



LAB 03

Network Scanning

TPAS

Leonardo Araújo Freitas | up202400832

outubro, 2024

1. Task 1 - Banner grabbing	3
2. Task 2 - Nmap	4
2.1. Ping Scan?	4
2.2. Aggressive scan?	4
2.3. Port range?	5
2.4. List scan?	6
3. Task 3 - WireShark	6
3.1. Ping Scan?	6
3.2. Aggressive scan?	7
3.3. Port range?	7
4. Task 4 - Solve the Secret Service	8
5. Task 5 - Special Tasks	9
5.1. Banner Grabbing Subs.txt	9
5.2. Scapy Script	9
5.3. SYN Port Scan	10

1. Task 1 - Banner grabbing

In this first task we're going to perform banner grabbing for the domain <https://developer.oculus.com>

We started trying to gather some information by running curl, as shown in the image.

```
curl -v https://developer.oculus.com
* Host developer.oculus.com:443 was resolved.
* IPv6: 2a03:2880:f252:c3:face:b00c:0:32c2
* IPv4: 157.240.212.50
* Trying [2a03:2880:f252:c3:face:b00c:0:32c2]:443...
* Immediate connect fail for 2a03:2880:f252:c3:face:b00c:0:32c2: Network is unreachable
* Trying 157.240.212.50:443...
* GnuTLS ciphers: NORMAL:-ARCFOUR-128:-CTYPE-ALL:-CTYPE-X509:-VERS-SSL3.0
* found 146 certificates in /etc/ssl/certs/ca-certificates.crt
* found 445 certificates in /etc/ssl/certs
* SSL connection using TLS1.3 / ECDHE_RSA_CHACHA20_POLY1305
* server certificate verification OK
* server certificate status verification SKIPPED
* common name: *.oculus.com (matched)
* server certificate expiration date OK
* server certificate activation date OK
* certificate public key: RSA
* certificate version: #3
* subject: C=US,ST=California,L=Menlo Park,O=Meta Platforms\, Inc.,CN=*.oculus.com
* start date: Fri, 19 Jul 2024 00:00:00 GMT
* expire date: Thu, 17 Oct 2024 23:59:59 GMT
* issuer: C=US,O=DigiCert Inc,OU=www.digicert.com,CN=DigiCert SHA2 High Assurance Server CA
* ALPN: server accepted h2
* Connected to developer.oculus.com (157.240.212.50) port 443
* using HTTP/2
* [HTTP/2] [1] OPENED stream for https://developer.oculus.com/
* [HTTP/2] [1] [:method: GET]
* [HTTP/2] [1] [:scheme: https]
* [HTTP/2] [1] [:authority: developer.oculus.com]
* [HTTP/2] [1] [:path: /]
* [HTTP/2] [1] user-agent: curl/8.10.1
* [HTTP/2] [1] accept: */*
> GET / HTTP/2
> Host: developer.oculus.com
> User-Agent: curl/8.10.1
> Accept: */*
<
* Request completely sent off
< HTTP/2 302
< vary: Accept-Encoding
< set-cookie: locale=en_US; expires=Thu, 17-Oct-2024 17:17:39 GMT; Max-Age=604800; path=/; domain=.oculus.com; secure
< location: https://developers.meta.com/horizon/
< reporting-endpoints: coop_report="https://www.facebook.com/browser_reporting/coop/?minimize=0", coop_report="https://www.facebook.com/browser_reporting/coop/?minimize=0"
< report-to: {"max_age":2592000,"endpoints":[{"url":"https://www.facebook.com/browser_reporting/coop/?minimize=0"}],"group":"coop_report"}
< cross-origin-embedder-policy-report-only: require-corp;report-to="coop_report"
< cross-origin-opener-policy: same-origin-allow-popups
< origin-agent-cluster: 71
< strict-transport-security: max-age=31536000; preload; includeSubDomains
< content-type: text/html; charset=utf-8
< x-fb-debug: B60760b09UyhShbCtnSMcnqksitC+E6nQtugHv13mu9Fkl16cRTTa390wHDzclIu9ChexVzY8PpnluazHtdFQ==
< content-length: 0
< date: Thu, 10 Oct 2024 17:17:39 GMT
* Connection #0 to host developer.oculus.com left intact
```

