

## NMAP COMMANDS

```
(kali㉿Kali)-[~]
$ nmap -sn 10.6.6.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-12 04:47 UTC
Nmap scan report for 10.6.6.1
Host is up (0.00060s latency).
Nmap scan report for webgoat.vm (10.6.6.11)
Host is up (0.000057s latency).
Nmap scan report for juice-shop.vm (10.6.6.12)
Host is up (0.00072s latency).
Nmap scan report for dvwa.vm (10.6.6.13)
Host is up (0.00015s latency).
Nmap scan report for mutillidae.vm (10.6.6.14)
Host is up (0.00010s latency).
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.00099s latency).
Nmap scan report for 10.6.6.100
Host is up (0.000083s latency).
Nmap done: 256 IP addresses (7 hosts up) scanned in 15.34 seconds
```

```
(kali㉿Kali)-[~]
$ nmap -p21 -sV -A -T4 10.6.6.23
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-12 04:48 UTC
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.00066s latency).
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
|_ftp-syst: 772935 192.168.100.20 239.255.255.250
|_STAT: 192.168.100.20 239.255.255.250
|_FTP server status: 192.168.100.20 239.255.255.250
|_Connected to 10.6.6.1 192.168.100.20 192.168.100.255 BROWSER 243 Host Announ
|_Logged in as ftp 192.168.100.19 239.255.255.250
|_TYPE: ASCII 192.168.100.1 239.255.255.250
|_No session bandwidth limit 192.168.100.19 239.255.255.250
|_Session timeout in seconds is 300 239.255.255.250
|_Control connection is plain text 239.255.255.250
|_Data connections will be plain text 239.255.255.250
|_At session startup, client count was 3 239.255.255.250
|_vsFTPD 3.0.3 - secure, fast, stable 239.255.255.250
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230) 0.251 MDNS 103 Standard qu
|_rw-r--r-- 1 0 0 16 Aug 13 2021 file1.txt SSDP 174 M-SEARCH *
|_rw-r--r-- 1 0 0 16 Aug 13 2021 file2.txt SSDP 175 M-SEARCH *
|_rw-r--r-- 1 0 0 29 Aug 13 2021 file3.txt SSDP 175 M-SEARCH *
|_rw-r--r-- 1 0 0 26 Aug 13 2021 supersecretfile.txt SSDP 175 M-SEARCH *
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.29 seconds
```

```
(kali㉿Kali)-[~]
$ nmap -p21 -sV -A -T4 10.6.6.23
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-12 04:48 UTC
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.00066s latency).
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
|_ftp-syst: 772935 192.168.100.20 239.255.255.250
|_STAT: 192.168.100.20 239.255.255.250
|_FTP server status: 192.168.100.20 239.255.255.250
|_Connected to 10.6.6.1 192.168.100.20 192.168.100.255 BROWSER 243 Host Announ
|_Logged in as ftp 192.168.100.19 239.255.255.250
|_TYPE: ASCII 192.168.100.1 239.255.255.250
|_No session bandwidth limit 192.168.100.19 239.255.255.250
|_Session timeout in seconds is 300 239.255.255.250
|_Control connection is plain text 239.255.255.250
|_Data connections will be plain text 239.255.255.250
|_At session startup, client count was 3 239.255.255.250
|_vsFTPD 3.0.3 - secure, fast, stable 239.255.255.250
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230) 0.251 MDNS 103 Standard qu
|_rw-r--r-- 1 0 0 16 Aug 13 2021 file1.txt SSDP 174 M-SEARCH *
|_rw-r--r-- 1 0 0 16 Aug 13 2021 file2.txt SSDP 175 M-SEARCH *
|_rw-r--r-- 1 0 0 29 Aug 13 2021 file3.txt SSDP 175 M-SEARCH *
|_rw-r--r-- 1 0 0 26 Aug 13 2021 supersecretfile.txt SSDP 175 M-SEARCH *
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.29 seconds
```

```

(kali@kali)-[~]
└─$ nmap -A p139.p445 10.6.6.23
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-12 04:49 UTC
Failed to resolve "p139.p445".
Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.00020s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp           vsftpd 3.0.3
ftp-anon: Anonymous FTP login allowed (FTP code 230)
-rw-r--r--  1 0 77560 192.168.100.1 16 Aug 13 2021 file1.txt
-rw-r--r--  1 0 0 192.168.100.1 16 Aug 13 2021 file2.txt
-rw-r--r--  1 0 3883 192.168.100.1 29 Aug 13 2021 file3.txt
-rw-r--r--  1 0 8113 192.168.100.1 26 Aug 13 2021 supersecretfile.txt
ftp-syst:
STAT: 0 55 860168 192.168.100.1 239.255.255.255
FTP server status: 200
Connected to 10.6.6.1
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
At session startup, client count was 4
vsftpd 3.0.3 - secure, fast, stable
End of status
22/tcp    open  ssh           OpenSSH 7.9p1 Debian 10-deb10u2 (protocol 2.0)
ssh-hostkey:
2048 7f:9d:b7:59:47:74:0e:8e:90:83:24:2a:33:6c:06:30 (RSA)
256 52:a2:29:69:72:54:dc:47:ab:9f:0f:ce:b9:79:e1:c1 (ECDSA)
256 cd:4b:02:54:ea:60:df:a7:2d:a2:05:7f:e1:df:af:9d (ED25519)
53/tcp    open  domain        ISC BIND 9.11.5-P4-5.1+deb10u5 (Debian Linux)
dns-nsid:
bind.version: 9.11.5-P4-5.1+deb10u5-Debian
80/tcp    open  http          nginx 1.14.2
http-server-header: nginx/1.14.2
http-title: Home
139/tcp   open  netbios-ssn   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  Netbios-ssn   Samba smbd 4.9.5-Debian (workgroup: WORKGROUP)
Service Info: Host: GRAVEMIND; OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
smb-os-discovery:
OS: Windows 6.1 (Samba 4.9.5-Debian)
Computer name: gravemind
NetBIOS computer name: GRAVEMIND\x00
Domain name: \x00
FQDN: gravemind
System time: 2025-12-12T04:49:41+00:00
smb2-security-mode:
3:1:1:
Message signing enabled but not required
smb2-time:
date: 2025-12-12T04:49:42
start_date: N/A
smb-security-mode:
account_used: guest
authentication_level: user
challenge_response: supported
message_signing: disabled (dangerous, but default)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 19.98 seconds

