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.

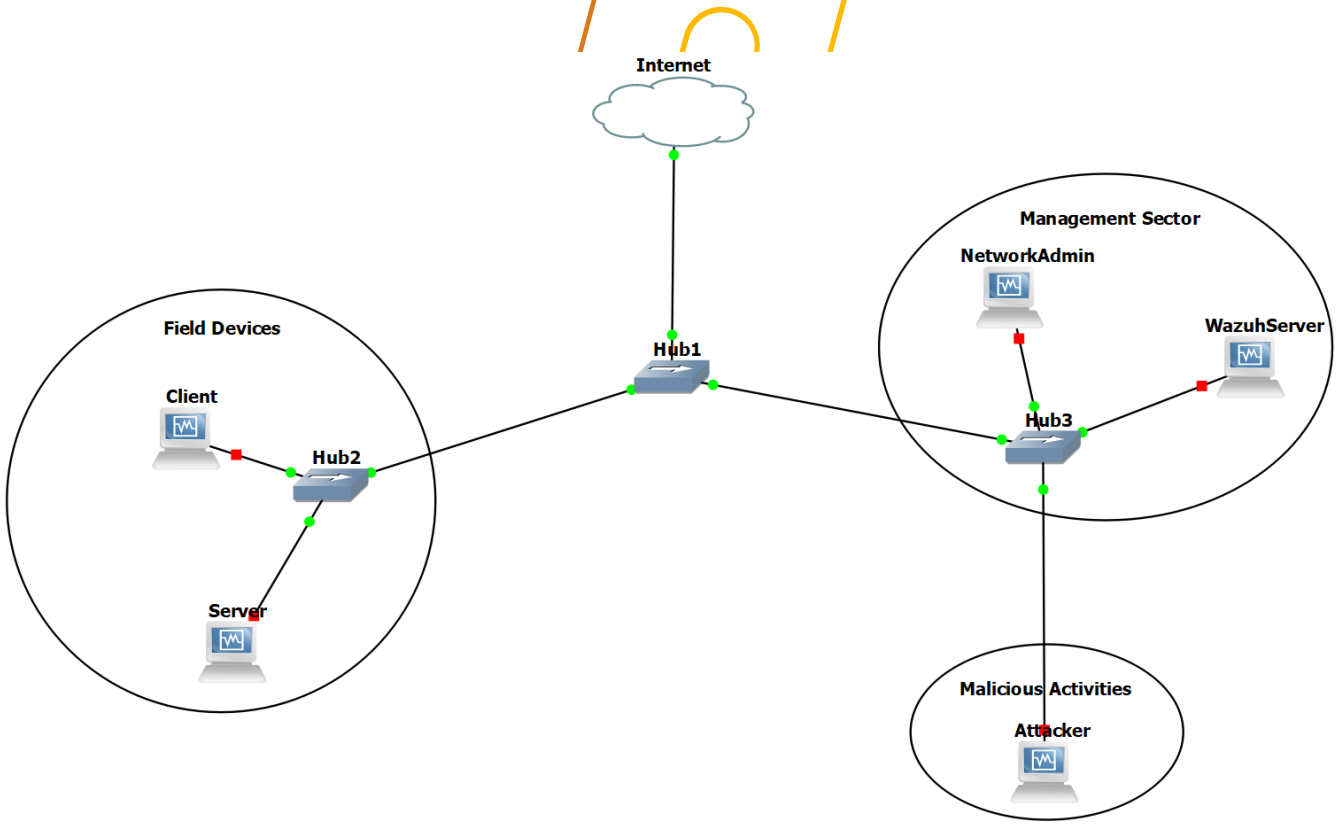
GNS3 Simulator

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

Offensive Tools

NMAP

MITM (Continue): Code Injection

- **Inject JavaScript** code into loaded pages.
- The code **will be executed** by the **browser**.
- Examples of code execution include:
  - **Replacing links**
  - **Modifying images**
  - And more
- **To do so**:
  - Write a simple JavaScript code:
    - Javascript: **alert('Hello World');**
    - Save the file "**InjectExample.js**"

- Then, we will use the `**hsthijack**` **caplet**. Update the configuration of the **caplet configuration file**, which is located at: `**/usr/share/bettercap/caplets/hsthijack.caplet**`

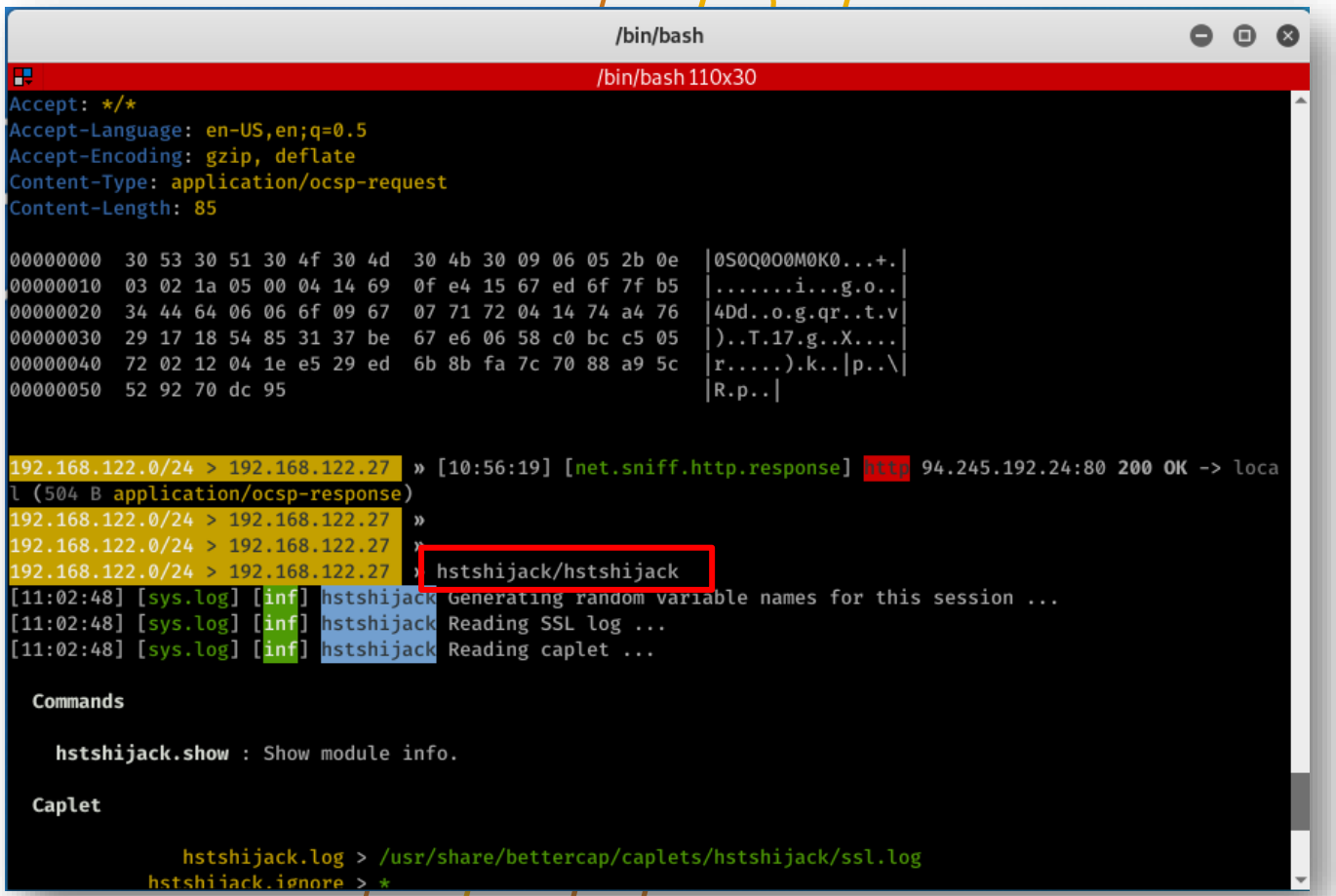
- Update the payloads with the path to your **JavaScript** code:
- ***:/usr/share/bettercap/caplets/hstshijack/payloads/InjectExample.js**
  - Here, the **code stored** on the **desktop** of **the Kali machine** (**attacker**) will be **loaded each** time the **user visits any website**.

