Network Protection for Energy Control Systems

CSP004_C_E

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

CyberSecPro
CC BY NC SA

Acknowledgement

- *Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.*
- *Project Agreement no. 101083594*

CyberSecPro CC BY NC SA

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.

CyberSecPro

CC BY NC SA

GNS3 Simulator

CyberSecPro
CC BY NC SA

GNS3 Simulator

- GNS3, is open-source and free software.
- It allows network engineers to virtualize real hardware devices.
- GNS3 consists of two main software components:
  - the **GNS3-all-in-one software** (**GUI**) and
  - the **GNS3** virtual machine (**VM**).
- The **GNS3-all-in-one software** (**GUI**) serves as the client interface, installed on local PCs (Windows, MAC, Linux) for creating network topologies.
- The local GNS3 server runs on the same PC as the GUI, along with additional processes like Dynamips.
- The **GNS3 VM** (recommended) can be run locally using virtualization software (e.g., VMware Workstation, Virtualbox) or remotely on a server (e.g., VMware ESXi, cloud).
- GNS3 allows us to create a network topology and an environment for an ideal platform for simulating victims and attackers' machines.

Getting Started with GNS3 | GNS3 Documentation

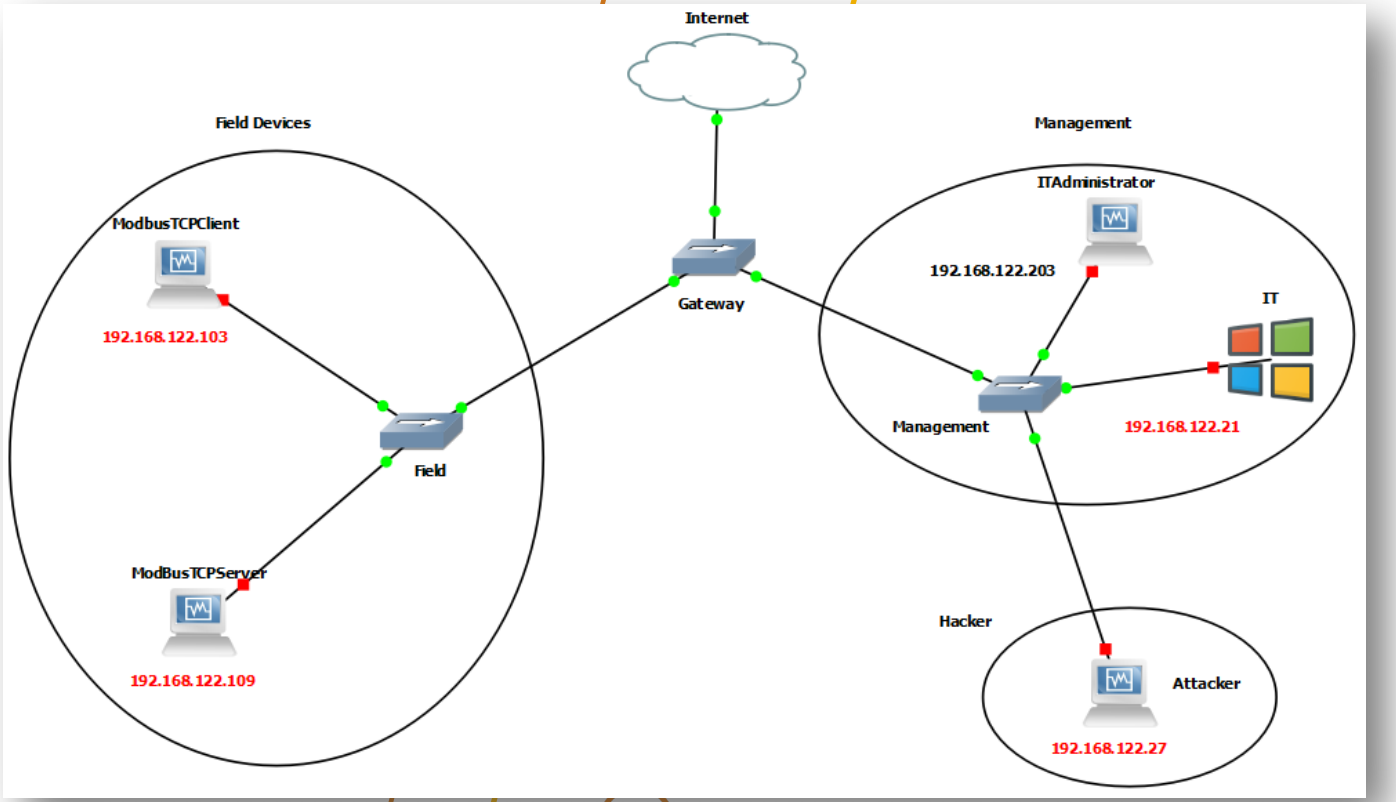
CyberSecPro
CC BY NC SA

Why GNS3?

- GNS3 facilitates the building of a complete lab environment by integrating multiple VMs (installed individually).

- This will help create a fully isolated environment consisting of multiple VMs with victim machines and an attacker, allowing you to perform your practical tasks within this course in a safer way.

- Here is an example of how the virtual lab could be designed on GNS3.

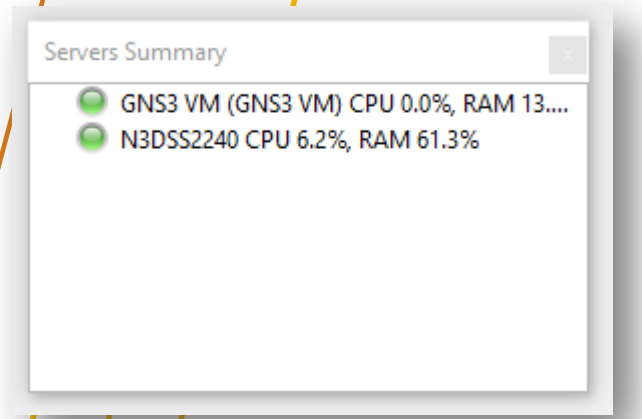


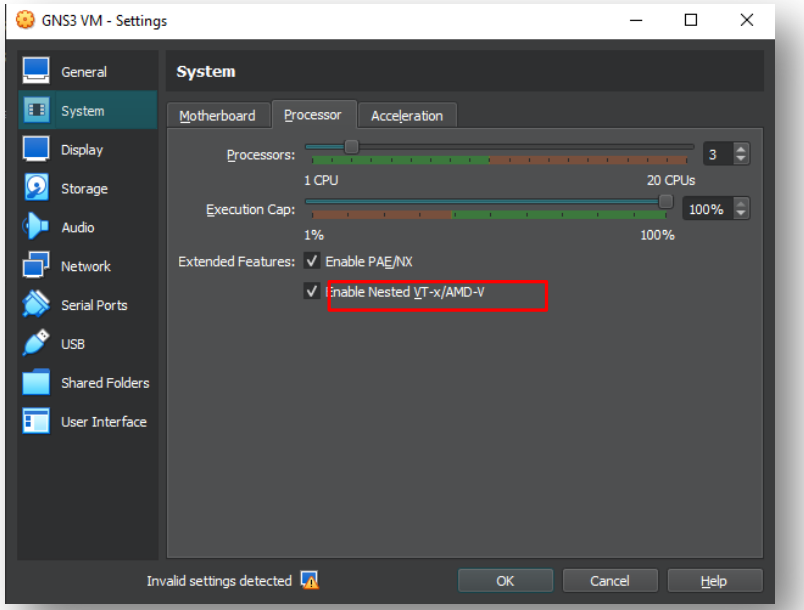
Targeting any external target not within this proposed virtual lab environment is strictly forbidden, and you are solely responsible for any consequences.

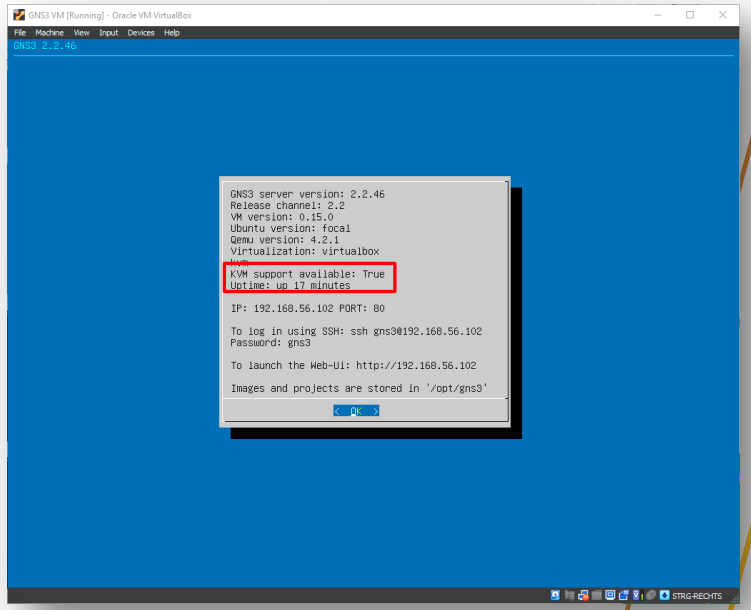
CyberSecPro
CC BY NC SA

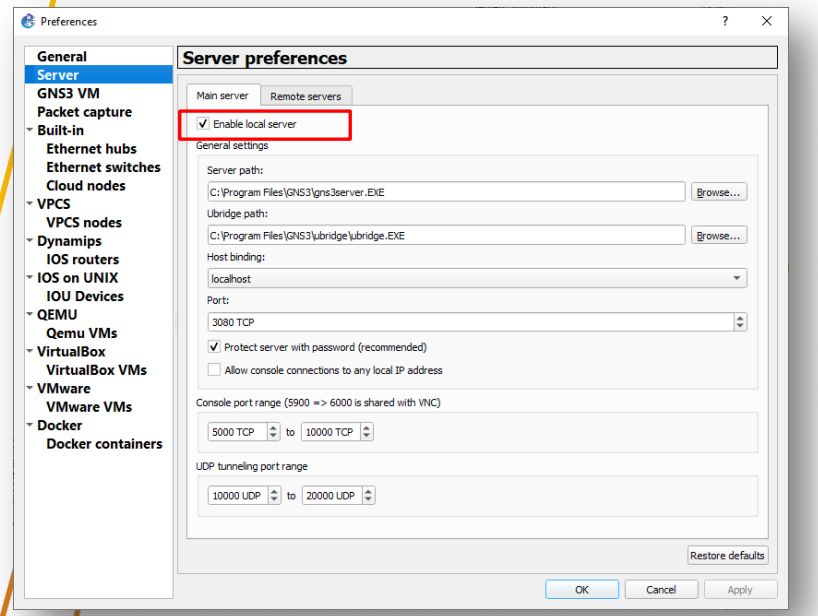
Installing GNS3

- Downlaod GNS3 from the official website: Software | GNS3, and then install it.
- **Download and install GNS3 VM based on your preferred VM:** Software | GNS3









Kali Linux - Attacker

- It is the most advanced Penetration Testing Linux Distribution.
- Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics, and Reverse Engineering.
- Download and install the Kali Linux as a normal VM on your PC.
- I will discuss later how to integrate it with GNS3

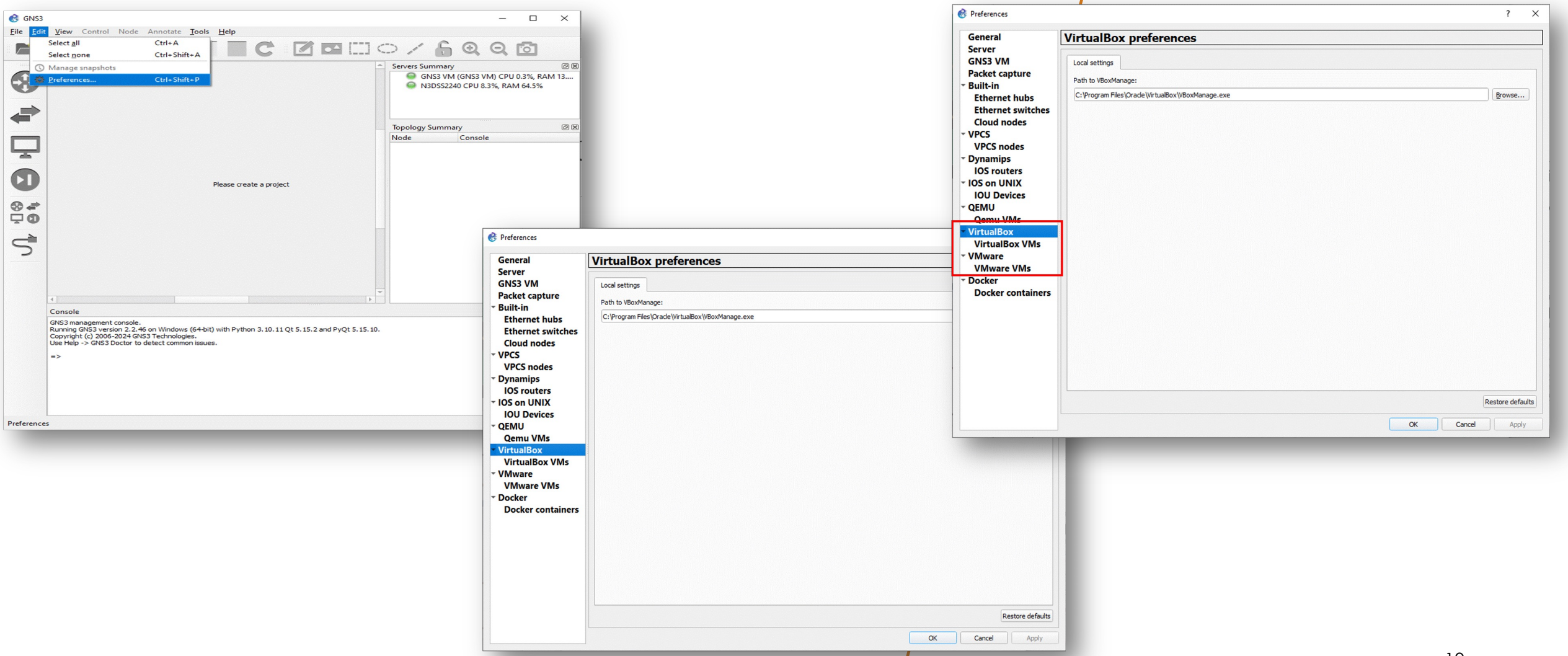
CyberSecPro
CC BY NC SA

Client/Server/IT – Victim Machines

- Set up two VMs as a client and server to transmit values through the Modbus protocol.
- Therefore, install Raspberry Pi Desktop on your computer. You can download the ISO image from HERE.
- After that, install pyModbusTCP on your Raspberry Pi Desktop. A useful example for a server and client can be found on Python Modbus Communication.
- Additionally, you can install a Windows VM/ or another Klai Linux as an IT management device for monitoring the network.

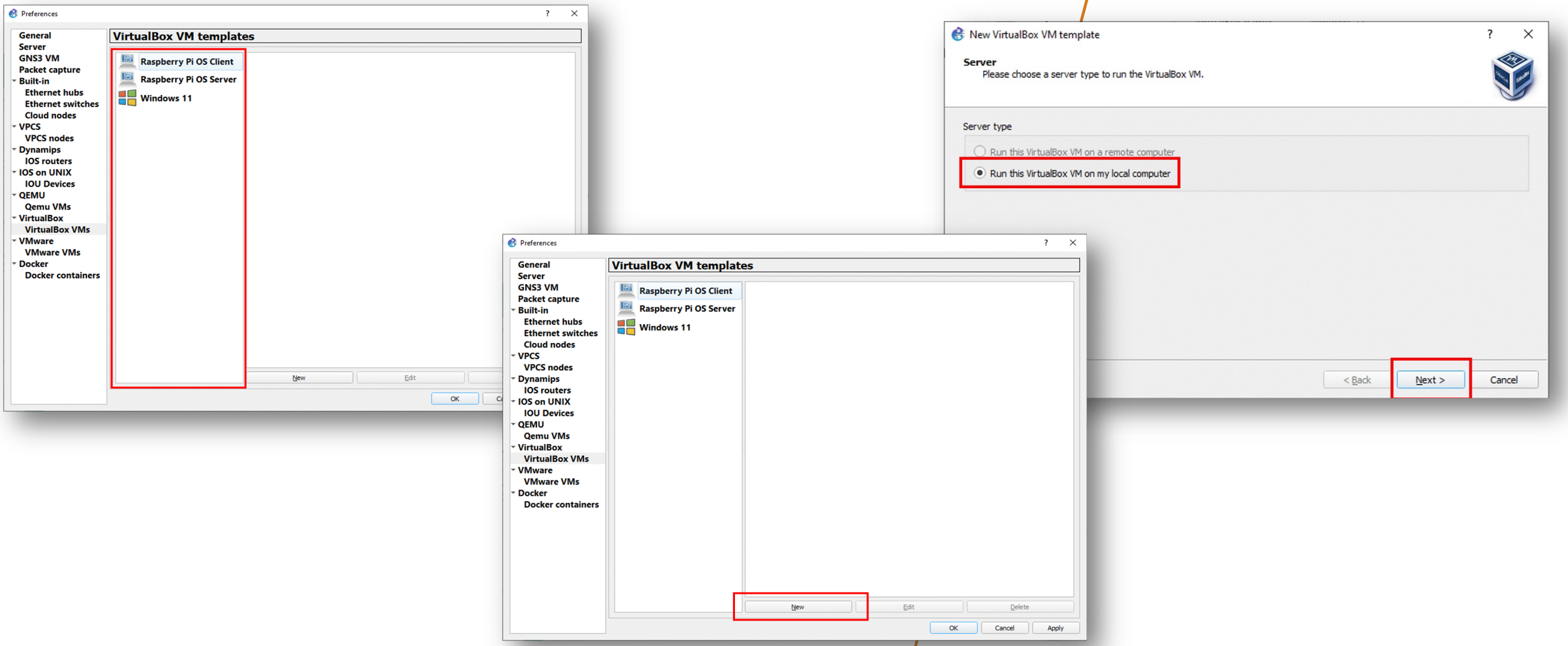
CyberSecPro
CC BY NC SA

Integrating VMs to GNS3



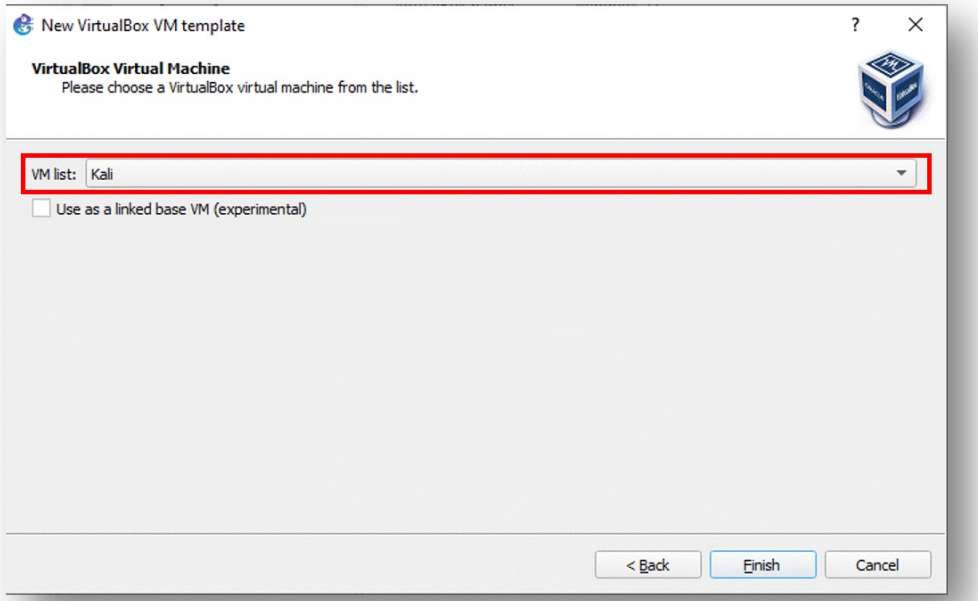
- Do the same for any VM you want to integrate with GNS3