```

```

(kali@kali)-[~]
└─$ smbclient //10.6.6.23/print$ -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ifconfig
ifconfig: command not found
smb: \> help
?          allinfo      altname      archive     backup
blocksize  cancel         case_sensitive cd          chmod
chown      close          del          deltree    dir
du         echo          exit        get         getfacl
geteas    hardlink      help        history     iosize
lcd       link          lock        lowercase  ls
l         mask          md          mget       mkdir
more      mput         newer       notify     open
posix     posix_encrypt posix_open  posix_mkdir posix_rmdir
posix_unlink posix_whoami  print      prompt     put
pwd       q            queue      quit       readlink
rd        recurse     reget      rename     reput
rm        rmdir      showacls   setea      setmode
scopy     stat       symlink    tar         tarmode
timeout   translate   unlock     volume     vuid
wdel      logon      listconnect showconnect tcon
tdis     tid        utimes     logoff     ..
!
smb: \> exit

```

```

(kali@kali)-[~]
$ smbclient //10.6.6.23/print$ -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ifconfig
ifconfig: command not found
smb: \> help
?          allinfo      altname      archive      backup
blocksize  cancel         case_sensitive cd            chmod
chown      close         del          deltree      dir
du         echo         exit         get          getfacl
geteas     hardlink      help         history      iosize
lcd        link          lock         lowercase    ls
l          mask         md           mget         mkdir
more       mput         newer        notify       open
posix      posix_encrypt posix_open   posix_mkdir  posix_rmdir
posix_unlink posix_whoami  print       prompt       put
pwd        q            queue        quit         readlink
rd         recurse      reget        rename       reput
rm         rmdir        showacls     setea        setmode
scopy      stat         symlink      tar          tarmode
timeout    translate    unlock       volume       void
wdel       logon        listconnect  showconnect  tcon
tdis       tid          utimes      logoff       ..
!
smb: \> exit