MITM (Continue): Code Injection

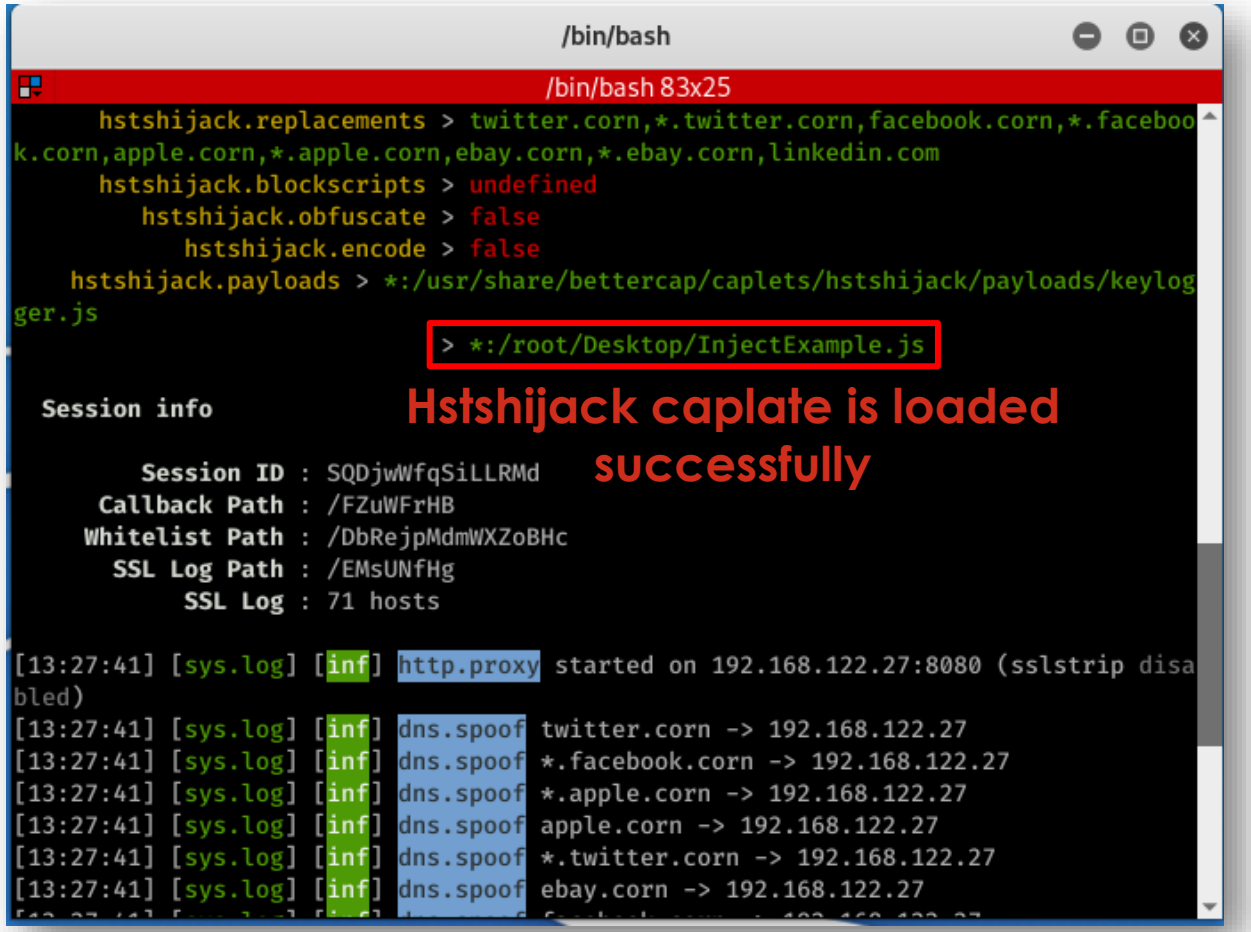
- Afterward run your caplet (or the bettercap spoofing attack commands)

