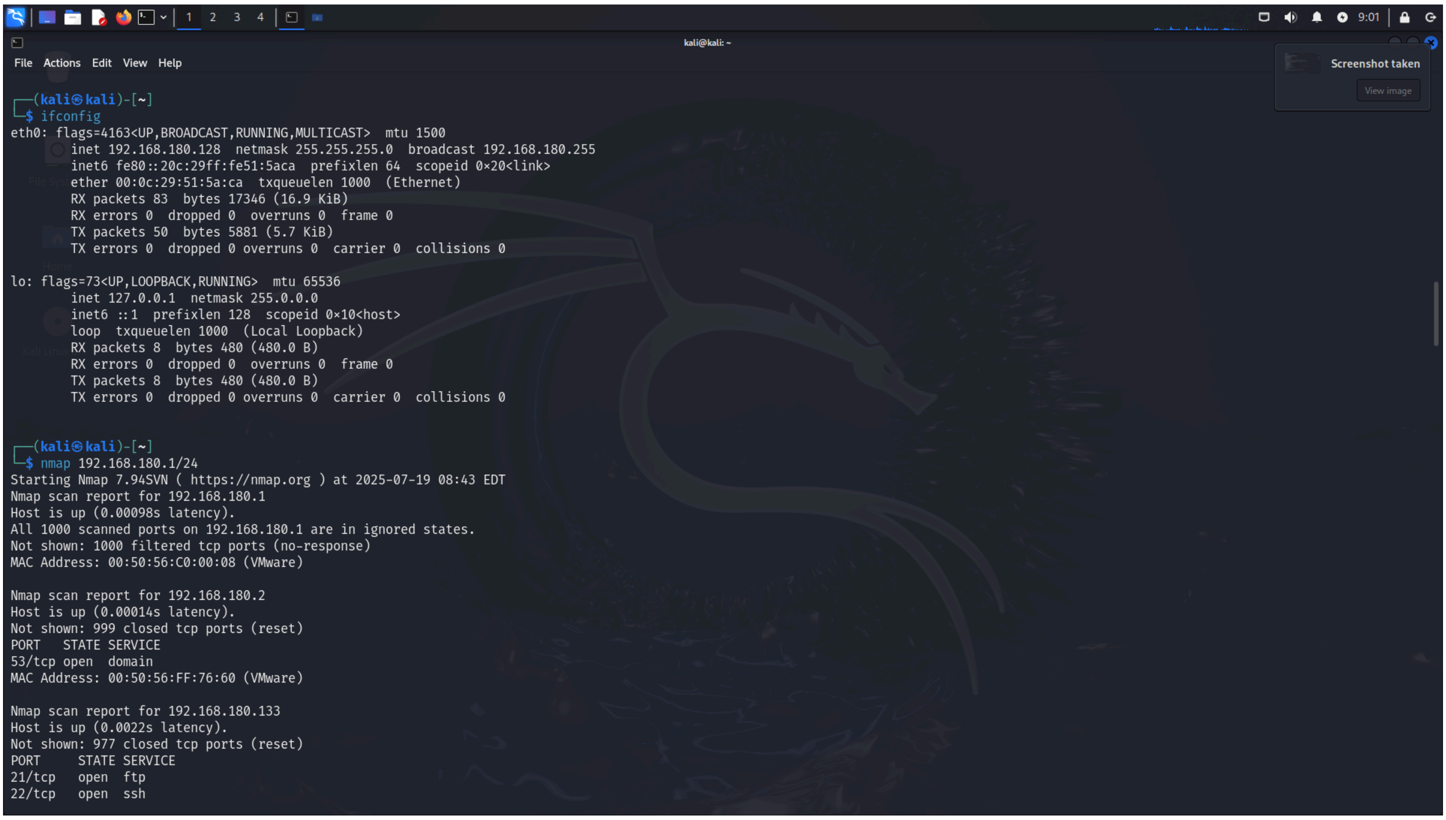
Remove Weak Ciphers: Disable SSLv2 and SSLv3 in favor of TLS 1.2+; use updated certificates.

Network Segmentation/Firewall: Block access to sensitive ports and services from untrusted networks.

