NETWORK SECURITY: **LAB 1**

Members:

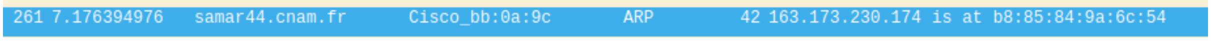
- *Medyan Mehi Eldine*

Outline

1. Capture and analyze protocols

Part 1: ARP

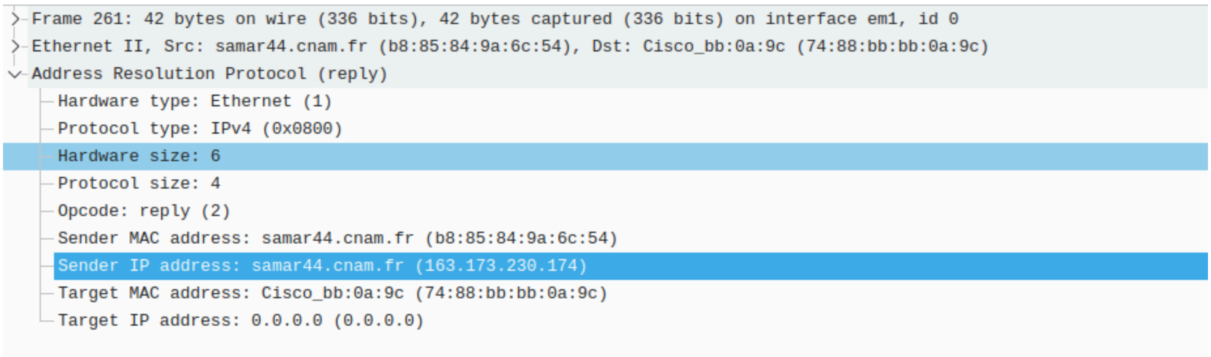
First we choose a packet that is not a broadcast, since we are receiving various broadcasts from different devices. And the packets that have a response are always have our device as either the sender or the receiver, we will analyze the following packet:



```
261 7.176394976    samar44.cnam.fr      Cisco_bb:0a:9c       ARP        42 163.173.230.174 is at b8:85:84:9a:6c:54
```

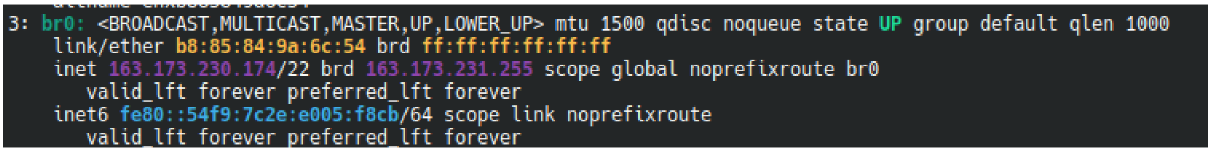
By opening the ARP section, we can find the following relevant information:

1. Our hostname: samar44.cnam.fr from sender IP **163.173.230.174**
2. Our MAC address: b8:85:84:9a:6c:54 from the sender mac
3. Exchanged data is our host replying with our MAC address to the router that was looking for it.
4. The source is **samara44.cnam.fr (b8:85:84:9a:6c:54)** and the destination is **Cisco_bb (74:88:bb:bb:0a:9c)**



```
> Frame 261: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface em1, id 0
> Ethernet II, Src: samar44.cnam.fr (b8:85:84:9a:6c:54), Dst: Cisco_bb:0a:9c (74:88:bb:bb:0a:9c)
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: samar44.cnam.fr (b8:85:84:9a:6c:54)
    Sender IP address: samar44.cnam.fr (163.173.230.174)
    Target MAC address: Cisco_bb:0a:9c (74:88:bb:bb:0a:9c)
    Target IP address: 0.0.0.0 (0.0.0.0)
```