Run the **hsthijack caplet**,
using the following command

hstshijack/hstshijack

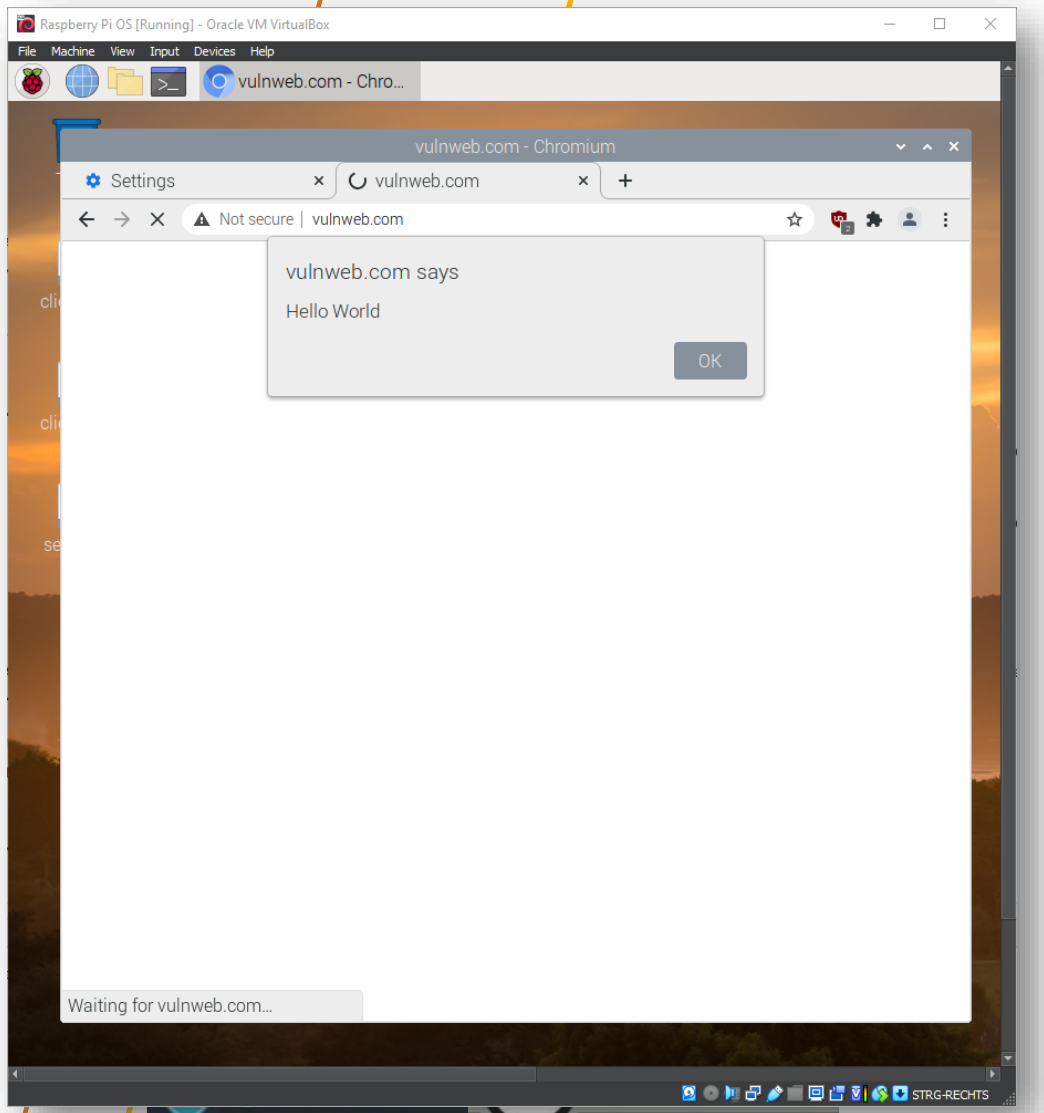


MITM (Continue): Code Injection



Hstshijack caplate is loaded successfully

How can we modify the code to ensure it only runs when the user visits a specific website?



Offensive Tools

NMAP

NMAP

- It is a network tool used for network scanning and device discovery.
- It can also be used for **network management** and **security testing purposes**.
- The tool is capable of **exploiting** network **devices**, **detecting open ports**, and **identifying** available **services**.
- Additionally, it can perform **vulnerability** and **OS scanning**, generating reports with scan results to **improve network security**.

NMAP

Scan for Open Ports

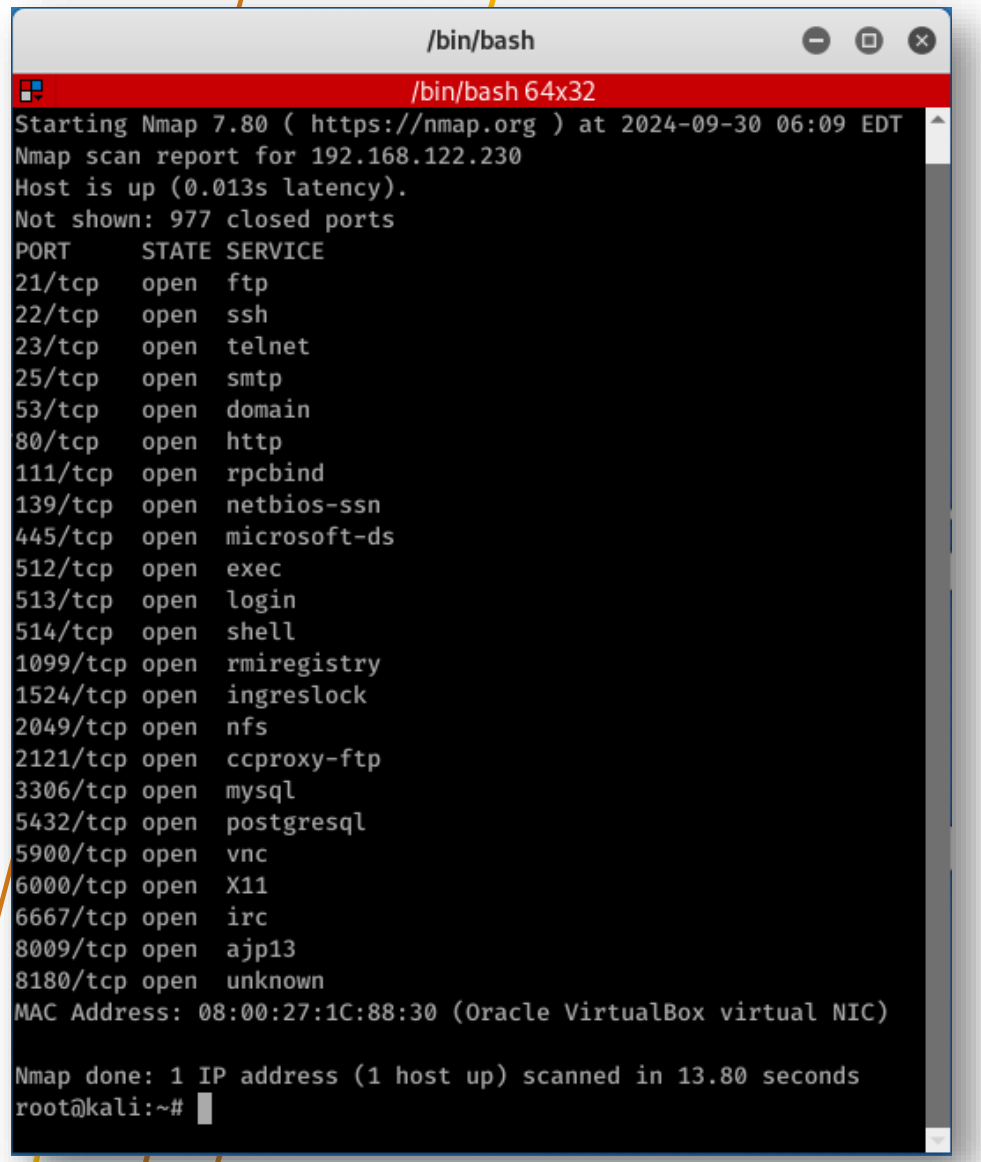
Let's target the **Metasploit** device to **identify** and **determine** the **existing** vulnerabilities.

Scans the **most common ports** on the target server

nmap 192.168.122.230

You can add **–F** to provide a fast scan

nmap -F 192.168.122.230



Nmap Commands - 17 Basic Commands for Linux Network (phoenixnap.com)

NMAP

Scan multiple hosts

Let's target the **Metasploit** device to **identify** and **determine** the **existing** vulnerabilities.