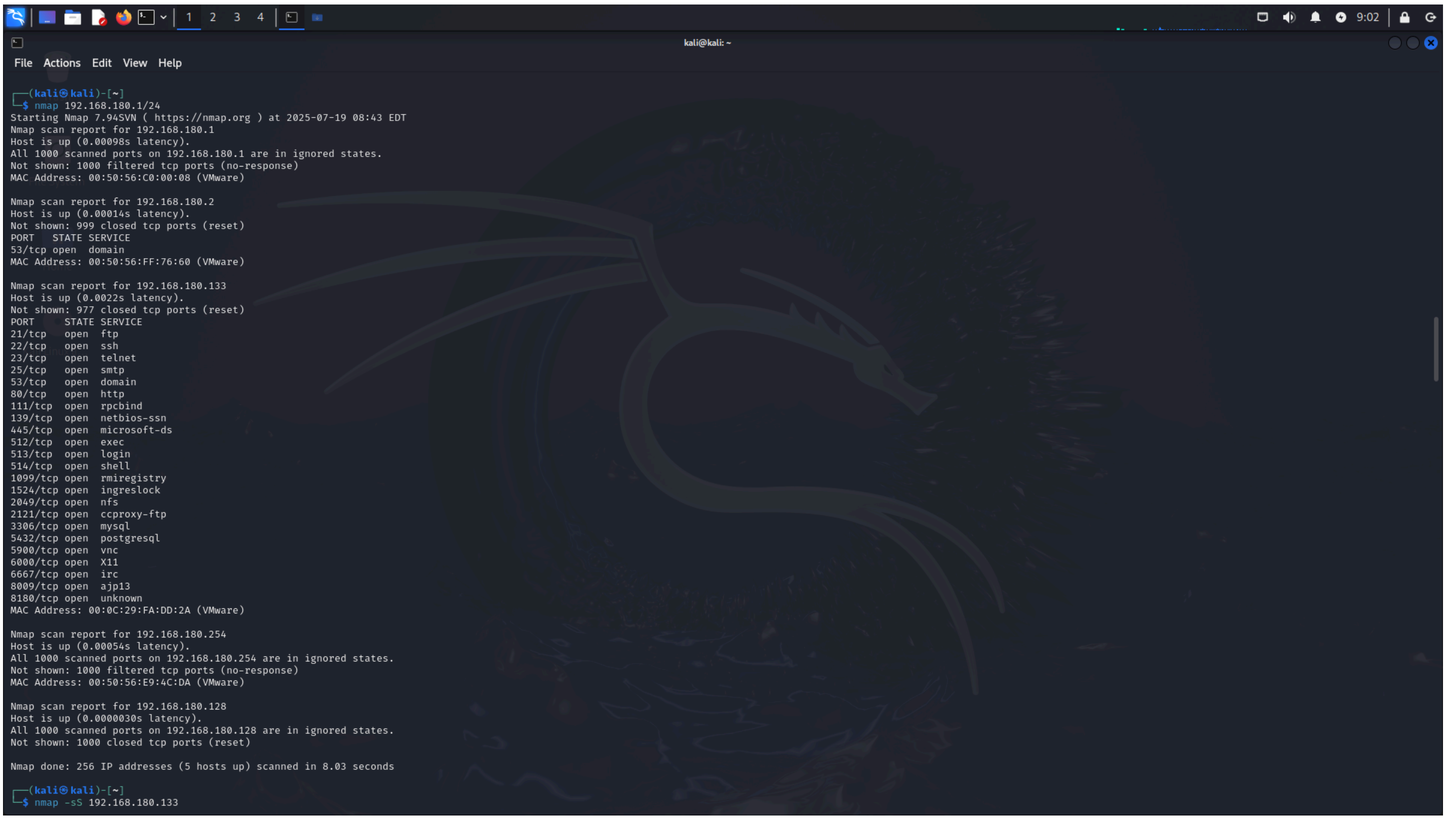
Monitor and Audit: Regularly monitor access logs and use tools like fail2ban to prevent brute-force attacks.

Summary:
The scan revealed numerous outdated, misconfigured, and potentially vulnerable services exposed to the network. Immediate action should be taken to harden these hosts, restrict unnecessary exposure, and apply patches to minimize attack surface and risk of compromise.