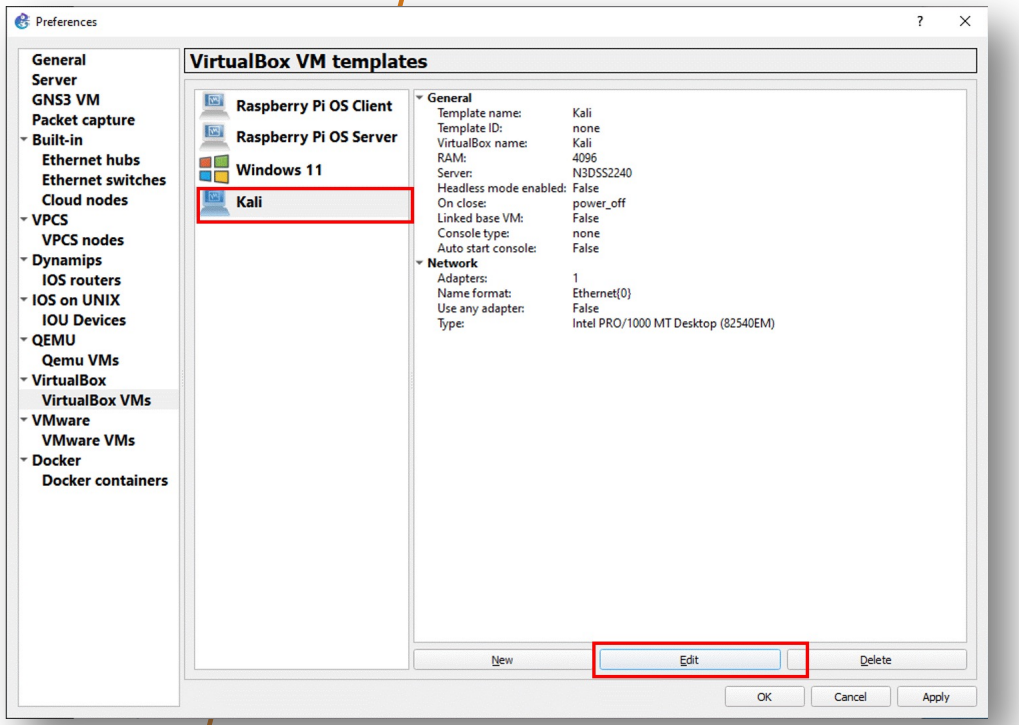
Integrating VMs to GNS3



- Do the same for any VM you want to integrate with GNS3

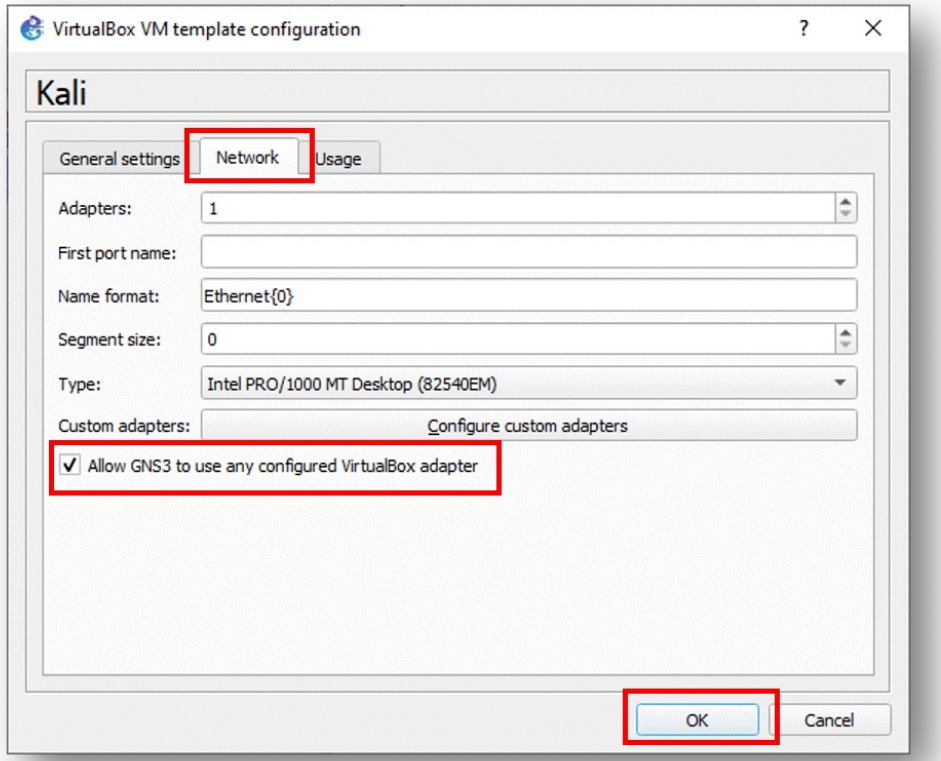
Integrating VMs to GNS3

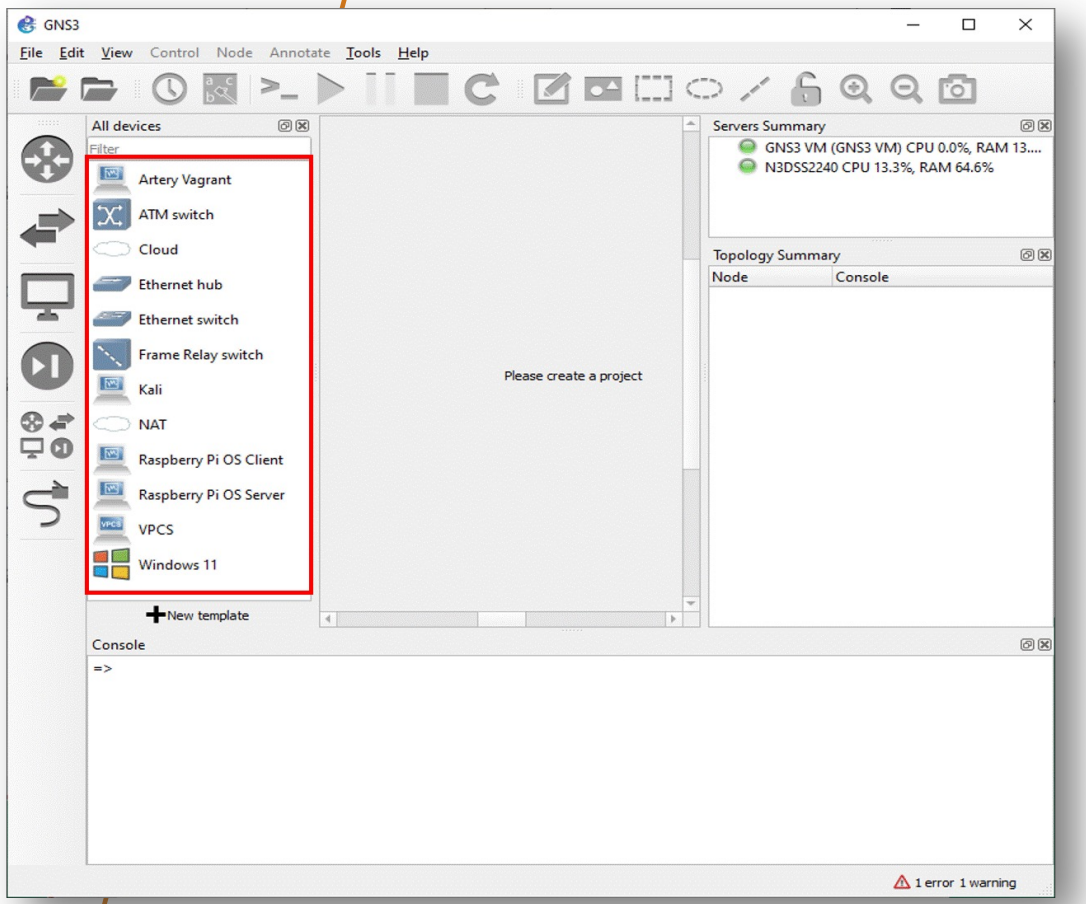




- Do the same for any VM you want to integrate with GNS3

Integrating VMs to GNS3



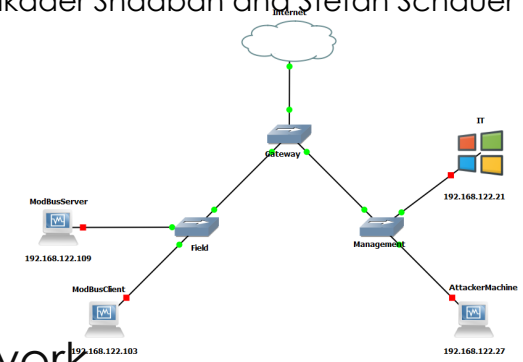


- Do the same for any VM you want to integrate with GNS3

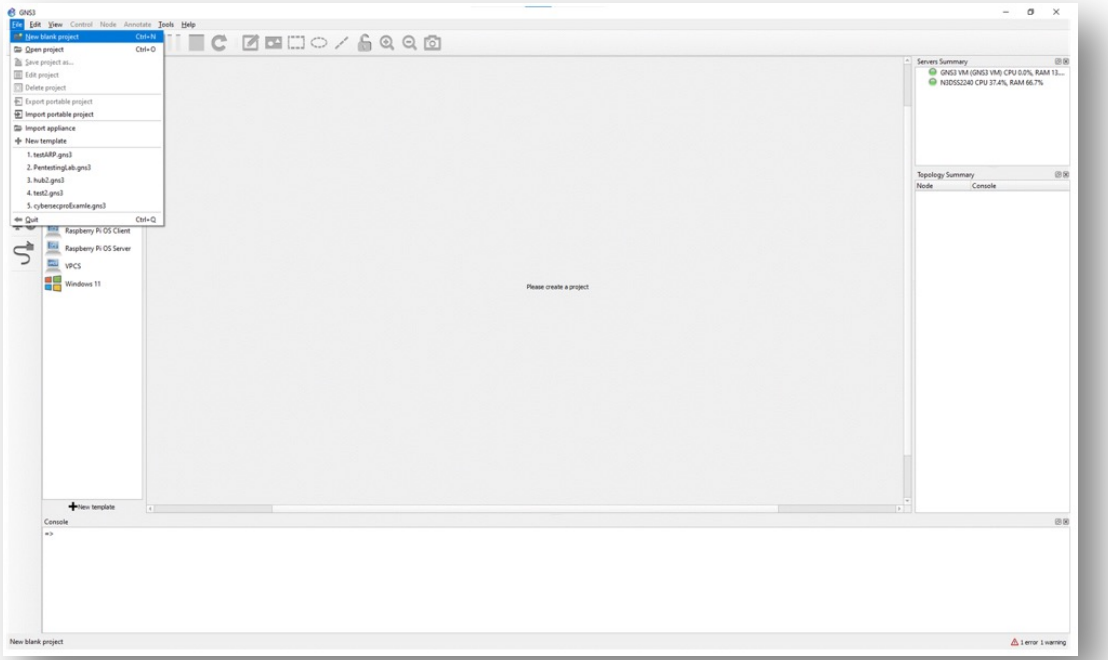
Network Topology Modeling

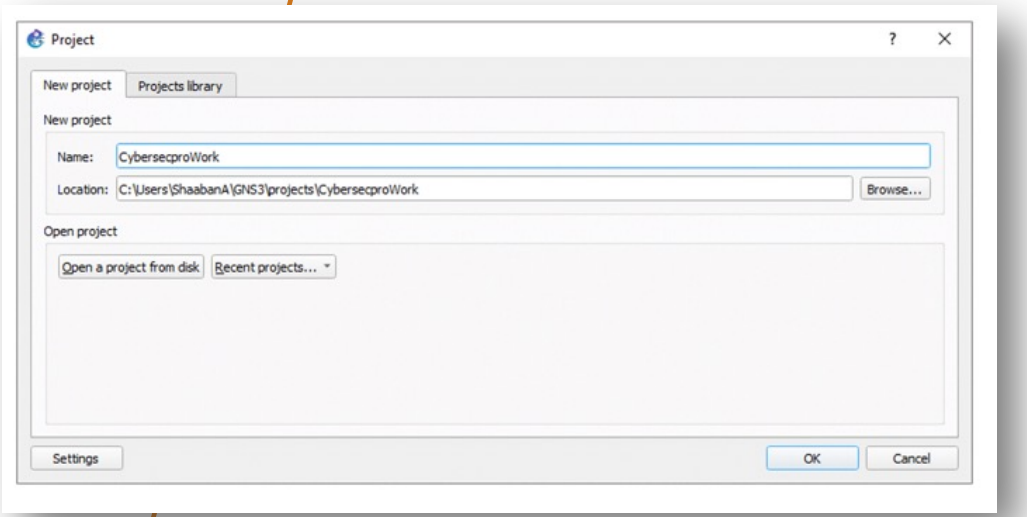
CyberSecPro
CC BY NC SA

GNS3 Client for Network Modeling

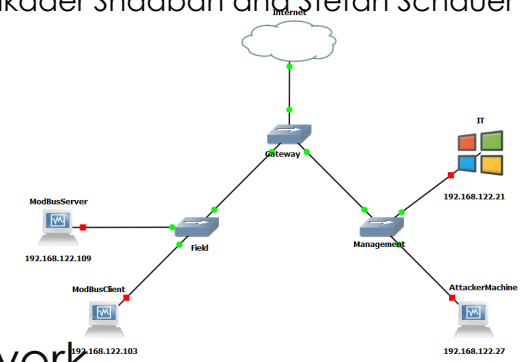


- You now have a list of all integrated VMs, and you can begin modeling your network.

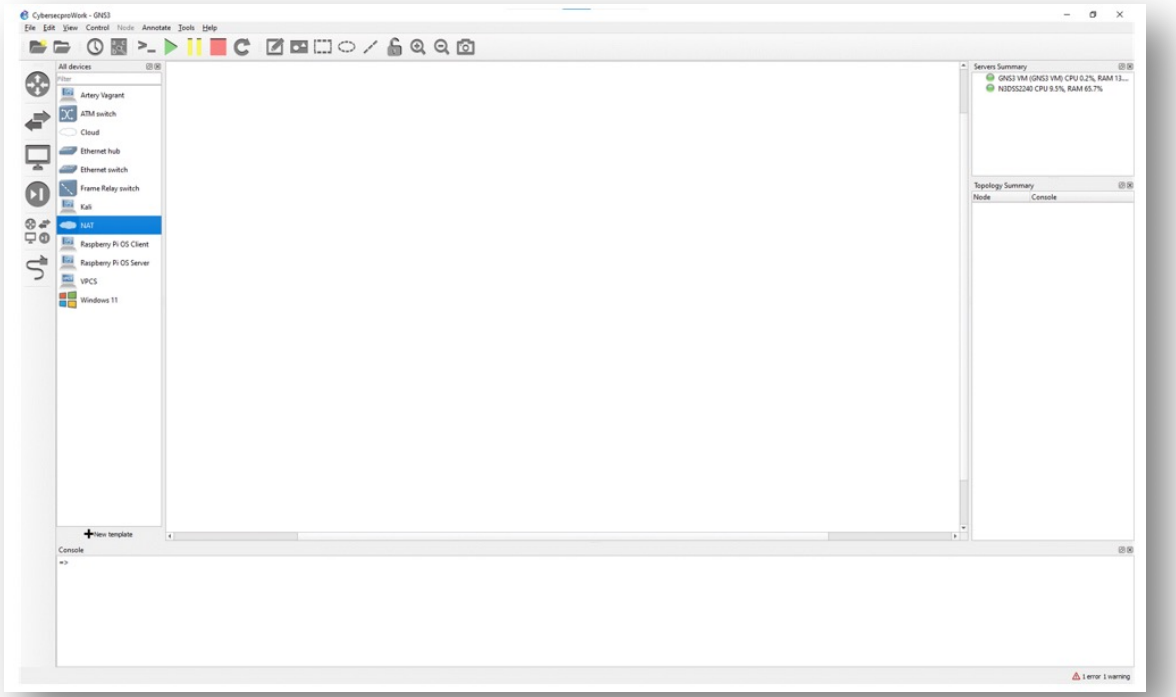


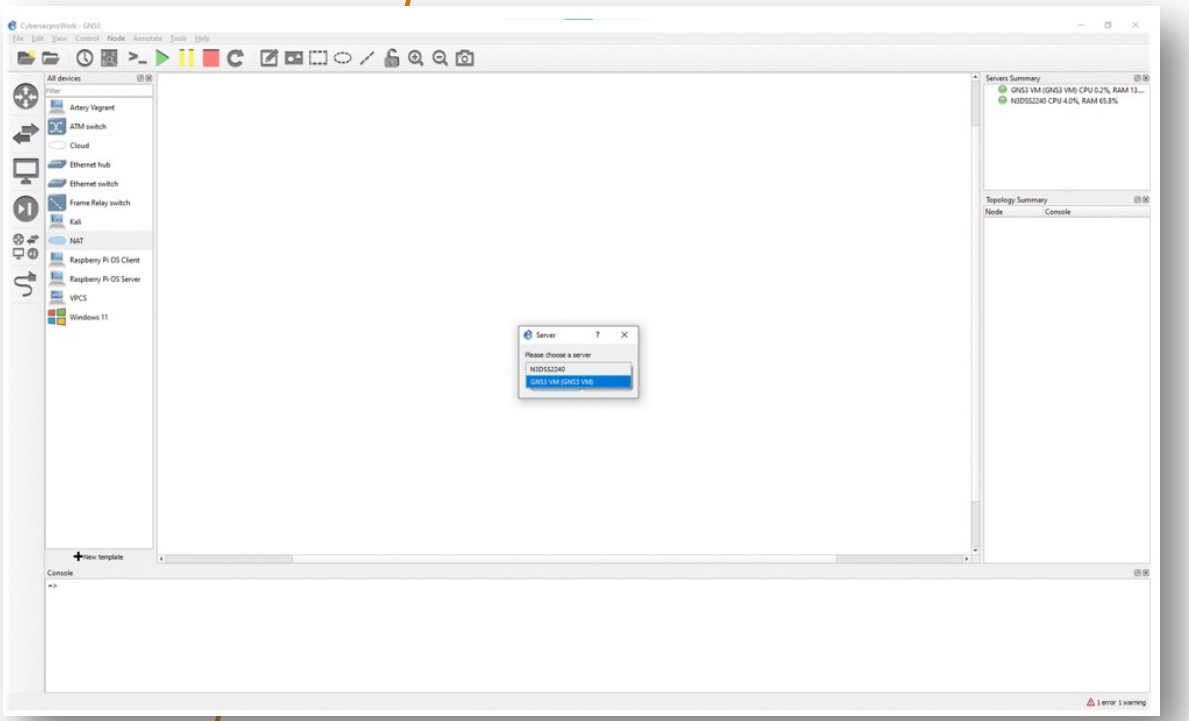


GNS3 Client for Network Modeling

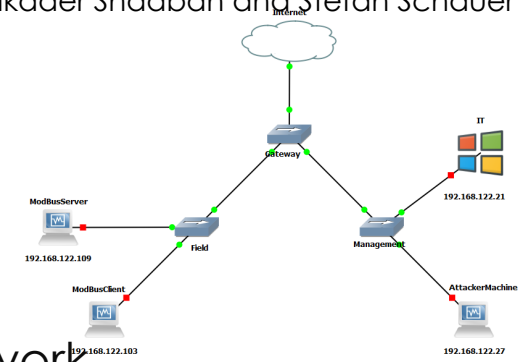


- You now have a list of all integrated VMs, and you can begin modeling your network.

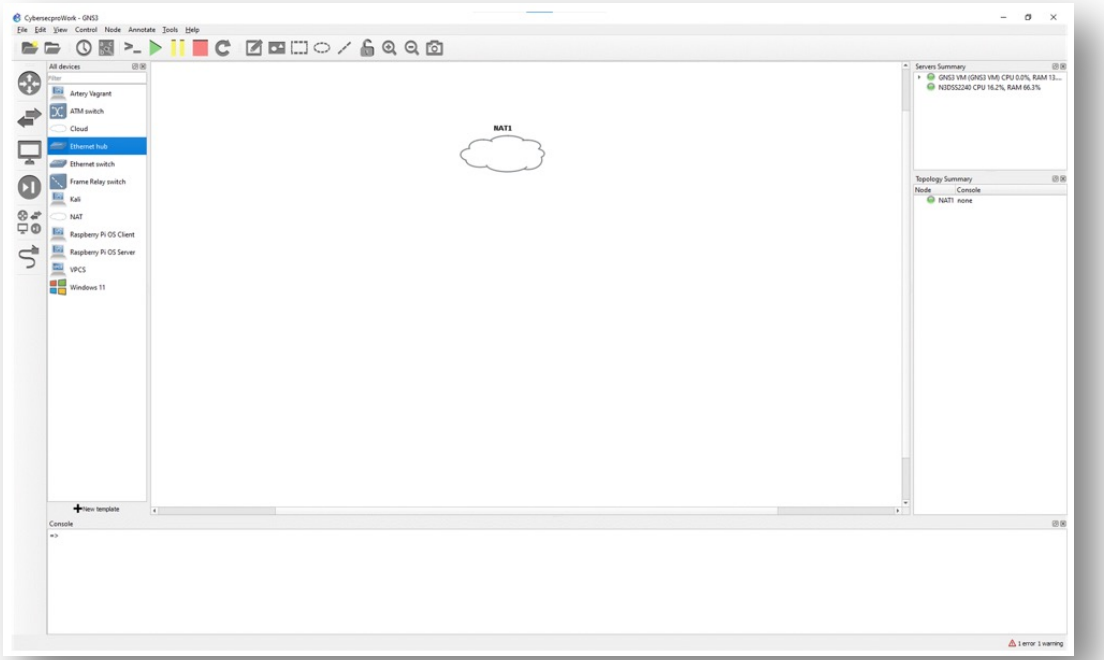


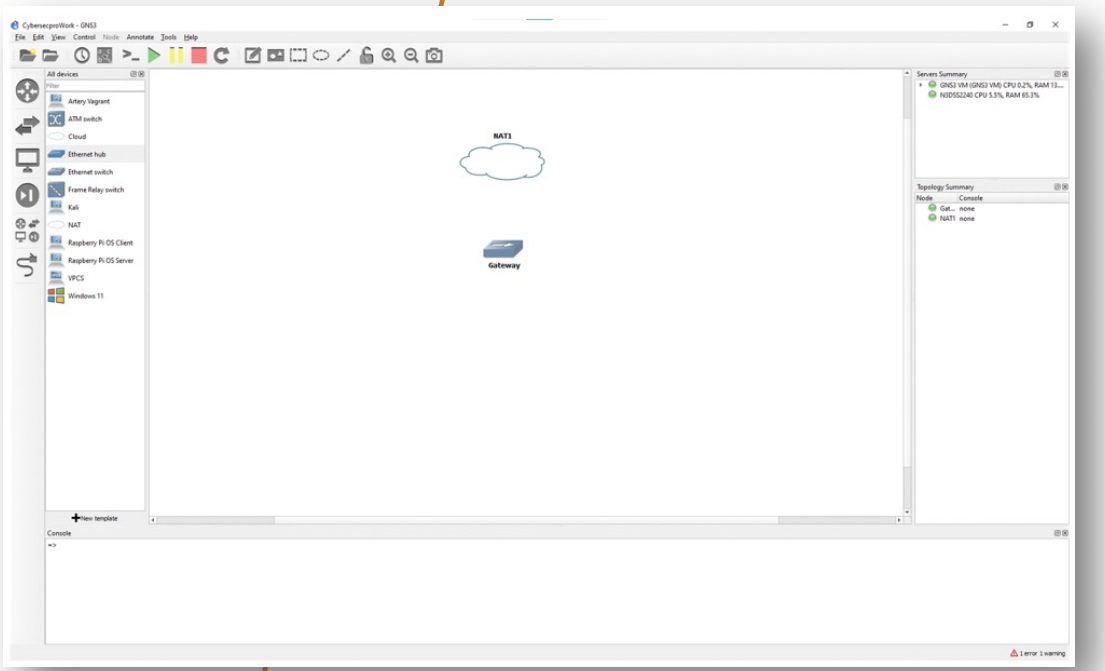


GNS3 Client for Network Modeling

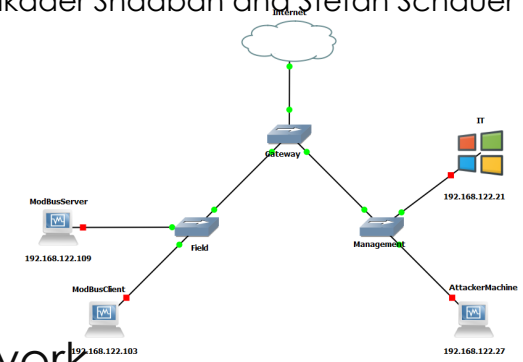


- You now have a list of all integrated VMs, and you can begin modeling your network.