```

```

(kali@kali)-[~]
$ ifconfig
br-339414195aeb: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.5.5.1 netmask 255.255.255.0 broadcast 10.5.5.255
    inet6 fe80::42:97ff:fe8a:614 prefixlen 64 scopeid 0<20<link>
    ether 02:42:97:8a:06:14 txqueuelen 0 (Ethernet)
    RX packets 236 bytes 13646 (13.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 25 bytes 2940 (2.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

br-355ee7945a88: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.1 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::42:97ff:fe05:d1c3 prefixlen 64 scopeid 0<20<link>
    ether 02:42:97:05:d1:c3 txqueuelen 0 (Ethernet)
    RX packets 120 bytes 22953 (22.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 15 bytes 2360 (2.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

br-internal: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.6.6.1 netmask 255.255.255.0 broadcast 10.6.6.255
    inet6 fe80::42:2eff:fe5e:31b1 prefixlen 64 scopeid 0<20<link>
    ether 02:42:2e:5e:31:b1 txqueuelen 0 (Ethernet)
    RX packets 9225 bytes 1320918 (1.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 11500 bytes 797971 (779.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

docker0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    inet6 fe80::42:98ff:fef0:f532 prefixlen 64 scopeid 0<20<link>
    ether 02:42:98:f0:f5:32 txqueuelen 0 (Ethernet)
    RX packets 130 bytes 23831 (23.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 32 bytes 3941 (3.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.160 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::a00:27ff:fe4a:f36e prefixlen 64 scopeid 0<20<link>
    ether 08:00:27:4a:f3:6e txqueuelen 1000 (Ethernet)
    RX packets 134369 bytes 156962985 (149.6 MiB)
    RX errors 8319 dropped 0 overruns 0 frame 8319
    TX packets 49233 bytes 5829474 (5.5 MiB)
    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 4071 bytes 829515 (810.0 KiB)

```



```

vethbc6af20: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::24d8:f6ff:fe35:4475 prefixlen 64 scopeid 0<20<link>
    ether 26:d8:f6:35:44:75 txqueuelen 0 (Ethernet)
    RX packets 4155 bytes 1175904 (1.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 6440 bytes 425134 (415.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

vethc22ba44: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::a0bd:42ff:fe67:1fe5 prefixlen 64 scopeid 0<20<link>
    ether a2:bd:42:67:1f:e5 txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 34 bytes 4269 (4.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

vethd4ba8da: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet6 fe80::5055:dfff:fecc:2f23 prefixlen 64 scopeid 0<20<link>
    ether 52:55:df:cc:2f:23 txqueuelen 0 (Ethernet)
    RX packets 1009 bytes 54494 (53.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3295 bytes 173771 (169.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
└─$ ip route
default via 192.168.100.1 dev eth0 proto dhcp src 192.168.100.160 metric 100
10.5.5.0/24 dev br-339414195aeb proto kernel scope link src 10.5.5.1
10.6.6.0/24 dev br-internal proto kernel scope link src 10.6.6.1
172.17.0.0/16 dev docker0 proto kernel scope link src 172.17.0.1
192.168.0.0/24 dev br-355ee7945a88 proto kernel scope link src 192.168.0.1
192.168.100.0/24 dev eth0 proto kernel scope link src 192.168.100.160 metric 100

(kali@kali)-[~]
└─$ cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 192.168.100.1

(kali@kali)-[~]
└─$ sudo tcpdump -i eth0 -s 0 -w ladies.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C257 packets captured
257 packets received by filter
0 packets dropped by kernel

(kali@kali)-[~]
└─$ ls ladies.pcap
ladies.pcap

(kali@kali)-[~]
└─$ wireshark

