HOMEWORK 2

Sara Bruzzese - 1648786

1. Target domain: www.psicologiareba.it

a) the host discovery is a method that makes us understand if a target host is alive. I added -sn option to specify I want to perform a host discovery and to exclude a port scanning, and I added -PR option because Nmap supports the ARP scanning via this option. Many systems block this kind of request, so the shell suggests me to use -Pn to perform this action. The output confirms that the host is online.

```
user@katha:~$ sudo nmap -sn -PR www.psicologiareba.it
[sudo] password for user:

Starting Nmap 7.60 ( https://nmap.org ) at 2020-03-28 22:54 CET
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.01 seconds
user@katha:~$ sudo nmap -sn -Pn www.psicologiareba.it

Starting Nmap 7.60 ( https://nmap.org ) at 2020-03-28 22:54 CET
Nmap scan report for www.psicologiareba.it (217.64.195.204)
Host is up.
Other addresses for www.psicologiareba.it (not scanned): 2001:4b78:1001::1101
rDNS record for 217.64.195.204: w-11.th.seeweb.it
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

b) port scanning is the process of sending packets to TCP and UDP ports on the target system to determine what services are running or are in listening state. I used the -sS option in my port scan, which is the simplest way to do this. It performs a TCP SYN port scan, this technique is called half-opening scanning because only a SYN packet is sent to the target port. All the ports detected in the scan sent a SYN/ACK response to my request.

```
user@katha:~$ sudo nmap -sS www.psicologiareba.it
[sudo] password for user:

Starting Nmap 7.60 ( https://nmap.org ) at 2020-03-28 23:30 CET
Nmap scan report for www.psicologiareba.it (217.64.195.204)
Host is up (0.0014s latency).
Other addresses for www.psicologiareba.it (not scanned): 2001:4b78:1001::1101
rDNS record for 217.64.195.204: w-11.th.seeweb.it
Not shown: 997 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 13.61 seconds
```

c) the active stack fingerprinting allows me to know the operating system of my target host with a high degree of probability. My result isn't very accurate because Nmap needs at least one port open and one port closed, and it couldn't find this condition when I performed this action.

```
user@katha:~$ sudo nmap -O www.psicologiareba.it

Starting Nmap 7.60 ( https://nmap.org ) at 2020-03-28 23:41 CET
Nmap scan report for www.psicologiareba.it (217.64.195.204)
Host is up (0.0072s latency).
Other addresses for www.psicologiareba.it (not scanned): 2001:4b78:1001::1101
rDNS record for 217.64.195.204: w-11.th.seeweb.it
Not shown: 997 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
80/tcp  open  http
443/tcp open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (93%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (93%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.31 seconds
```

d) version scanning lists service names along with ports, even the hidden ones and it utilizes the -sV option.

```
user@katha:~$ sudo nmap -sV www.psicologiareba.it

Starting Nmap 7.60 ( https://nmap.org ) at 2020-03-28 23:49 CET
Nmap scan report for www.psicologiareba.it (217.64.195.204)
Host is up (0.0030s latency).
Other addresses for www.psicologiareba.it (not scanned): 2001:4b78:1001::1101
rDNS record for 217.64.195.204: w-11.th.seeweb.it
Not shown: 997 filtered ports
PORT    STATE SERVICE  VERSION
21/tcp  open  ftp      ProFTPD 1.3.5b
80/tcp  open  http     Apache httpd
443/tcp open  ssl/http nginx 1.10.3
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 31.82 seconds
```

e) Vulnerability scanning consists of using a Nmap script, in this case the "vuln" one. My result didn't reveal any vulnerabilities.