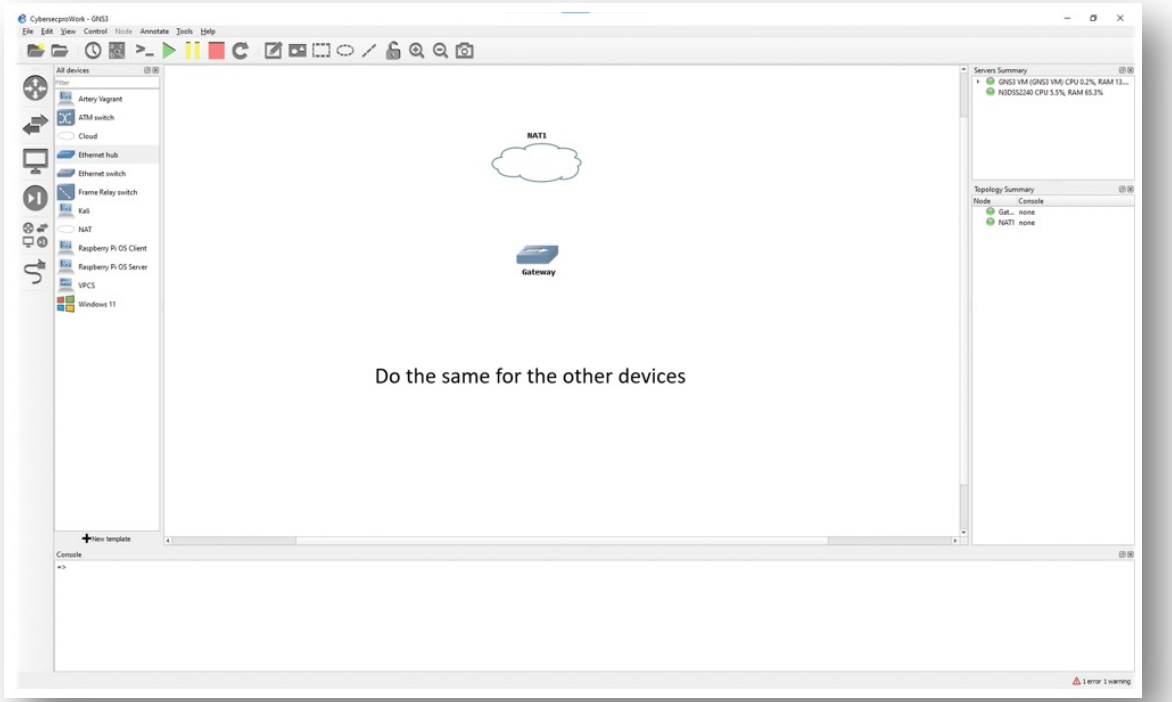


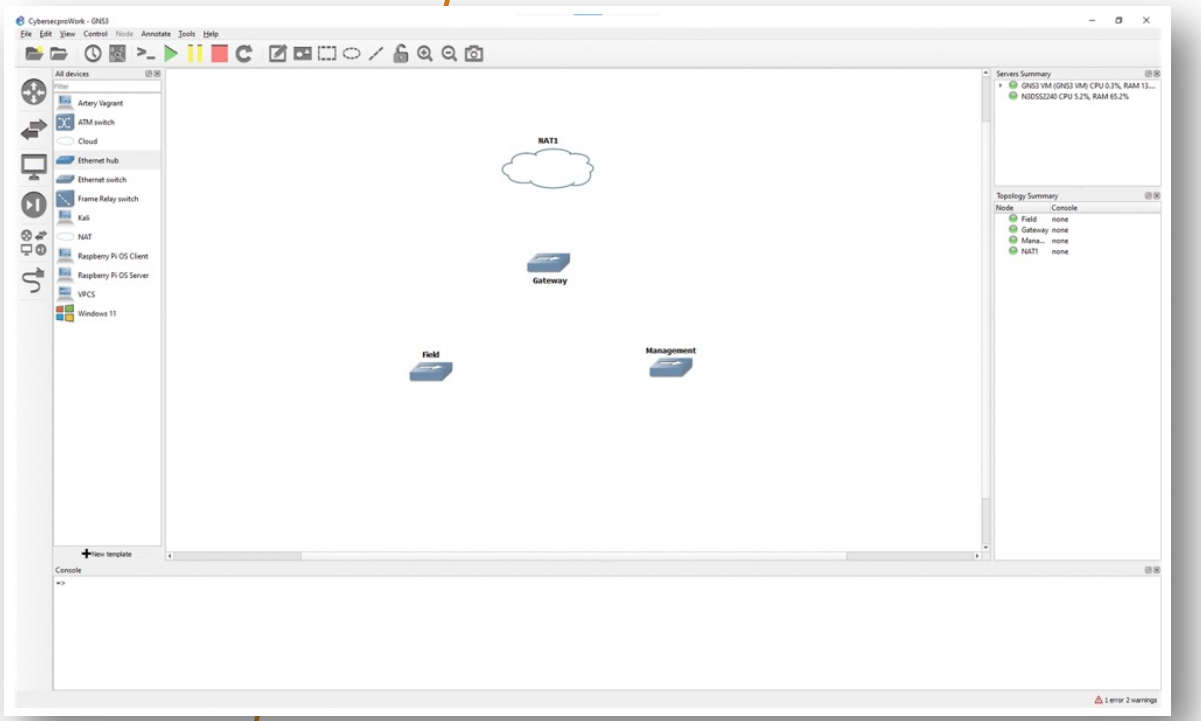


GNS3 Client for Network Modeling

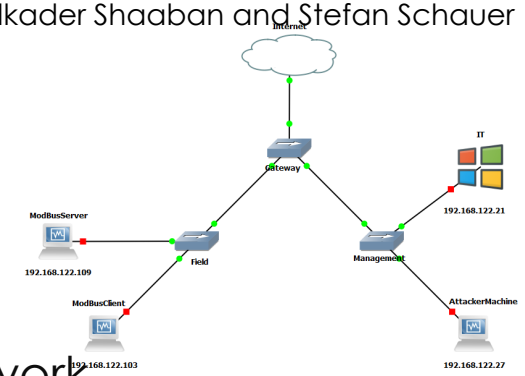


- You now have a list of all integrated VMs, and you can begin modeling your network.

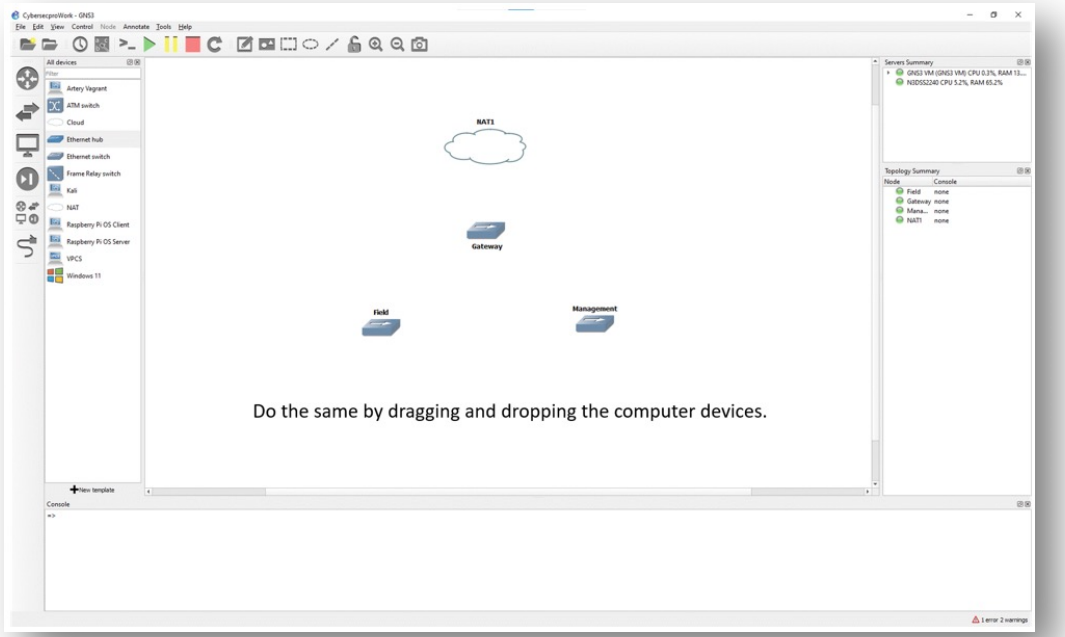


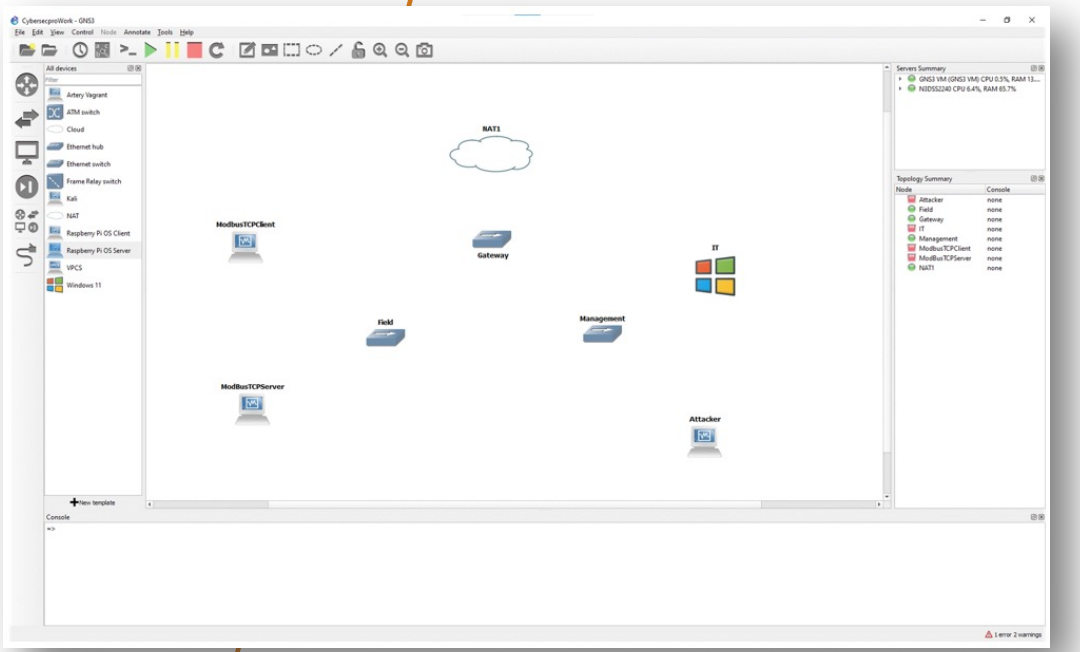


GNS3 Client for Network Modeling

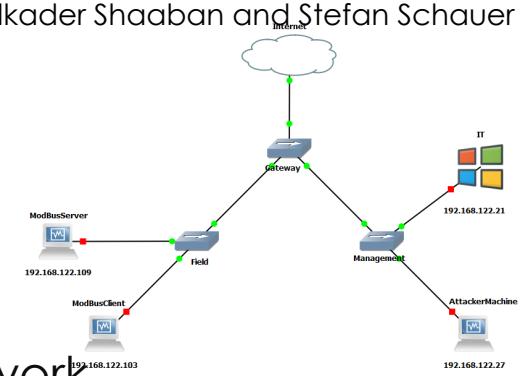


- You now have a list of all integrated VMs, and you can begin modeling your network.

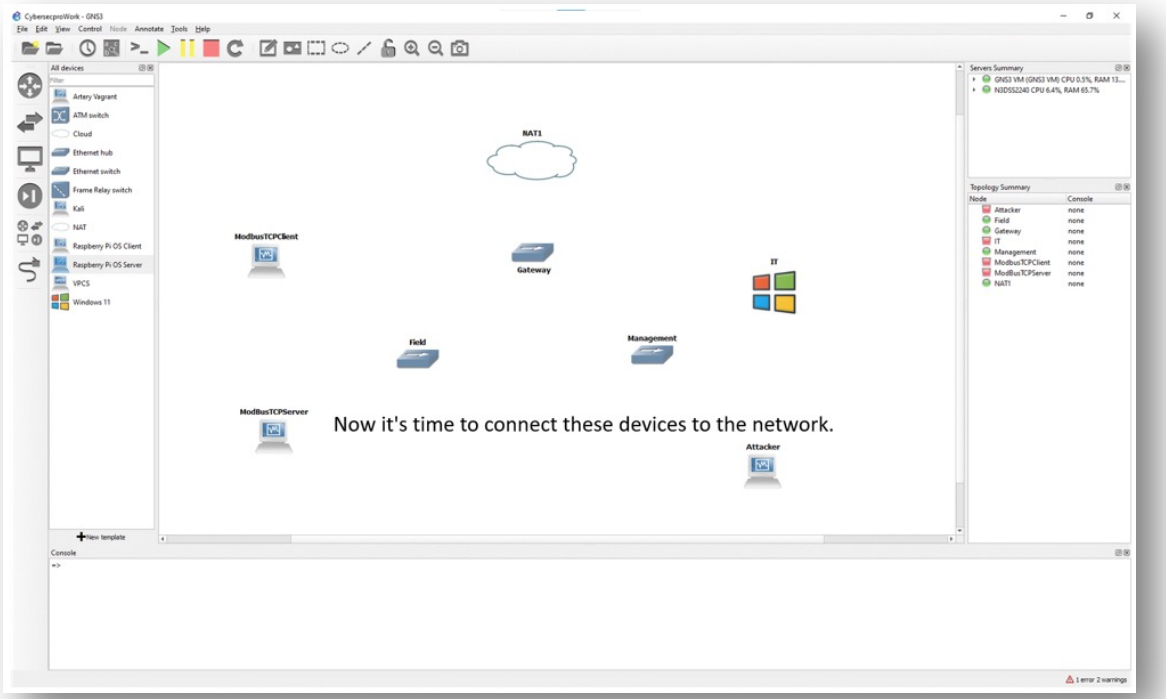


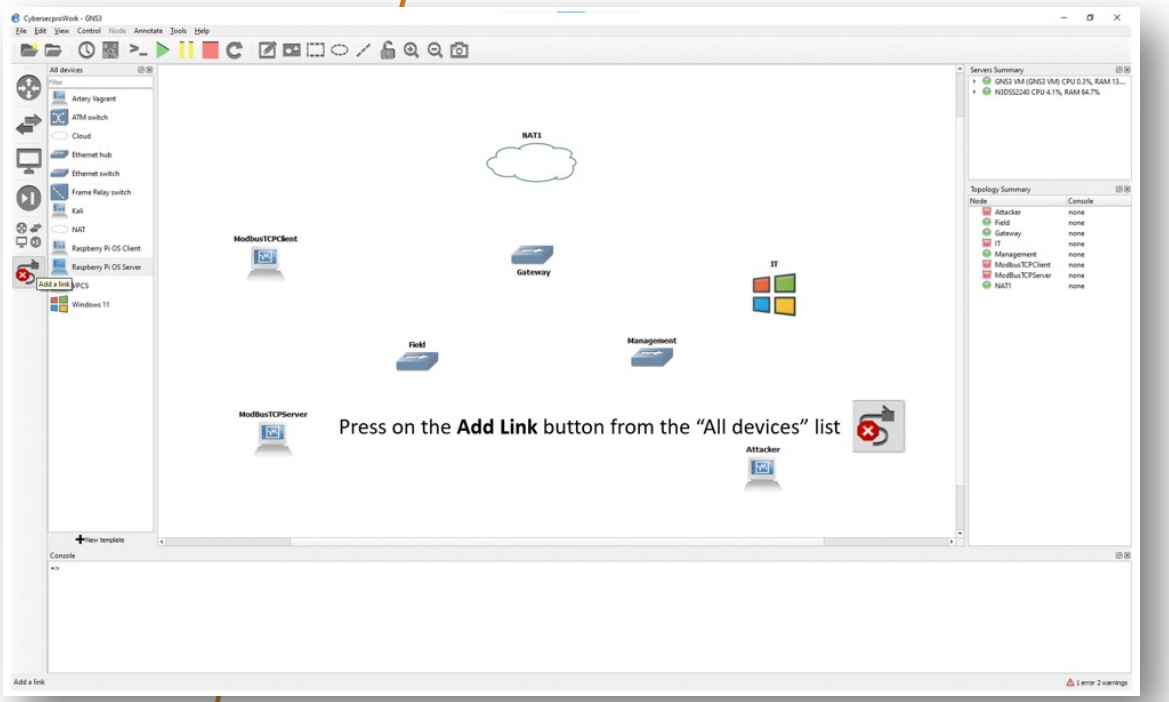


GNS3 Client for Network Modeling

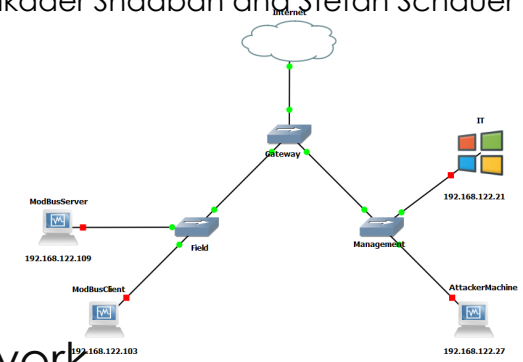


- You now have a list of all integrated VMs, and you can begin modeling your network.

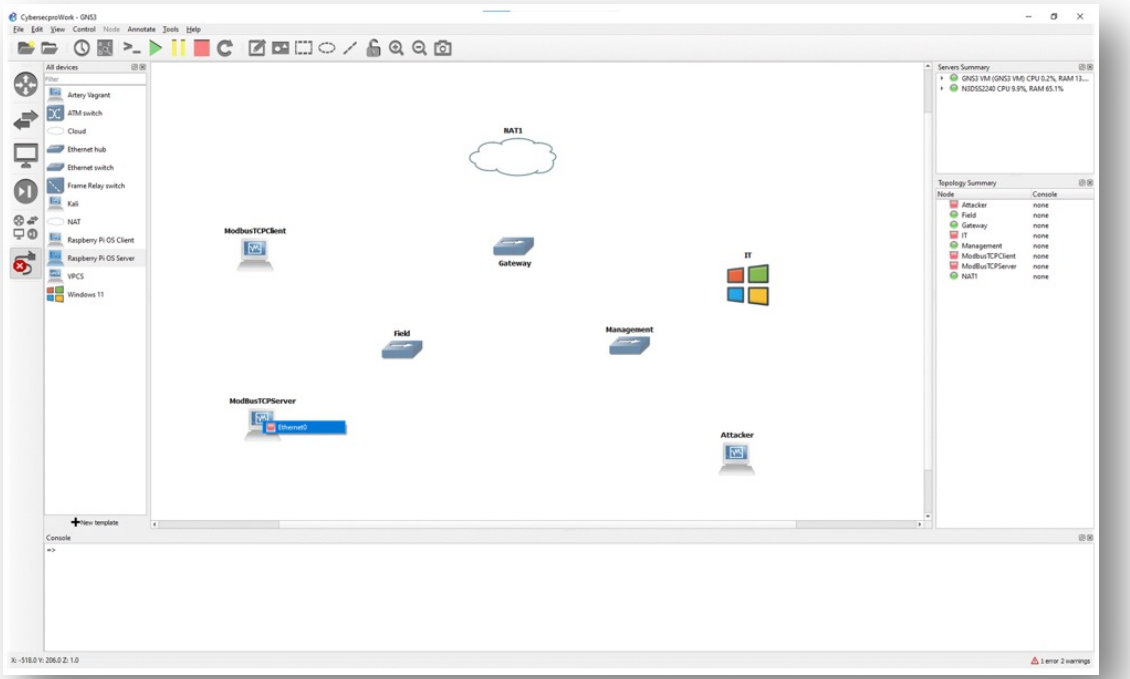


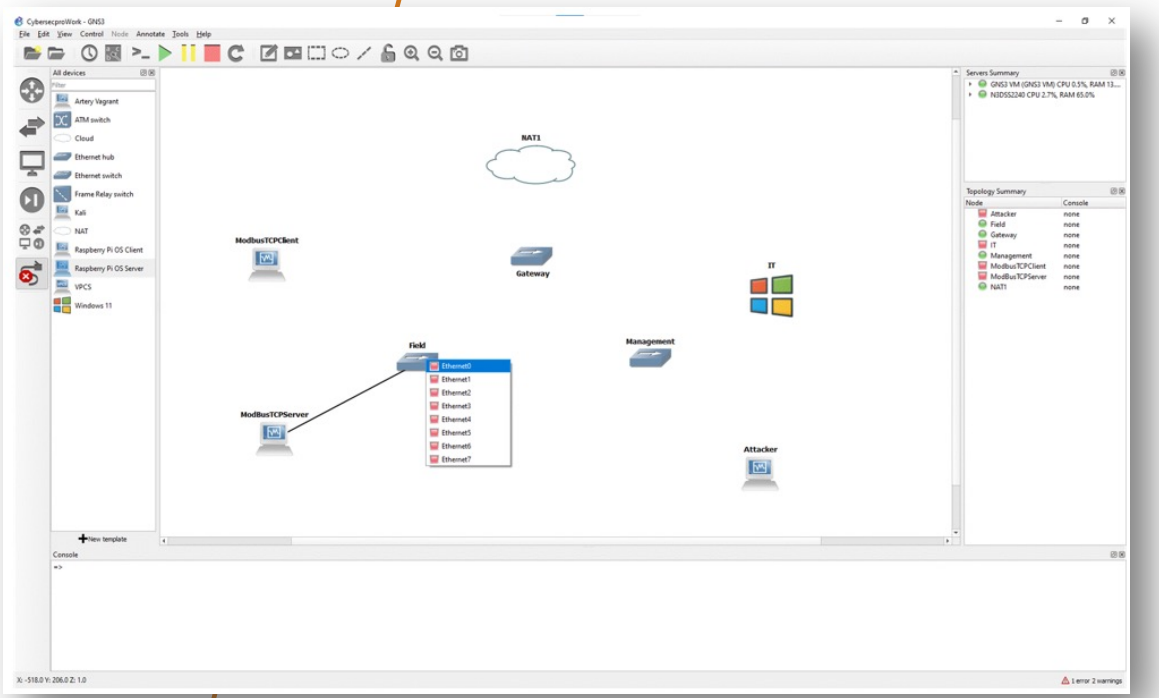


GNS3 Client for Network Modeling

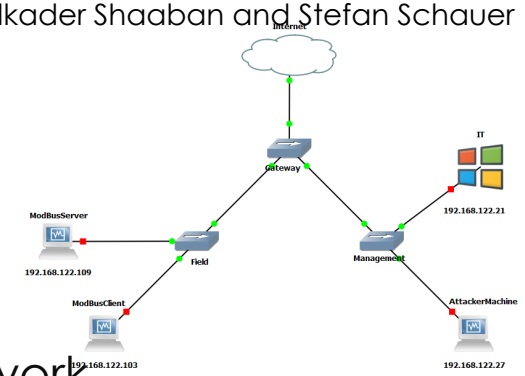


- You now have a list of all integrated VMs, and you can begin modeling your network.