Figure 1

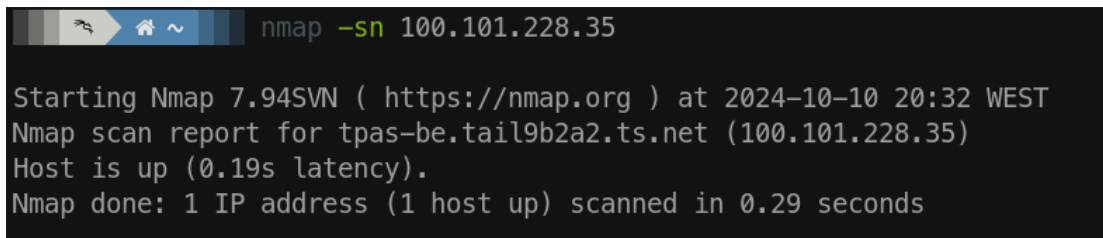
Based on this output, we cannot directly see the web server software version (such as Apache or Nginx). However, the headers show the server uses strict security practices and HTTP/2, with an encrypted connection via TLS 1.3.

2. Task 2 - Nmap

In this task, we will use the IP 100.101.228.35 provided in the statement since many of the domains in the Lab02 scope are no longer available or are simply redirects to the meta page.

2.1. Ping Scan?

A ping scan can be used to determine if a host is online by sending an echo request. This can be performed by running the following command:

A terminal window with a dark background. The command 'nmap -sn 100.101.228.35' is entered at the prompt. The output shows the Nmap version (7.94SVN), the target IP (100.101.228.35), and the result: 'Host is up (0.19s latency)'.

```
nmap -sn 100.101.228.35

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-10 20:32 WEST
Nmap scan report for tpas-be.tail9b2a2.ts.net (100.101.228.35)
Host is up (0.19s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
```

Figure 2

The **-sn** flag, tells nmap to perform a ping scan without scanning any ports. In Figure 2, we can see information about the host, such as their status.

2.2. Aggressive scan?

An aggressive scan is the opposite of the ping scan, performs a thorough scan of the target, including port scanning, OS detection, service version, and script scanning. This can be performed by running the following:

```
nmap -A 100.101.228.35

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-10 21:28 WEST
Nmap scan report for tpas-be.tail9b2a2.ts.net (100.101.228.35)
Host is up (0.087s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; pro
tocol 2.0)
|_ ssh-hostkey:
|   256 fb:ad:d2:7b:62:da:fd:cb:75:d9:73:86:35:63:22:08 (ECDSA)
|   256 55:4a:cc:f4:7e:3b:ca:cd:8b:99:7c:66:a8:12:82:8b (ED25519)
80/tcp    open  http         nginx/1.27.1
|_ http-title: Did not follow redirect to https://tpas-be.tail9b2a2.ts.net/
|_ http-server-header: nginx/1.27.1
443/tcp    open  ssl/http     nginx/1.27.1
|_ http-server-header: nginx/1.27.1
|_ http-title: TPAS 2024/2025
|_ ssl-date: TLS randomness does not represent time
|_ ssl-cert: Subject: commonName=tpas-desafios.alunos.dcc.fc.up.pt/organizationName=
Universidade do Porto/stateOrProvinceName=Porto/countryName=PT
|_ Subject Alternative Name: DNS:tpas-desafios.alunos.dcc.fc.up.pt, DNS:www.tpas-des
afios.alunos.dcc.fc.up.pt
|_ Not valid before: 2024-08-04T00:00:00
|_ Not valid after: 2025-08-04T23:59:59
|_ tls-alpn:
|   http/1.1
|   http/1.0
|   http/0.9
|_ http-robots.txt: 1 disallowed entry
|_ /admin
5001/tcp   open  complex-link?
|_ fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, LANDesk-RC, LDAPBindReq, NULL, RPCCH
eck, SMBProgNeg, TerminalServer, WMSRequest, X11Probe, ZendJavaBridge:
```

Figure 3

With this, we can obtain information like:

- Open ports and their services
- Operating system and version
- Service versions
- Any scripts that can be executed on the services
- Traceroute information to the host

2.3. Port range?

To scan a specific range of ports, such as ports between 1 a 1000, we can use the following command:

```
nmap -p 1-1000 100.101.228.35

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-10 20:55 WEST
Nmap scan report for tpas-be.tail9b2a2.ts.net (100.101.228.35)
Host is up (0.17s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp    open  https

Nmap done: 1 IP address (1 host up) scanned in 2.28 seconds
```

Figure 4

With this command we receive a list of open ports within the specified range along with the services running on those ports.

