Information systems security
Information gathering (Reconnaissance)

One of the key steps during the penetration testing is the information gathering process. All the other penetration testing steps are relaying on it. This exercise will introduce the students with basic tools used for the information gathering.

1. Usage of the `nslookup` (`dig`) commands

`Nslookup` command allows for the requests to be sent to the DNS servers. There are several record types stored in the DNS database which are important during the information gathering, such as:

A – address resource record (RR) which maps the name to the IP address
NS – Name Service RR that defines domain DNS servers.
MX – Mail Exchanger RR which defines domain e-mail servers.
CNAME – canonical name RR which defines another name for the existing A host record.

Om windows VM or physical host open the command prompt and type nslookup followed by ENTER. This is interactive mode and to define the RR type, one must define it. We can use the following command to define the A RR type:

```
set type=A
```

Find the A and NS RRs for the following domain names and FQDNs (Fully Qualified Domain Names):

www.racunarstvo.hr: A RR: _____
racunarstvo.hr: NS RR: _____
"A" RR of the racunarstvo.hr DNS server: _____
racunarstvo.hr: MX RR: _____

www.google.com: CNAME: _____
A RR i: _____
_____
google.com: NS RR: _____
_____
google.com: MX RR: _____
_____

Which is the FIRST mail server the e/mail will be sent to for the google.com domain?
_____

Repeat all the above exercises on Kali Linux VM with the dig command!

2. Using WHOIS command

WHOIS allows for the information gathering on the DNS names and IP address ranges owners. Unfortunately, GDPR made this less usable on domain and IP address ranges belonging to EU citizens, but it is still usable tool for the rest of the world. We will use Kali Linux and `whois` command embedded in Linux distributions. On Windows we would have to install the client (Win32Whois), or we can use online services (find one of the online services one can use for this purpose):

Where is the google.com domain registered (with which company)?
_____
When is the google.com domain registered (date)?
_____
When will the google.com domain expire?
_____

Where is the cnn.com registered (with which company)?
_____
When is the cnn.com domain registered (date)?
_____
When will the cnn.com domain expire?
_____

Ca you use `whois` on racunarstvo.hr domain?
_____
Check the racunarstvo.hr domain `whois` records on
https://www.domene.hr/portal/about/web-whois
What is the racunarstvo.hr domain registered postal address and responsible?
_____

Check any .hr domain you like and list the data returned by the service:
_____

There are five IP address registers for world regions::
1. ARIN – US and Canada
2. LACNIC – Latin America
3. APNIC – Asia Pacific
4. AFRINIC - Africa
5. RIPE NCC - EU

Find the information on these registers and answer the questions below:

Who owns the IP address 161.53.45.45? _____
Who owns the IP address 161.53.178.24? _____
Who owns the IP address 92.122.230.135? _____
Who owns the IP address 10.1.1.1? _____
Who owns the IP address 1.1.1.1? _____
Who owns the IP address 251.251.251.251? _____
Who owns the IP address 107.181.169.48? _____
Who owns the IP address 40.112.92.184? _____

3. Using the `tracert` (`traceroute`) command

`Tracert` (`traceroute` on Linux) allows for the packet trace and helps in understanding on which route (which routers) packet used to reach the destination. On Windows VM or physical computer open the command prompt and answer the following questions by using the `tracert` command on Windows:
How many routers are on the route to www.algebra.hr?

_____
What is the IP address of the first router?
How many routers are on the route to www.fer.hr?

_____

How many routers are on the route to www.t-com.hr?

_____
For which country is the TLD .KZ in www.kimep.kz? TLD (Top Level Domain) defines (among other things) countries, like for instance, .HR defines Croatia (Hrvatska). Find the TLD information of all the world countries and find the country name behind the .KZ.

