

INGENIERIA DE SISTEMAS – SPTI 2021-1

LABORATORIO 6:

**Laboratory Weapons to Exploit Network Layer**

GERSON DAVID QUINTERO RODRIGUEZ

Autor:

Torres Segura Duck James Alexander

Jimmy Armando Chirivi Nivi

1. **SECTION ONE**

(CAPTURE NETWORK TRAFFIC WHIT SCAPY):

SNIFFING:

Sniffing is a technique that involves capturing all the information that circulates through a network. This information is stored and interpreted to discover sensitive data such as passwords, bank information, etc. This attack is one of the main ones that are made when you try to steal information.

SCAPY:

Scapy is a powerful library written and supported in Python which allows the creation, manipulation and injection of packages from a network environment. It allows to perform different tasks such as Fingerprinting, Discovering, Enumeration, among others.

* 1. EXPLAIN THE FOLLOWING TASKS SCAPY PERFORMS:

|  |
| --- |
| **FINGERPRINTING:**  Fingerprinting maps an arbitrarily large data set or piece of data to a much shorter string of bits, your fingerprint, which uniquely identifies the original data by uniquely identifying people for practical purposes, and SCAPY analyzes these data sets. |

|  |
| --- |
| **DISCOVERING:**  SCAPY discovers hosts on the network during communication by using port scans. |

|  |
| --- |
| **ENUMERATION:**  SCAPY discovers network information by discovering and enumerating devices or computers on a network. |

VERIFY YOURSELF AS A USER:

1. Open terminal.
2. Cd /etc.
3. Nano hostname.
4. Enter your last name.
5. Save and exit.
6. Reboot the machine.



Ilustración 1: VERIFY YOURSELF AS A USER

CAPTURE NETWORK TRAFFIC WHIT SCAPY:

1. Open terminal.
2. Execute the command “scapy”.

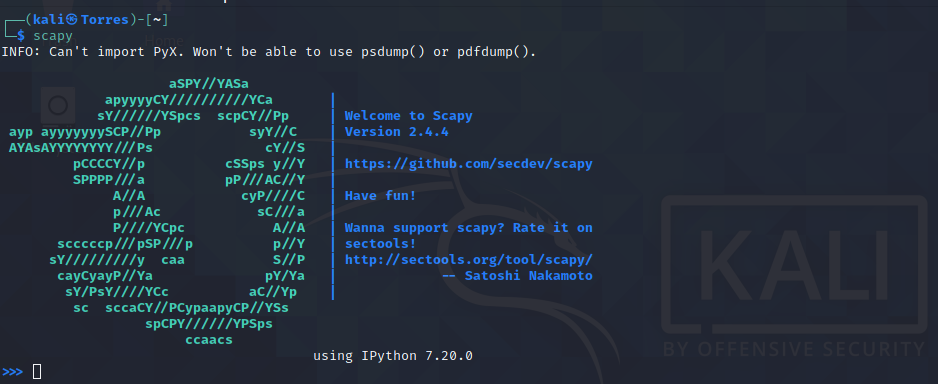


Ilustración 2: scapy

1. Execute the command “sniff(count=20, prn=lambda x: x.summary())”.

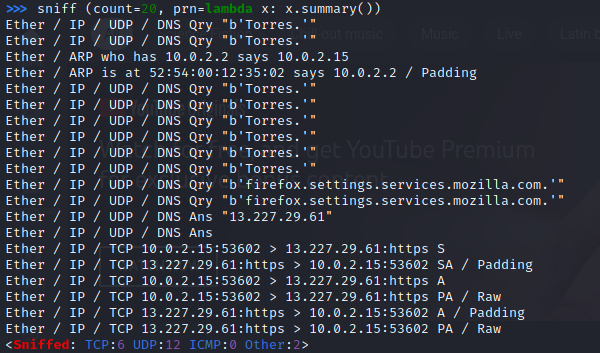


Ilustración 3: command

1. Explain the parameters of the command used:

|  |
| --- |
| count = number of packets to capture. 0 means infinity.  prn = function to apply to each packet. If something is returned, it is displayed.  prn = lambda x: x.summary(). |

1. Explain that important packets were captured:

|  |
| --- |
| The sniff listens to all the packets on the network some of these packets contain their protocols, dns, ips, input and output ports. |

1. Execute the following commands:

a=sniff(count=300).

a.plot(lambda x:len(x)).

Explain the information given by the graphic.