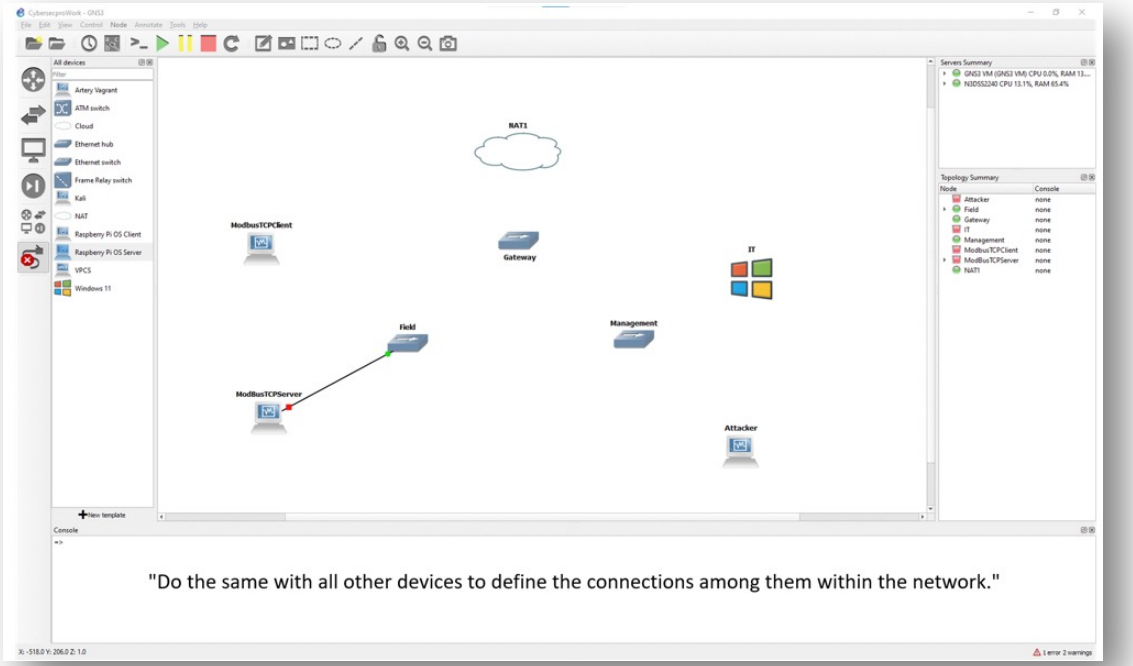


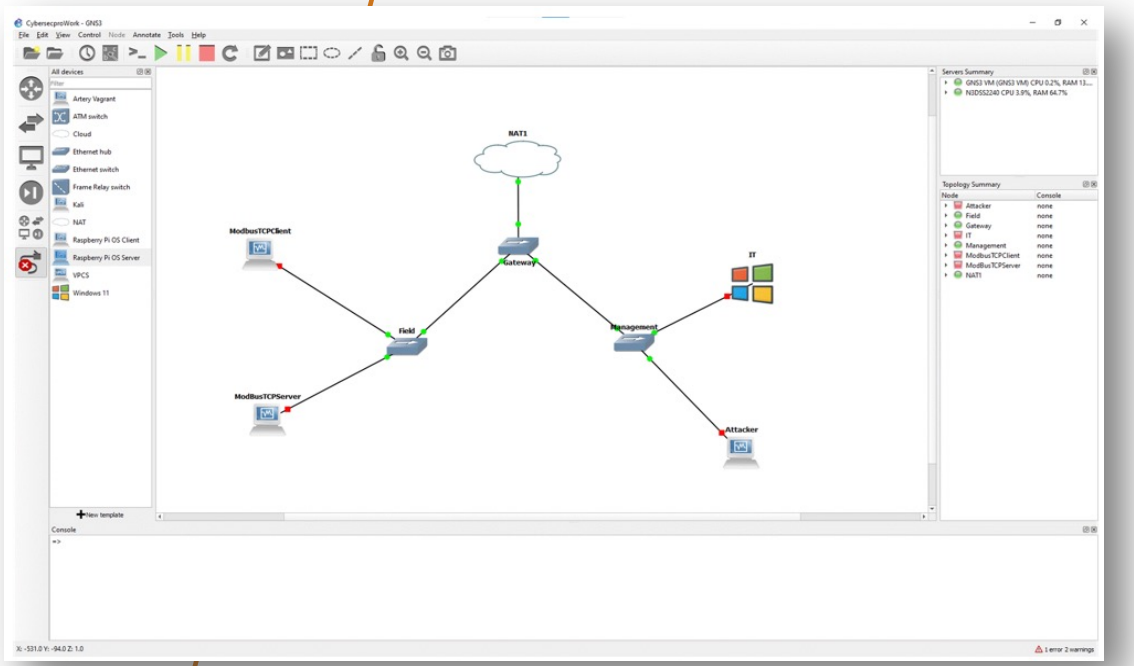


GNS3 Client for Network Modeling

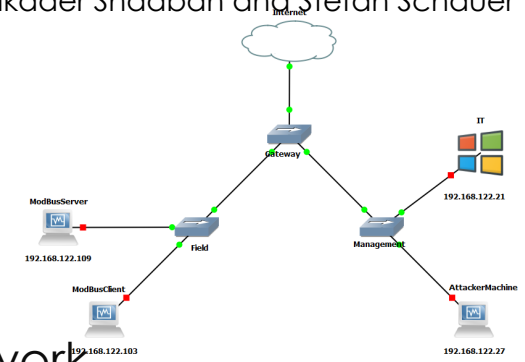


- You now have a list of all integrated VMs, and you can begin modeling your network.

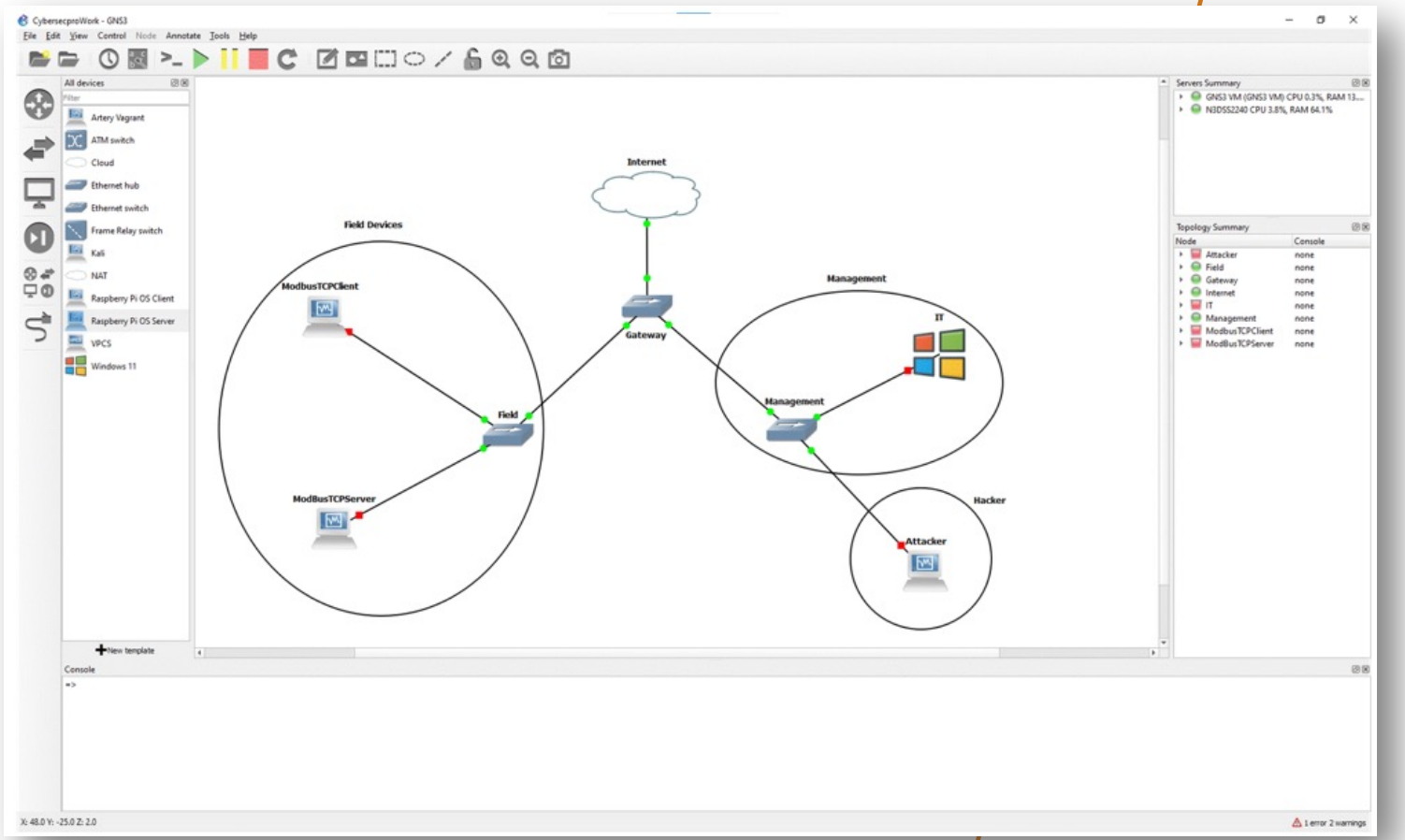




GNS3 Client for Network Modeling



- You now have a list of all integrated VMs, and you can begin modeling your network.

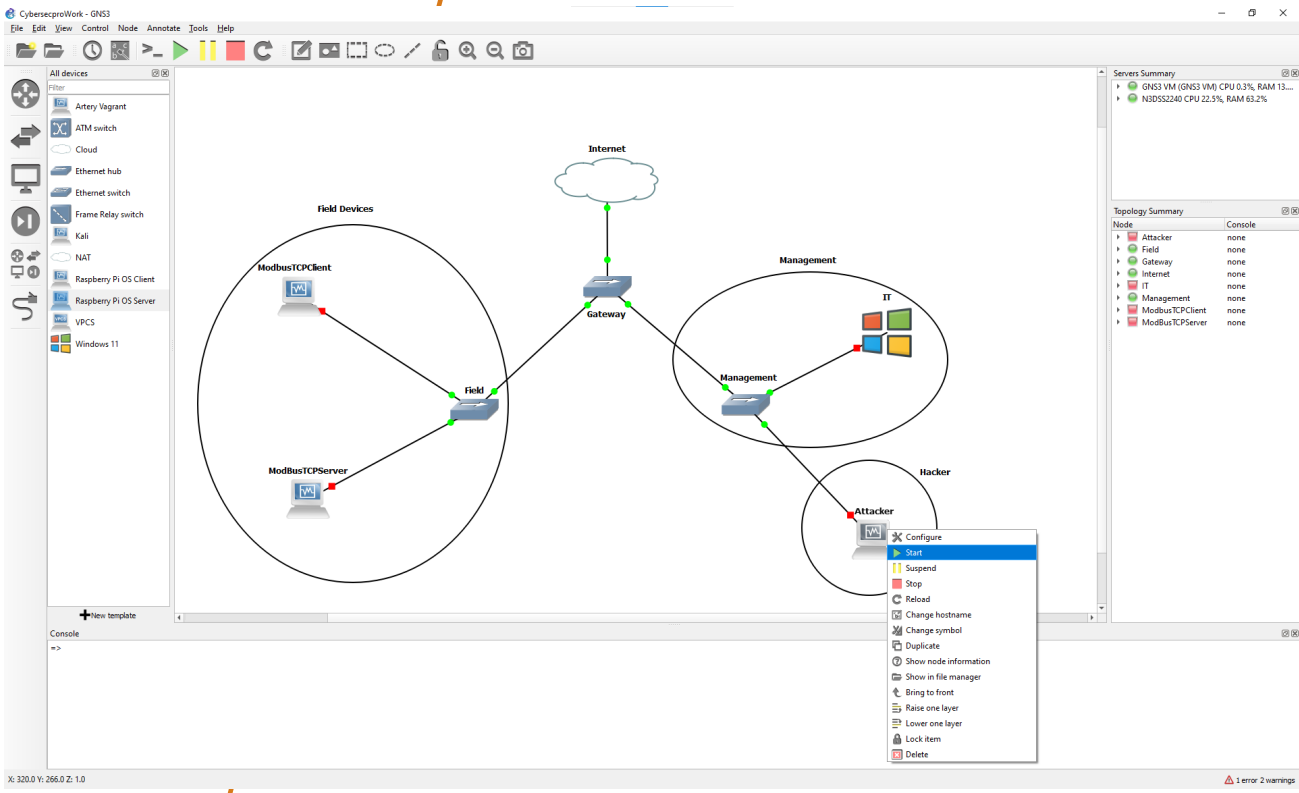


GNS3 Client for Network Modeling

- Before start performing any penetration testing activities, it is crucial to discover the IP addresses of all connected devices in the network.

- Additionally, it is important to ensure that all devices on the network can communicate with each other.

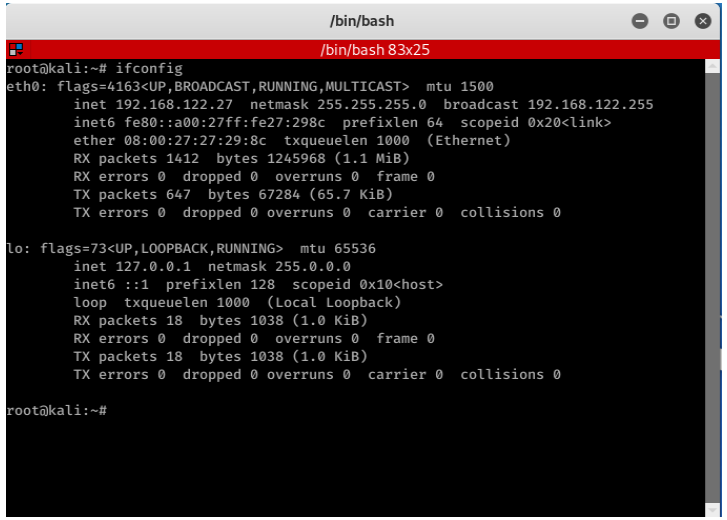
- Therefore, start all devices and verify their IPs.



GNS3 Client for Network Modeling

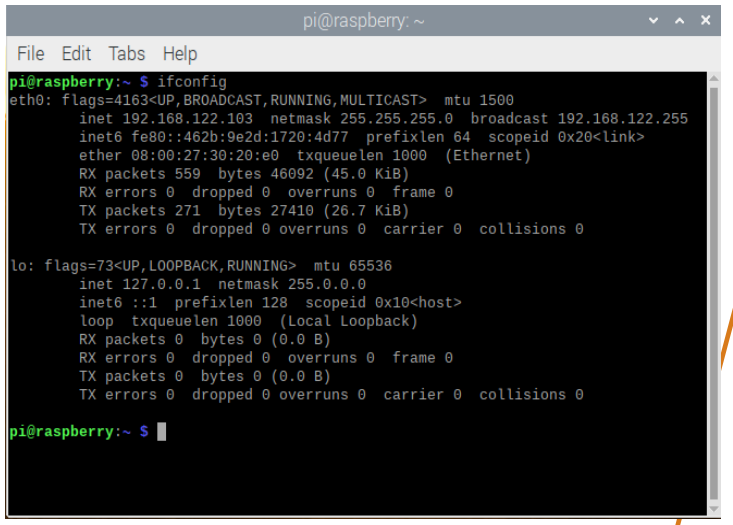
- Use the ifconfig command on the Linux devices to know more about the network configuration

Kali



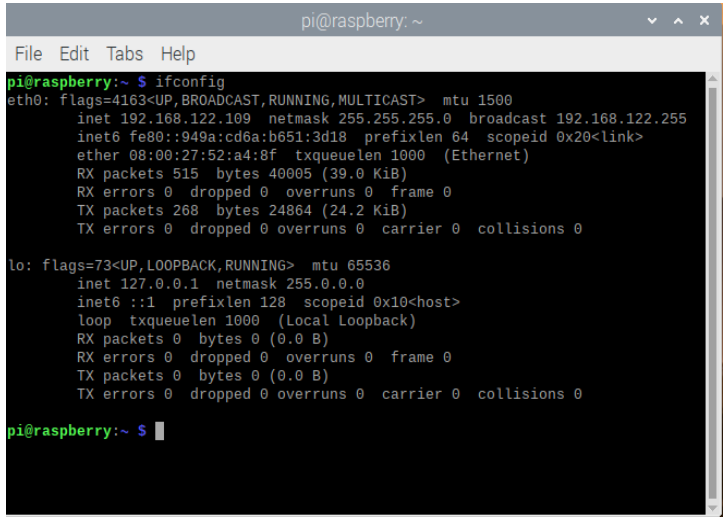
192.168.122.27

Server



192.168.122.109

Client

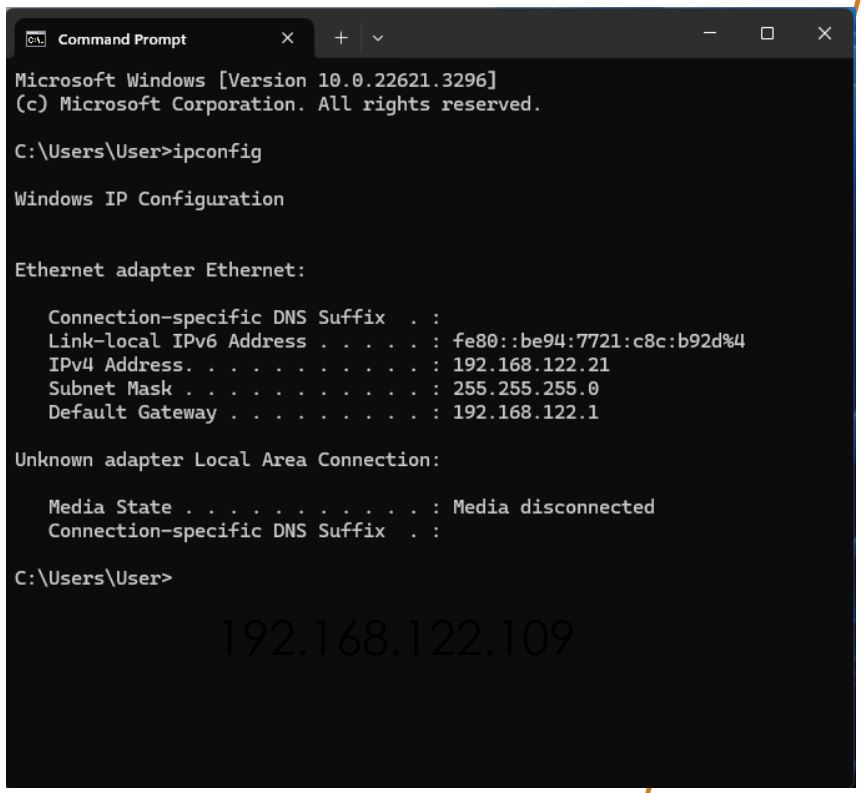


192.168.122.103

GNS3 Client for Network Modeling

•Use the ipconfig command (if you use a windows OS) to know more about the network configuration

