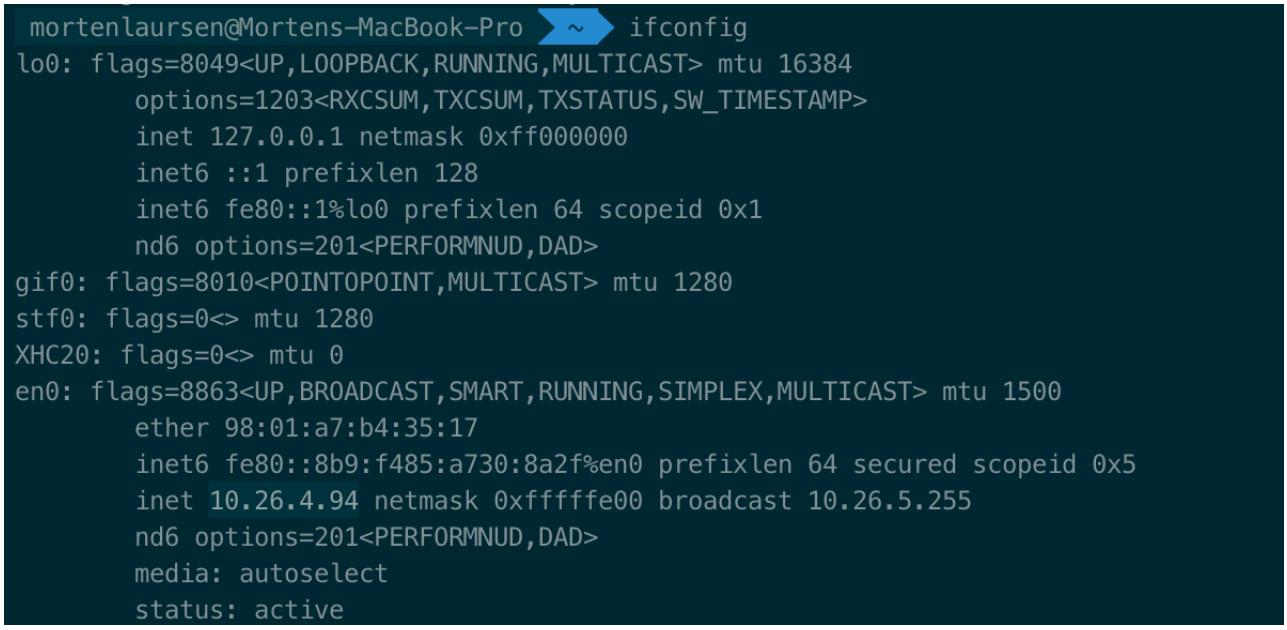
# Assignment 1: Port Scanning

Initially we ran ifconfig to figure out our IP-address.

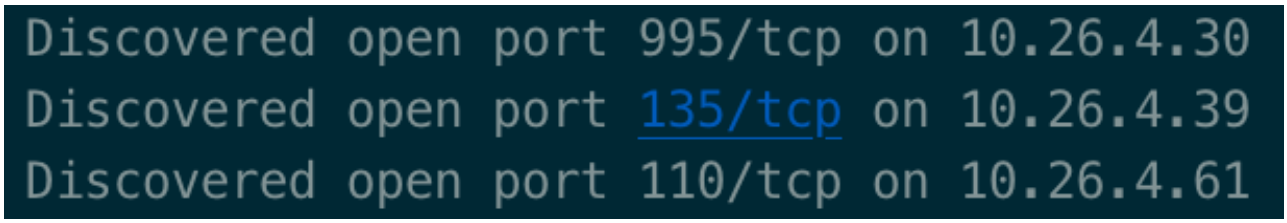



In this case out ip were *10.26.4.94*. Since the last number refers to our own computer, we next ran a scan on the local network using the three first numbers and then the range 0 - 255

```
nmap 10.26.4.0-255 -vv
```

The -vv is the *very verbose* flag which outputs additional information.

This gave us a long list of servers formatted like this




On this list we looked for atypical open port numbers and ran our comprehensive scan on these.

The first line on the screenshots underneath is the command we ran, with the following format

```
sudo nmap -A -vv 11.22.33.44 -p 123
```

sudo is used to run the code as a superuser. This enables us to run it with the *-A* flag, which enables OS detection, version detection, script scanning, and traceroute. The *-vv* flag has already been explained. The *-p* flag specifies a specific port. So we run the command on a specific ip on a specific port.

