Cryptography and VPNs

1.2 Cryptography and VPNs

+ **How does this support my pentesting career?**

  - Understanding how information is transmitted over computer networks
  - Choosing the right protocol for the job
  - Knowing how to protect your traffic

1.2 Cryptography and VPNs

- Why do we introduce Cryptography here?

- The main goal of this chapter is to introduce you to concepts that will be useful throughout the course; for instance, accessing our virtual labs.

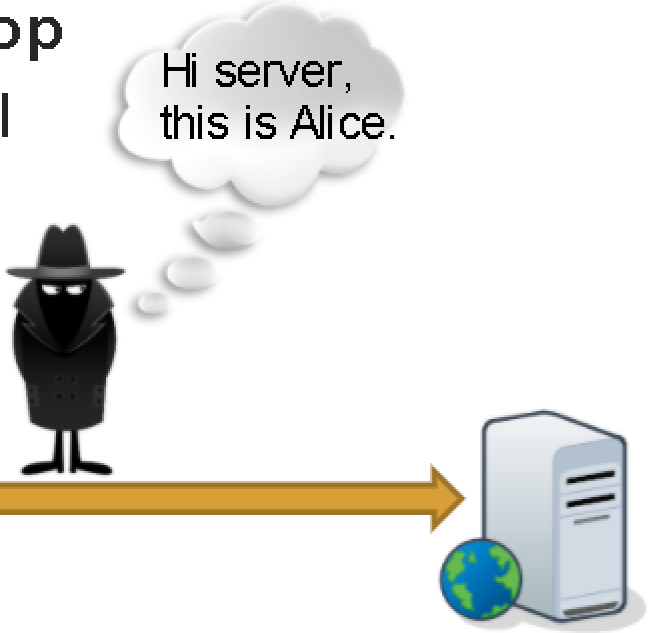
- We will now explain the main difference between clear-text and cryptographic protocols.

- Additionally, you will learn what a VPN (Virtual Private Network) is and how it works. All our virtual labs use VPN so knowing what it is will help you get most of out this course!

1.2.1 Clear-text Protocols

- **Clear-text** protocols transmit data over the network without any kind of transformation (encryption).

- This lets an attacker **eavesdrop** on the communication, as well as perform other malicious actions.



1.2.1 Clear-text Protocols

- Because of their nature, clear-text protocols are **easy to intercept, eavesdrop and mangle**. They should not be used to transmit critical or private information.

- If there is **absolutely no alternative** to a clear-text protocol, you should use it **only on trusted networks**.