_____
How many routers are on the route www.kimep.kz?

_____
Where is the server for www.kimep.kz physically located?

_____
How many routers are on the route www.petrunic.com?

_____
Where is the server for www.petrunic.com physically located?

_____

4. Identifying the computers on local network

It is not an easy task to identify "live" hosts on the network, because there are tools like firewalls and IDS (Intrusion Detection Systems) deployed on the same network, and their purpose is to prevent the host enumeration. This might produce wrong identification, hence the tasks that follows and the tools used to identify open ports, services and vulnerabilities will work on the wrong subset of data, hence the tools like `nmap` might not identify important services. One of the best methods to identify live hosts on the same broadcast domain (computers connected to the same switch with no VLANs between them) is to use ARP scan. ARP is the protocol used on IPv4 networks to map NIC (Network Interface Card) MAC (Media Access Control) address to an IP address. The ARP resolution process must be done before the computer A will send the packet to computer B. This is valid for the same broadcast domain only. Let us quickly review the TCP/IP model:

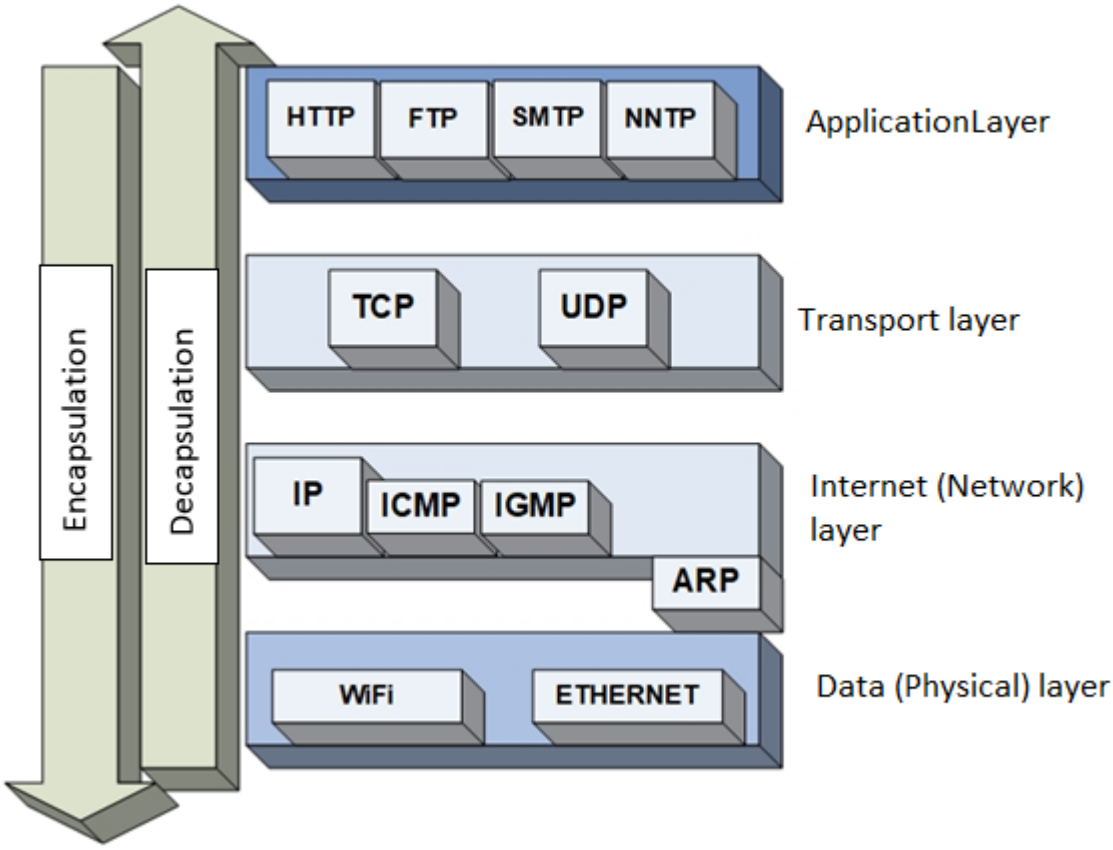

Image 1: TCP/IP model

ARP protocol is on the OSI model on the 2nd layer (Data-Link layer), while the IP protocol exists on the 3rd layer (Network layer). Firewalls operate on the 3rd layer and above, which means that the firewalls do not have any influence on the ARP scanning process.