Windows

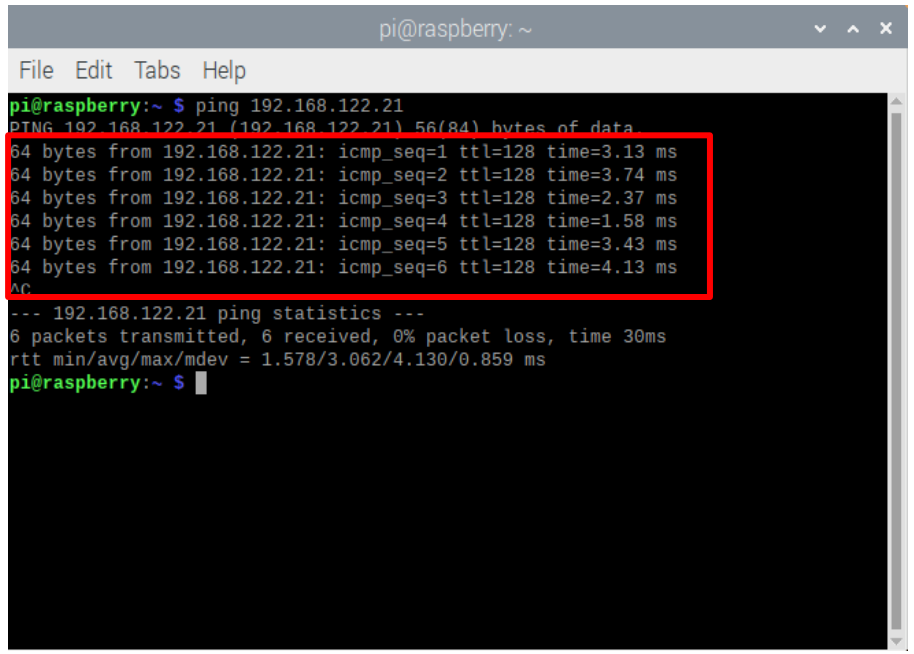


192.168.122.21

GNS3 Client for Network Modeling

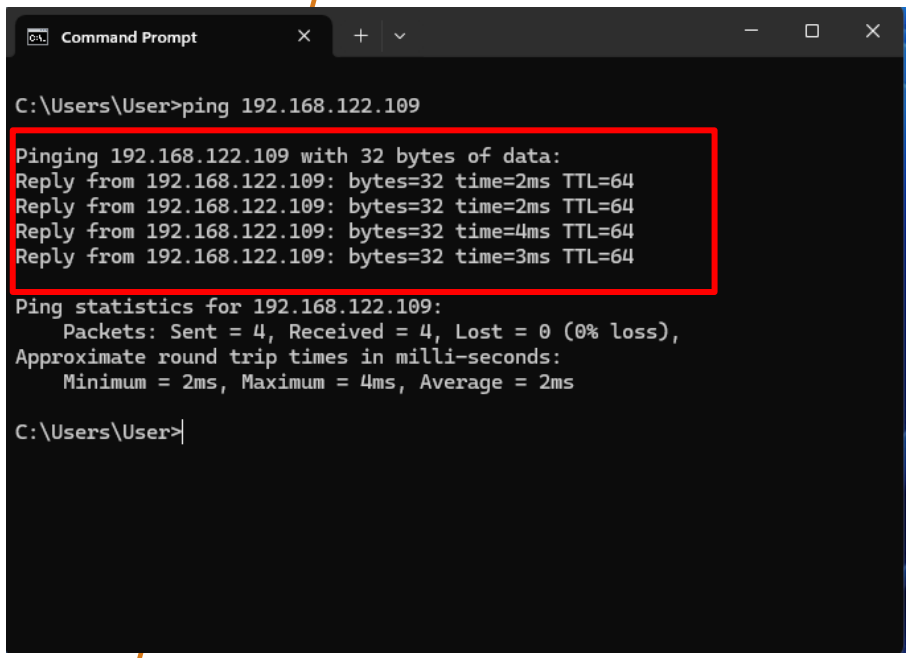
- Now we have the IPs of the network devices, be sure that all devices can reach each other.
- Use the **ping <destination IP-address>** to test the successful establishment of the network.

Server



192.168.122.109

Windows



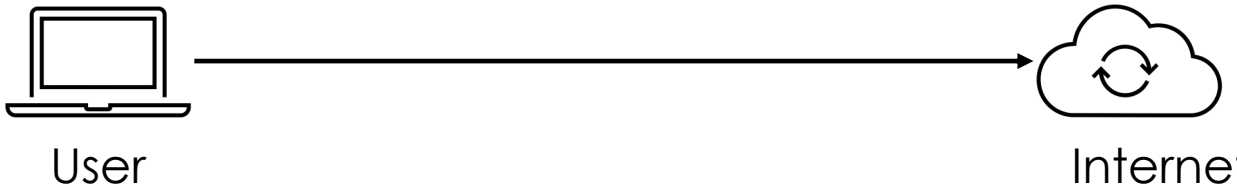
192.168.122.21

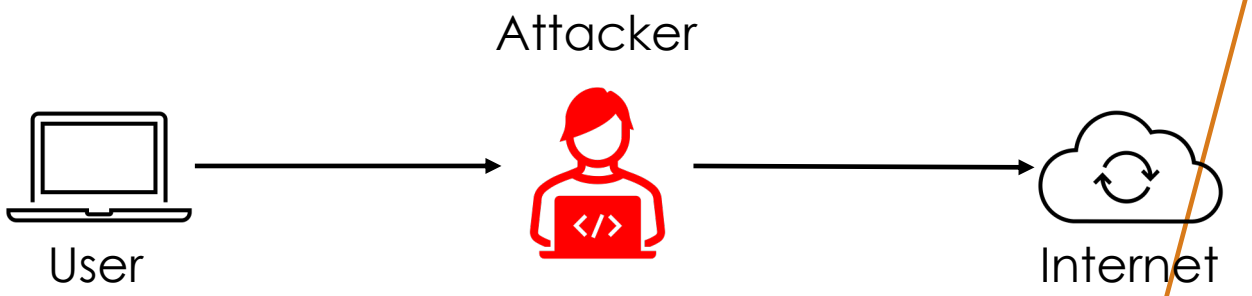
Offensive Tools

CyberSecPro

CC BY NC SA

MITM Attack





Credentials disclosure
Packet sniffing
Code injection
And more…

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

CyberSecPro
CC BY NC SA

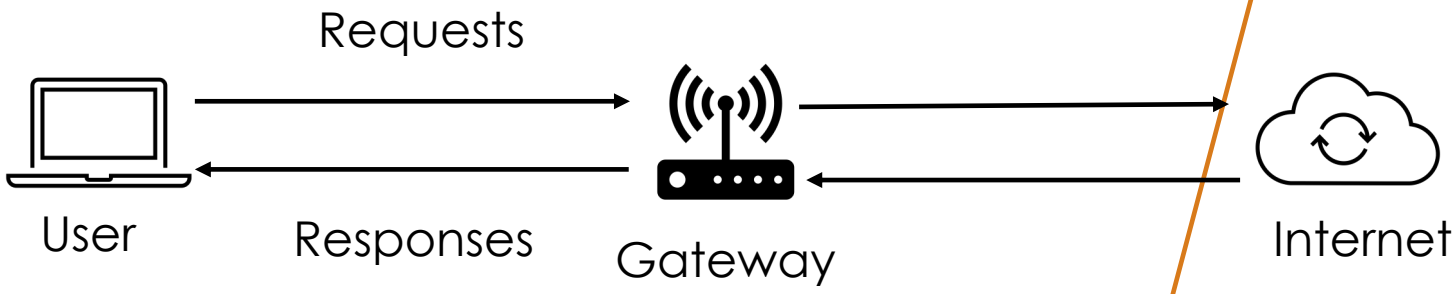
What is the ARP Spoofing Attack?

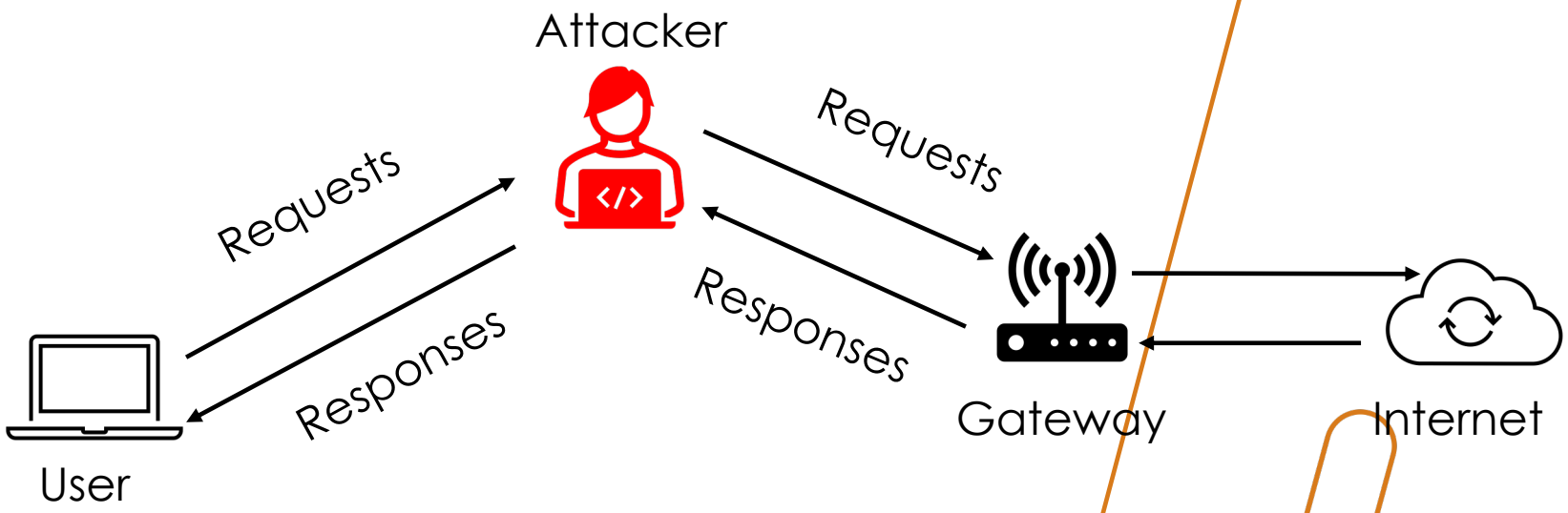
- **ARP spoofing** takes place within a **local area network** (**LAN**) and relies on the **Address Resolution Protocol (ARP).**
- **ARP serves** as a **communication protocol** linking **dynamic IP addresses** to **physical MAC** addresses of machines.
- **ARP spoofing**, also known as **ARP poisoning**, 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

CyberSecPro
CC BY NC SA

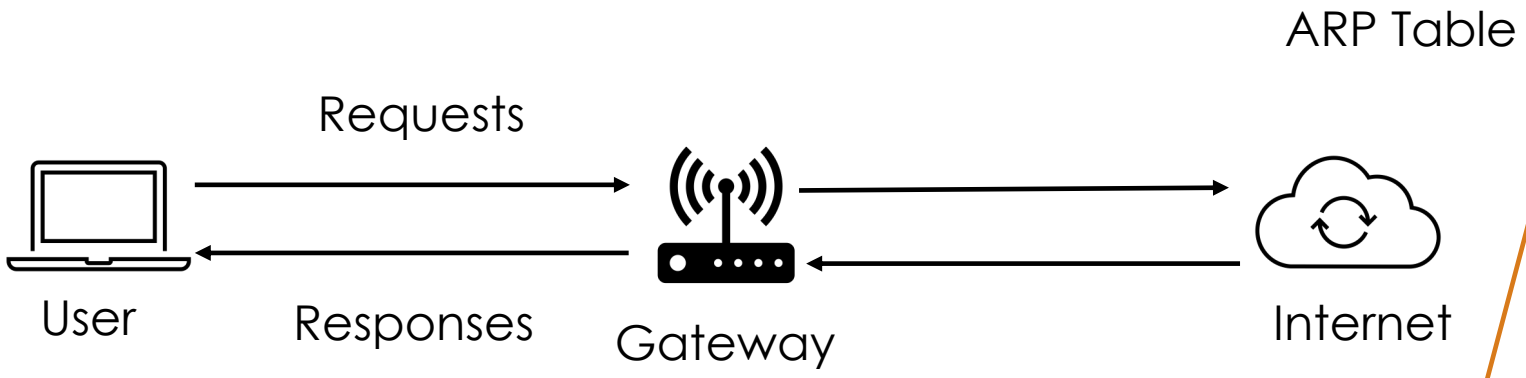
What is the ARP Spoofing Attack?