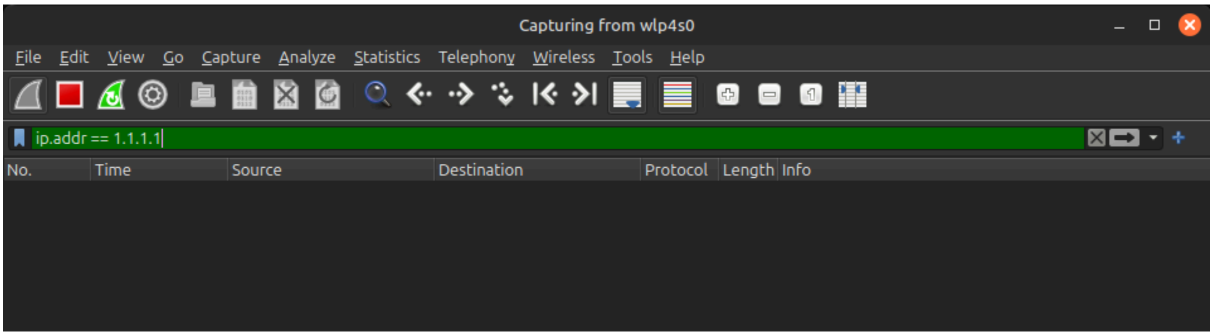
We can confirm the hostname name by running the command **ifconfig -a** and finding our corresponding private IP address which is **163.173.230.174**



```
3: br0: <BROADCAST,MULTICAST,MASTER,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether b8:85:84:9a:6c:54 brd ff:ff:ff:ff:ff:ff
    inet 163.173.230.174/22 brd 163.173.231.255 scope global noprefixroute br0
       valid_lft forever preferred_lft forever
    inet6 fe80::54f9:7c2e:e005:f8cb/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

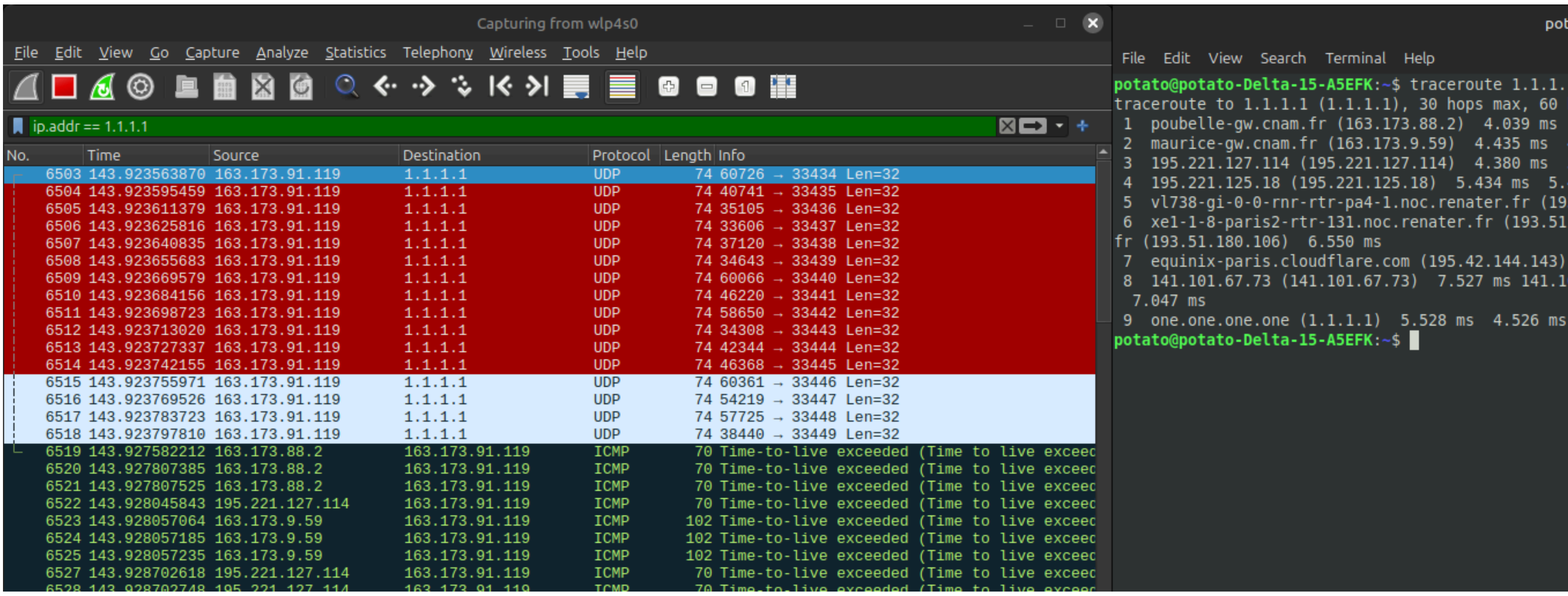
Part 2: Traceroute

To make things easier in wireshark, first we set a filter to search for the ip address 1.1.1.1 in the contents of each packet, and as shown there's no packets being sent currently:


Capturing from wlp4s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 1.1.1.1
No.    Time    Source    Destination    Protocol  Length  Info
```

