```
┌──(root㉿kali)-[~]
└─# sudo nmap -sn 192.168.224.0/24

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-07 11:49 EST
Stats: 0:00:06 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Scan
Parallel DNS resolution of 3 hosts. Timing: About 0.00% done
Stats: 0:00:09 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Scan
Parallel DNS resolution of 3 hosts. Timing: About 0.00% done
Nmap scan report for 192.168.224.1
Host is up (0.0014s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.224.132
Host is up (0.0021s latency).
MAC Address: 00:0C:29:0D:05:8C (VMware)
Nmap scan report for 192.168.224.254
Host is up (0.0015s latency).
MAC Address: 00:50:56:E8:5B:B7 (VMware)
Stats: 0:00:20 elapsed; 255 hosts completed (3 up), 255 undergoing Host Discovery
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.224.131
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 28.09 seconds
```

```
┌──(root㉿kali)-[~]
└─# cat firstscan.txt
# Nmap 7.94SVN scan initiated Thu Nov  7 11:56:17 2024 as: /usr/lib/nmap/nmap -A -oN firstscan.txt 192.168.224.132
Nmap scan report for 192.168.224.132
Host is up (0.00097s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 b5:38:66:0f:a1:ee:cd:41:69:3b:82:cf:ad:a1:f7:13 (DSA)
|   2048 58:5a:63:69:d0:da:dd:51:cc:c1:6e:00:fd:7e:61:d0 (RSA)
|   256 61:30:f3:55:1a:0d:de:c8:6a:59:5b:c9:9c:b4:92:04 (ECDSA)
|_  256 1f:65:c0:dd:15:e6:e4:21:f2:c1:9b:a3:b6:55:a0:45 (ED25519)
80/tcp   open  http        Apache httpd 2.4.7 ((Ubuntu))
|_http-title: Backnode
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-generator: Silex v2.2.7
| http-robots.txt: 4 disallowed entries
|_/old/ /test/ /TR2/ /Backnode_files/
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
3306/tcp open  mysql       MySQL (unauthorized)
6667/tcp open  irc         InspIRCd
| irc-info:
|   server: Admin.local
|   users: 1
|   servers: 1
|   chans: 0
|   lusers: 1
|   lservers: 0
|   source ident: nmap
|   source host: 192.168.224.131
|_  error: Closing link: (nmap@192.168.224.131) [Client exited]
MAC Address: 00:0C:29:0D:05:8C (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Hosts: TRUSTYOURSELF, Admin.local; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   NetBIOS computer name: TRUSTYOURSELF\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-11-08T04:56:48+10:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: -7h59m57s
|_nbstat: NetBIOS name: TRUSTYOURSELF, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

TRACEROUTE
```

```
┌──(root㉿kali)-[~]
└─# cat fullportcTCP.txt
# Nmap 7.94SVN scan initiated Thu Nov  7 11:57:18 2024 as: /usr/lib/nmap/nmap -sV -p- -oN fullportcTCP.txt 192.168.224.132
Nmap scan report for 192.168.224.132
Host is up (0.0021s latency).
Not shown: 65529 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http        Apache httpd 2.4.7 ((Ubuntu))
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)
3306/tcp open  mysql       MySQL (unauthorized)
6667/tcp open  irc         InspIRCd
MAC Address: 00:0C:29:0D:05:8C (VMware)
Service Info: Hosts: TRUSTYOURSELF, Admin.local; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Nov  7 11:57:53 2024 -- 1 IP address (1 host up) scanned in 35.03 seconds
```

```
┌──(root㉿kali)-[~]
└─# dirb http://192.168.224.132:80/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Nov  7 12:31:14 2024
URL_BASE: http://192.168.224.132:80/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.224.132:80/ ----
==> DIRECTORY: http://192.168.224.132:80/apache/
+ http://192.168.224.132:80/index.html (CODE:200|SIZE:36072)
+ http://192.168.224.132:80/info.php (CODE:200|SIZE:77280)
==> DIRECTORY: http://192.168.224.132:80/javascript/
==> DIRECTORY: http://192.168.224.132:80/old/
==> DIRECTORY: http://192.168.224.132:80/phpmyadmin/
+ http://192.168.224.132:80/robots.txt (CODE:200|SIZE:92)
+ http://192.168.224.132:80/server-status (CODE:403|SIZE:295)
==> DIRECTORY: http://192.168.224.132:80/test/
==> DIRECTORY: http://192.168.224.132:80/wordpress/
==> DIRECTORY: http://192.168.224.132:80/wp/

---- Entering directory: http://192.168.224.132:80/apache/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```