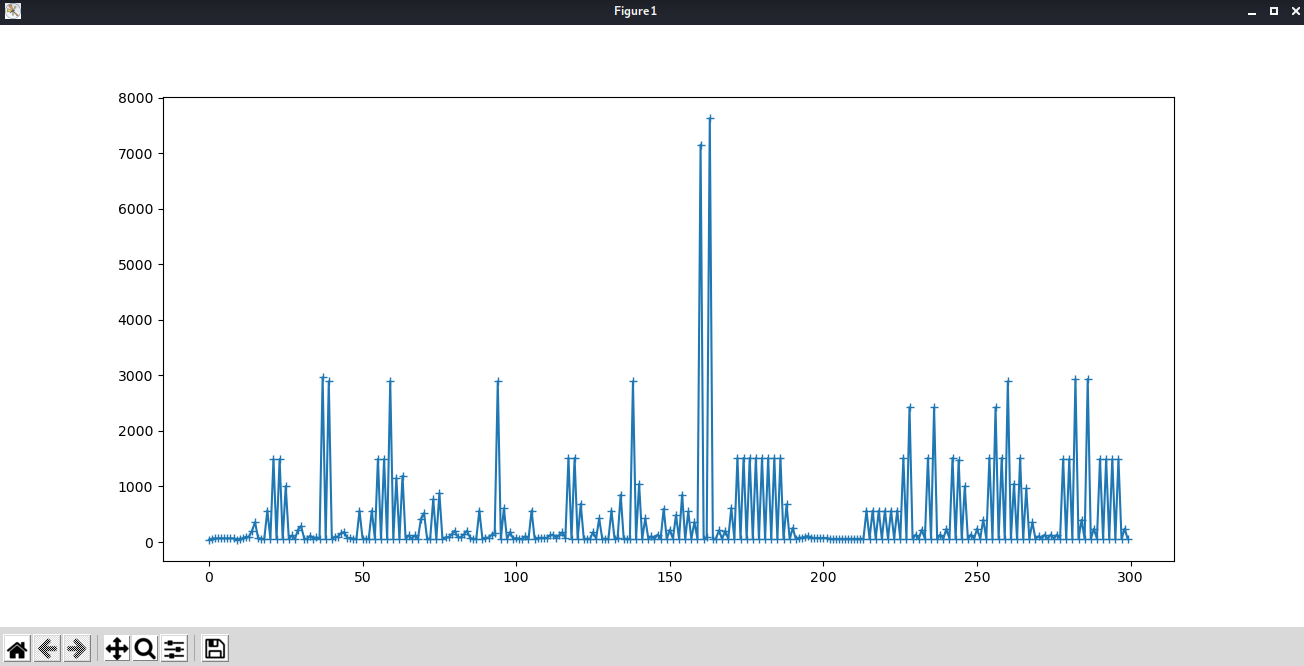
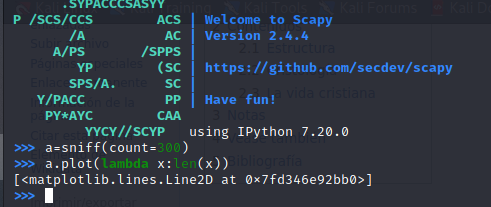


Ilustración 4: Explain the information given by the graphic

|  |
| --- |
| This function generates a graph with the data obtained in the sniff, where x is the amount of data and and its length. |

**2.2.** (CAPTURE NETWORK TRAFFIC WHIT WIRESHARK):

**WIRESHARK:**

Multiplatform tool with graphical interface for network analysis. This allows you to see, even at a low and detailed level, everything that is happening on the network. It is open source and multiplatform. It is often used as a better option when auditing networks usually Ethernet networks and is compatible with some others.

**CAPTURE NETWORK TRAFFIC WHIT WIRESHARK:**

1. Start the other machine.
2. Open terminal and start the services apache and mysql with the following commands:
   1. Service apache2 start.
   2. Service mysql start.
3. Execute the command “Wireshark” in the first machine.