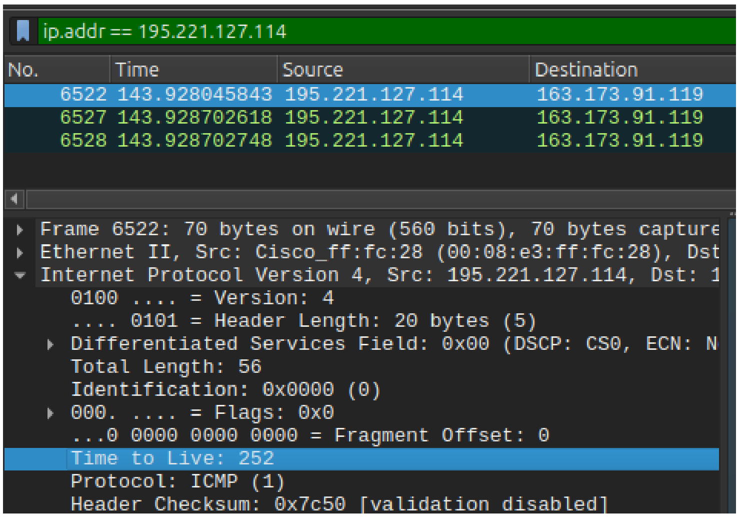
Starting a **traceroute 1.1.1.1** in the terminal, we get the following packets:


Capturing from wlp4s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
File Edit View Search Terminal Help

```
ip.addr == 1.1.1.1
No.  Time           Source           Destination      Protocol  Length Info
6503 143.923563870 163.173.91.119  1.1.1.1          UDP        74 60726 → 33434 Len=32
6504 143.923595459 163.173.91.119  1.1.1.1          UDP        74 40741 → 33435 Len=32
6505 143.923611379 163.173.91.119  1.1.1.1          UDP        74 35105 → 33436 Len=32
6506 143.923625816 163.173.91.119  1.1.1.1          UDP        74 33606 → 33437 Len=32
6507 143.923640835 163.173.91.119  1.1.1.1          UDP        74 37120 → 33438 Len=32
6508 143.923655683 163.173.91.119  1.1.1.1          UDP        74 34643 → 33439 Len=32
6509 143.923669579 163.173.91.119  1.1.1.1          UDP        74 60066 → 33440 Len=32
6510 143.923684156 163.173.91.119  1.1.1.1          UDP        74 46220 → 33441 Len=32
6511 143.923698723 163.173.91.119  1.1.1.1          UDP        74 58650 → 33442 Len=32
6512 143.923713020 163.173.91.119  1.1.1.1          UDP        74 34308 → 33443 Len=32
6513 143.923727337 163.173.91.119  1.1.1.1          UDP        74 42344 → 33444 Len=32
6514 143.923742155 163.173.91.119  1.1.1.1          UDP        74 46368 → 33445 Len=32
6515 143.923755971 163.173.91.119  1.1.1.1          UDP        74 60361 → 33446 Len=32
6516 143.923769526 163.173.91.119  1.1.1.1          UDP        74 54219 → 33447 Len=32
6517 143.923783723 163.173.91.119  1.1.1.1          UDP        74 57725 → 33448 Len=32
6518 143.923797810 163.173.91.119  1.1.1.1          UDP        74 38440 → 33449 Len=32
6519 143.927582212 163.173.88.2    163.173.91.119   ICMP       70 Time-to-live exceeded (Time to live exceed
6520 143.927807385 163.173.88.2    163.173.91.119   ICMP       70 Time-to-live exceeded (Time to live exceed
6521 143.927807525 163.173.88.2    163.173.91.119   ICMP       70 Time-to-live exceeded (Time to live exceed
6522 143.928045843 195.221.127.114 163.173.91.119   ICMP       70 Time-to-live exceeded (Time to live exceed
6523 143.928057064 163.173.9.59    163.173.91.119   ICMP      102 Time-to-live exceeded (Time to live exceed
6524 143.928057185 163.173.9.59    163.173.91.119   ICMP      102 Time-to-live exceeded (Time to live exceed
6525 143.928057235 163.173.9.59    163.173.91.119   ICMP      102 Time-to-live exceeded (Time to live exceed
6527 143.928702618 195.221.127.114 163.173.91.119   ICMP       70 Time-to-live exceeded (Time to live exceed
6528 143.928702748 195.221.127.114 163.173.91.119   ICMP       70 Time-to-live exceeded (Time to live exceed
```