2.4. List scan?

A list scan can be used to discover hosts on a network without scanning ports. To scan my home network, i can use the following command:

```
nmap -sn 192.168.255.34/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-10 21:07 WEST
Nmap scan report for 192.168.255.29
Host is up (0.0056s latency).
MAC Address: A6:B7:59:34:EA:D8 (Unknown)
Nmap scan report for 192.168.255.34
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.24 seconds
```

Figure 5

The difference from the ping scan is that we pass a subnet that covers all addresses from 192.168.1.1 to 192.168.1.254. We receive a list of all hosts that are up within the specified subnet, their IP addresses and possibly their MAC addresses.

3. Task 3 - WireShark

3.1. Ping Scan?

The traffic generated by the ping scan can be seen below

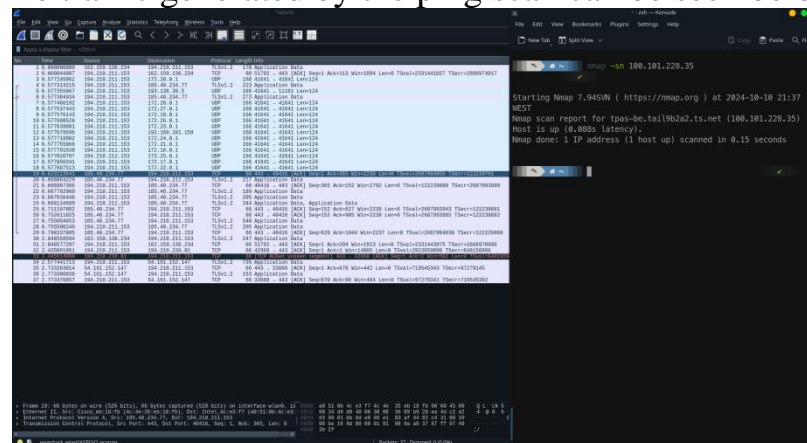
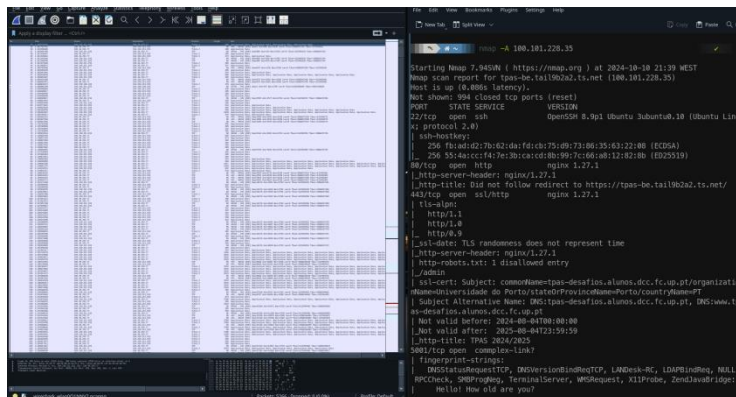


Figure 6

3.2. Aggressive scan?



Figure

7

This scan generates significantly more traffic as it probes open ports and attempts to gather detailed information about services and operating systems. The file generated by the Wireshark is inside the folder of this lab03.

3.3. Port range?

This will generate even more traffic as it attempts to scan multiple ports within a specified range. The file is also inside the folder lab03.