Port 135

```
mortenlaursen@Mortens-MacBook-Pro ~ sudo nmap -A -vv 10.26.4.39 -p 135
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-12 15:35 CEST
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 15:35
Completed NSE at 15:35, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 15:35
Completed NSE at 15:35, 0.00s elapsed
Initiating ARP Ping Scan at 15:35
Scanning 10.26.4.39 [1 port]
Completed ARP Ping Scan at 15:35, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:35
Completed Parallel DNS resolution of 1 host. at 15:35, 13.01s elapsed
Initiating SYN Stealth Scan at 15:35
Scanning 10.26.4.39 [1 port]
Completed SYN Stealth Scan at 15:35, 0.23s elapsed (1 total ports)
Initiating Service scan at 15:35
Initiating OS detection (try #1) against 10.26.4.39
Retrying OS detection (try #2) against 10.26.4.39
NSE: Script scanning 10.26.4.39.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 15:35
Completed NSE at 15:35, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 15:35
Completed NSE at 15:35, 0.00s elapsed
Nmap scan report for 10.26.4.39
Host is up, received arp-response (0.0020s latency).
Scanned at 2018-10-12 15:35:26 CEST for 16s

PORT    STATE    SERVICE REASON      VERSION
135/tcp filtered msrpc   no-response
MAC Address: 60:F6:77:37:1D:60 (Intel Corporate)
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=7.70%E=4%D=10/12%OT=%CT=%CU=%PV=Y%DS=1%DC=D%G=N%M=60F677%TM=5BC0A32E%P=x86_64-apple-darwin17.3.0)
U1(R=N)
IE(R=N)

Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   1.98 ms 10.26.4.39

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 15:35
Completed NSE at 15:35, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 15:35
Completed NSE at 15:35, 0.00s elapsed
Read data files from: /usr/local/bin/../share/nmap
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 17.34 seconds
           Raw packets sent: 51 (6.788KB) | Rcvd: 1 (28B)
```

The port number 135 is usually the Remote Procedure Call (RPC) port. Since nmap is unable to detect the OS for what ever reason, it's unclear how to exploit this open port.

Port 49154

```
✘ mortenlaursen@Mortens-MacBook-Pro ~ sudo nmap -A -vv 10.26.4.46 -p 49154
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-12 15:49 CEST
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 15:49
Completed NSE at 15:49, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 15:49
Completed NSE at 15:49, 0.00s elapsed
Initiating ARP Ping Scan at 15:49
Scanning 10.26.4.46 [1 port]
Completed ARP Ping Scan at 15:49, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:49
Completed Parallel DNS resolution of 1 host. at 15:49, 0.00s elapsed
Initiating SYN Stealth Scan at 15:49
Scanning 10.26.4.46 [1 port]
Discovered open port 49154/tcp on 10.26.4.46
Completed SYN Stealth Scan at 15:49, 0.05s elapsed (1 total ports)
Initiating Service scan at 15:49
Scanning 1 service on 10.26.4.46
Completed Service scan at 15:52, 141.31s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 10.26.4.46
NSE: Script scanning 10.26.4.46.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 15:52
Completed NSE at 15:52, 7.03s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 15:52
Completed NSE at 15:52, 0.21s elapsed
Nmap scan report for 10.26.4.46
Host is up, received arp-response (0.0056s latency).
Scanned at 2018-10-12 15:49:57 CEST for 151s

PORT      STATE SERVICE REASON         VERSION
49154/tcp open  unknown syn-ack ttl 64
MAC Address: 28:A0:2B:DB:5A:93 (Apple)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Apple Mac OS X 10.4.X
OS CPE: cpe:/o:apple:mac_os_x:10.4
OS details: Apple Mac OS X 10.4.8 - 10.4.11 (Tiger) (Darwin 8.8.0 - 8.11.0)
TCP/IP fingerprint:
OS:SCAN(V=7.70%E=4%D=10/12%OT=49154%CT=%CU=43608%PV=Y%DS=1%DC=D%G=N%M=28A02
OS:B%TM=5BC0A71C%P=x86_64-apple-darwin17.3.0)SEQ(CI=RD)OPS(O1=M5B4NW6NNT11S
OS:LL%O2=M5B4NW6NNT11SLL%O3=M5B4NW6NNT11%O4=M5B4NW6NNT11SLL%O5=M5B4NW6NNT11
OS:SLL%O6=M5B4NNT11SLL)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)
OS:ECN(R=Y%DF=Y%T=40%W=FFFF%O=M5B4NW6SLL%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%
OS:F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T
OS:5(R=Y%DF=N%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=
OS:Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=N%T=40%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)U1(R=Y%DF=
OS:N%T=40%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=0%RUD=G)IE(R=Y%DFI=S%T=40%C
OS:D=S)

Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   5.62 ms 10.26.4.46
```

```
NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 15:52
Completed NSE at 15:52, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 15:52
Completed NSE at 15:52, 0.00s elapsed
Read data files from: /usr/local/bin/../share/nmap
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 151.56 seconds
           Raw packets sent: 39 (2.948KB) | Rcvd: 27 (1.710KB)
```

Port 49154 is a custom port which isn't reserved for anything. Since we determine the OS to Mac OS X 10.4.11 (assumed highest version), we can exploit this server by using one of the exploits found on this link: https://www.cvedetails.com/vulnerability-list/vendor_id-49/product_id-156/version_id-42310/year-2018/Apple-Mac-Os-X-10.4.11.html