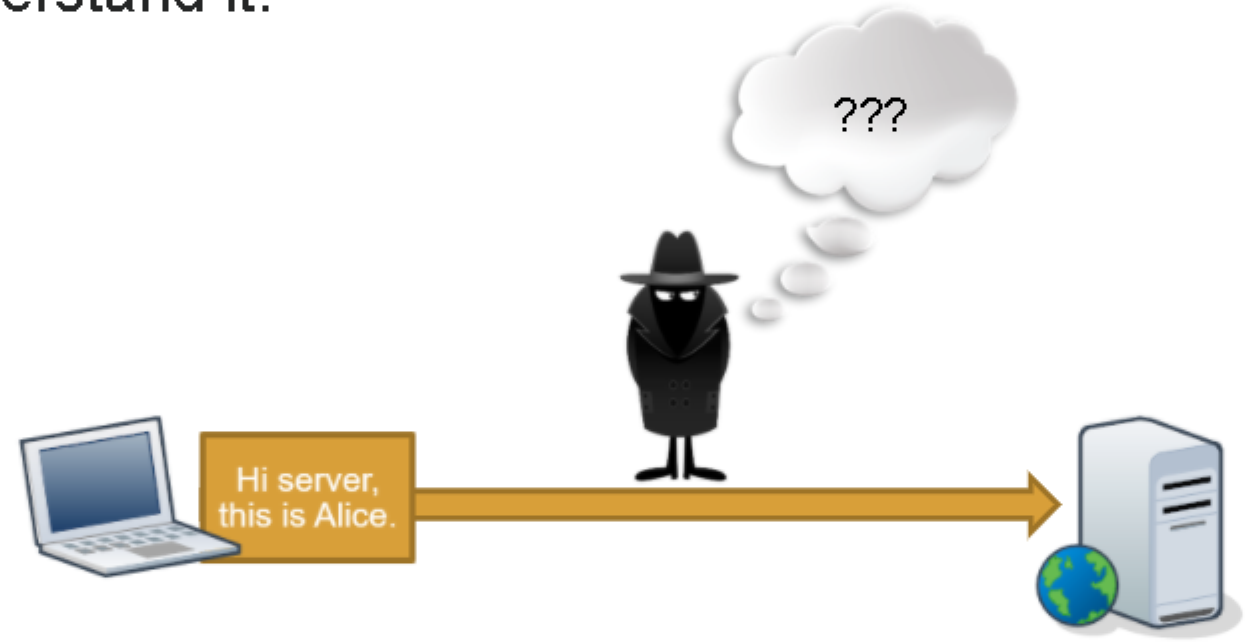
1.2.2 Cryptographic Protocols

- On the other hand, **cryptographic** protocols transform (encrypt) the information transmitted to protect the communication.

- Cryptographic protocols have many different goals. One of them is to **prevent eavesdropping.**

1.2.2 Cryptographic Protocols

- If an attacker intercepts the traffic, they will not be able to understand it.