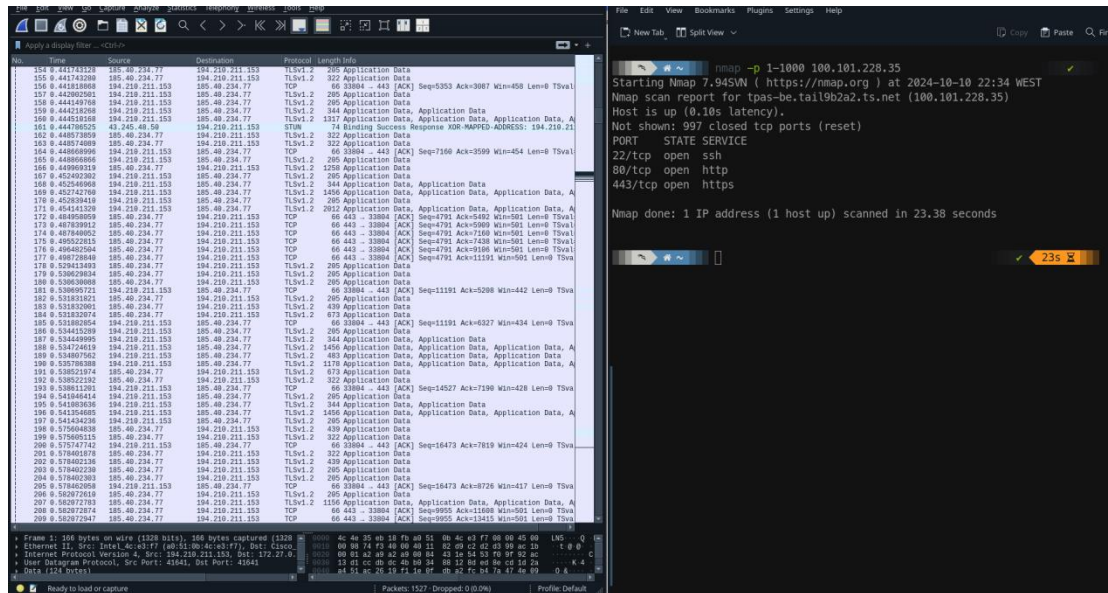


Figure 8

So basically the ping scan (-sn) leads to the least network traffic, as it simply checks whether the host is alive without further probing ports or services.

4. Task 4 - Solve the Secret Service

(Regular flag submission - no need to send the solution for this one).

5. Task 5 - Special Tasks

5.1. Banner Grabbing Subs.txt

For this task the following command was run

```
~/Documents/FCUP MSI/Teoria & Pratica Attack/LAB3 nmap -sV -oX output.xml -iL subs.txt
```