```
user@katha:~$ nmap -Pn --script vuln www.psicologiareba.it

Starting Nmap 7.60 ( https://nmap.org ) at 2020-03-29 00:01 CET
Nmap scan report for www.psicologiareba.it (217.64.195.204)
Host is up (0.0090s latency).
Other addresses for www.psicologiareba.it (not scanned): 2001:4b78:1001::1101
rDNS record for 217.64.195.204: w-11.th.seeweb.it
Not shown: 997 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
|_sslv2-drown:
80/tcp  open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
443/tcp open  https
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_sslv2-drown:

Nmap done: 1 IP address (1 host up) scanned in 80.73 seconds
```

2. nmap-os-fingerprints: https://nmap.org/data/nmap-os-fingerprints

osprints.conf: https://github.com/unmarshal/siphon/blob/master/osprints.conf

The big difference between the two files lies in the accuracy and correctness of the information provided: Nmap has many meters of judgment in its test, in the link we can see in the description the types of requests that it uses to make sure of the operating system. Siphon instead uses only 3: window size, TTL and DF. Siphon is used for *passive stack fingerprinting*, a technique that consists in passively monitors network traffic between various systems without sending a single packet to the target, but it's less reliable than Nmap.

3. nmap-services: https://svn.nmap.org/nmap/nmap-services

nmap-service-probes: https://svn.nmap.org/nmap/nmap-service-probes

Nmap uses both files to perform port scanning, but each of them has different specifications. Nmap lists service names along with ports, and it utilizes nmap-services file for this purpose. This is simply a text file mapping services with their commonly associated ports. Then, if we want to go a step further with the scan, we can use the -sV option that uses the nmap-service-probes file. This file contains information on known service responses, so we can identify even "hidden" services.

4. in this extract of inetd.conf, there are different services. The first column of the row defines the name of the service, so there are shell, login, exec, comsat, talk, ntalk and dtalk services. The second column defines the socket type, we have stream and dgram. Then we have the protocol, tcp and udp. The other options define if the service is wait or nowait entry, the user, the server program and some arguments.

```
# Shell, login, exec, comsat and talk are BSD protocols.
#
#shell   stream  tcp     nowait  root    /usr/sbin/tcpd  in.rshd
#login   stream  tcp     nowait  root    /usr/sbin/tcpd  in.rlogind
#exec    stream  tcp     nowait  root    /usr/sbin/tcpd  in.rexecd
#comsat  dgram   udp     wait    root    /usr/sbin/tcpd  in.comsat
#talk    dgram   udp     wait    root    /usr/sbin/tcpd  in.talkd
#ntalk   dgram   udp     wait    root    /usr/sbin/tcpd  in.ntalkd
#dtalk   stream  tcp     waut    nobody  /usr/sbin/tcpd  in.dtalkd
```

5. The target host is the one I've chosen at the top of this file. I set up the Metasploit's database and then I started the scan from msfconsole. First, I used the "sudo nmap -O www.psicologiareba.it" command and then I imported the output into the database with the "db_import" command. Then, to show my result, I performed the query "services -s ssh" because the scope was to find the host and the available ports.