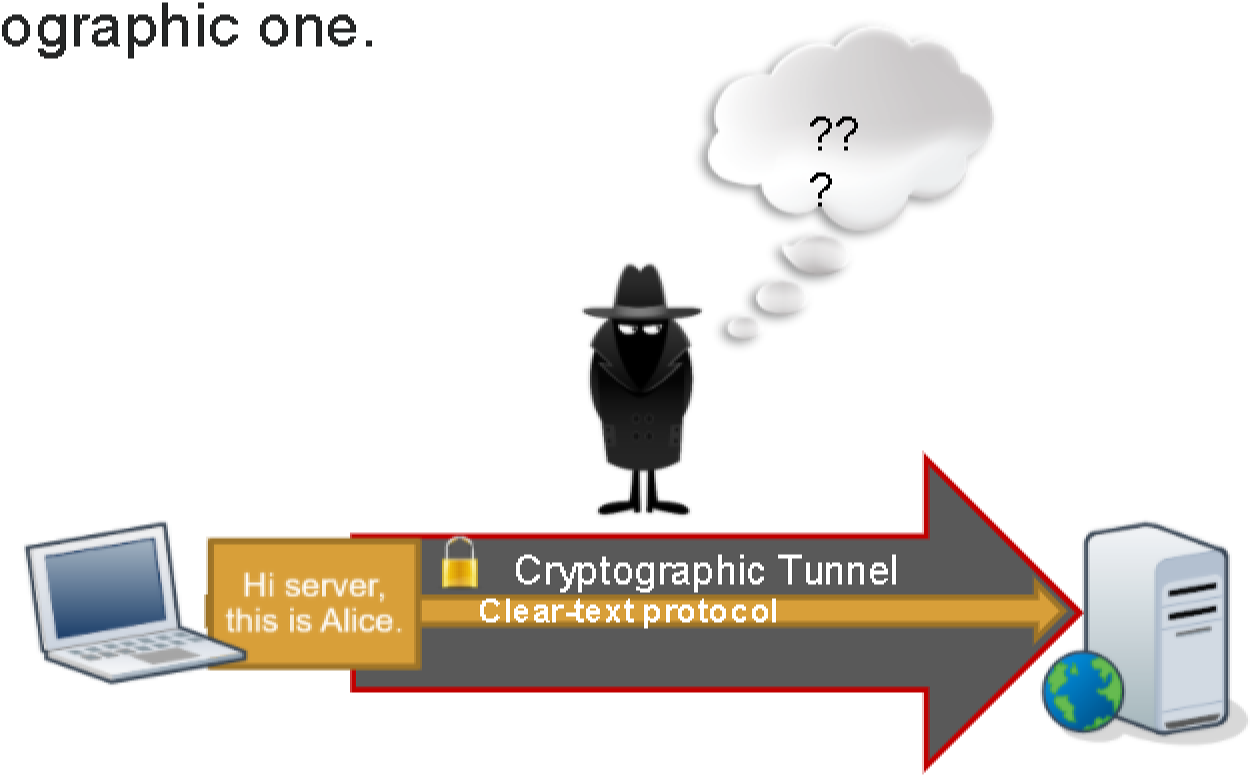
1.2.2 Cryptographic Protocols

- If you need to transmit private information, for example - a username and a password, you should always **use a cryptographic protocol** to protect the communication over the network.

- What if you need to run a clear-text protocol on an untrusted network?

1.2.2 Cryptographic Protocols

- You can wrap (**tunnel**) a clear-text protocol into a cryptographic one.



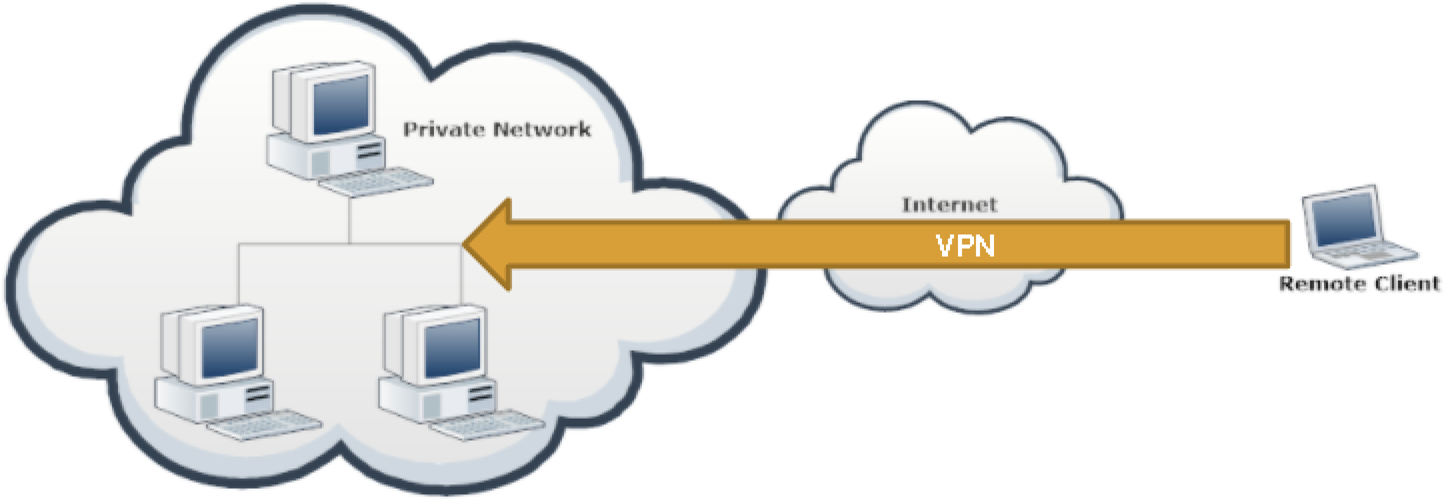
1.2.2 Cryptographic Protocols

- A great example of protocol tunneling is a **VPN**.

1.2.3 Virtual Private Networks

- A **Virtual Private Network** (VPN) uses cryptography to extend a private network over a public one, like the Internet.

- The extension is made by performing a protected connection to a private network (*such as your office or home network*).



1.2.3 Virtual Private Networks

- From the client point of view, being in the VPN **is the same as being directly connected** to the private network.

- For example, when you launch a *Hera Lab* scenario from your member’s area, a VPN tunnel is created, letting you connect directly to the lab network.

1.2.3 Virtual Private Networks

- When you are connected via VPN, you are actually running the very same protocols of the private network.

- This lets you perform even low-level network operations. For example, you can use a packet sniffer like **Wireshark**.