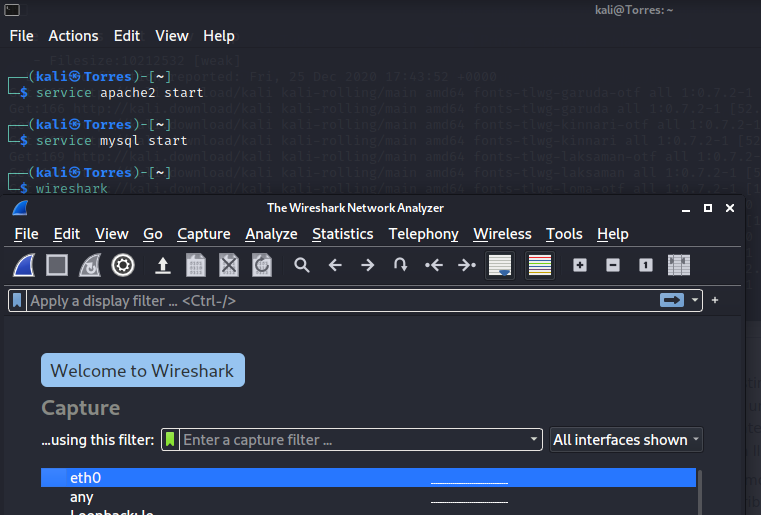


Ilustración 5: capture wireshark

1. Start traffic capture.
2. Open Firefox browser.
3. Enter to (second machine IP) / DVWA

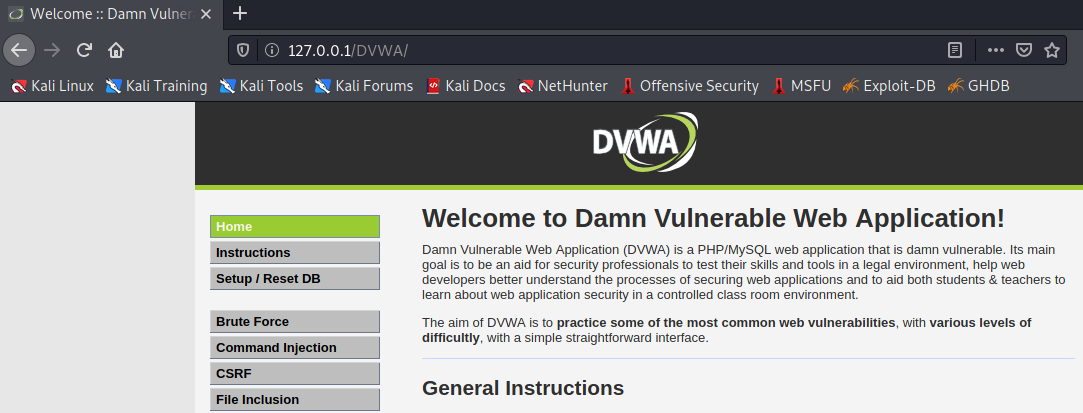


Ilustración 6: DWA

1. Enter to DVWA.
2. Enter whit User= “1337” and password=” charley”.

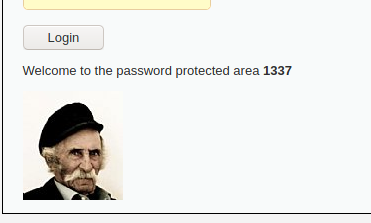
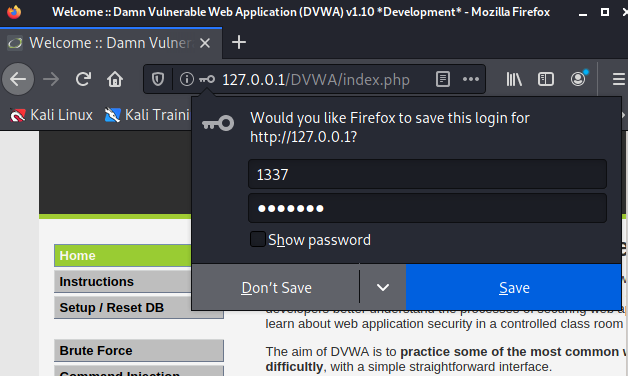