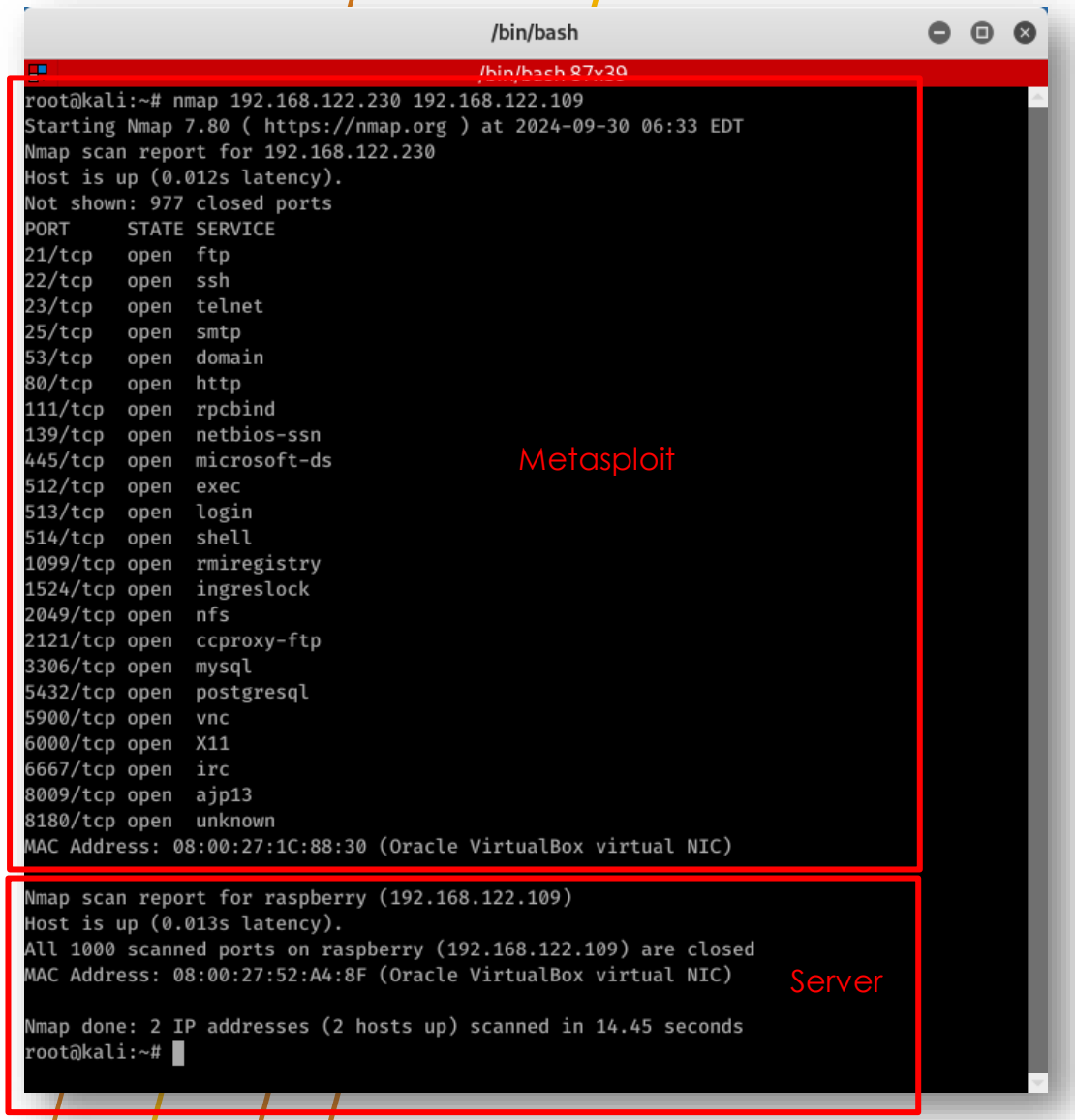
Scan more than **one host** at the same time; let's scan the **Metasploit** and **server** devices.

nmap 192.168.122.230 192.168.122.109

Additional commands

nmap 192.168.122.* Scan the entire subnet

nmap 192.168.122.103-109 Scan for a range



Nmap Commands - 17 Basic Commands for Linux Network (phoenixnap.com)