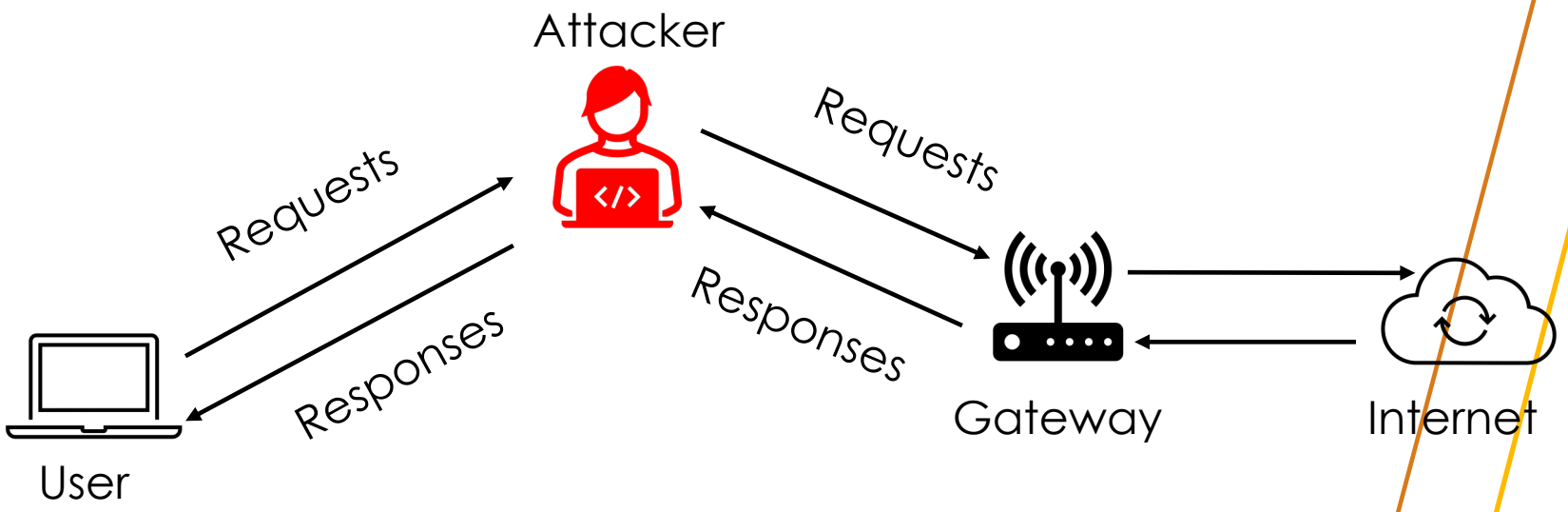




CyberSecPro
BY NC SA

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>
```

CyberSecPro
CC BY NC SA

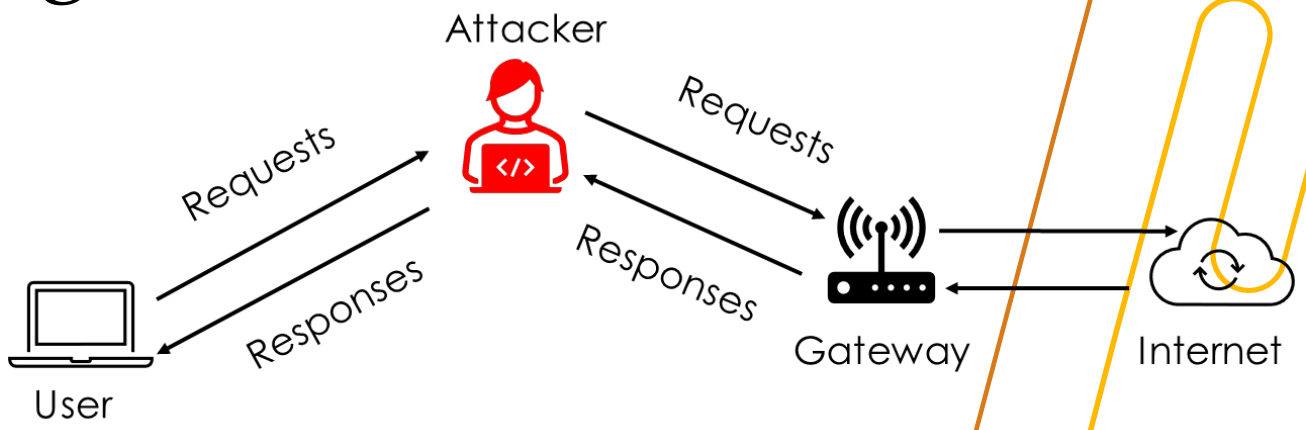
Offensive Tools

Arpspoofing

CyberSecPro

CC BY NC SA

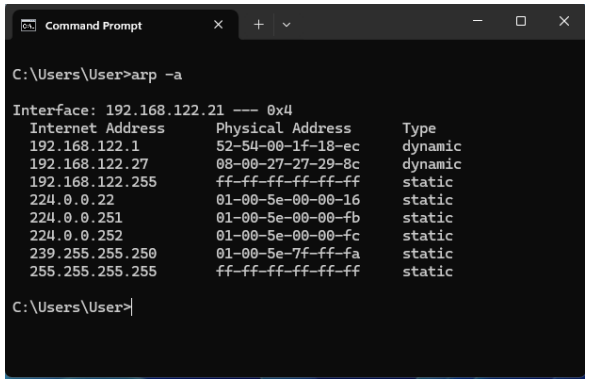
Arpspoofing



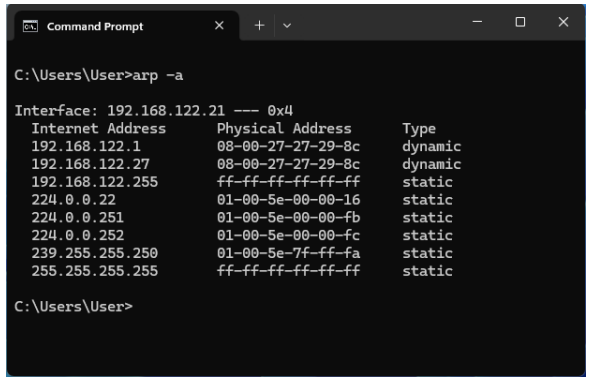
arpspoof -i [interface] -t [clientIP] [gatewayIP] (Trick the victim)

arpspoof -i [interface] -t [gatewayIP] [clientIP] (Trick the gateway)

Before



After



Note: You need to allow the Linux machine (attacker) to perform port forwarding in order for it to act as a gateway.

CyberSecPro
CC BY NC SA

Offensive Tools

Bettercap

CyberSecPro

CC BY NC SA

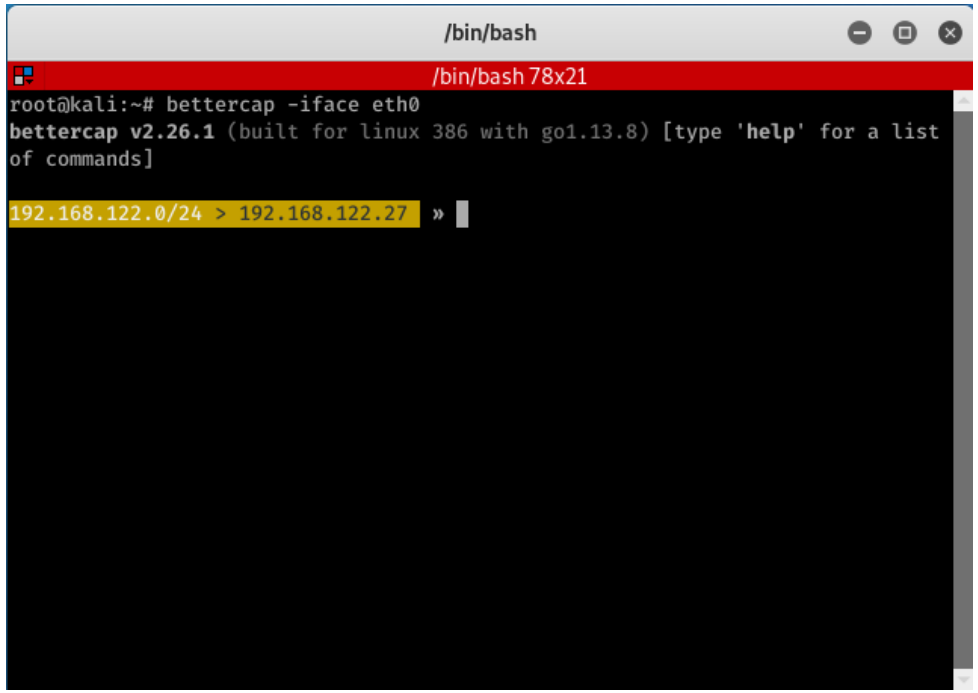
Bettercap tool

- 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

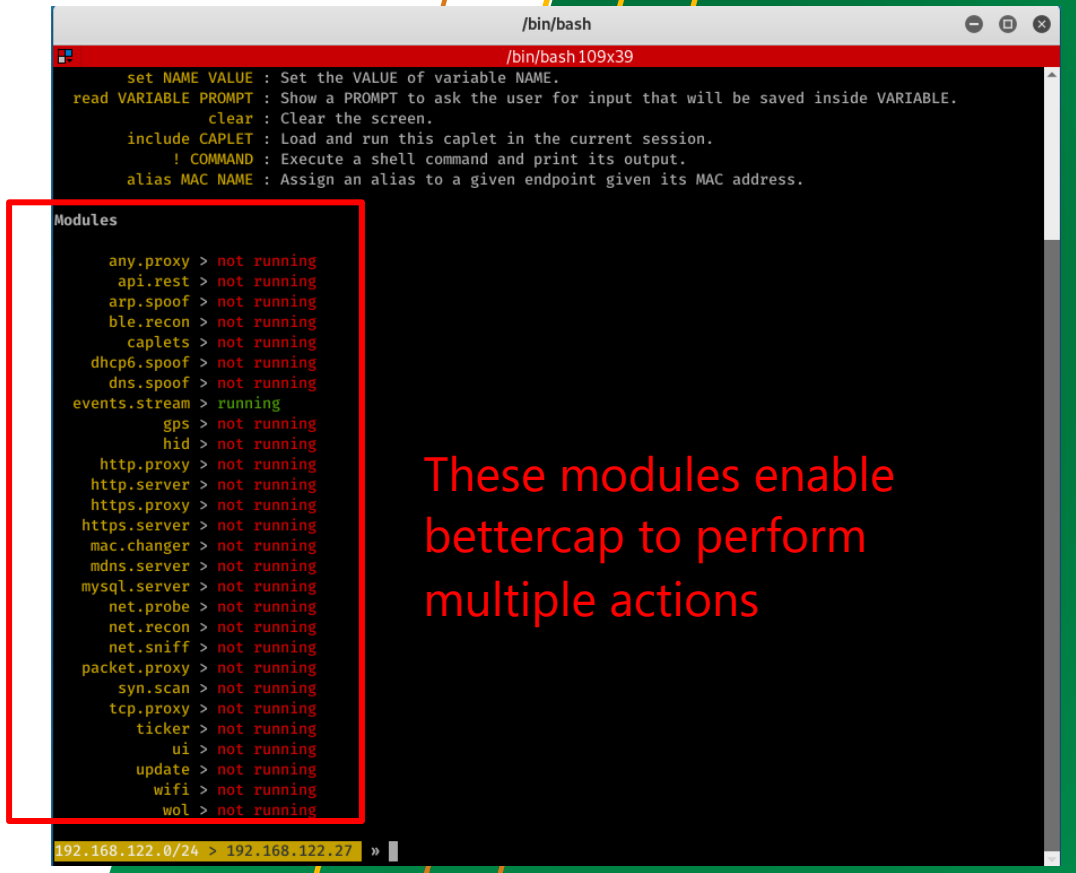
CyberSecPro
BY NC SA

Bettercap tool

Bettercap –iface eth0



Type: help (to get more information)

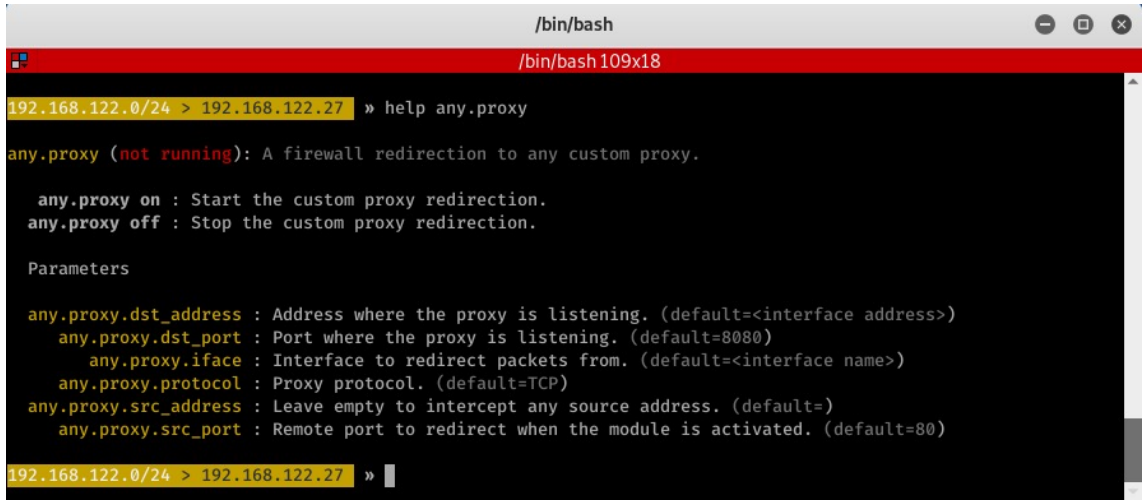


These modules enable bettercap to perform multiple actions

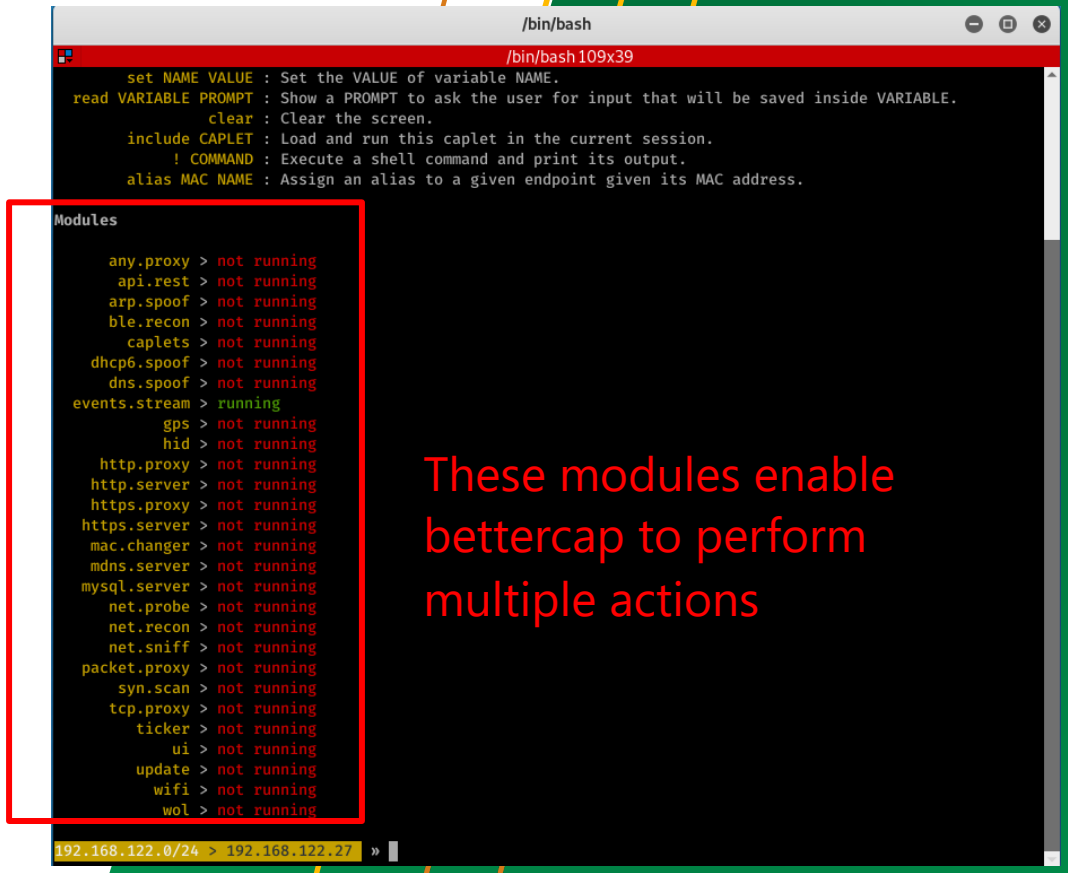
Bettercap tool

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

Help Module_Name



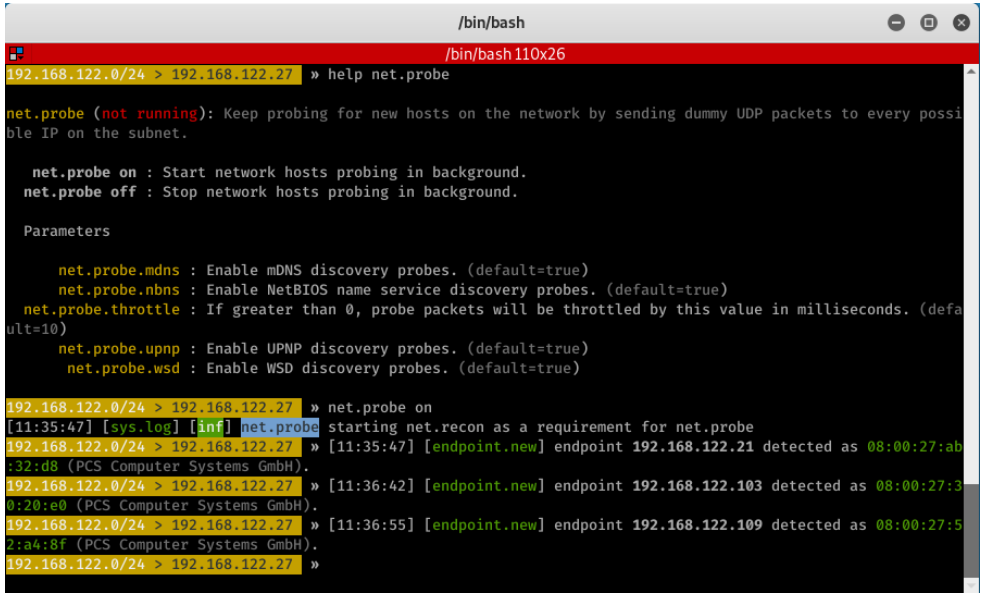
Type: help (to get more information)



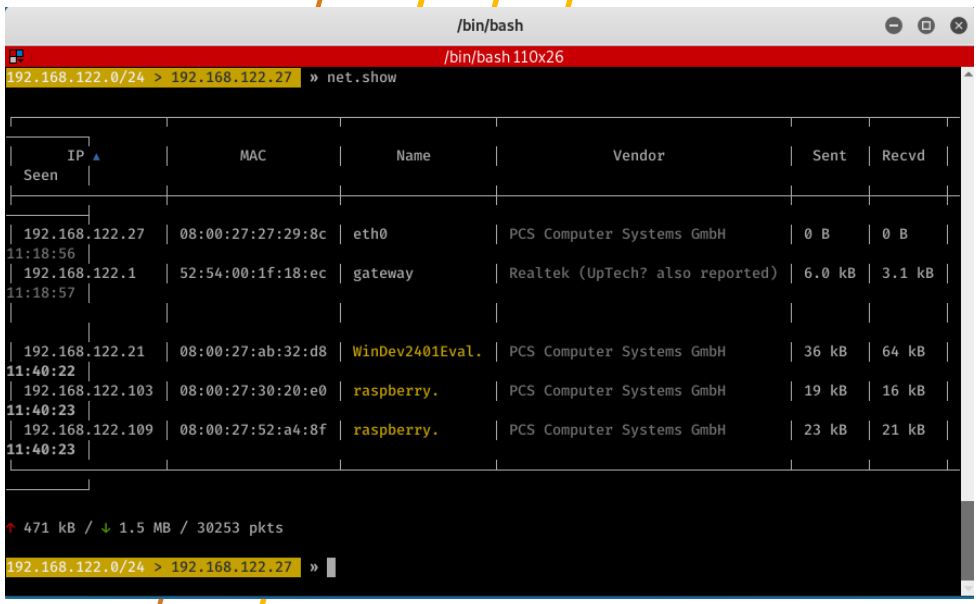
These modules enable bettercap to perform multiple actions

Bettercap tool

- Net.probe on
  - Keep investigating for new hosts on the network



- Net.show

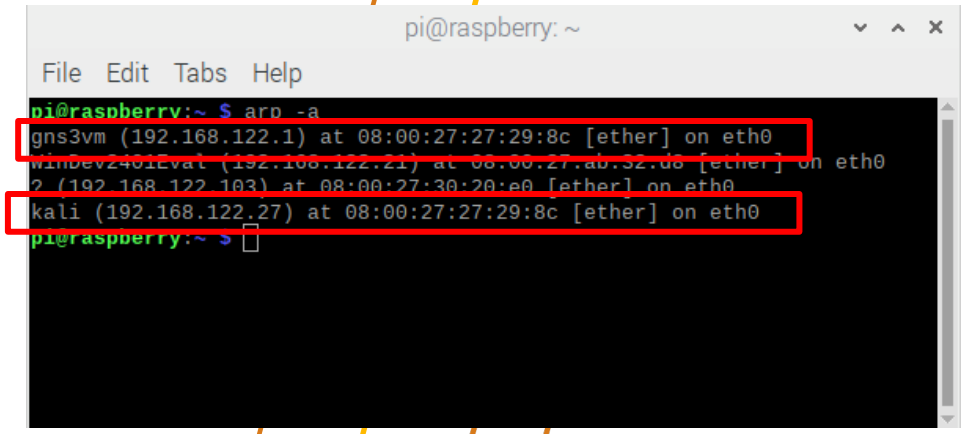


More information about all discovered devcies

CyberSecPro
CC BY NC SA

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).
- Set arp.spoof.targets IP_address
  - A comma separated list of MAC addresses, IP addresses, IP ranges or aliases to spoof
- Set arp.spoof on
  - This module keeps spoofing selected hosts on the network using crafted ARP packets in order to perform a MITM attack.
- Now the victim machine (server) arp table



CyberSecPro
CC BY NC SA

Bettercab for sniffing packets

- Net.sniff on
  - This module is a network packet sniffer
  - So all packets passing the kali Linux (attacker machine) will be captured

CyberSecPro
CC BY NC SA

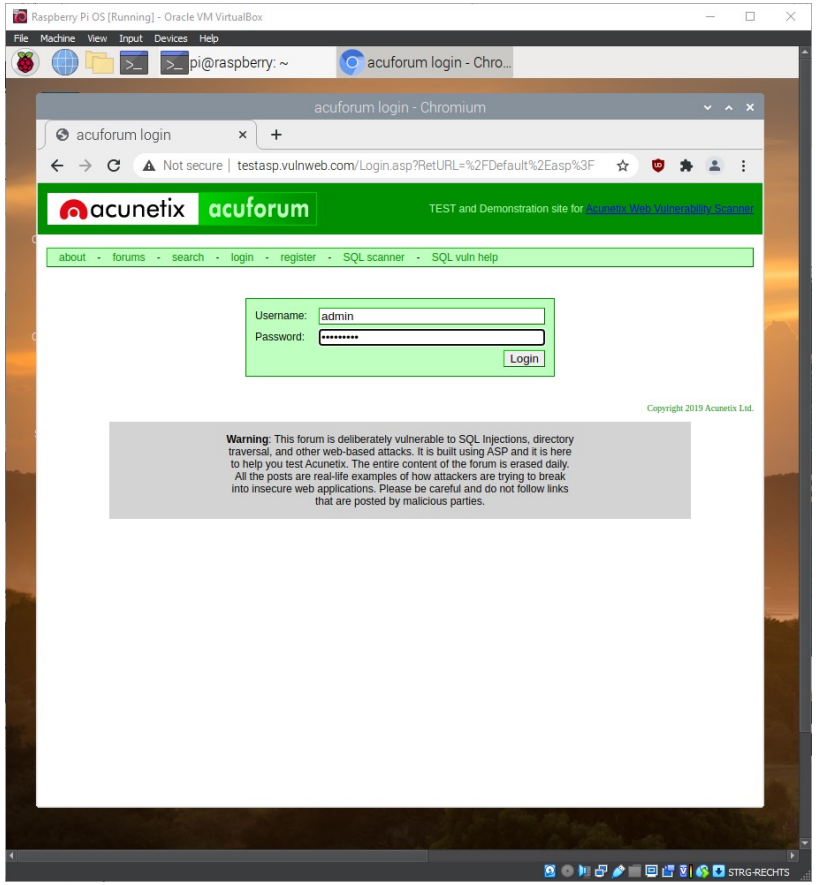
Bettercap Caplets

- 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>

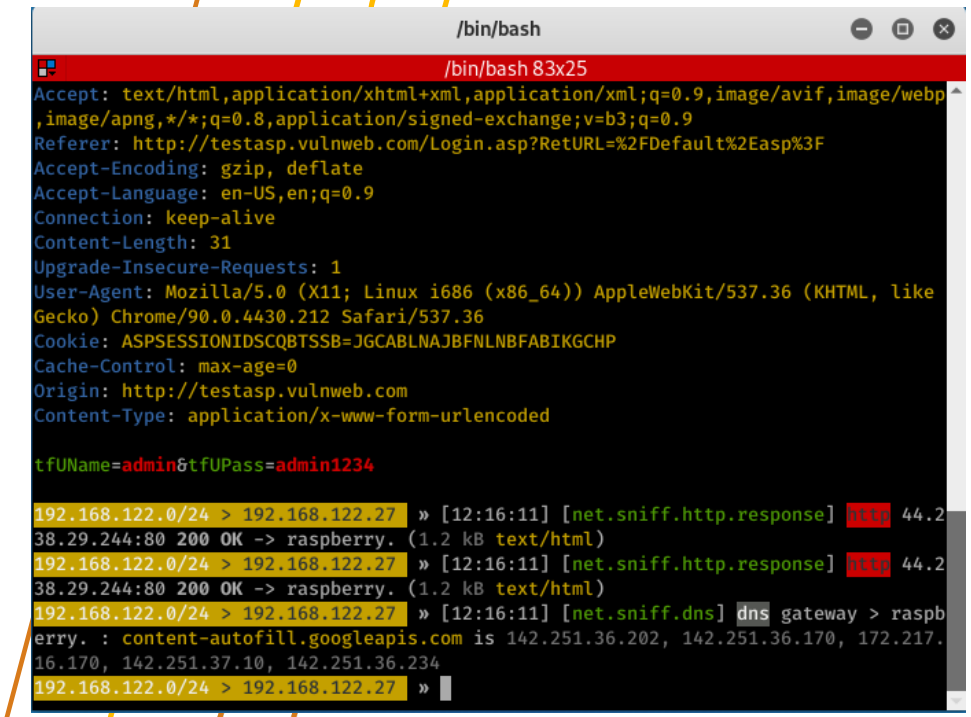
CyberSecPro
CC BY NC SA

MITM: Sniffing Packets

