Exercises

Exercise 1:

1- Recall the security services
   Confidentiality, Authentication, Integrity, Availability
2- Give in a table for each security service with a type of attack that corresponds to it
3-

service	*attack*
Confidentiality	usurpation of identity
Authentication	interception of messages
Integrity	message modification
Availability	Dos

4- Give a way to achieve: authentication, confidentiality
   Authentication: password.
   Confidentiality: coding.
5- which service among the security services is attacked in the following cases:
   A- an attacker who succeeds in consulting a file transmitted on the network, he manages to see its content but can't decrypt it. **Confidentiality**
   B- B- The database of air Algerie has been attacked and all the seats available on the flight to London have been reserved under the name "L3". **Integrity**
   C- a user accidentally deletes a file and for fear of being punished, he hides this act. **Integrity**
   D- an attacker floods a DB server with non-stop requests. **Availability**
   E- a hacker manages to use an individual's credit card and buys an iPhone on the Apple website. **Authentication**
6- what is cybercrime? who is primarily targeted by it?
   cybercrime represents any malicious act committed on the Internet (network in general) using computer equipment.
   statistics have shown that cybercrime primarily affects companies.

7- what are the most common solutions used in companies to counter cybercrime?
   firewall, antivirus, ...

Exercise 2:

Alice wants to know if she can connect to the example.com site. To do this, she uses the ping command which sends a request to the site which responds by sending back data packets.

```
C:\>ping example.com

Pinging example.com [93.184.216.34] with 32 bytes of data:
Reply from 93.184.216.34: bytes=32 time=93ms TTL=53
Reply from 93.184.216.34: bytes=32 time=92ms TTL=53
Reply from 93.184.216.34: bytes=32 time=96ms TTL=53
Reply from 93.184.216.34: bytes=32 time=91ms TTL=53
```

1. Identify the IP of example.com. 93.184.216.34
2. 2. How does the computer link example.com to its IP address?
   The request is sent to a DNS server which has in memory the correlation between the domain name example.com and its ip address.

Exercise 3:

1- What is phishing?
   Technique used by hackers to steal personal information; the goal is to steal an identity. It involves making the victim think that he is communicating with a trusted third party to steal his information.
2- Name two ways to prevent fishing.
   check domain orthography.
   Write the url manually
3- what is the difference between a virus and a worm?
4- what is a backdoor?

   a backdoor is an unknown feature to the legitimate user, which provides secret access to the system.
5- how can an attacker proceed to install one?
6- what is a trojan horse?
   appears as a legitimate and harmless software, but once introduced into the system, actually behaves in a malicious way.
7- How can an attacker install one?
8- what technique does an antivirus use to detect malware?
   Two techniques:
   1- Signature search: search a special sequence of bits, but this way is not always good
   2- Behavior analysis: study the behavior of the software to discover dangerous actions

Exercise 4:

1- What is a DNS domain? To which domain does the name abc.def.gh.fr belong?
2- What is a DNS zone? Which zone does the name abc.def.gh.fr probably belong to?
3- Name some rules that govern the structuring of names (the way names are formed). are formed).

Exercise 5:

1- What is the difference between command injection, Xml injection, Xpath injection and SQL injection?
2- How can we secure a system against Injection attack?
   Verification of user input + use of secure functions for user input processing.
3- Describe a scenario of a SQL injection attack on a website.