```

## Wireshark(ladies.pcap)

Wireshark interface showing a packet capture of ladies.pcap. The packet list on the left shows various network protocols including ICMPv6, MDNS, SSDP, HTTP, ARP, and DNS. The packet details pane on the right shows the structure of a selected packet, including Ethernet II, Internet Protocol Version 6, and Internet Control Message Protocol (ICMPv6). The packet bytes pane at the bottom shows the raw hex and ASCII data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::1	ff02::1	ICMPv6	86	Router Advertisement from a4:a4:6b:a2:45:7c
2	0.248649	192.168.100.91	224.0.0.251	MDNS	87	Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" question
3	0.242388	fe80::e85f:b66b:3fe	ff02::fb	MDNS	187	Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" question
4	21.771372	192.168.100.91	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
5	25.028648	192.168.100.91	192.168.100.255	UDP	86	57621 - 57621 Len=44
6	55.037750	192.168.100.91	192.168.100.255	SSDP	174	M-SEARCH * HTTP/1.1
7	55.043903	192.168.100.1	239.255.255.250	SSDP	174	M-SEARCH * HTTP/1.1
8	55.248113	192.168.100.1	239.255.255.250	SSDP	174	M-SEARCH * HTTP/1.1
9	55.560168	192.168.100.1	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
10	55.862936	192.168.100.1	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
11	65.504125	70:08:10:73:87:19	Broadcast	ARP	60	Who has 192.168.100.1? Tell 192.168.100.20
12	65.830964	192.168.100.20	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
13	65.830965	192.168.100.20	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
14	67.468427	HuaweiTe.a2:45:7c	Broadcast	ARP	60	Who has 192.168.100.91? Tell 192.168.100.1
15	68.772935	192.168.100.20	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
16	68.798867	192.168.100.20	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
17	70.012060	192.168.100.20	192.168.100.255	BROWSER	243	Host Announcement LTMPA064, Workstation, Server, NT Workstation
18	72.854274	192.168.100.19	239.255.255.250	SSDP	415	NOTIFY * HTTP/1.1
19	72.854274	192.168.100.1	239.255.255.250	SSDP	174	M-SEARCH * HTTP/1.1
20	72.854274	192.168.100.19	239.255.255.250	SSDP	401	NOTIFY * HTTP/1.1
21	72.854274	192.168.100.19	239.255.255.250	SSDP	353	NOTIFY * HTTP/1.1
22	72.854275	192.168.100.19	239.255.255.250	SSDP	362	NOTIFY * HTTP/1.1
23	72.854275	192.168.100.19	239.255.255.250	SSDP	415	NOTIFY * HTTP/1.1
24	72.854275	192.168.100.19	239.255.255.250	SSDP	401	NOTIFY * HTTP/1.1
25	72.858678	fe80::1aef:da4f:fe4	ff02::fb	MDNS	123	Standard query response 0x0000 PTR 55* Crystal UHD_airplay._tcp.local
26	72.869269	192.168.100.19	224.0.0.251	MDNS	103	Standard query response 0x0000 PTR 55* Crystal UHD_airplay._tcp.local
27	73.184118	192.168.100.1	239.255.255.250	SSDP	174	M-SEARCH * HTTP/1.1
28	73.854331	192.168.100.1	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1

Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0  
 Ethernet II, Src: HuaweiTe.a2:45:7c (a4:a4:6b:a2:45:7c), Dst: IPv6multicast\_01 (33:33:00:00:00:01)  
 Internet Protocol Version 6, Src: fe80::1, Dst: ff02::1  
 Internet Control Message Protocol v6

Bytes 12-13: Type (eth.type)

Packets: 257 · Displayed: 257 (100.0%)