- Once the MITM attack is successfully set up, the attacker can carry out various malicious actions.
- Packet sniffing is one example of how MITM can exploit information from the target machine.



- Username: admin
- Pwd: admin1234



MITM: DNS Spoofing

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

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

CyberSecPro
CC BY NC SA

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.

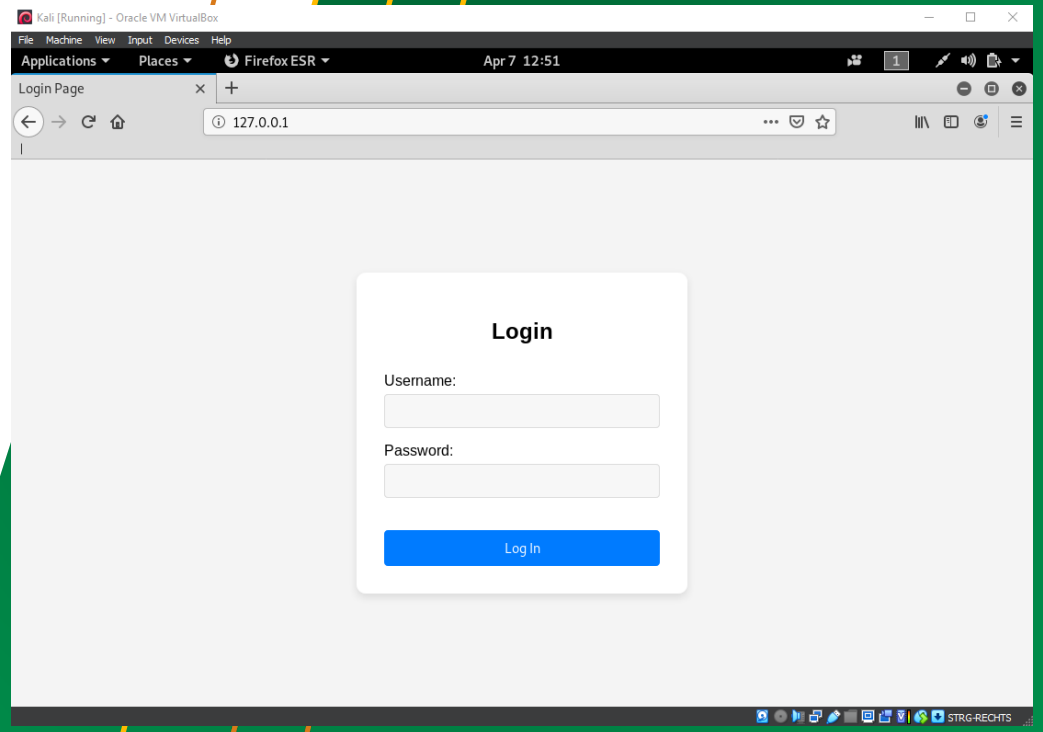
Domain	IP address
Google.com	10.20.130.40
Facebook.com	20.30.40.50
Twitter.com	40.50.60.6
……	_·_·_·_

CyberSecPro
CC BY NC SA

MITM for Redirecting a Website

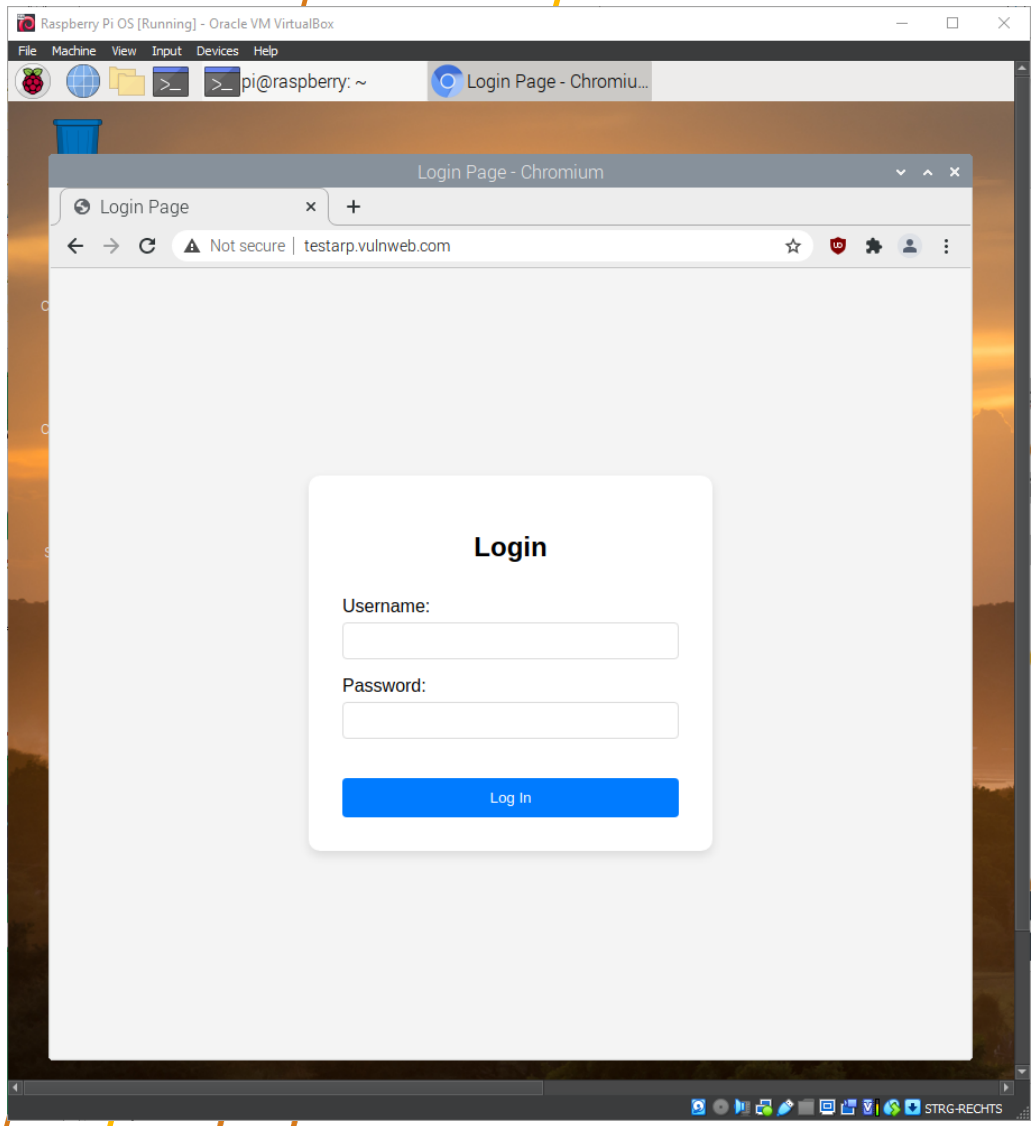
- Create a fake webpage that can be used for redirecting the request of a particular website by the user.

- Use Apache server to do that
  - Service appache2 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 testarp.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)



MITM: 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"

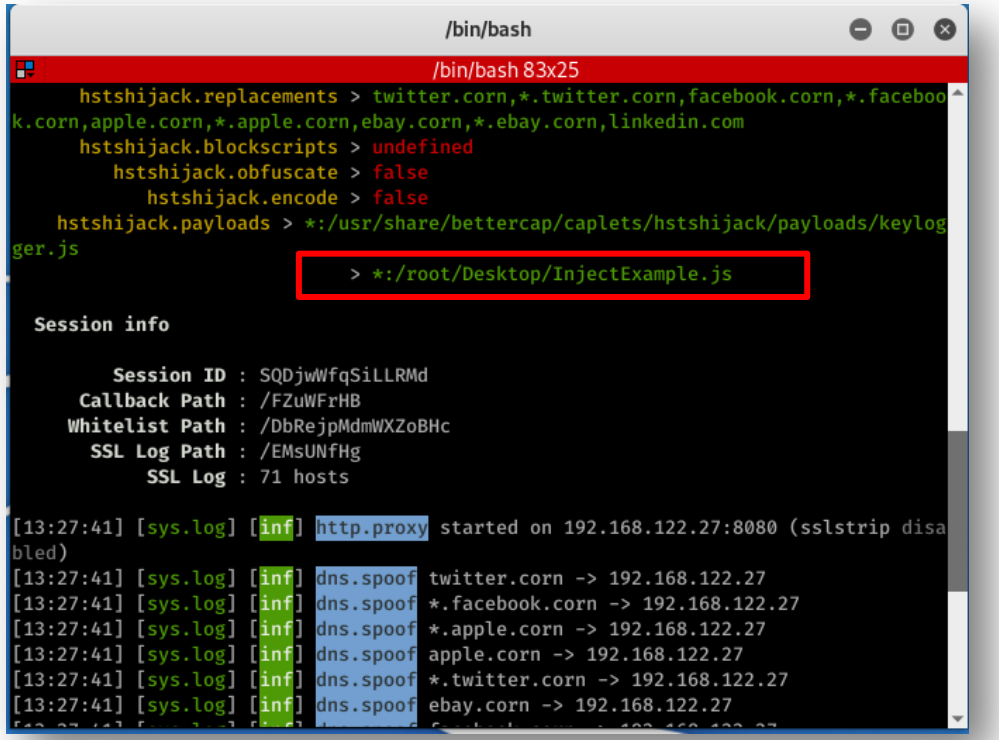
- Then, we will use the `hsthijack` caplet. Update the configuration of the caplet configuration file, which is located at: `/usr/share/bettercap/caplets/hsthijack.caplet`

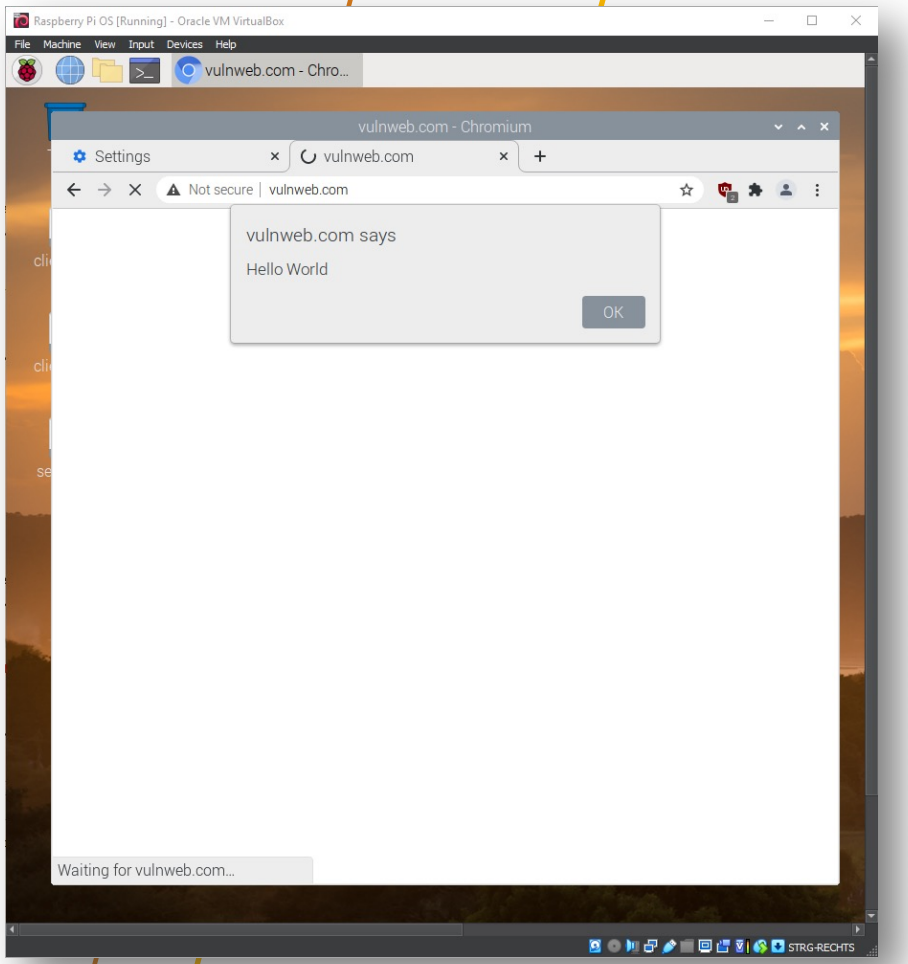
- Update the payloads with the path to your JavaScript code:
- *:/root/Desktop/InjectExample.js
  - Here, the code stored on the desktop of the Kali machine (attacker) will be loaded each time the user visits any website.

CyberSecPro
CC BY NC SA

MITM: Code Injection

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





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

CyberSecPro
CC BY NC SA

Offensive Tools

Wireshark

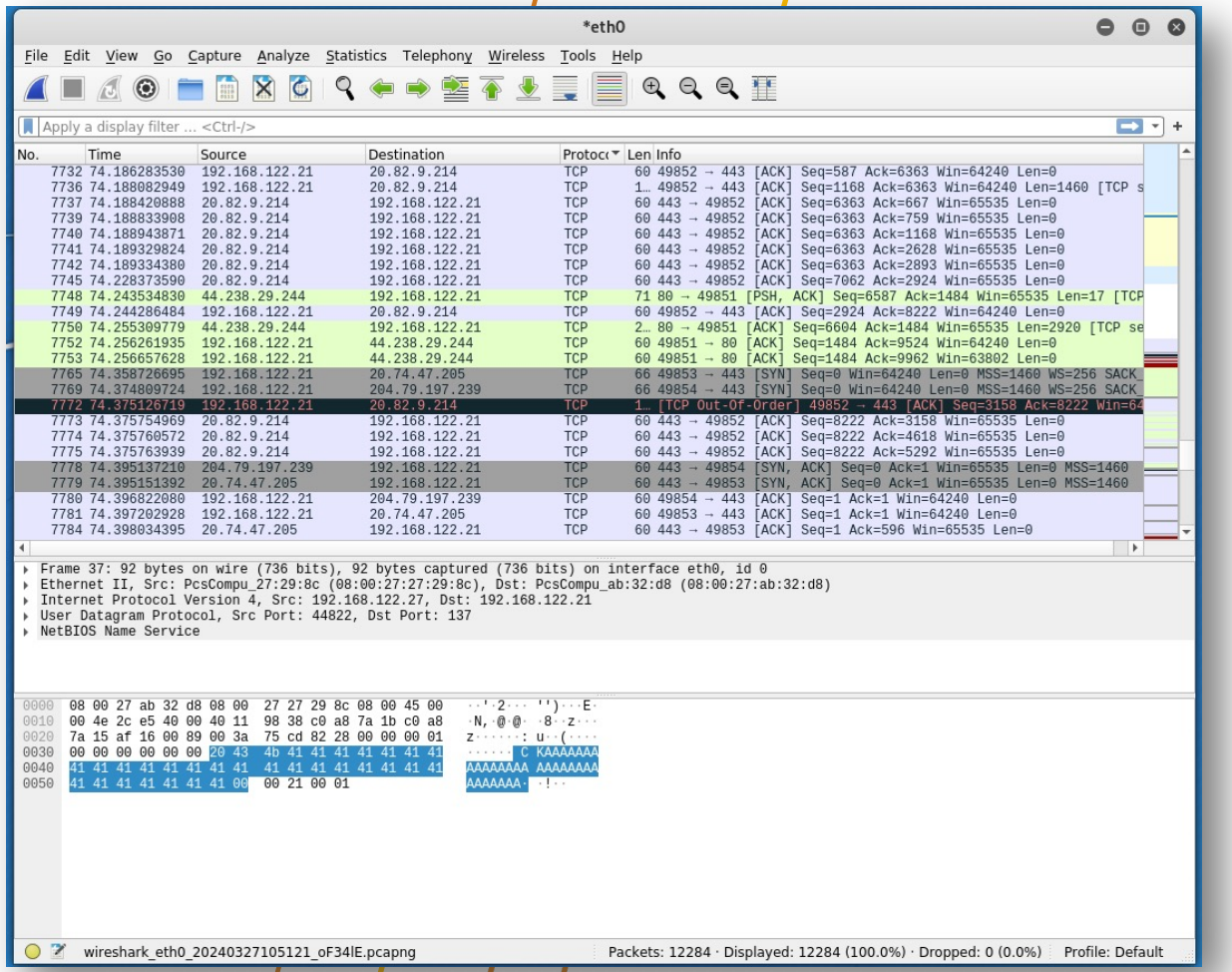
CyberSecPro

CC BY NC SA

Wireshark Sniffing & Packets Analysis

- **Wireshark** is a network protocol **analyzer** designed to help network **administrators** keep track of what is **happening** in their network.
- When you **become** an **MITM**, the **Wireshark tool** can be used to **sniff** and **analyze** traffic **sent** and **received** by the targets.

Green – TCP packets
Dark blue - is DNS packet
Black – TCP packets that have an issue



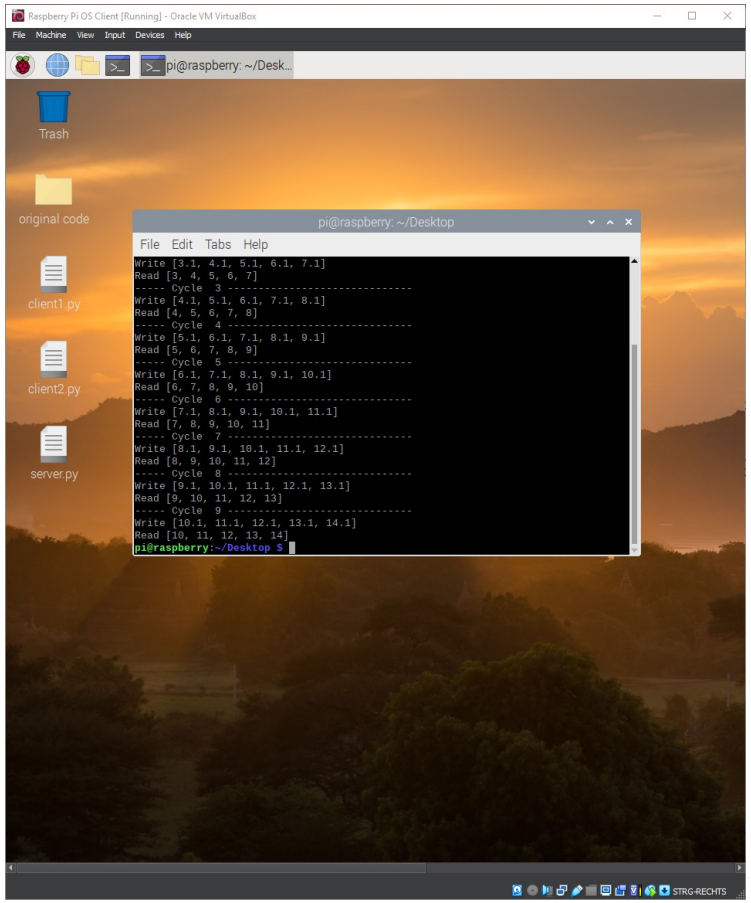
Wireshark – Client/Server Example

- In the Server/Client example, we have two Linux machines: the client sending data to the server through the **ModbusTCP** protocol.