NMAP

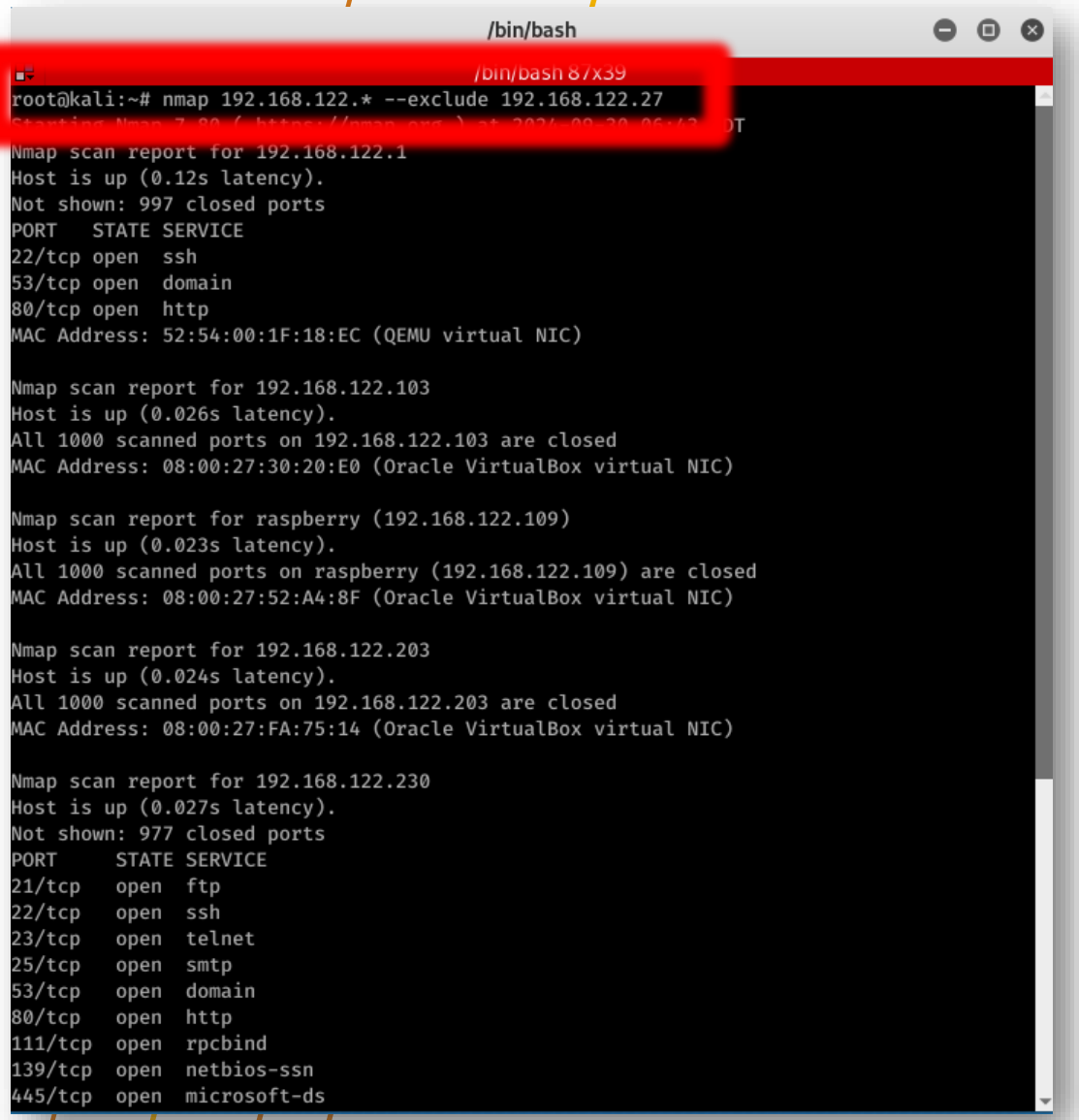
Scan multiple hosts

Let's target the **Metasploit** device to **identify** and **determine** the **existing** vulnerabilities.

Scan more than **one host** at the same time; let's scan the **Metasploit** and **server** devices.

nmap 192.168.122.* --exclude 192.168.122.27

Scan the **entire network**, **excluding** the attacker device with the IP ending in **.27**.



Nmap Commands - 17 Basic Commands for Linux Network (phoenixnap.com)

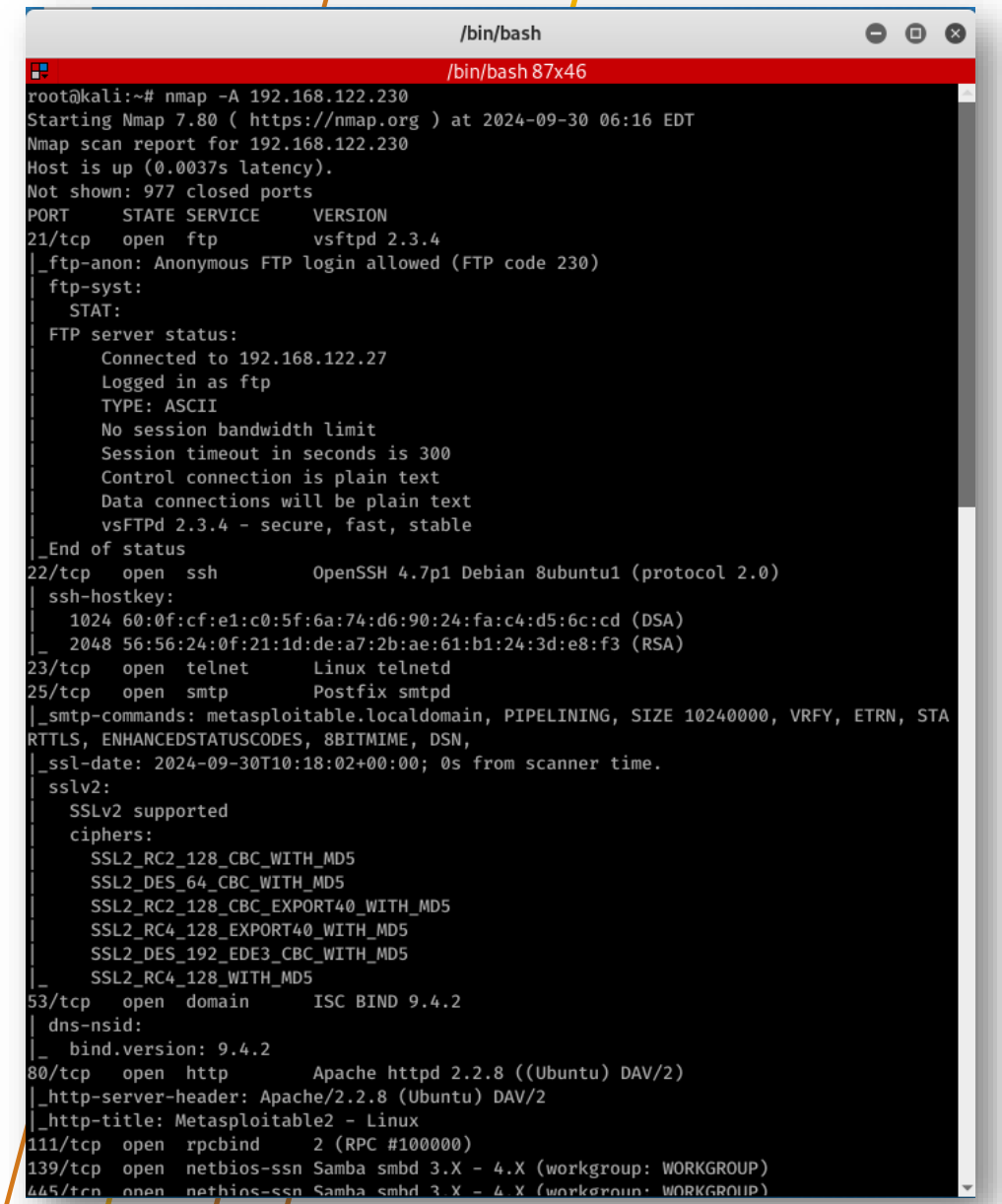
NMAP

Scan to Find out OS Information

Let's target the **Metasploit** device to **identify** and **determine** the **existing** vulnerabilities.

Discover the **operating system** information of the hosts that are mapped.

nmap -A 192.168.122.230



Nmap Commands - 17 Basic Commands for Linux Network (phoenixnap.com)