Ilustración 7: enter whith user

1. Stop traffic capture.
2. Filter capture by http.
3. Discover the vulnerability and explain

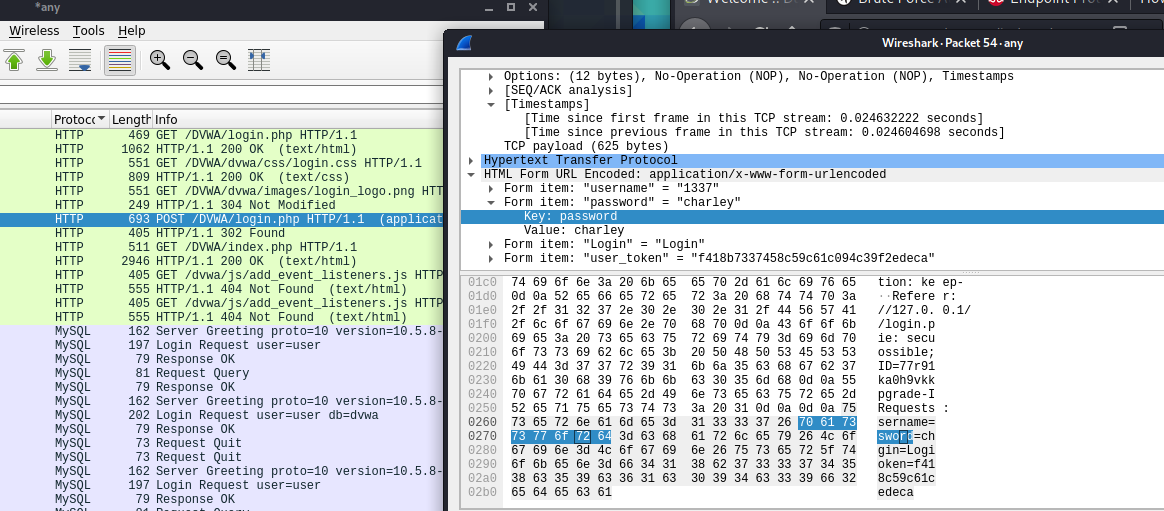


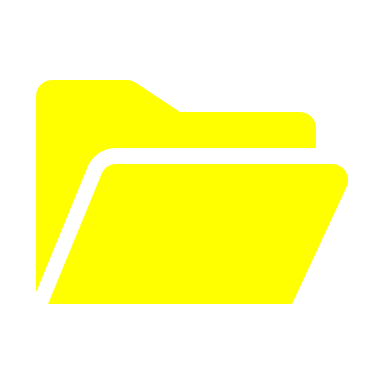
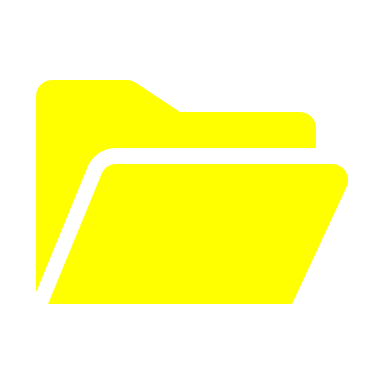
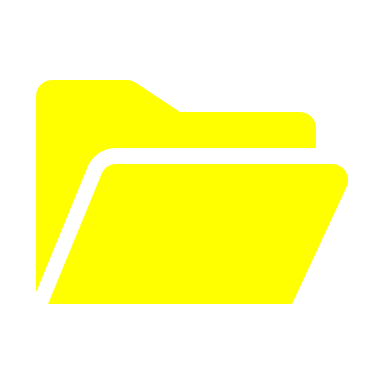
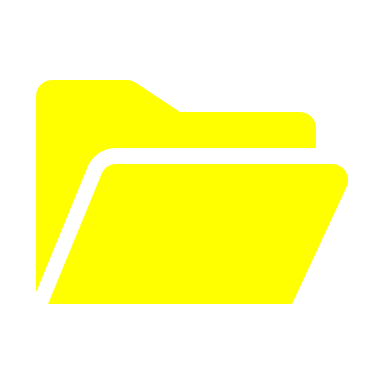
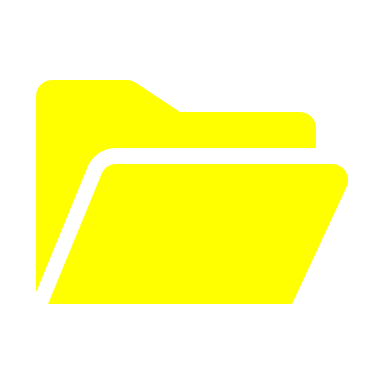
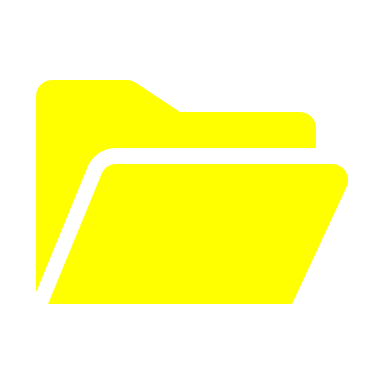
Ilustración 8: Discover the vulnerability and explain

|  |
| --- |
| With the WIRESHARK tool we have analyzed the packets sent and received with the http protocol where we found its vulnerability since it shows the username and password to access the DVWA application consulted in the MYSQL database. |

1. **SECTION TWO**

In section number two we are going to experience how to perform a man attack in the middle. For this we are going to need three machines, two of them sharing information and a third one that is going to be the spy or attacker, all within the same network.