Profile: Default

## SCAPY COMMANDS

```
File Actions Edit View Help

(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(kali@kali)-[/home/kali]
# scapy
INFO: Can't import PyX. Won't be able to use psdump() or pdfdump().

      aSPY//YASa
    apyyyyCY/////////YCa
  sY////////YSpCs  scpCY//Pp
ayp ayyyyyySCP//Pp      syY//C
AYAsAYYYYYYYY///Ps      cY//S
      pCCCY//p      cSSps y//Y
    SPPPP///a      pP///AC//Y
      A//A      cyP///C
      p///Ac      sC///a
      P///YCpc      A//A
    sccccp///pSP//p      p//Y
  sY/////////y caa      S//P
    cayCyayP//Ya      pY/Ya
    sY/PsY///YCc      aC//Yp
      sc  sccaCY//PCypaapyCP//YSs
        spCPY/////////YPSps
          ccaacs

| Welcome to Scapy
| Version 2.5.0
| https://github.com/secdev/scapy
| Have fun!
| Craft packets like it is your last
| day on earth.
| -- Lao-Tze

using IPython 8.14.0

>>> ls()
AD_AND_OR : None
AD_KDCIssued : None
AH : AH
AKMSuite : AKM suite
ARP : ARP
ASN1P_INTEGER : None
ASN1P_OID : None
ASN1P_PRIVSEQ : None
ASN1_Packet : None
ASN1_Packet : None
ATT_Error_Response : Error Response
ATT_Exchange_MTU_Request : Exchange MTU Request
ATT_Exchange_MTU_Response : Exchange MTU Response
ATT_Execute_Write_Request : Execute Write Request
ATT_Execute_Write_Response : Execute Write Response
ATT_Find_By_Type_Value_Request : Find By Type Value Request
ATT_Find_By_Type_Value_Response : Find By Type Value Response
ATT_Find_Information_Request : Find Information Request
ATT_Find_Information_Response : Find Information Response
ATT_Handle : ATT Short Handle
ATT_Handle_UUID128 : ATT Handle (UUID 128)
ATT_Handle_Value_Indication : Handle Value Indication
ATT_Handle_Value_Notification : Handle Value Notification
ATT_Handle_Variable : None
ATT_Hdr : ATT header
ATT_Prepare_Write_Request : Prepare Write Request

>>> ls(IP)
version : BitField (4 bits) bit-level scope = ('4')
ihl : BitField (4 bits) bit-level scope = ('None') len: 100
tos : XByteField = ('0')
len : ShortField = ('None')
id : ShortField = ('1')
flags : FlagsField = ('<Flag 0 (>')
frag : BitField (13 bits) = ('0')
ttl : ByteField = ('64')
proto : ByteEnumField = ('0')
chksum : XShortField bit-level scope = ('None')
src : SourceIPField bit-level scope = ('None') with 2014x bytes
dst : DestIPField = ('None')
options : PacketListField = ('[]')
```

```
>>> ls(IP)
version      : BitField (4 bits)      = ('4')
ihl          : BitField (4 bits)      = ('None')
tos          : XByteField              = ('0')
len          : ShortField              = ('None')
id           : ShortField              = ('1')
flags        : FlagsField              = ('<Flag 0 (>)')
frag         : BitField (13 bits)     = ('0')
ttl          : ByteField               = ('64')
proto        : ByteEnumField           = ('0')
chksum       : XShortField             = ('None')
src          : SourceIPField           = ('None')
dst          : DestIPField             = ('None')
options      : PacketListField        = ('[]')
```

```
>>> sniff()
^C<Sniffed: TCP:0 UDP:64 ICMP:8 Other:6>
>>> paro=
>>> paro.summary()
Ether / IP / UDP 192.168.100.19:47544 > 239.255.255.250:15600 / Raw
Ether / ARP who has 192.168.100.1 says 192.168.100.160
Ether / ARP is at a4:a4:6b:a2:45:7c says 192.168.100.1 / Padding
Ether / IP / UDP 192.168.100.19:42335 > 192.168.100.255:15600 / Raw
Ether / IP / UDP 192.168.100.19:46798 > 239.255.255.250:15600 / Raw
Ether / IP / UDP 192.168.100.19:34980 > 192.168.100.255:15600 / Raw
Ether / IPv6 / UDP / DNS Qry "b'proxy2.local.'"
Ether / IPv6 / UDP / DNS Qry "b'proxy2.local.'"
Ether / IP / UDP 192.168.100.20:61909 > 224.0.0.252:5355 / LLMNRQuery who has 'proxy2.'
Ether / IP / UDP 192.168.100.20:62386 > 224.0.0.252:5355 / LLMNRQuery who has 'proxy2.'
Ether / IP / UDP / NBNSHeader / NBNSQueryRequest who has '\\PROXY2'
Ether / IP / UDP / DNS Qry "b'proxy2.local.'"
Ether / IP / UDP / DNS Qry "b'proxy2.local.'"
Ether / IPv6 / UDP fe80::49be:9502:261e:7a61:61909 > ff02::1:3:5355 / LLMNRQuery who has 'proxy2.'
Ether / IPv6 / UDP fe80::49be:9502:261e:7a61:62386 > ff02::1:3:5355 / LLMNRQuery who has 'proxy2.'
Ether / IPv6 / UDP fe80::49be:9502:261e:7a61:61909 > ff02::1:3:5355 / LLMNRQuery who has 'proxy2.'
Ether / IPv6 / UDP fe80::49be:9502:261e:7a61:62386 > ff02::1:3:5355 / LLMNRQuery who has 'proxy2.'
Ether / IP / UDP 192.168.100.20:62386 > 224.0.0.252:5355 / LLMNRQuery who has 'proxy2.'
Ether / IP / UDP 192.168.100.20:61909 > 224.0.0.252:5355 / LLMNRQuery who has 'proxy2.'
Ether / IP / UDP / NBNSHeader / NBNSQueryRequest who has '\\PROXY2'
Ether / IPv6 / UDP / DNS Qry "b'proxy2.local.'"
Ether / IP / UDP / DNS Qry "b'proxy2.local.'"
Ether / IPv6 / UDP / DNS Qry "b'proxy2.local.'"
Ether / IP / UDP / NBNSHeader / NBNSQueryRequest who has '\\PROXY2'
Ether / IP / UDP 192.168.100.19:45633 > 239.255.255.250:15600 / Raw
Ether / IP / UDP / DNS Ans "b'LENOVOs-iPhone-2.local.'"
Ether / IP / UDP / DNS Qry "b'_companion-link._tcp.local.'"
Ether / 192.168.100.151 > 224.0.0.22 igmp / Raw / Padding
Ether / fe80::811:175:c426:8179 > ff02::16 (0) / IPv6ExtHdrHopByHop / ICMPv6MLReport2
Ether / IPv6 / UDP / DNS Ans "b'LENOVOs-iPhone-2.local.'"
Ether / IPv6 / UDP / DNS Qry "b'_companion-link._tcp.local.'"
Ether / IP / UDP / DNS Qry "b'LENOVO\xe2\x80\x99s iPhone (2)._rdlink._tcp.local.'"
Ether / IPv6 / UDP / DNS Qry "b'LENOVO\xe2\x80\x99s iPhone (2)._rdlink._tcp.local.'"
Ether / IPv6 / UDP / DNS Qry "b'LENOVO\xe2\x80\x99s iPhone (2)._rdlink._tcp.local.'"
Ether / IP / UDP 192.168.100.19:54374 > 192.168.100.255:15600 / Raw
Ether / IP / UDP / DNS Qry "b'LENOVO\xe2\x80\x99s iPhone (2)._rdlink._tcp.local.'"
Ether / IP / UDP / DNS Ans "b'LENOVOs-iPhone-2.local.'"
Ether / IP / UDP / DNS Qry "b'_companion-link._tcp.local.'"
Ether / IPv6 / UDP / DNS Qry "b'LENOVO\xe2\x80\x99s iPhone (2)._rdlink._tcp.local.'"
Ether / IPv6 / UDP / DNS Ans "b'_companion-link._tcp.local.'"
Ether / IP / UDP / DNS Ans "[b'rpBA=0F:B3:2F:FB:6B:48', b'rpVr=440.10', b'rpAD=c3749a9ecca9']]"
Ether / IPv6 / UDP / DNS Ans "[b'rpBA=0F:B3:2F:FB:6B:48', b'rpVr=440.10', b'rpAD=c3749a9ecca9']]"
Ether / IP / UDP / DNS Ans "[b'rpBA=0F:B3:2F:FB:6B:48', b'rpVr=440.10', b'rpAD=c3749a9ecca9']]"
Ether / IPv6 / UDP / DNS Ans "[b'rpBA=0F:B3:2F:FB:6B:48', b'rpVr=440.10', b'rpAD=c3749a9ecca9']]"
Ether / IP / UDP / DNS Qry "b'google.com.'"