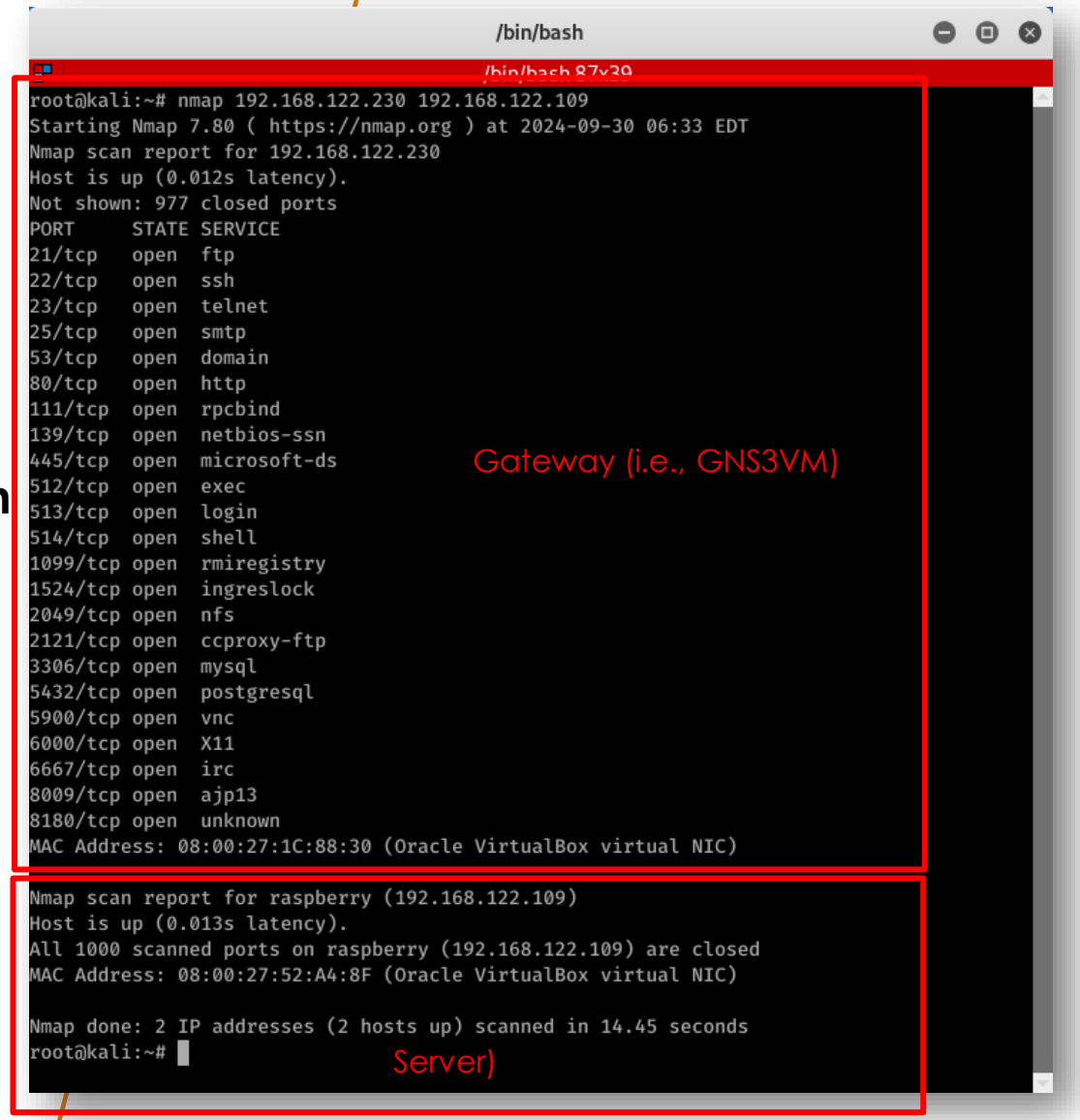
NMAP

Scan to Find out OS Information

Let's target the **Metasploit** device to **identify** and **determine** the **existing** vulnerabilities.

Retrieve **additional** details about the **operating system** of the **mapped** host.

nmap -O 192.168.122.230



Nmap Commands - 17 Basic Commands for Linux Network (phoenixnap.com)

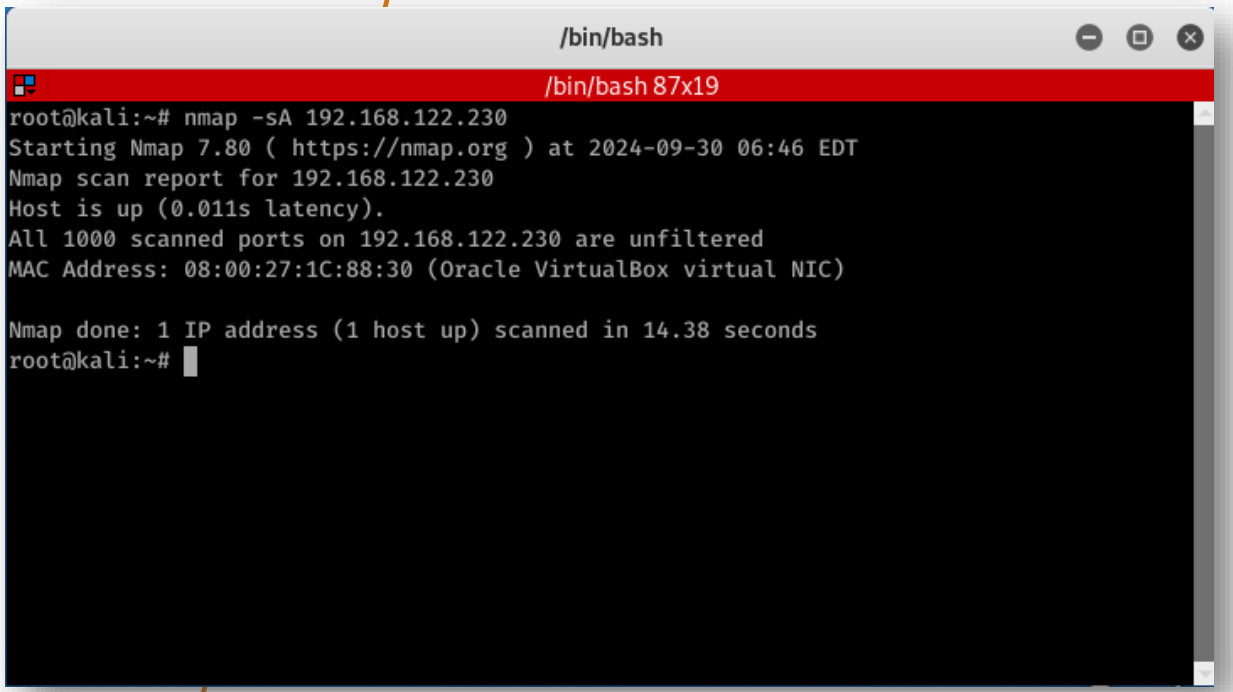
NMAP

Scan to Detect Firewall Settings

Let's target the **Metasploit** device to **identify** and **determine** the **existing** vulnerabilities.

Retrieve whether a **firewall** is **active** on the host.

nmap -sA 192.168.122.230



[Nmap Commands - 17 Basic Commands for Linux Network (phoenixnap.com)]

NMAP

Scan for Ports

Let's target the **Metasploit** device to **identify** and **determine** the **existing** vulnerabilities.