Web Client

192.168.1.155

Internet Information Server

192.168.1.211

Man in the middle

192.168.1.204

When you have the machines running, check the IP's and MAC addresses, you would have to ping between all the machines.

|  |  |
| --- | --- |
| Web Client | **192.168.0.14** |
| Internet Information Server | **192.168.0.15** |
| Man in the middle | **192.168.0.17** |
| MAC Web Client | **08:00:27:83:74:da** |
| MAC Internet Information Server | **3C:91:80:90:68:0D** |
| MAC Man in the middle | **08:00:27:a6:1f:86** |

Verification of the connection of all machines.

Web Client:

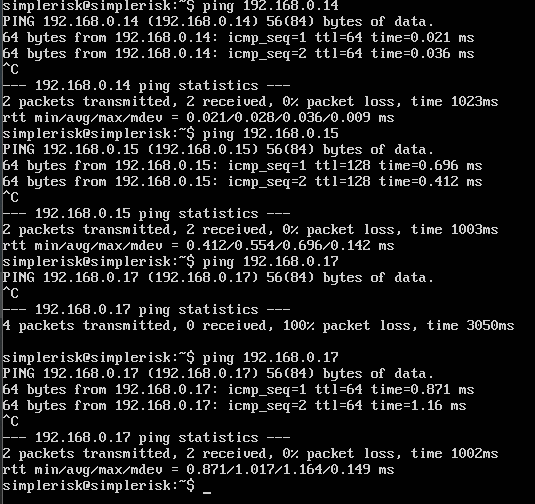


Ilustración 9:Verification of the connection

Internet Information Server:

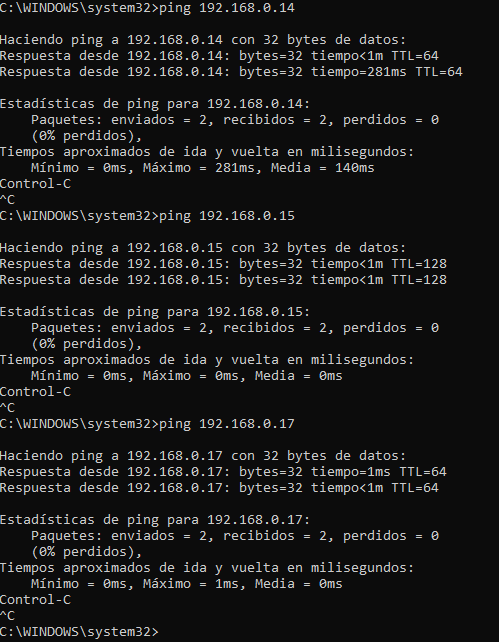


Ilustración 10:Verification of the connection

Man in the middle:

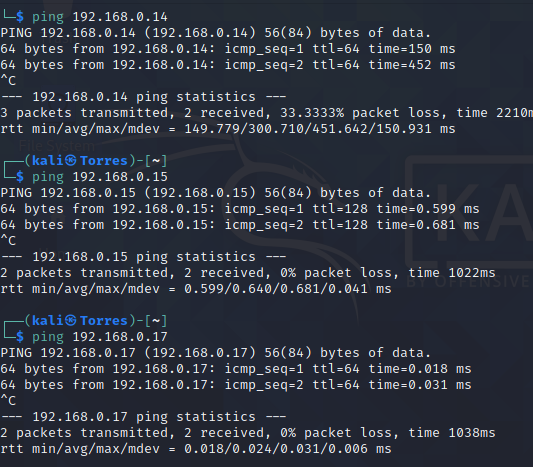


Ilustración 11: Verification of the connection

Note that MAC addresses must be different:

1. Run the following command "ifconfig eth0 down".
2. Run the following command "macchanger -A eth0" and explain what -A is for in the command.