```



```

File Actions Edit View Help
>>> sniff(iface="br-internal")
^C<Sniffed: TCP:91 UDP:26 ICMP:0 Other:2>
>>> paro2=_
>>> paro2.summary()
Ether / IP / UDP / DNS Qry "b'.'"
Ether / IP / UDP / DNS Qry "b'.'"
Ether / IP / UDP / DNS Qry "b'.'"
Ether / IP / UDP / DNS Qry "b'.'"
Ether / IP / UDP / DNS Qry "b'.'"
Ether / IP / UDP / DNS Qry "b'.'"
Ether / IP / UDP / DNS Qry "b'.'"
Ether / IP / UDP / DNS Qry "b'.'"
Ether / IP / UDP / DNS Qry "b'.'"
Ether / IP / UDP / DNS Qry "b'.'"
Ether / IP / UDP / DNS Qry "b'.'"
Ether / IP / UDP / DNS Qry "b'.'"
Ether / IP / UDP / DNS Qry "b'.'"
Ether / IP / UDP / DNS Qry "b'.'"
Ether / IP / UDP / DNS Qry "b'.'"
Ether / ARP who has 10.6.6.1 says 10.6.6.23
Ether / ARP is at 02:42:2e:5e:31:b1 says 10.6.6.1
Ether / IP / UDP / DNS Qry "b'.'"
Ether / IP / UDP / DNS Qry "b'.'"
Ether / IP / UDP / DNS Qry "b'.'"
Ether / IP / UDP / DNS Qry "b'.'"
Ether / IP / UDP / DNS Qry "b'.'"
Ether / IP / UDP / DNS Qry "b'.'"
Ether / IP / UDP / DNS Qry "b'.'"
Ether / IP / UDP / DNS Qry "b'.'"
Ether / IP / UDP / DNS Qry "b'.'"
Ether / IP / UDP / DNS Qry "b'.'"
Ether / IP / UDP / DNS Qry "b'.'"
Ether / IP / UDP / DNS Qry "b'.'"
Ether / IP / TCP 10.6.6.1:37514 > 10.6.6.23:http S
Ether / IP / TCP 10.6.6.23:http > 10.6.6.1:37514 SA
Ether / IP / TCP 10.6.6.1:37514 > 10.6.6.23:http A
Ether / IP / TCP 10.6.6.1:37514 > 10.6.6.23:http PA / Raw
Ether / IP / TCP 10.6.6.23:http > 10.6.6.1:37514 A
Ether / IP / TCP 10.6.6.23:http > 10.6.6.1:37514 PA / Raw
Ether / IP / TCP 10.6.6.1:37514 > 10.6.6.23:http A
Ether / IP / TCP 10.6.6.23:http > 10.6.6.1:37514 PA / Raw
Ether / IP / TCP 10.6.6.1:37514 > 10.6.6.23:http A
Ether / IP / TCP 10.6.6.23:http > 10.6.6.1:37514 PA / Raw
Ether / IP / TCP 10.6.6.1:37518 > 10.6.6.23:http S
Ether / IP / TCP 10.6.6.23:http > 10.6.6.1:37518 SA
Ether / IP / TCP 10.6.6.1:37518 > 10.6.6.23:http A
Ether / IP / TCP 10.6.6.23:http > 10.6.6.1:37518 PA / Raw
Ether / IP / TCP 10.6.6.1:37518 > 10.6.6.23:http A
Ether / IP / TCP 10.6.6.23:http > 10.6.6.1:37518 PA / Raw
Ether / IP / TCP 10.6.6.1:37518 > 10.6.6.23:http A
Ether / IP / TCP 10.6.6.23:http > 10.6.6.1:37518 PA / Raw