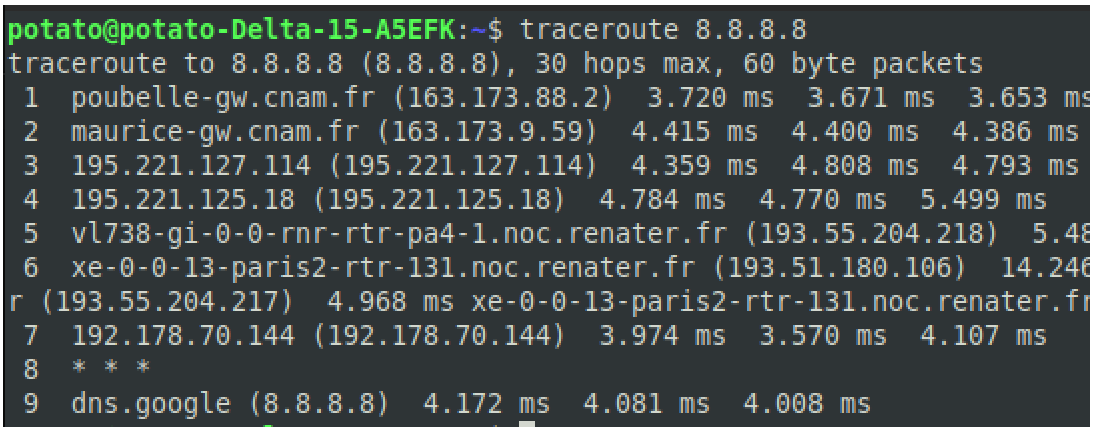
```
potato@potato-Delta-15-A5EFK:~$ traceroute 1.1.1.
traceroute to 1.1.1.1 (1.1.1.1), 30 hops max, 60
 1  poubelle-gw.cnam.fr (163.173.88.2)  4.039 ms
 2  maurice-gw.cnam.fr (163.173.9.59)  4.435 ms
 3  195.221.127.114 (195.221.127.114)  4.380 ms
 4  195.221.125.18 (195.221.125.18)  5.434 ms  5.
 5  vl738-gi-0-0-rnr-rtr-pa4-1.noc.renater.fr (19
 6  xe1-1-8-paris2-rtr-131.noc.renater.fr (193.51
fr (193.51.180.106)  6.550 ms
 7  equinix-paris.cloudflare.com (195.42.144.143)
 8  141.101.67.73 (141.101.67.73)  7.527 ms 141.1
  7.047 ms
 9  one.one.one.one (1.1.1.1)  5.528 ms  4.526 ms
potato@potato-Delta-15-A5EFK:~$
```

Which means that traceroute uses a mix of **UDP and ICMP protocols.** And to see the value of TTL on the third hop, we simply filter for the third hop address, which is 195.221.127.114 in our case, and we can find in the IPv4 section the time to live field equal to **252**



```
ip.addr == 195.221.127.114
No.     Time          Source           Destination
   6522 143.928045843 195.221.127.114  163.173.91.119
   6527 143.928702618 195.221.127.114  163.173.91.119
   6528 143.928702748 195.221.127.114  163.173.91.119

▸ Frame 6522: 70 bytes on wire (560 bits), 70 bytes capture
▸ Ethernet II, Src: Cisco_ff:fc:28 (00:08:e3:ff:fc:28), Dst
▾ Internet Protocol Version 4, Src: 195.221.127.114, Dst: 1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: N
    Total Length: 56
    Identification: 0x0000 (0)
  ▸ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 252
    Protocol: ICMP (1)
    Header Checksum: 0x7c50 [validation disabled]
```

To get some starts i had to use the google address 8.8.8.8 instead:



```
potato@potato-Delta-15-A5EFK:~$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  poubelle-gw.cnam.fr (163.173.88.2)  3.720 ms  3.671 ms  3.653 ms
 2  maurice-gw.cnam.fr (163.173.9.59)  4.415 ms  4.400 ms  4.386 ms
 3  195.221.127.114 (195.221.127.114)  4.359 ms  4.808 ms  4.793 ms
 4  195.221.125.18 (195.221.125.18)  4.784 ms  4.770 ms  5.499 ms
 5  vl738-gi-0-0-rnr-rtr-pa4-1.noc.renater.fr (193.55.204.218)  5.48
 6  xe-0-0-13-paris2-rtr-131.noc.renater.fr (193.51.180.106)  14.246
r (193.55.204.217)  4.968 ms xe-0-0-13-paris2-rtr-131.noc.renater.fr
 7  192.178.70.144 (192.178.70.144)  3.974 ms  3.570 ms  4.107 ms
 8  * * *
 9  dns.google (8.8.8.8)  4.172 ms  4.081 ms  4.008 ms
```

In wireshark however, there is no packet that contains 8.8.8.8 in its message with IP not found in the traceroute, so It is either we reached a timeout or we did not receive a reply from a hop.

2. Network scanning

Host enumeration and Service Discovery

By using **ifconfig -a** i can get information about the network interfaces used on my machine:

```
user3652@user3652:~$ ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.11.5  netmask 255.255.255.0  broadcast 192.168.11.255
        ether 96:d4:85:36:a8:a1  txqueuelen 0  (Ethernet)
        RX packets 24549  bytes 1462474 (1.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 30064  bytes 5028919 (5.0 MB)
        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 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 155980  bytes 10052331 (10.0 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 155980  bytes 10052331 (10.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

```

We have an ethernet interface **eth0** and **lo** which is used by the machine to communicate with itself.The subnet mask for eth0 is 255.255.255.0 indicating the subnet to be **/24**

Using nmap to search this network **192.168.11.0/24** we get 5 hosts and their services open ports:

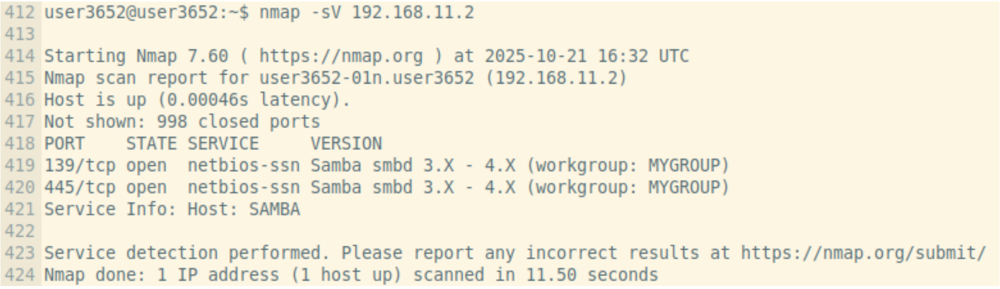
```
user3652@user3652:~$ nmap 192.168.11.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2025-10-21 13:58 UTC
Nmap scan report for 100dell7060-01.esgt.cnam.fr (192.168.11.1)
Host is up (0.0012s latency).
All 1000 scanned ports on 100dell7060-01.esgt.cnam.fr (192.168.11.1) are closed

Nmap scan report for user3652-01n.user3652 (192.168.11.2)
Host is up (0.0012s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap scan report for user3652-secret_service.user3652 (192.168.11.3)
Host is up (0.0011s latency).
All 1000 scanned ports on user3652-secret_service.user3652 (192.168.11.3) are closed

Nmap scan report for user3652-service.user3652 (192.168.11.4)
Host is up (0.0012s latency).
All 1000 scanned ports on user3652-service.user3652 (192.168.11.4) are closed

Nmap scan report for user3652 (192.168.11.5)
Host is up (0.0012s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (5 hosts up) scanned in 3.41 seconds
```

We have 5 hosts, we will go through them one by one:

- **192.168.11.1:** By convention the first address is assigned for the router, further proof to that is that it does not have any open ports, i.e. no services.
- **192.168.11.2:** This machine has 2 services open: **139/tcp netbios-ssn, 445/tcp** microsoft-ds. We will discuss these services more later on.
- **192.168.11.3:** No open ports for this machine.
- **192.168.11.4:** Despite not having any open ports, there is a **dbm service on port 2345** we will find later.
- **192.168.11.5:** We know this is the address of our machine from previously in **ifconfig**, and to support that we have an **ssh** service running which allow us to connect to this virtual network.

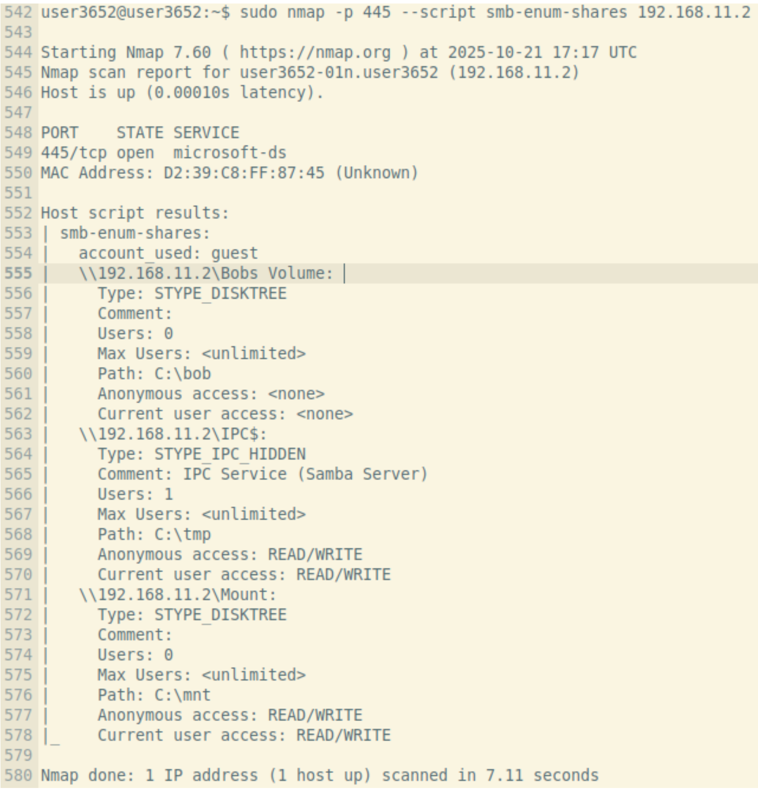
Analysing 192.168.11.2 and finding more ports:

Getting the version number of the services running on this host, we get that this is am **smbd** service which allows us to access the host machine files remotely.



```
user3652@user3652:~$ nmap -sV 192.168.11.2

Starting Nmap 7.60 ( https://nmap.org ) at 2025-10-21 16:32 UTC
Nmap scan report for user3652-01n.user3652 (192.168.11.2)
Host is up (0.00046s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE     VERSION
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: MYGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: MYGROUP)
Service Info: Host: SAMBA

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 11.50 seconds
```

By using the **smb-enum-shares** script for nmap, we can see the shared folders using this service:



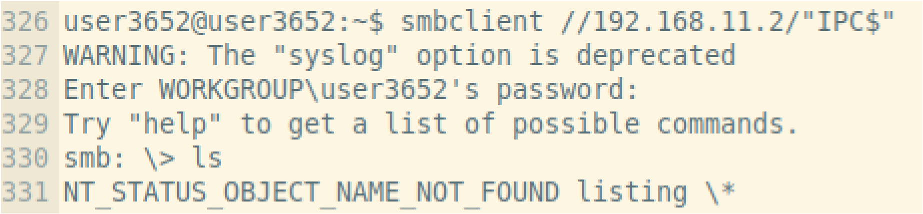
```
user3652@user3652:~$ sudo nmap -p 445 --script smb-enum-shares 192.168.11.2

Starting Nmap 7.60 ( https://nmap.org ) at 2025-10-21 17:17 UTC
Nmap scan report for user3652-01n.user3652 (192.168.11.2)
Host is up (0.00010s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: D2:39:C8:FF:87:45 (Unknown)

Host script results:
| smb-enum-shares:
|   account_used: guest
|   \\192.168.11.2\Bobs Volume:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\bob
|     Anonymous access: <none>
|     Current user access: <none>
|   \\192.168.11.2\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (Samba Server)
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\192.168.11.2\Mount:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\mnt
|     Anonymous access: READ/WRITE
|_    Current user access: READ/WRITE

Nmap done: 1 IP address (1 host up) scanned in 7.11 seconds
```

We have 3 volumes:

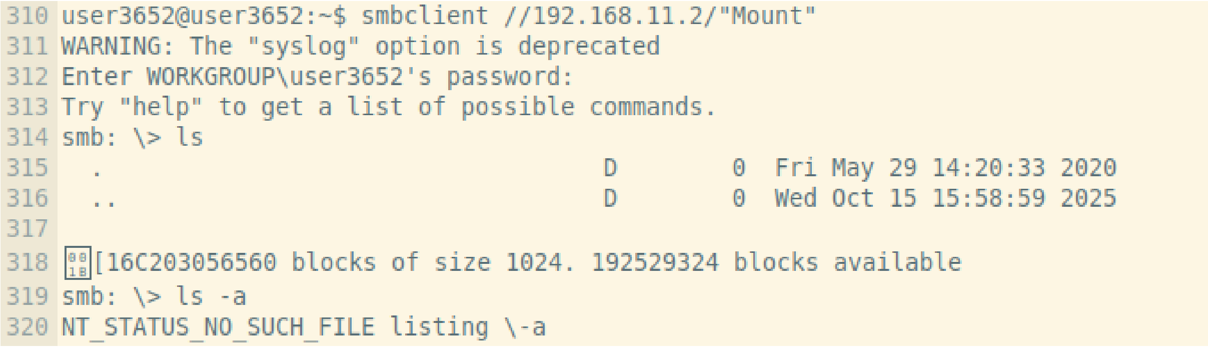
- **Bobs Volume:** Most likely the machine's owner volume, since it does not allow for anonymous access
- **IPC$**
- **Mount:** Some drive connected to this machine which our user has read and write permissions

To access these volumes we need to install the smb client using **sudo apt install smbclient.**

We can't access "Bob's Volume" without having their password, and unfortunately it is not stored in the other two volumes as seen here:



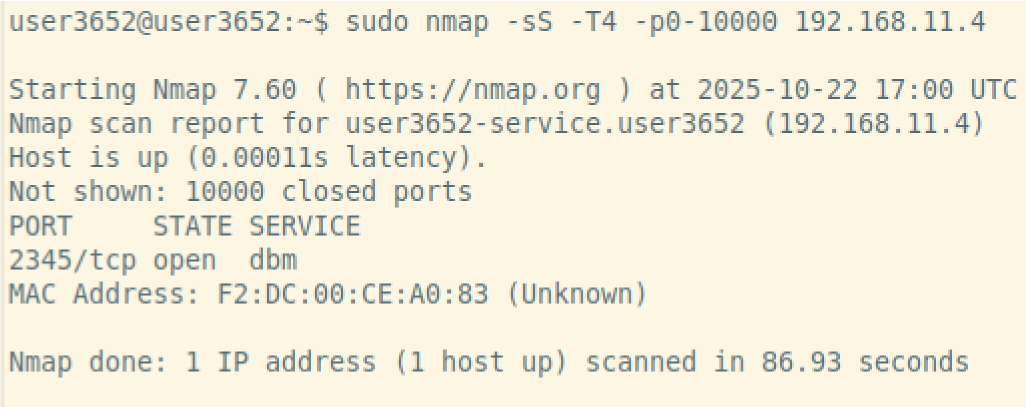
```
user3652@user3652:~$ smbclient //192.168.11.2/"IPC$"
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\user3652's password:
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
```



```
user3652@user3652:~$ smbclient //192.168.11.2/"Mount"
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\user3652's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Fri May 29 14:20:33 2020
  ..                                  D        0  Wed Oct 15 15:58:59 2025

␘[16C203056560 blocks of size 1024. 192529324 blocks available
smb: \> ls -a
NT_STATUS_NO_SUCH_FILE listing \-a
```