|  |
| --- |
| -A: set random vendor MAC of any Kind. |

1. Run the following command "ifconfig eth0 up".

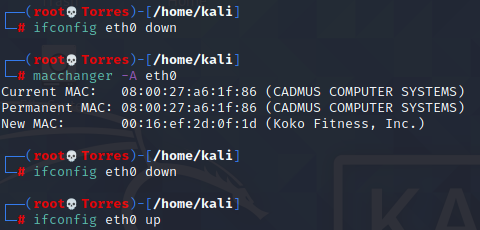


Ilustración 12: run command

1. Verify with the command "ifconfig" that the MAC address was changed.

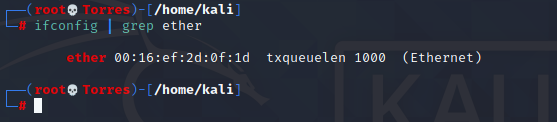


Ilustración 13: run command

Ping

1. Finally, check the ARP tables of each machine with the command "arp" and "arp -a" in Windows.

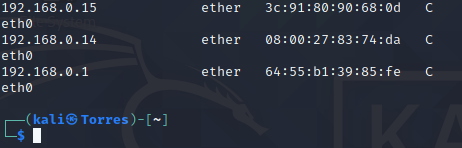


Ilustración 14: run command arp

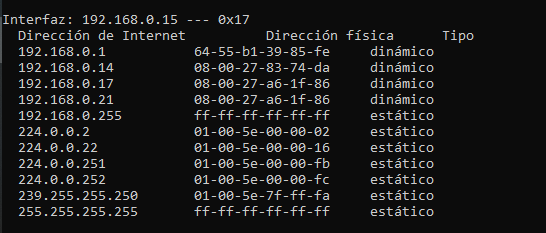


Ilustración 15: run command arp

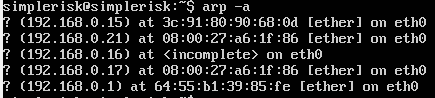


Ilustración 16: run command arp

1. **SECTION THREE**

Config the internet information server with the following steps:

1. Go to control panel.
2. Go to programs and features.
3. Go to turn windows features on or off.
4. Search the item “Internet information services” and active.
5. Save the changes.
6. Change the folder “wwwroot” by the given. The folder is locater a C:/inetpub/wwwroot
7. Verified that the page http://192.168.56.1/ /Loggin.html works.

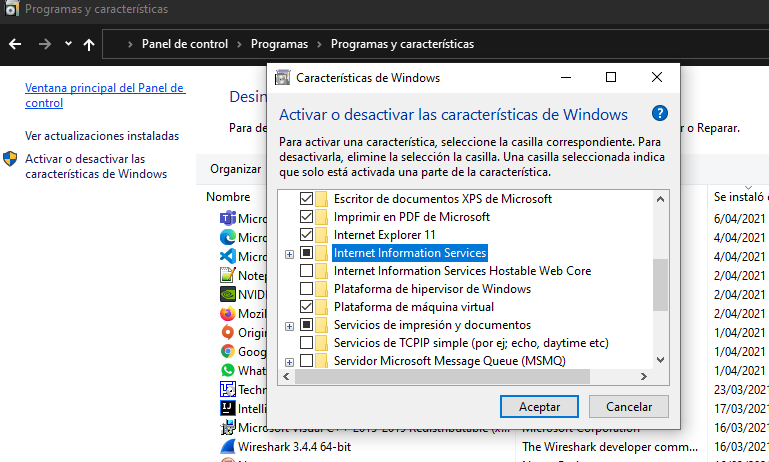


Ilustración 17: Internet information services

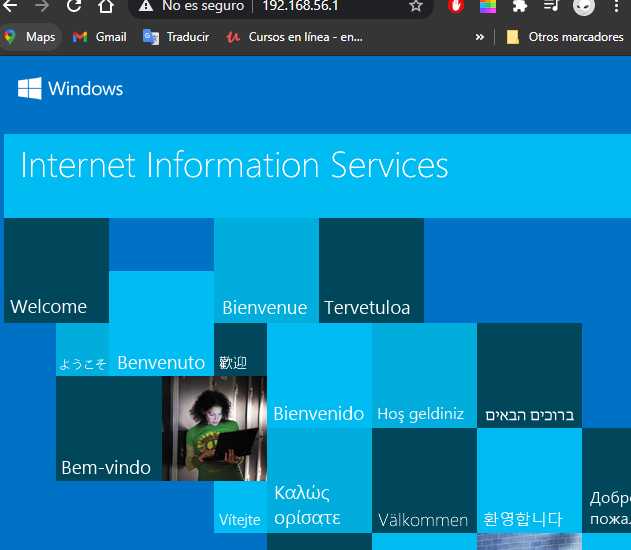


Ilustración 18: run Internet information services