```

```

>>> sniff(iface="br-internal",filter = "icmp", count = 3)
^C<Sniffed: TCP:0 UDP:0 ICMP:0 Other:0>
>>> paro3=_
>>> paro3.summary()
>>> sniff(iface="br-internal",filter = "icmp", count = 3)
^C<Sniffed: TCP:0 UDP:0 ICMP:0 Other:0>
>>> sniff(iface="br-internal",filter = "icmp", count = 10)
^C<Sniffed: TCP:0 UDP:0 ICMP:0 Other:0>
>>> sniff(iface="br-internal",filter = "icmp", count = 5)
<Sniffed: TCP:0 UDP:0 ICMP:5 Other:0>
>>> paro3=_
>>> paro3.summary()
Ether / IP / ICMP 10.6.6.1 > 10.6.6.23 echo-request 0 / Raw
Ether / IP / ICMP 10.6.6.23 > 10.6.6.1 echo-reply 0 / Raw
Ether / IP / ICMP 10.6.6.1 > 10.6.6.23 echo-request 0 / Raw
Ether / IP / ICMP 10.6.6.23 > 10.6.6.1 echo-reply 0 / Raw
Ether / IP / ICMP 10.6.6.1 > 10.6.6.23 echo-request 0 / Raw
>>> paro3.nsummary()
0000 Ether / IP / ICMP 10.6.6.1 > 10.6.6.23 echo-request 0 / Raw
0001 Ether / IP / ICMP 10.6.6.23 > 10.6.6.1 echo-reply 0 / Raw
0002 Ether / IP / ICMP 10.6.6.1 > 10.6.6.23 echo-request 0 / Raw
0003 Ether / IP / ICMP 10.6.6.23 > 10.6.6.1 echo-reply 0 / Raw
0004 Ether / IP / ICMP 10.6.6.1 > 10.6.6.23 echo-request 0 / Raw
>>> paro3[3]
<Ether dst=02:42:2e:5e:31:b1 src=02:42:0a:06:06:17 type=IPv4 |<IP version=4 ihl=5 tos=0x0 len=84 id=29787 flags= frag=0 ttl=64 proto=icmp checksum=0xe62a src=10.6.6.23 dst=10.6.6.1 |<ICMP type=echo-reply code=0 checksum=0xe94 id=0xec47 seq=0x2 unused='' |<Raw load='0;i\x00\x00\x00\x006M\x06\x00\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !"#%&'()*+,-./01234567' |>>>>
>>> paro3[2]
<Ether dst=02:42:0a:06:06:17 src=02:42:2e:5e:31:b1 type=IPv4 |<IP version=4 ihl=5 tos=0x0 len=84 id=54255 flags=DF frag=0 ttl=64 proto=icmp checksum=0x4696 src=10.6.6.1 dst=10.6.6.23 |<ICMP type=echo-request code=0 checksum=0x694 id=0xec47 seq=0x2 unused='' |<Raw load='0;i\x00\x00\x00\x006M\x06\x00\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !"#%&'()*+,-./01234567' |>>>>
>>> wrpcap("capture1.pcap", paro3)
>>>