Scan for a **particular port**

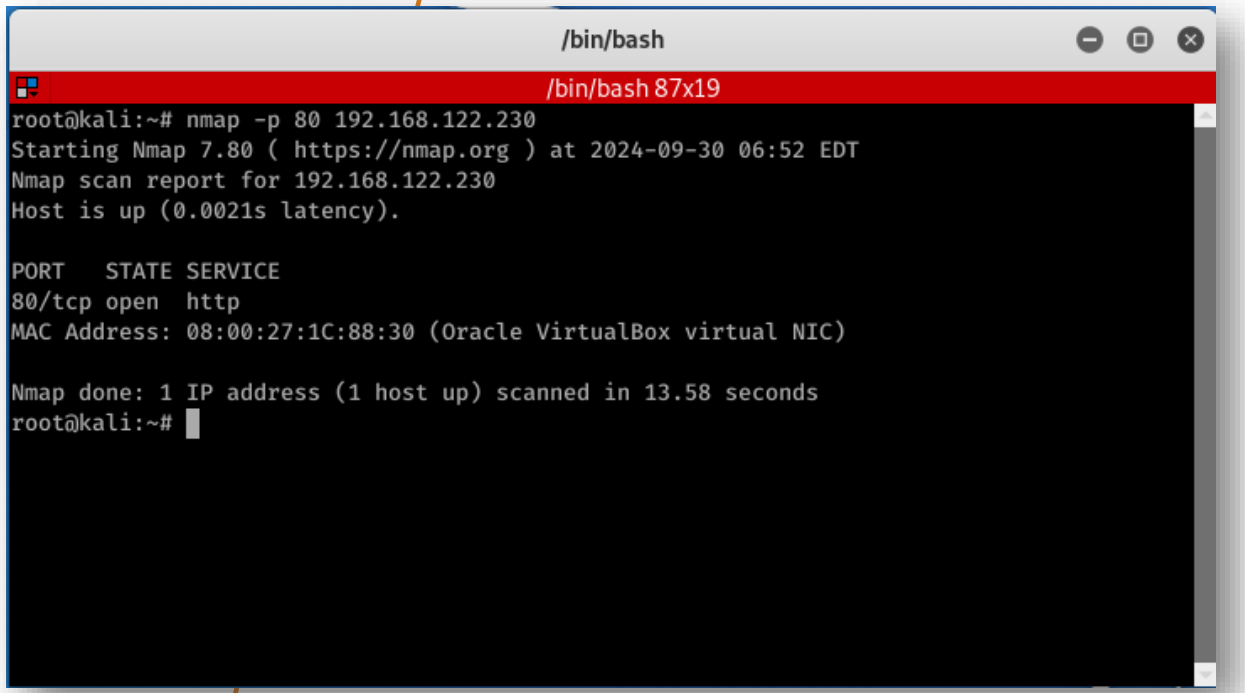
nmap -p 80 192.168.122.230

You can scan for **multiple ports**

nmap -p 80, 443 192.168.122.230

You can scan a **range** of ports

nmap -p 80-100 192.168.122.230



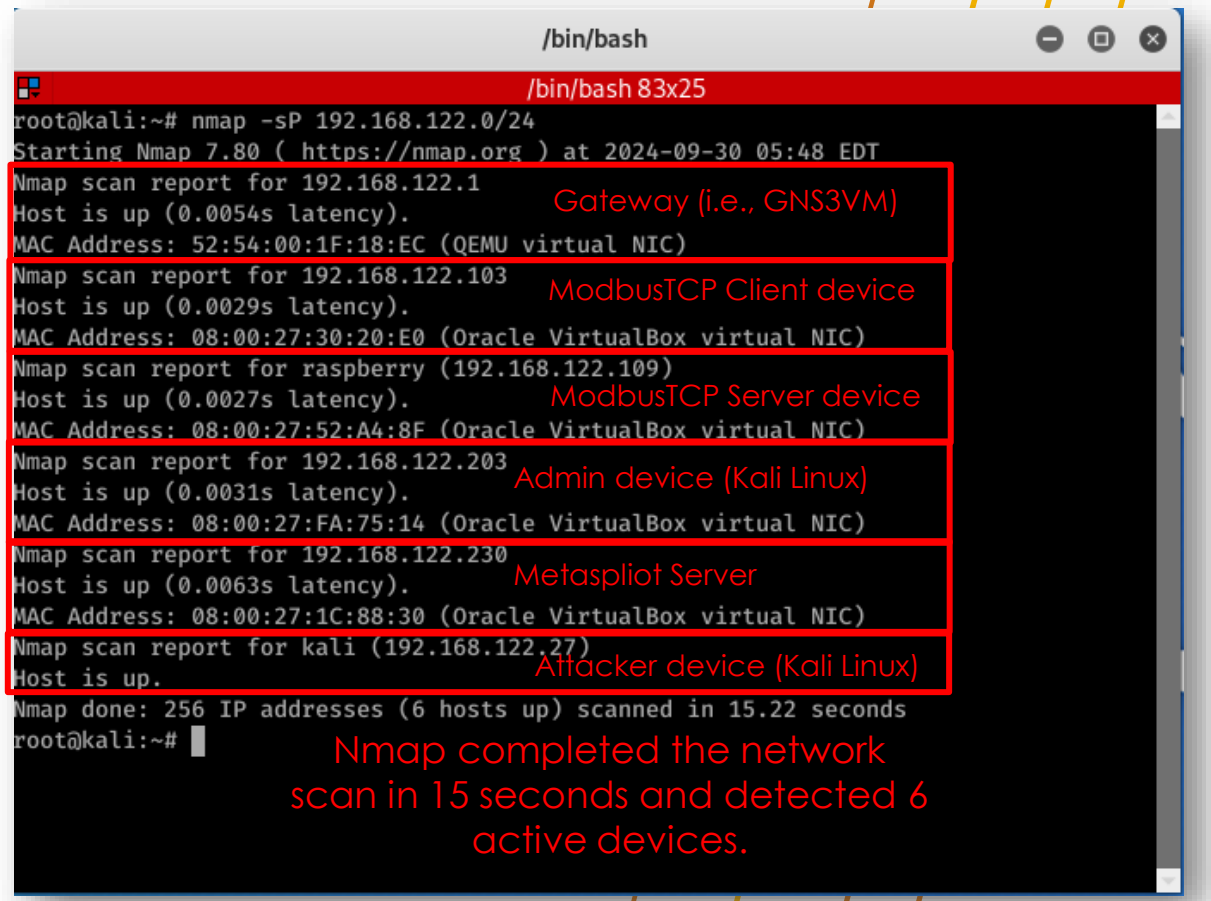
Nmap Commands - 17 Basic Commands for Linux Network (phoenixnap.com)

NMAP

- Scan all **available devices** in your network (instead do **ping** for **each device**). Use the following command:
  - **Nmap –sP <network>**

Nmap –sP 192.168.122.0/24

The **-sP command will produce a list of which machines are active and available**