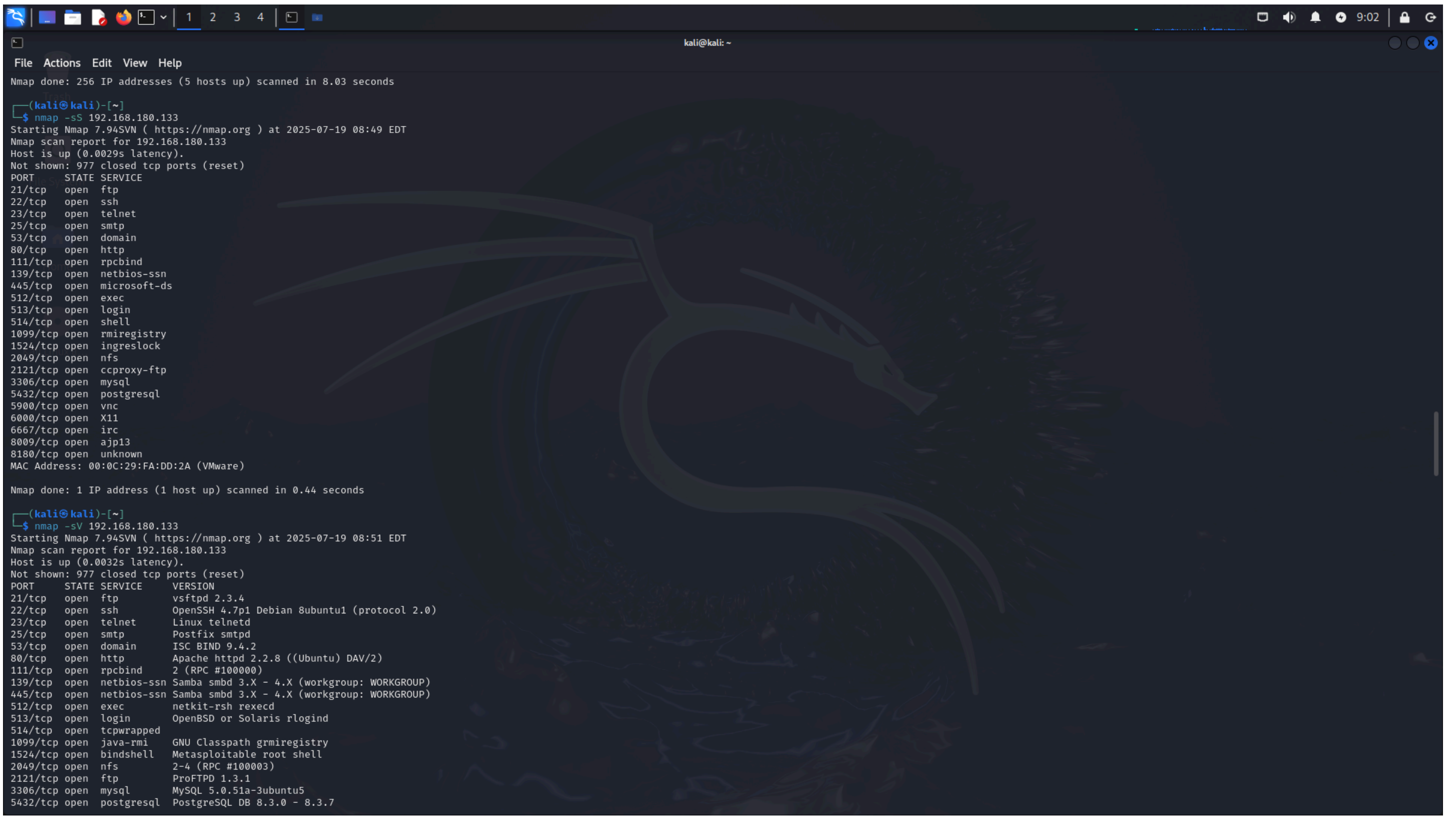
Screenshots:



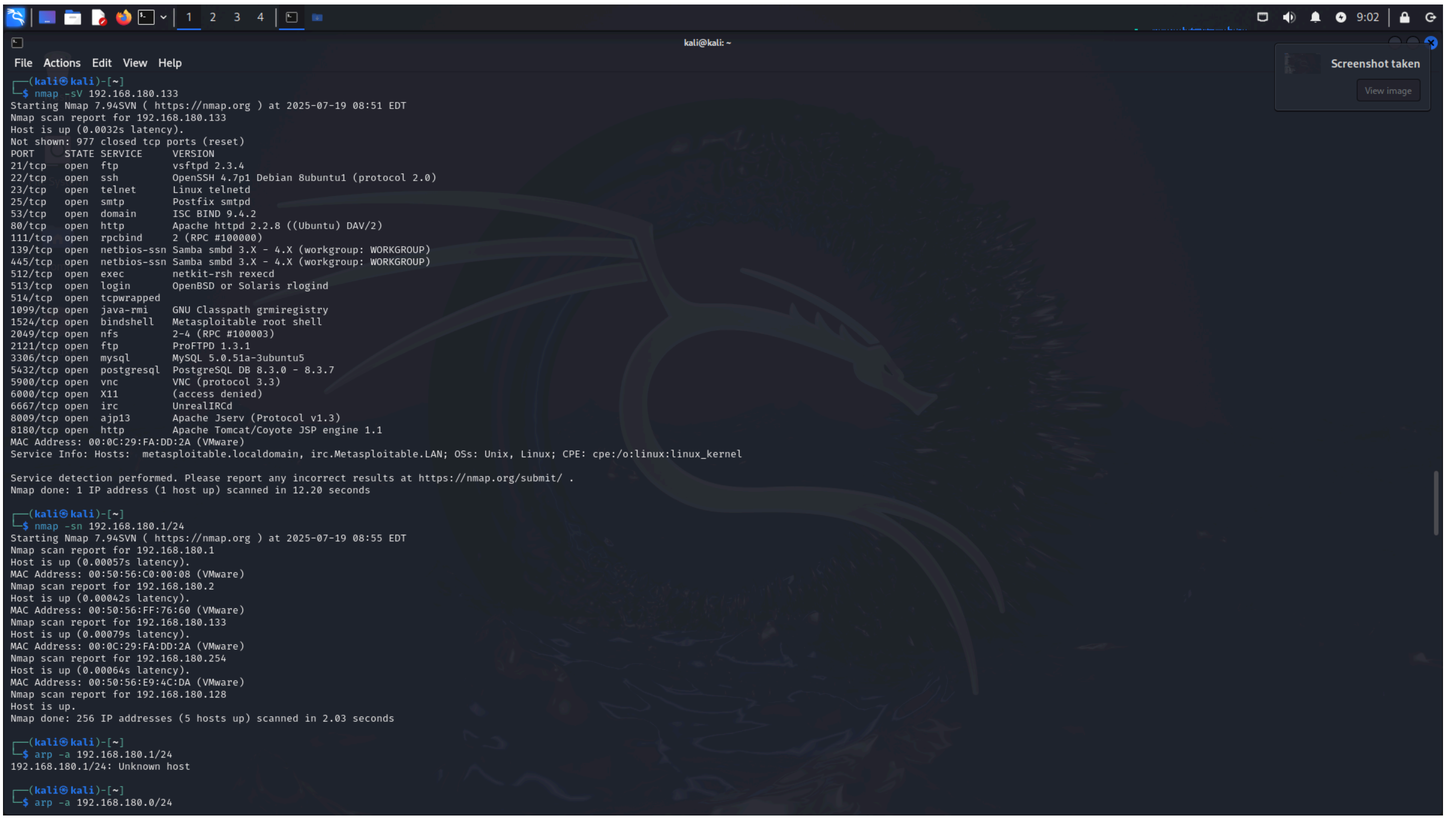
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.180.128  netmask 255.255.255.0  broadcast 192.168.180.255
        inet6 fe80::20c:29ff:fe51:5aca  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:51:5a:ca  txqueuelen 1000  (Ethernet)
        RX packets 83  bytes 17346 (16.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 50  bytes 5881 (5.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ nmap 192.168.180.1/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-19 08:43 EDT
Nmap scan report for 192.168.180.1
Host is up (0.00098s latency).