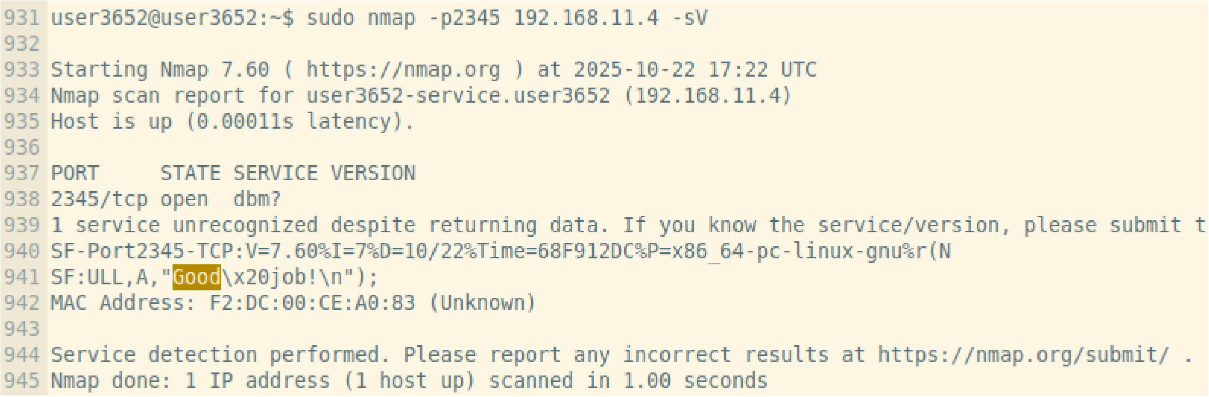
We know by default nmap scans the most 1000 common ports, if we do a scan of at least the first 10000 ports (they contain common ports) and change our protocol to stealth SYN and set the timing to T4, on the other 2 machines, we get the following:

In **192.168.11.4:** we found a **dbm service on port 2345/tcp**



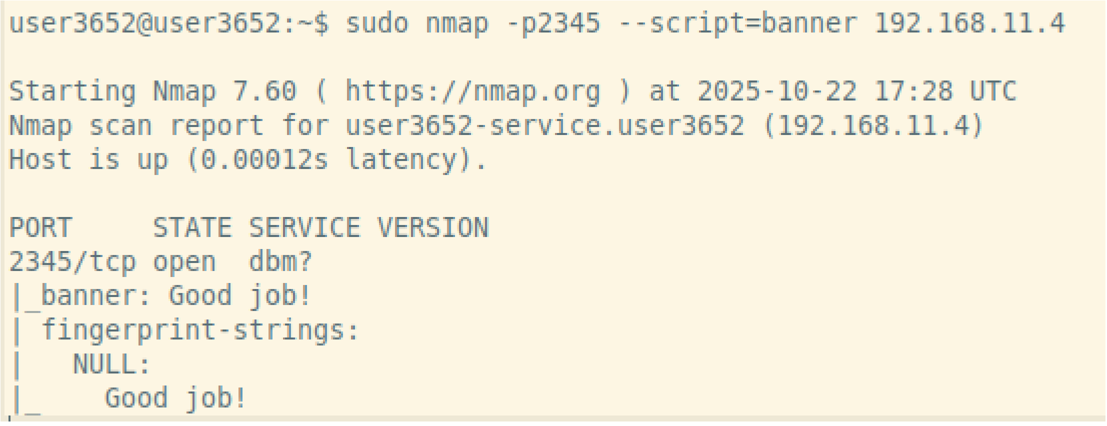
```
user3652@user3652:~$ sudo nmap -sS -T4 -p0-10000 192.168.11.4

Starting Nmap 7.60 ( https://nmap.org ) at 2025-10-22 17:00 UTC
Nmap scan report for user3652-service.user3652 (192.168.11.4)
Host is up (0.00011s latency).
Not shown: 10000 closed ports
PORT     STATE SERVICE
2345/tcp open  dbm
MAC Address: F2:DC:00:CE:A0:83 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 86.93 seconds
```