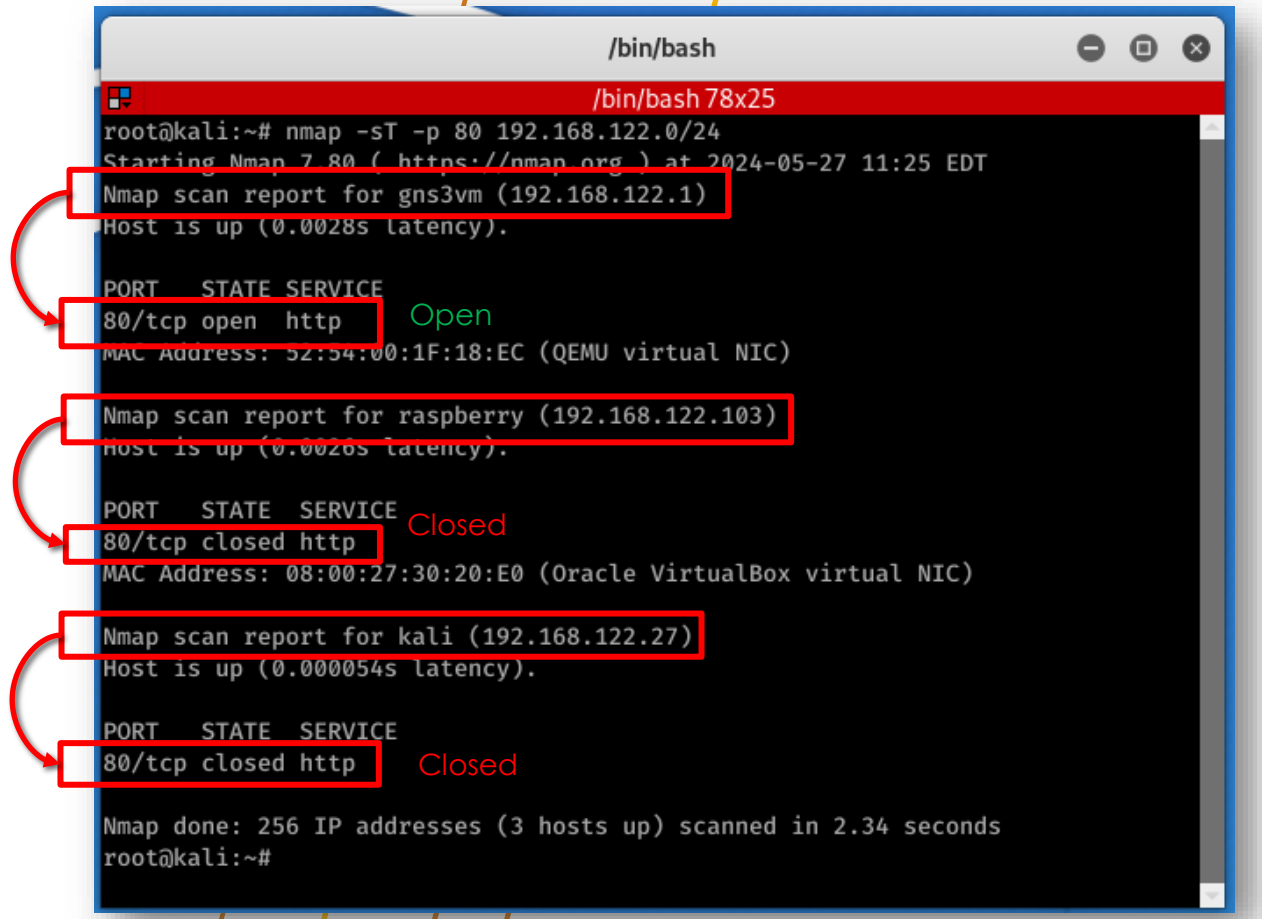
Nmap Commands - 17 Basic Commands for Linux Network (phoenixnap.com)

NMAP

- Scan all **all open** ports in the network/a particular device:

nmap –sT –p 80 192.168.122.0/24

- **sT**: **TCP** connect (3-way handshake)
- **p**: ports (you can use a **comma** "," for multiple **searching** of **ports**)

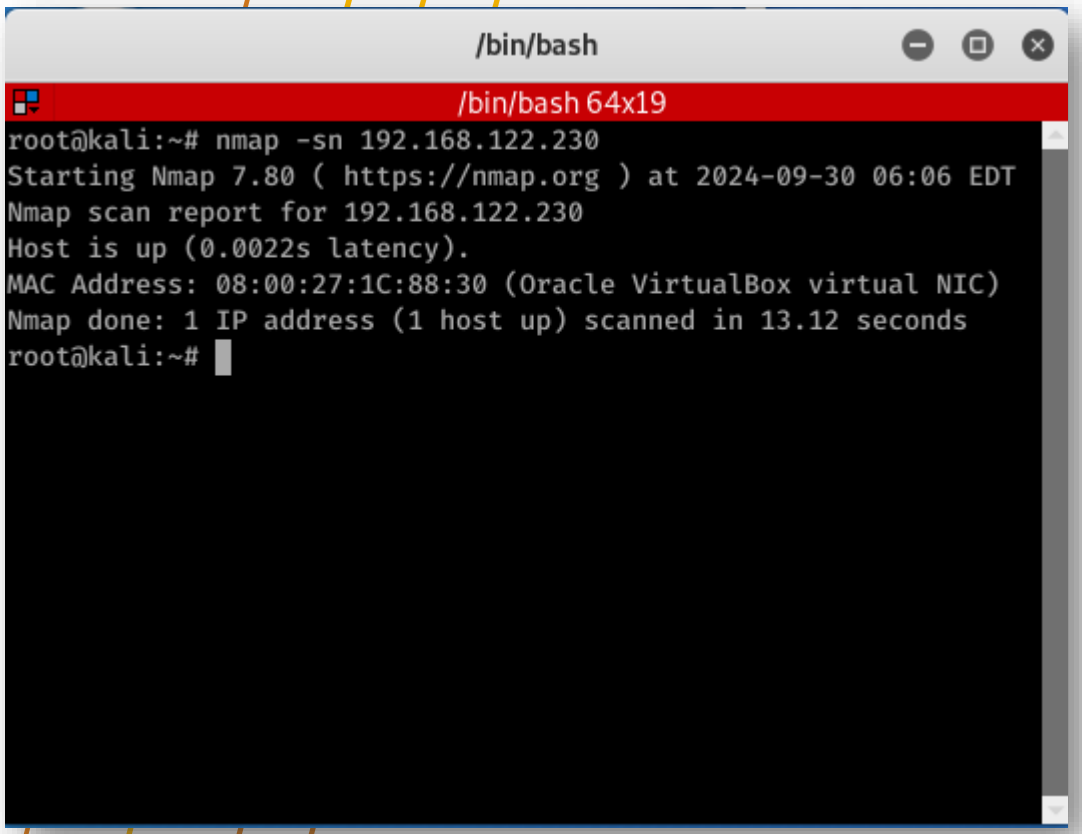


NMAP

Let's target the **Metasploit** device to **identify** and **determine** the **existing** vulnerabilities.

check if the **Metasploit** server is **online** and **reachable**:

nmap -sn 192.168.122.230



Thank you

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