All 1000 scanned ports on 192.168.180.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.180.2
Host is up (0.00014s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:FF:76:60 (VMware)

Nmap scan report for 192.168.180.133
Host is up (0.0022s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
```



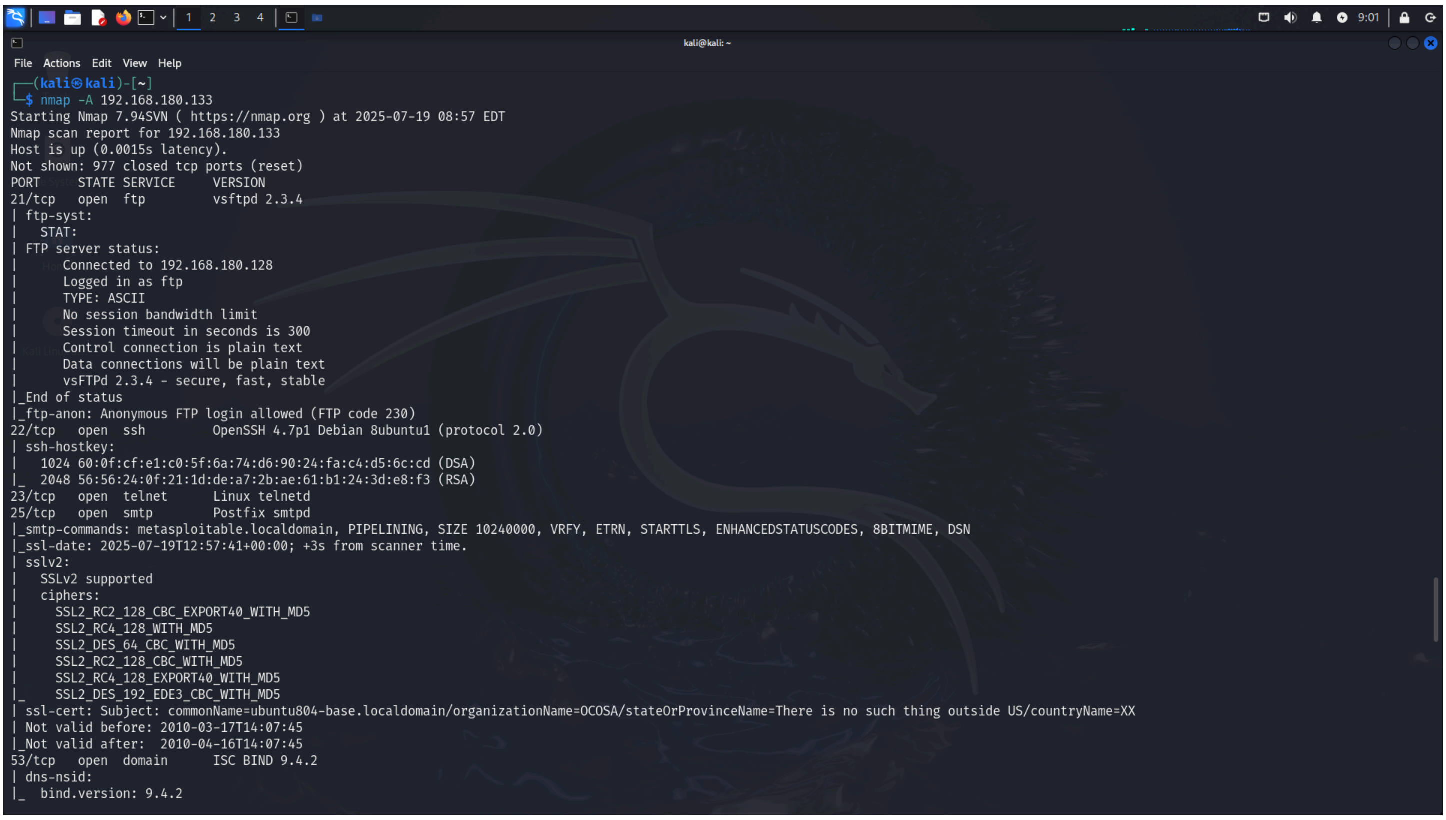
```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.180.1/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-19 08:43 EDT
Nmap scan report for 192.168.180.1
Host is up (0.00098s latency).
All 1000 scanned ports on 192.168.180.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.180.2
Host is up (0.00014s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:FF:76:60 (VMware)

Nmap scan report for 192.168.180.133
Host is up (0.0022s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap scan report for 192.168.180.254
Host is up (0.00054s latency).
All 1000 scanned ports on 192.168.180.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:E9:4C:DA (VMware)

Nmap scan report for 192.168.180.128
Host is up (0.0000030s latency).