dbm is some sort of a database, but using -sV flag to know which type of database yields no results



```
user3652@user3652:~$ sudo nmap -p2345 192.168.11.4 -sV

Starting Nmap 7.60 ( https://nmap.org ) at 2025-10-22 17:22 UTC
Nmap scan report for user3652-service.user3652 (192.168.11.4)
Host is up (0.00011s latency).

PORT     STATE SERVICE VERSION
2345/tcp open  dbm?
1 service unrecognized despite returning data. If you know the service/version, please submit t
SF-Port2345-TCP:V=7.60%I=7%D=10/22%Time=68F912DC%P=x86_64-pc-linux-gnu%r(N
SF:ULL,A,"Good\x20job!\n");
MAC Address: F2:DC:00:CE:A0:83 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.00 seconds
```

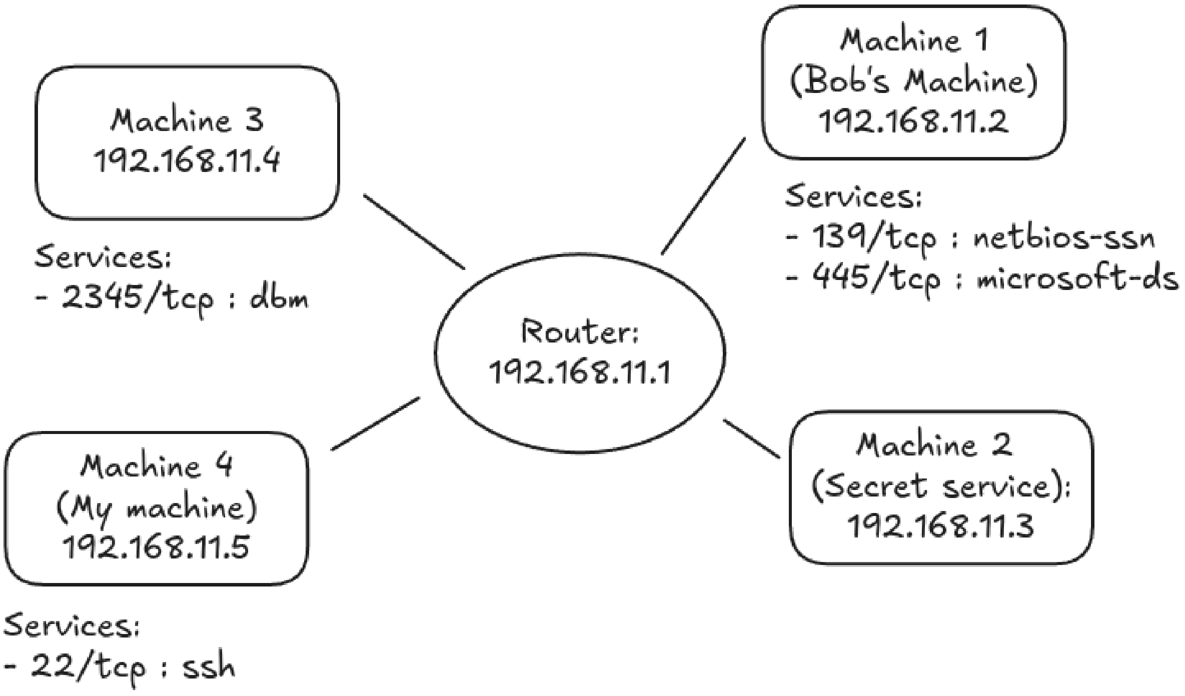
But we can see a good job in there, it is some sort of basic key value pair basic database, using a banner script confirms this:



```
user3652@user3652:~$ sudo nmap -p2345 --script=banner 192.168.11.4

Starting Nmap 7.60 ( https://nmap.org ) at 2025-10-22 17:28 UTC
Nmap scan report for user3652-service.user3652 (192.168.11.4)
Host is up (0.00012s latency).

PORT     STATE SERVICE VERSION
2345/tcp open  dbm?
|_banner: Good job!
| fingerprint-strings:
|   NULL:
|_    Good job!
```

Unfortunately no matter what timing or protocol i used on host **192.168.11.3**, i could not find an open port, but i know for a fact that it has one and in it i can find bob’s password, but i give up, let bob keep his files >:[

Topology of the network


Machine 3
192.168.11.4
Services:
- 2345/tcp : dbm
Machine 1
(Bob's Machine)
192.168.11.2
Services:
- 139/tcp : netbios-ssn
- 445/tcp : microsoft-ds
Router:
192.168.11.1
Machine 4
(My machine)
192.168.11.5
Services:
- 22/tcp : ssh
Machine 2
(Secret service):
192.168.11.3