```

## Wireshark(capture1.pcap)

The image shows the Wireshark network protocol analyzer interface. The main display area shows a list of five captured packets, all of which are ICMP Echo (ping) requests and replies. The packets are filtered by the display filter 'No.' and are displayed in a table with columns for No., Time, Source, Destination, Protocol, and Length. The details pane on the right shows the structure of the first packet, which is an ICMP Echo (ping) request. The packet structure is shown in a tree view, with the following details:

- Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
- Ethernet II, Src: 02:42:2e:5e:31:b1 (02:42:2e:5e:31:b1), Dst: 02:42:0a:06:06:06
- Internet Protocol Version 4, Src: 10.6.6.1, Dst: 10.6.6.23
- Internet Control Message Protocol

The packet data is displayed in hexadecimal and ASCII format. The hexadecimal data is shown in the top pane, and the ASCII data is shown in the bottom pane. The ASCII data is a representation of the packet's contents, showing the ICMP Echo (ping) request structure.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.6.6.1	10.6.6.23	ICMP	98	Echo (ping) request id=0xec47, seq=1/256, ttl=64 (reply in 2)
2	0.000242	10.6.6.23	10.6.6.1	ICMP	98	Echo (ping) reply id=0xec47, seq=1/256, ttl=64 (request in 1)
3	1.001690	10.6.6.1	10.6.6.23	ICMP	98	Echo (ping) request id=0xec47, seq=2/512, ttl=64 (reply in 4)
4	1.001733	10.6.6.23	10.6.6.1	ICMP	98	Echo (ping) reply id=0xec47, seq=2/512, ttl=64 (request in 3)
5	2.005585	10.6.6.1	10.6.6.23	ICMP	98	Echo (ping) request id=0xec47, seq=3/768, ttl=64 (no response found!)

Packets: 5 - Displayed: 5 (100.0%) Profile: Default