All 1000 scanned ports on 192.168.180.128 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (5 hosts up) scanned in 8.03 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.180.133
```



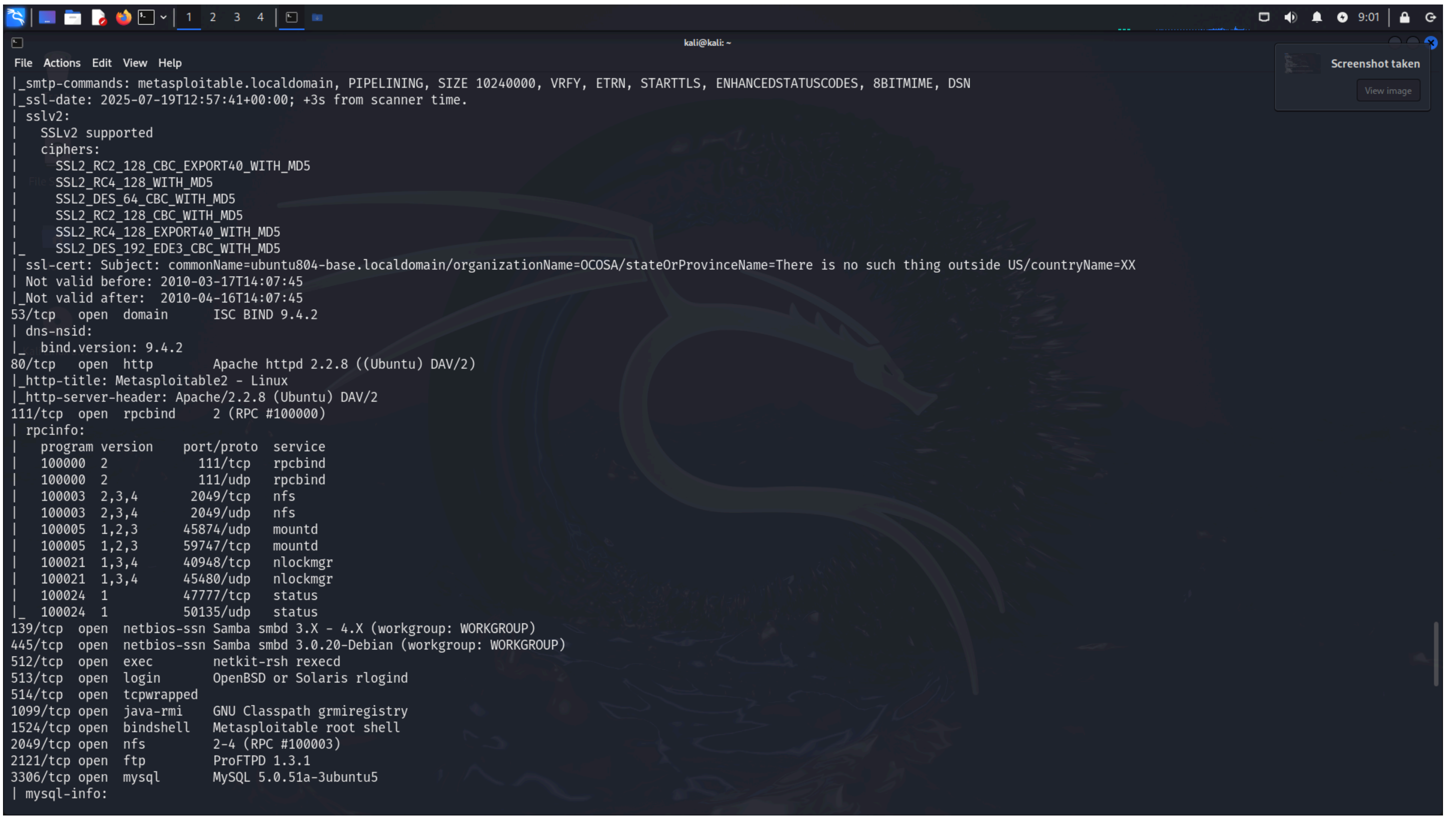
```
Nmap done: 256 IP addresses (5 hosts up) scanned in 8.03 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.180.133
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-19 08:49 EDT
Nmap scan report for 192.168.180.133
Host is up (0.0029s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:FA:DD:2A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.180.133
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-19 08:51 EDT
Nmap scan report for 192.168.180.133
Host is up (0.0032s latency).