Port 2179

```
✘ mortenlaursen@Mortens-MacBook-Pro ~ sudo nmap -A -vv 10.26.4.39 -p 2179
Password:
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-12 15:34 CEST
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 15:34
Completed NSE at 15:34, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 15:34
Completed NSE at 15:34, 0.00s elapsed
Initiating ARP Ping Scan at 15:34
Scanning 10.26.4.39 [1 port]
Completed ARP Ping Scan at 15:34, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:34
Completed Parallel DNS resolution of 1 host. at 15:34, 0.00s elapsed
Initiating SYN Stealth Scan at 15:34
Scanning 10.26.4.39 [1 port]
Discovered open port 2179/tcp on 10.26.4.39
Completed SYN Stealth Scan at 15:34, 0.02s elapsed (1 total ports)
Initiating Service scan at 15:34
Scanning 1 service on 10.26.4.39
Completed Service scan at 15:34, 5.00s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 10.26.4.39
NSE: Script scanning 10.26.4.39.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 15:34
Completed NSE at 15:34, 5.03s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 15:34
Completed NSE at 15:34, 0.00s elapsed
Nmap scan report for 10.26.4.39
Host is up, received arp-response (0.014s latency).
Scanned at 2018-10-12 15:34:32 CEST for 13s

PORT     STATE SERVICE    REASON          VERSION
2179/tcp open  tcpwrapped syn-ack ttl 128
MAC Address: 60:F6:77:37:1D:60 (Intel Corporate)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|WAP|phone
Running: iPXE 1.X, Linux 2.4.X|2.6.X, Sony Ericsson embedded
OS CPE: cpe:/o:ipxe:ipxe:1.0.0%2b cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6.22 cpe:/h:sonyericsson:u8i_vivaz
OS details: iPXE 1.0.0+, Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.22), Sony Ericsson U8i Vivaz mobile phone
TCP/IP fingerprint:
OS:SCAN(V=7.70%E=4%D=10/12%OT=2179%CT=%CU=%PV=Y%DS=1%DC=D%G=N%M=60F677%TM=5
OS:BC0A2F5%P=x86_64-apple-darwin17.3.0)ECN(R=N)T1(R=N)T2(R=N)T3(R=N)T4(R=N)
OS:U1(R=N)IE(R=N)

Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   13.81 ms 10.26.4.39

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 15:34
Completed NSE at 15:34, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 15:34
Completed NSE at 15:34, 0.00s elapsed
Read data files from: /usr/local/bin/../share/nmap
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 14.03 seconds
           Raw packets sent: 70 (5.976KB) | Rcvd: 4 (176B)
```

Port 2179 is also not reserved for any particular service, and in this case is a *tcpwrapper*. A tcpwrapper is a host-based network access control program on Unix and Linux, which actually protects some program.

> *What you are probably seeing is a network security device like a firewall or IPS. Many of these are configured to respond to TCP portscans, even for IP addresses which are not assigned to them. This behavior can slow down a port scan and cloud the results with false positives.*

From https://security.stackexchange.com/questions/23407/how-to-bypass-tcpwrapped-with-nmap-scan

According to the scan above, the device is a *Sony Ericsson u8i Vivaz mobile phone* but this is probably not the case, since we probably are talking to a firewall. This issue is referenced in an open nmap issue: https://github.com/nmap/nmap/issues/914

## Assignment 2: Adversarial Mind

The following is inspired by a personal episode of two of our group members, referenced in the following paragraphs as Alice and Bob.

Two years ago, Alice and Bob were members of a wellness center which included a gym, indoor pool and spa area. Because of the investments made during the construction of the center, as well as the costly membership fees for any type of membership, the need for a security system in regards to people permitted to enter the facilities was of high importance.

The center had employed such a system, in which every member had a bracelet with a chip in it, which they had to use when they wished to enter the facilities. Upon check in at the reception, the member's personal details (such as name, surname, sex, age, etc.) along with a picture of them would appear in the receptionist's screen. The chip would later on only permit them to enter the areas which were included in their membership type.

This is where the first security issue appears. A few days after their membership had begun, Alice notices that while checking in her personail details appear without her picture next to them, while Bob's check in always displays his picture next to his personal details. This creates a loophole in the system. Alice could give her bracelet to any friend or family member of the same sex and appearing to be in the same age group as her (Mallory), and they could gain easy access to the center without the need to pay for a membership.

A second security issue that would help Mallory even more was, as Alice and Bob noticed, that sometimes people would get through the reception by just showing their bracelets or keeping them visible. If the person seemed insuspicious enough when entering the facilities with the bracelet present, a person of any age or sex could make use of a member's bracelet.

The third security issue concerned the locker rooms. It happened many times that Bob, while searching for an empty locker, would find someones belongings in different lockers. These lockers were not locked either from peoples' laziness or because oftentimes the locking mechanism would not work. Since there were no cameras in the changing rooms, this situation also presented a potential security breach on the members' belongings as they could be stolen and the person accountable for the theft would never be found.