```
msf5 > services -s ssh
Services
========

host            port  proto  name   state  info
----            ----  -----  ----   -----  ----
217.64.195.204  21    tcp    ftp    open
217.64.195.204  80    tcp    http   open
217.64.195.204  443   tcp    https  open
```

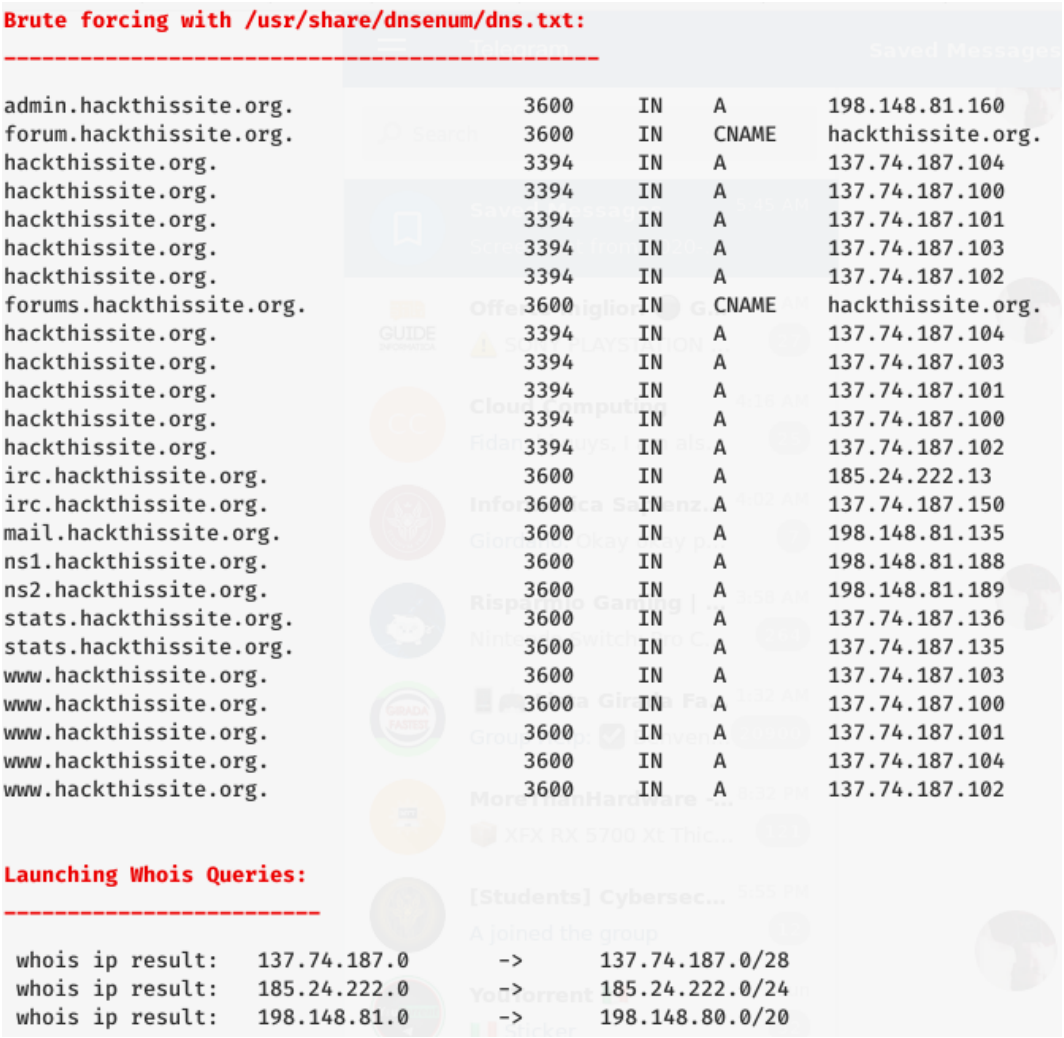
6. The *banner grabbing* is an enumeration technique that consists in connecting to remote services and observing the output. In the following two pictures I used telnet and netcat for this purpose, the output is the same and I found out that I'm connecting to an Apache server.

```
user@katha:~$ telnet www.psicologiareba.it 80
Trying 217.64.195.204...
Connected to www.psicologiareba.it.
Escape character is '^]'.
^[[A
HTTP/1.1 400 Bad Request
Date: Mon, 30 Mar 2020 07:59:09 GMT
Server: Apache
Content-Length: 293
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache Server at w-11.th.seeweb.it Port 80</address>
</body></html>
Connection closed by foreign host.
```

```
user@katha:~$ nc -v www.psicologiareba.it 80
Connection to www.psicologiareba.it 80 port [tcp/http] succeeded!
^[[A
HTTP/1.1 400 Bad Request
Date: Mon, 30 Mar 2020 08:05:09 GMT
Server: Apache
Content-Length: 293
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache Server at w-11.th.seeweb.it Port 80</address>
</body></html>
```

7. dnsenum is a tool that performs a variety of different tasks, such as Google scrapping for additional names and subdomains, brute forcing subdomains, performing reverse lookups, listing domain network ranges and performing WHOIS queries on the range identified. I post here the output.