Figure 9

```
2144,2160-2161,2170,2179,2190-2191,2196,2200,2222,2251,2260,2288,2301,2323,2366,2381-2383,2393-2394,2399,2401,2492,2500,2522,2525,2557,2601-2602,2604-2605,2607-2608,2630,2
701-2702,2710,2717-2718,2725,2800,2809,2811,2869,2875,2909-2910,2920,2967-2968,2998,3000-3001,3003,3005-3007,3011,3013,3017,3030-3031,3052,3071,3077,3128,3168,3211,3221,32
60-3261,3268-3269,3283,3300-3301,3306,3322-3325,3333,3351,3367,3369-3372,3389-3390,3404,3476,3493,3517,3527,3546,3551,3580,3659,3689-3690,3703,3737,3766,3784,3800-3801,380
9,3814,3826-3828,3851,3869,3871,3878,3880,3889,3905,3914,3918,3920,3945,3971,3986,3995,3998,4000-4006,4045,4111,4125-4126,4129,4224,4242,4279,4321,4343,4443-4446,4449,4550
,4567,4662,4848,4899-4900,4998,5000-5004,5009,5030,5033,5050-5051,5054,5060-5061,5080,5087,5100-5102,5120,5190,5200,5214,5221-5222,5225-5226,5269,5280,5298,5357,5405,5414,
5431-5432,5440,5500,5510,5544,5550,5555,5560,5566,5631,5633,5666,5678-5679,5718,5730,5800-5802,5810-5811,5815,5822,5825,5850,5859,5862,5877,5900-5904,5906-5907,5910-5911,5
915,5922,5925,5950,5952,5959-5963,5987-5989,5998-6007,6009,6025,6059,6100-6101,6106,6112,6123,6129,6156,6346,6389,6502,6510,6543,6547,6565-6567,6580,6646,6666-6669,6689,66
92,6699,6779,6788-6789,6792,6839,6881,6901,6969,7000-7002,7004,7007,7019,7025,7070,7100,7103,7106,7200-7201,7402,7435,7443,7496,7512,7625,7627,7676,7741,7777-7778,7800,791
1,7920-7921,7937-7938,7999-8002,8007-8011,8021-8022,8031,8042,8045,8080-8090,8093,8099-8100,8100-8101,8102-8104,8200,8222,8254,8290-8292,8300,8333,8383,8400,8402,8443,8500
,8600,8649,8651-8652,8654,8701,8800,8873,8888,8899,8994,9000-9003,9009-9011,9040,9050,9071,9080-9081,9090-9091,9099-9103,9110-9111,9200,9207,9220,9290,9415,9418,9483,9500,
9502-9503,9535,9575,9593-9595,9618,9666,9676-9678,9898,9900,9917,9929,9943-9944,9968,9998-10004,10009-10010,10012,10024-10025,10082,10180,10215,10243,10566,10616-10617,106
21,10626,10628-10629,10778,11110-11111,11967,12000,12174,12265,12345,13456,13722,13782-13783,14000,14238,14441-14442,15000,15002-15004,15660,15742,16000-16001,16012,16016,
16018,16080,16113,16992-16993,17877,17988,18040,18101,18988,19101,19283,19315,19350,19780,19801,19842,20000,20005,20031,20221-20222,20828,21571,22939,23502,24444,24800,257
34-25735,26214,27000,27352-27353,27355-27356,27715,28201,30000,30718,30951,31038,31337,32768-32785,33354,33899,34571-34573,35500,38292,40193,40911,41511,42510,44176,44442-
44443,44501,45100,48080,49152-49161,49163,49165,49167,49175-49176,49400,49999-50003,50006,50300,50389,50500,50636,50800,51103,51493,52673,52822,52848,52869,54045,54328,550
55-55056,55555,55600,56737-56738,57294,57797,58080,60020,60443,61532,61900,62078,63331,64623,64680,65000,65129,65389"/>
<verbose level="0"/>
<debugging level="0"/>
<hosthint><status state="up" reason="unknown-response" reason_ttl="0"/>
<address addr="157.240.212.35" addrtype="ipv4"/>
<hostnames>
<hostname name="www.facebook.com" type="user"/>
</hostnames>
</hosthint>
<hosthint><status state="up" reason="unknown-response" reason_ttl="0"/>
<address addr="157.240.212.16" addrtype="ipv4"/>
<hostnames>
<hostname name="developer.fa-ir.developers.prod.oculus.com" type="user"/>
</hostnames>
</hosthint>
<hosthint><status state="up" reason="unknown-response" reason_ttl="0"/>
<address addr="157.240.212.50" addrtype="ipv4"/>
<hostnames>
<hostname name="account.oculus.com" type="user"/>
</hostnames>
</hosthint>
<hosthint><status state="up" reason="unknown-response" reason_ttl="0"/>
```

Figure 10

This is a little sample of the result; the full result is in output.xml. Nothing relevant was found, so there's nothing more I can do. A lot of these domains are redirects or deprecated.

5.2. Scapy Script

```
exercico.py > ...
1 from scapy.all import *
2 from scapy.layers.inet import IP
3
4 # Script to Parse Wireshark .pcapng File and Extract IP Addresses
5
6 packet = rdpcap('capture.pcapng')
7
8 ip_addresses = set()
9
10 for pkt in packet:
11     if IP in pkt:
12         ip_addresses.add(pkt[IP].src)
13         ip_addresses.add(pkt[IP].dst)
14
15 for ip in ip_addresses:
16     print(ip)
17
18 |
```

Figure 11

5.3. SYN Port Scan

```
# Script to Perform a SYN Port Scan

def syn_scan(target_ip, ports):
    for port in ports:
        syn_packet = IP(dst=target_ip)/TCP(dport=port, flags='S')
        response = sr1(syn_packet, timeout=1, verbose=0)

        if response:
            if response.haslayer(TCP) and response.getlayer(TCP).flags == 0x12:
                print(f'Port {port} is open')
                sr(IP(dst=target_ip)/TCP(dport=port, flags='R'), timeout=1, verbose=0)
            else:
                print(f'Port {port} is closed')
        else:
            print(f'Port {port} is filtered')

target = "192.168.1.1"
ports = [22, 23, 80, 443, 3389]
syn_scan(target, ports)

# End of File
```

Figure 12

The python file with this code is inside the zip folder with this report.