Not shown: 977 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
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
```



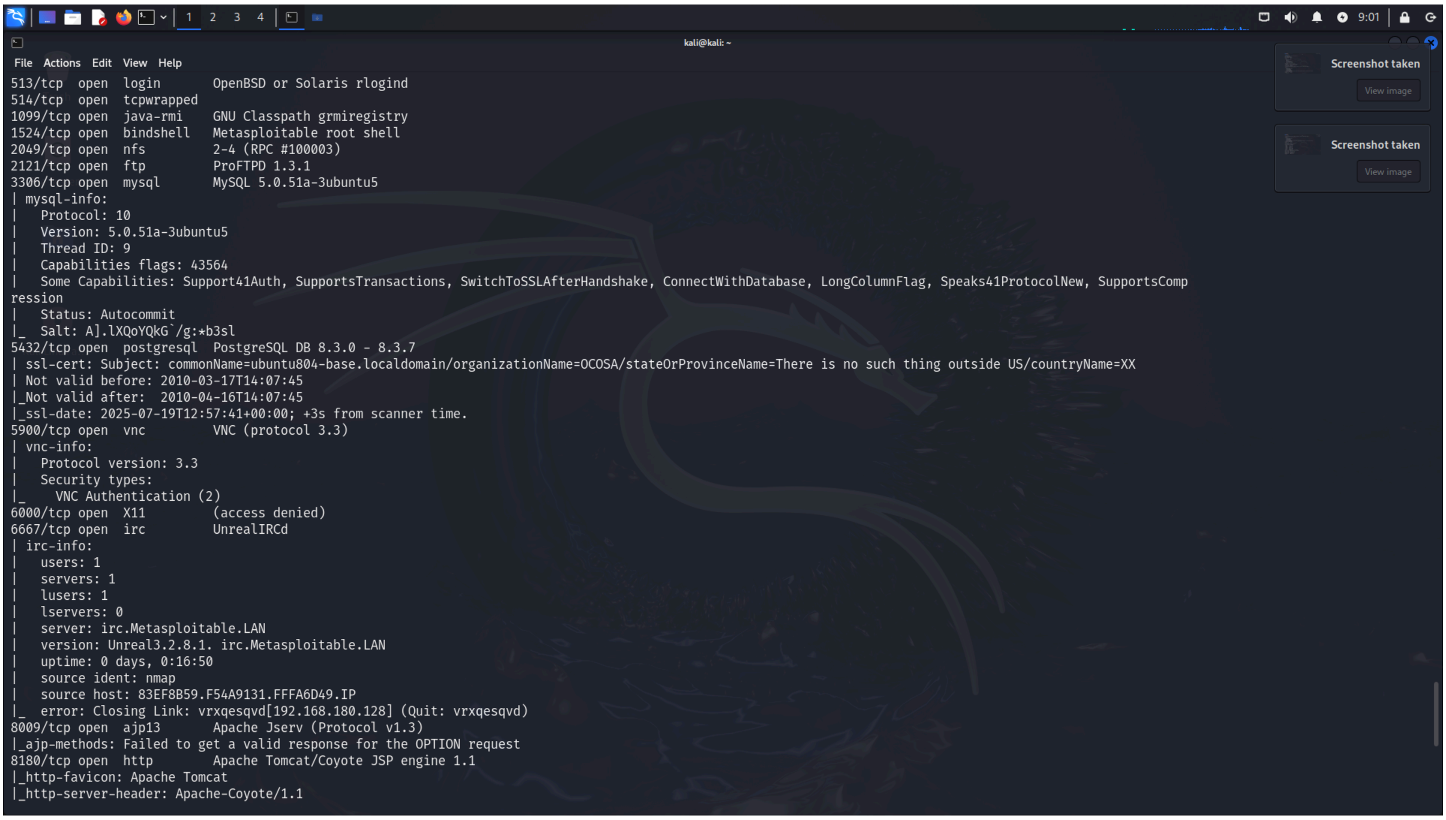
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.180.133
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-19 08:51 EDT
Nmap scan report for 192.168.180.133
Host is up (0.0032s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
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
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
MAC Address: 00:0C:29:FA:DD:2A (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.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.20 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.180.1/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-19 08:55 EDT
Nmap scan report for 192.168.180.1
Host is up (0.00057s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.180.2
Host is up (0.00042s latency).
MAC Address: 00:50:56:FF:76:60 (VMware)
Nmap scan report for 192.168.180.133
Host is up (0.00079s latency).
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Nmap scan report for 192.168.180.254
Host is up (0.00064s latency).