Homework: Watch the short (13 minutes) animated video named "Warriors of the net" on YouTube. This video explains around 100 milliseconds of the network packet fife in the first 11 minutes.

Using the `arp-scan` tool on Kali Linux VM, check the live Ips on the local network. What is the exact command you can use for this purpose?

_____

The result shows three columns with data: IP address, MAC address and NIC manufacturer (derived from the MAC address). IP address is the computer IPv4 address assigned either manually or automatically through DHCP server, MAC address is the unique NIC identifier imprinted in the NIC EEPROM chip in the factory, while the column manufacturer represents the NIC manufacturer derived from the first 3 HEX pairs of the MAC address and check against the list of manufacturers called UOI (Unique Object identifier). Each NIC manufacturer is assigned the unique number(s) of 24 bits, while the rest of the MAC 24 bits is used by the manufacturer to define unique MAC for each produced NIC. If there are two NIC cards with the SAME MAC address in the network, we will have networking issues, because switches and computers will have problems uniquely identifying the endpoint and they will not be able to send the packet to the correct location. MAC address example je: 00:15:5d:63:43:12. In this case, the manufacturer is Microsoft does not produce the network cards, but they have virtualization platform (Hyper-V) that is using virtual NICs, and one of the Microsoft assigned UOI is 00:15:5d. Manufacturers are assigned multiple UOIs like this one, for instance one other UOI Microsoft is assigned is 00:50:f2 (When this was written, Microsoft had 21 UOIs assigned).
By using the `arp-scan` and grep commands try to filter only Hyper-V virtual machines in your scan results with `arp-scan`. Write down the command used:

_____

Try to expand the above command and by using the cut command (careful, NOT cat command, it is cut) extract only the IP addresses from the result. The result will be the IP addresses of identified Hyper-V VMs on the network. Write down the command used:

_____

5. using `nmap` tool

Nmap is the tool used for network scanning (for live hosts, ports, services and to some extent vulnerabilities identification). It is one of the most popular and most powerful tools in this category. We will use Kali Linux with preinstalled `nmap`.
First try to understand the basic options the tool offers by checking the help:

```
nmap
```

What is the option –sT used for? _____
What is the option –PN used for? _____
What is the option–sU used for? _____
What is the option –O used for? _____

Start the port scanning on the computer `scanme.nmap.org` with full TCP connection option:

```
nmap –PN -p 21,22,25,53,70,80,110,113,137,31337,50000 –sT scanme.nmap.org
```

Which are the three states `nmap` returns for TCP ports?

_____
How many open ports/services were identified?

_____
Name the services based on the port they are listening on (for instance: port 80=HTTP protocol? _____

Start the SYN scan:
`nmap –PN -p 21,22,25,53,70,80,110,113,137,31337,50000 –sS scanme.nmap.org`
How many open ports/services were identified?

_____

How many closed ports were identified? _____
There is one potentially strange service/port. Which one is it?

_____

Start UDP port scanning:
`nmap –PN -p 21,22,25,53,70,80,110,113,137,31337,50000 –sU scanme.nmap.org`
How many open ports/services were identified?

_____

How many closed ports were identified?

_____

What is the difference compared to Full TCP connect, SYN scan and this one?

_____

_____

Start port scanning for `www.racunarstvo.hr` with full TCP connection scan:
`nmap –PN -p 21,22,25,53,70,80,110,113,137,31337,50000 –sT www.racunarstvo.hr`
How many open ports/services were identified?

_____

Name the services based on the port they are listening on (for instance: port 80=HTTP protocol ? _____

Start SYN scan against same server as in the previous step:
`nmap –PN -p 21,22,25,53,70,80,110,113,137,31337,50000 –sS www.racunarstvo.hr`
How many open ports/services were identified?

_____

How many closed ports were identified?

_____

Start UDP port scanning:
`nmap –PN -p 21,22,25,53,70,80,110,113,137,31337,50000 –sU www.racunarstvo.hr`
How many open ports/services were identified?

_____

How many closed ports were identified?

_____