```
root@kali:~# dnsenum --enum hackthissite.org
dnsenum VERSION:1.2.6

-----   hackthissite.org   -----


Host's addresses:
__________________

hackthissite.org.                        3522     IN    A        137.74.187.100
hackthissite.org.                        3522     IN    A        137.74.187.102
hackthissite.org.                        3522     IN    A        137.74.187.103
hackthissite.org.                        3522     IN    A        137.74.187.101
hackthissite.org.                        3522     IN    A        137.74.187.104


Name Servers:
______________

c.ns.buddyns.com.                        133953   IN    A        116.203.6.3
f.ns.buddyns.com.                        69001    IN    A        103.6.87.125
g.ns.buddyns.com.                        34262    IN    A        192.184.93.99
h.ns.buddyns.com.                        69001    IN    A        119.252.20.56
j.ns.buddyns.com.                        133953   IN    A        185.34.136.178


Mail (MX) Servers:
___________________

aspmx.l.google.com.                      164      IN    A        173.194.76.27
alt1.aspmx.l.google.com.                 164      IN    A        209.85.233.27
alt2.aspmx.l.google.com.                 164      IN    A        142.250.4.27
aspmx2.googlemail.com.                   164      IN    A        209.85.233.27
aspmx3.googlemail.com.                   34       IN    A        142.250.4.27
aspmx4.googlemail.com.                   216      IN    A        108.177.97.27
aspmx5.googlemail.com.                   216      IN    A        74.125.28.27
Scraping hackthissite.org subdomains from Google:
_________________________________________________


----   Google search page: 1   ----

 paste

----   Google search page: 2   ----

 radio

----   Google search page: 3   ----

 v3stage
 mirror
 mirror
 mirror

----   Google search page: 4   ----

 tor

----   Google search page: 5   ----

 tor


Google Results:
________________

mirror.hackthissite.org.                 3600     IN    A        137.74.187.134
mirror.hackthissite.org.                 3600     IN    A        137.74.187.133
tor.hackthissite.org.                    3600     IN    A        198.148.81.167
paste.hackthissite.org.                  3600     IN    A        198.148.81.163
paste.hackthissite.org.                  3600     IN    A        198.148.81.162
radio.hackthissite.org.                  3600     IN    A        198.148.81.170
v3stage.hackthissite.org.                3600     IN    A        198.148.81.147
```



```
Brute forcing with /usr/share/dnsenum/dns.txt:
-----------------------------------------------

admin.hackthissite.org.                  3600     IN    A        198.148.81.160
forum.hackthissite.org.                  3600     IN    CNAME    hackthissite.org.
hackthissite.org.                        3394     IN    A        137.74.187.104
hackthissite.org.                        3394     IN    A        137.74.187.100
hackthissite.org.                        3394     IN    A        137.74.187.101
hackthissite.org.                        3394     IN    A        137.74.187.103
hackthissite.org.                        3394     IN    A        137.74.187.102
forums.hackthissite.org.                 3600     IN    CNAME    hackthissite.org.
hackthissite.org.                        3394     IN    A        137.74.187.104
hackthissite.org.                        3394     IN    A        137.74.187.103
hackthissite.org.                        3394     IN    A        137.74.187.101
hackthissite.org.                        3394     IN    A        137.74.187.100
hackthissite.org.                        3394     IN    A        137.74.187.102
irc.hackthissite.org.                    3600     IN    A        185.24.222.13
irc.hackthissite.org.                    3600     IN    A        137.74.187.150
mail.hackthissite.org.                   3600     IN    A        198.148.81.135
ns1.hackthissite.org.                    3600     IN    A        198.148.81.188
ns2.hackthissite.org.                    3600     IN    A        198.148.81.189
stats.hackthissite.org.                  3600     IN    A        137.74.187.136
stats.hackthissite.org.                  3600     IN    A        137.74.187.135
www.hackthissite.org.                    3600     IN    A        137.74.187.103
www.hackthissite.org.                    3600     IN    A        137.74.187.100
www.hackthissite.org.                    3600     IN    A        137.74.187.101
www.hackthissite.org.                    3600     IN    A        137.74.187.104
www.hackthissite.org.                    3600     IN    A        137.74.187.102


Launching Whois Queries:
-------------------------

 whois ip result:   137.74.187.0       ->      137.74.187.0/28
 whois ip result:   185.24.222.0       ->      185.24.222.0/24
 whois ip result:   198.148.81.0       ->      198.148.80.0/20
```

These pictures are just an example of some of the capability of dnsenum. After a complete execution it's able to output many interesting information about the DNS, which are very interesting because they are a fundamental part of footprinting.