MAC Address: 00:50:56:E9:4C:DA (VMware)
Nmap scan report for 192.168.180.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.03 seconds

┌──(kali㉿kali)-[~]
└─$ arp -a 192.168.180.1/24
192.168.180.1/24: Unknown host

┌──(kali㉿kali)-[~]
└─$ arp -a 192.168.180.0/24
```



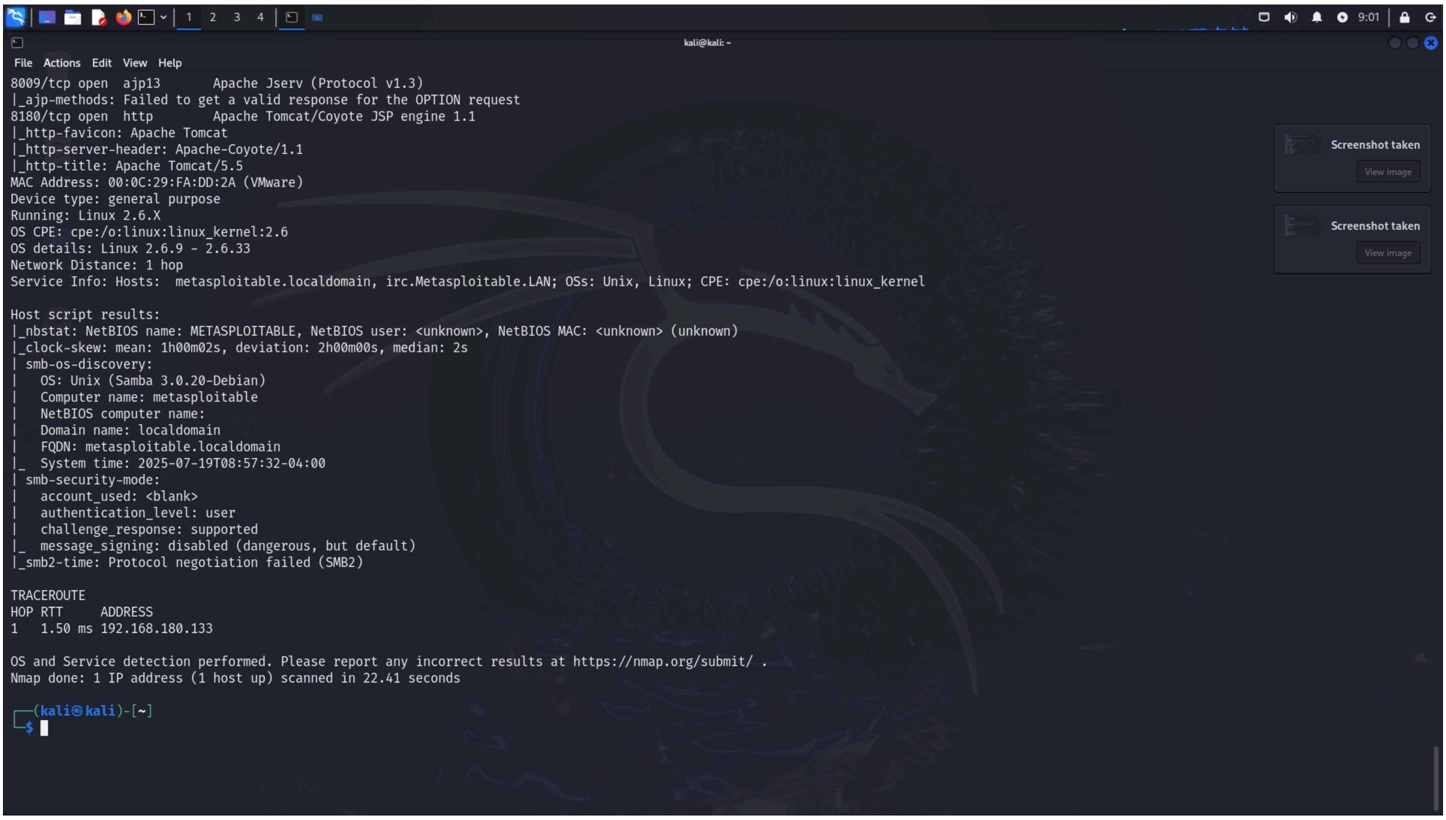
```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.180.133
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-19 08:57 EDT
Nmap scan report for 192.168.180.133
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.180.128
|      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
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
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)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2025-07-19T12:57:41+00:00; +3s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
```



```
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2025-07-19T12:57:41+00:00; +3s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      45874/udp   mountd
|   100005  1,2,3      59747/tcp   mountd
|   100021  1,3,4      40948/tcp   nlockmgr
|   100021  1,3,4      45480/udp   nlockmgr
|   100024  1          47777/tcp   status
|_  100024  1          50135/udp   status
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)
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
| mysql-info:
```



```
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
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 9
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, SupportsTransactions, SwitchToSSLAfterHandshake, ConnectWithDatabase, LongColumnFlag, Speaks41ProtocolNew, SupportsComp
ression
|   Status: Autocommit
|_  Salt: A].lXQoYQkG`/g:*b3sl
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2025-07-19T12:57:41+00:00; +3s from scanner time.
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:16:50
|   source ident: nmap
|   source host: 83EF8B59.F54A9131.FFFA6D49.IP
|_  error: Closing Link: vrxqesqvd[192.168.180.128] (Quit: vrxqesqvd)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
```



```
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_clock-skew: mean: 1h00m02s, deviation: 2h00m00s, median: 2s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-07-19T08:57:32-04:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT     ADDRESS
1   1.50 ms 192.168.180.133

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.41 seconds

┌──(kali㉿kali)-[~]
└─$ 
```