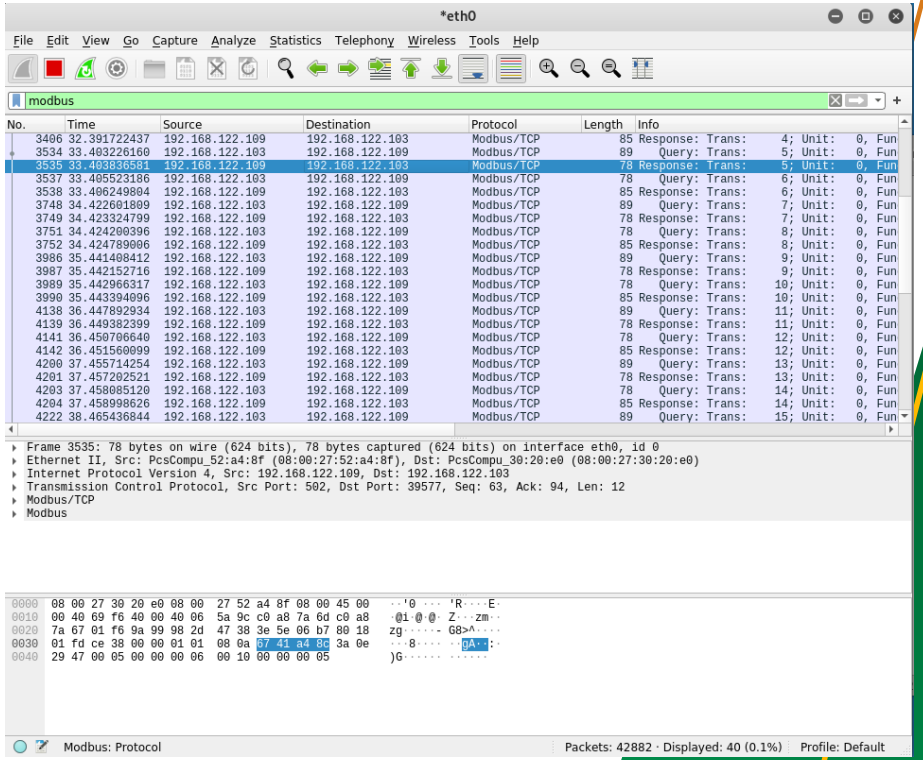
- When the attacker is a **Man-in-the-Middle**, Wireshark tool can be used for capturing all data transmitting, and other actions could be applied, such as:
  - Filtering collected data (**Modbus**)
  - Analysis traffic

CyberSecPro
CC BY NC SA

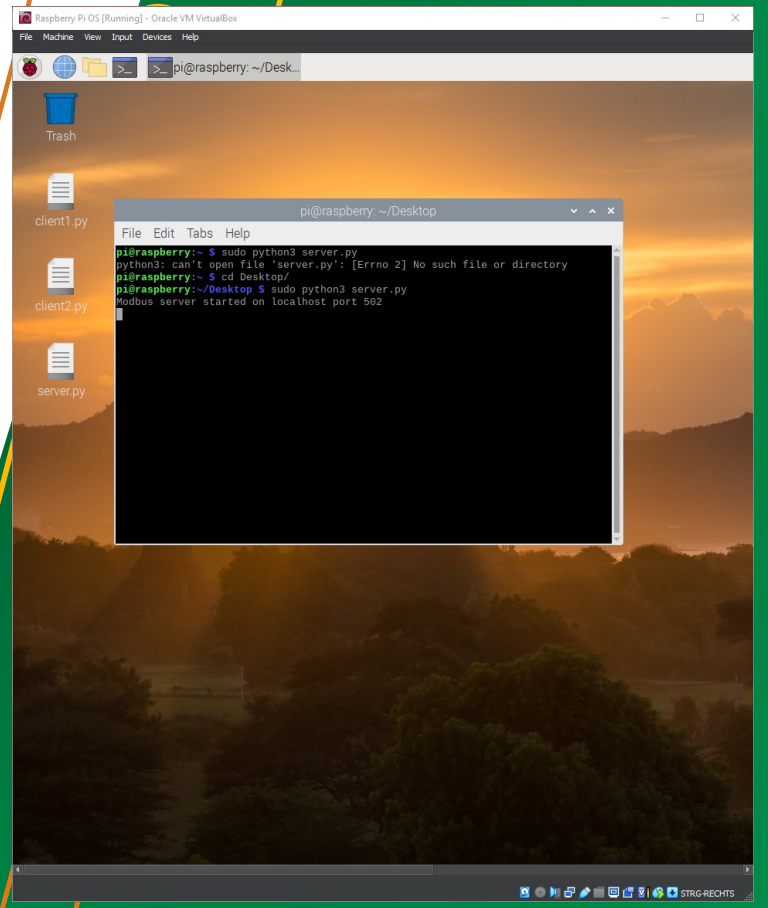
Wireshark – Client/Server Example



Client



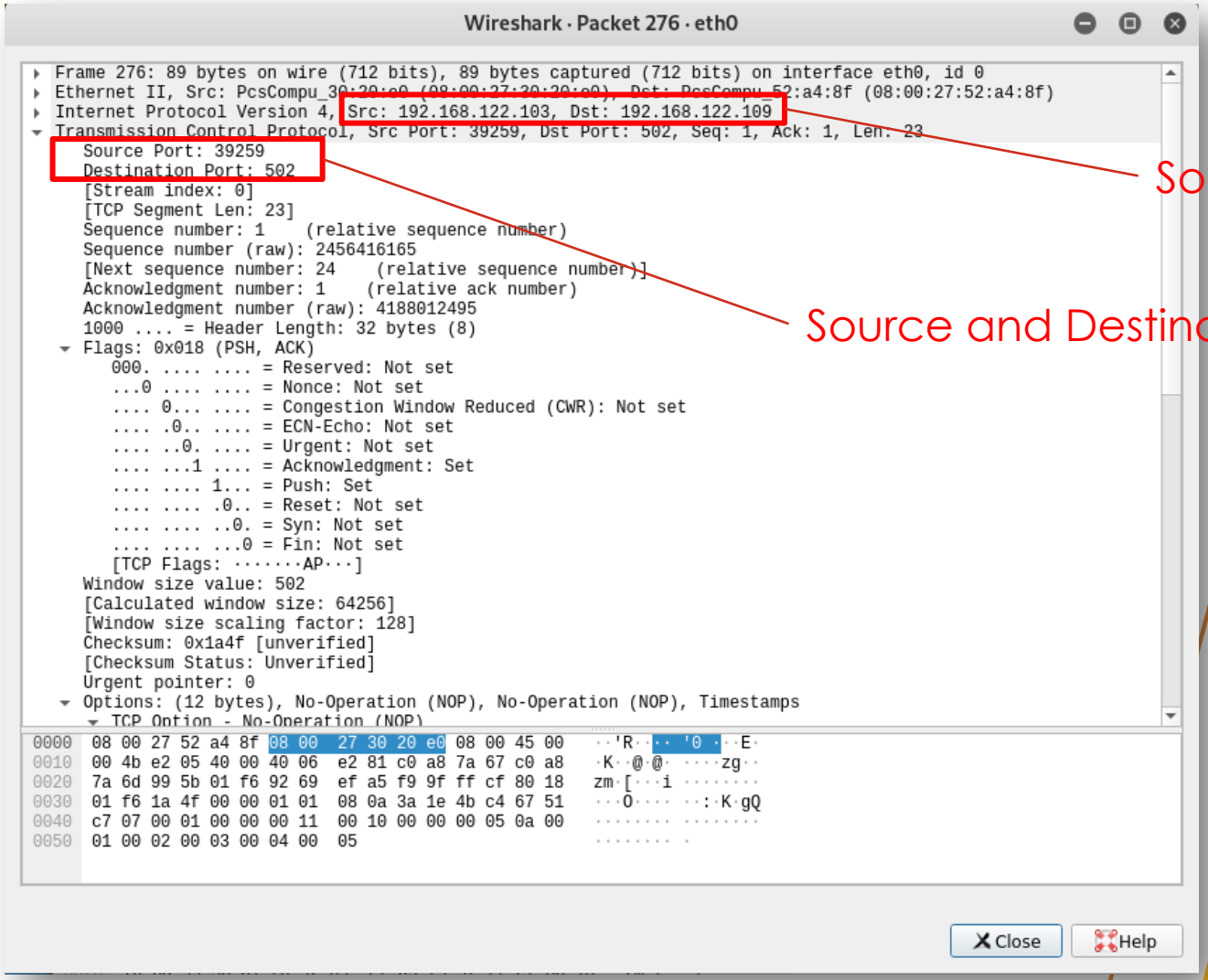
Kali



Server

CyberSecPro
CC BY NC SA

Wireshark – Client/Server Example

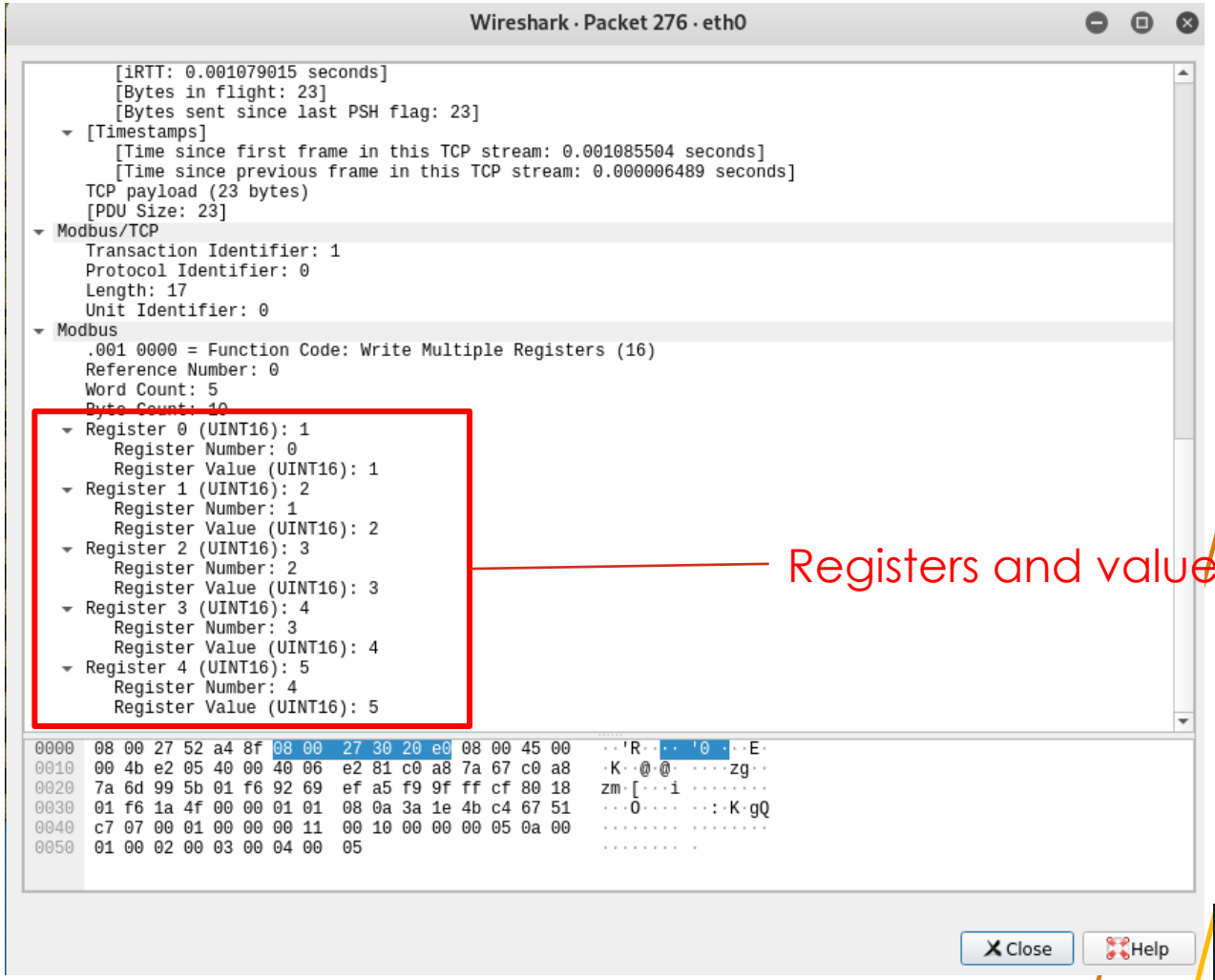


Source and Destination IP

Source and Destination Ports

CyberSecPro
CC BY NC SA

Wireshark – Client/Server Example



Registers and values

Offensive Tools

hping3

CyberSecPro

CC BY NC SA

DoS: Denial of Service Attack

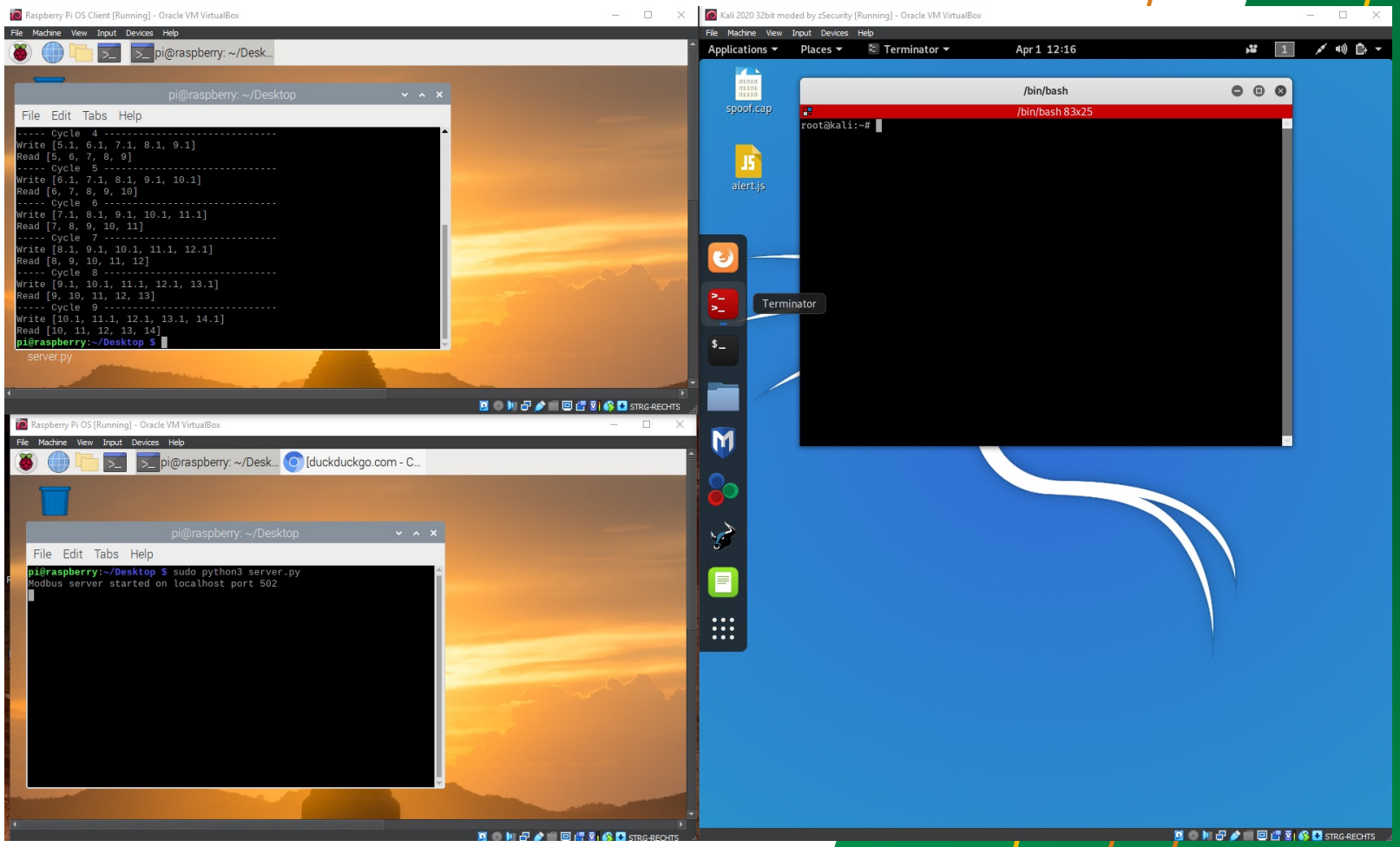
Sending too much packets to the target machine

Hping3: hping3 is a network tool able to send custom ICMP/UDP/TCP packets and to display target replies like ping does with ICMP replies. It handles fragmentation and arbitrary packet body and size, and can be used to transfer files under supported protocols. Using hping3, you can test firewall rules, perform (spoofed) port scanning, test network performance using different protocols, do path MTU discovery, perform traceroute-like actions under different protocols, fingerprint remote operating systems, audit TCP/IP stacks, etc. hping3 is scriptable using the Tcl language.

hping3 | Kali Linux Tools

CyberSecPro
CC BY NC SA

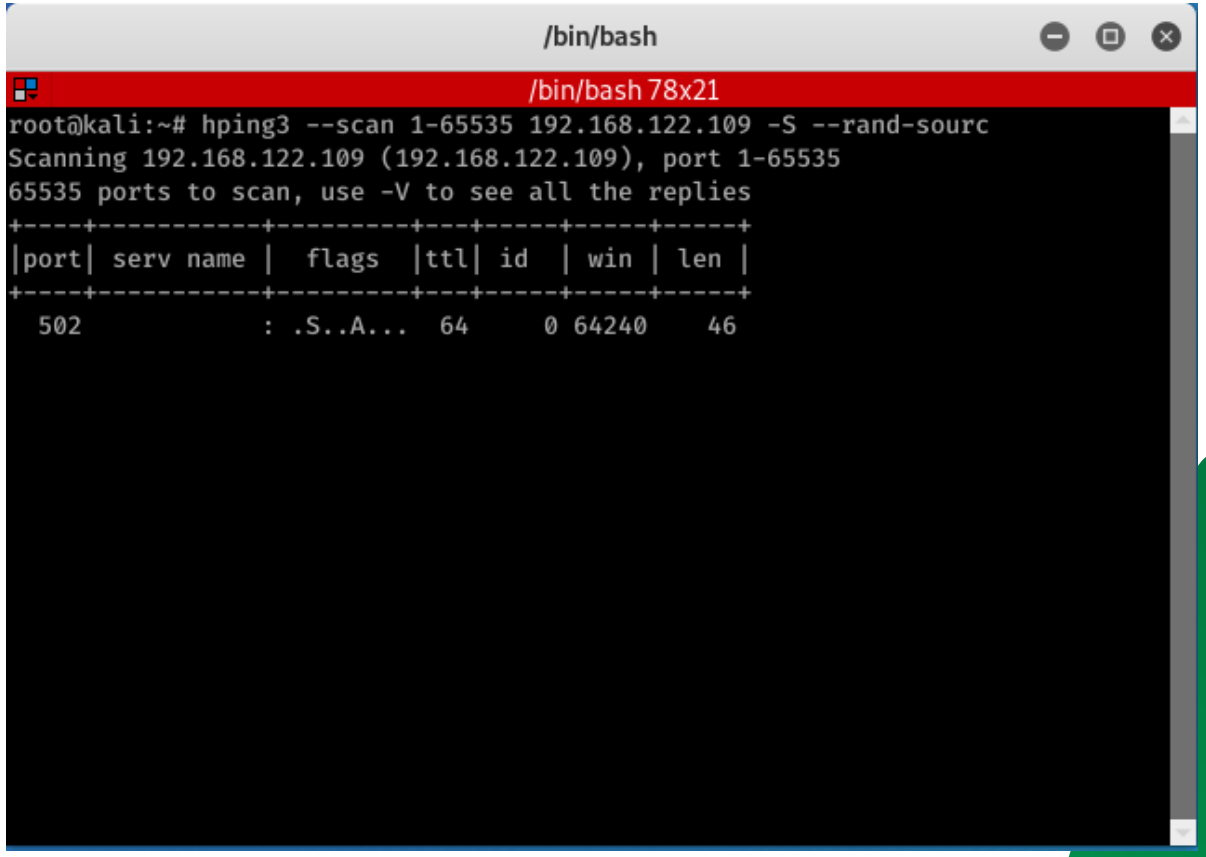
Hping3: Normal (no attack)



Hping3: Scan Ports

Scan all available ports on the victim machines

hping3 --scan 1-65535 192.168.122.109 –S –rand-source



1-65535 all ports from – to 192.168.122.109 target address
–S services
–rand-source to hide your identity

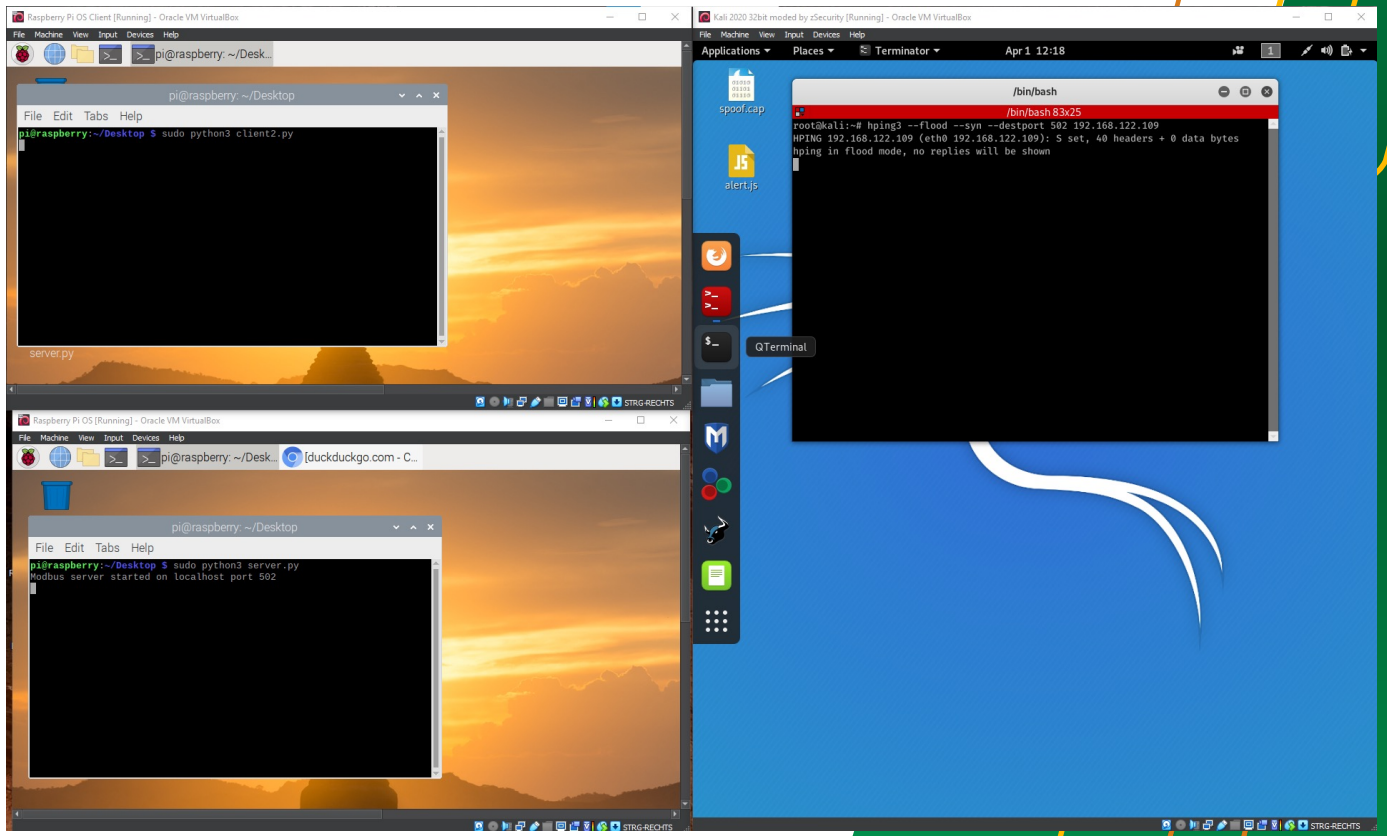
Now we have port 502 (server ModbusTCP example) as the only one available on the target machine

CyberSecPro
CC BY NC SA

Hping3: with attack

The port number can be collected from Wireshark. As shown before

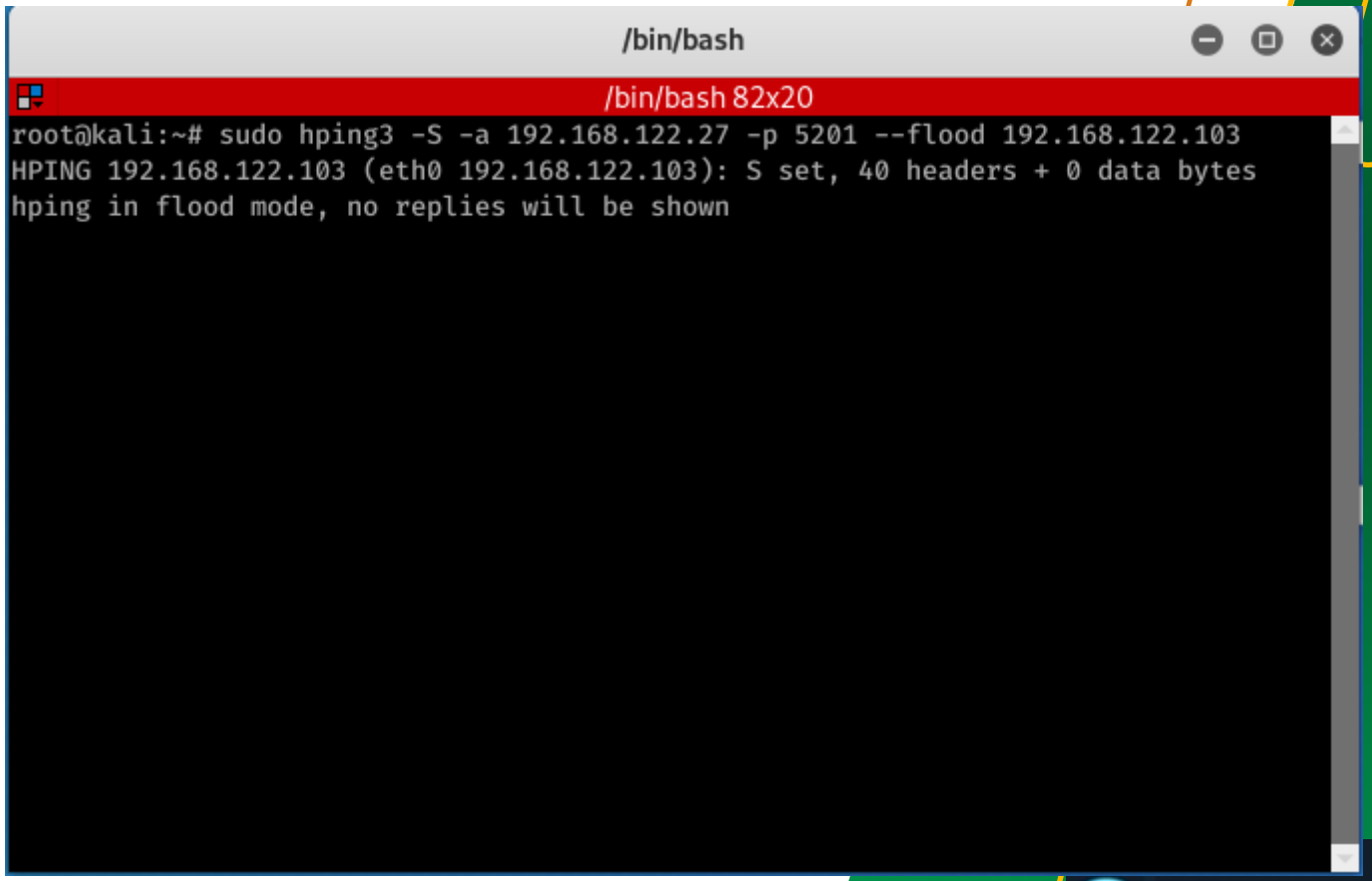
hping3 --flood --syn --destport 502 <target_IP>



From help check other formats for the tool to apply DoS against the server

Hping3: Perform Attack

hping3 –S –a **sourceIP** –p **portNumber** –flood **targetIP**



CyberSecPro
BY NC SA

Offensive Tools

Scapy

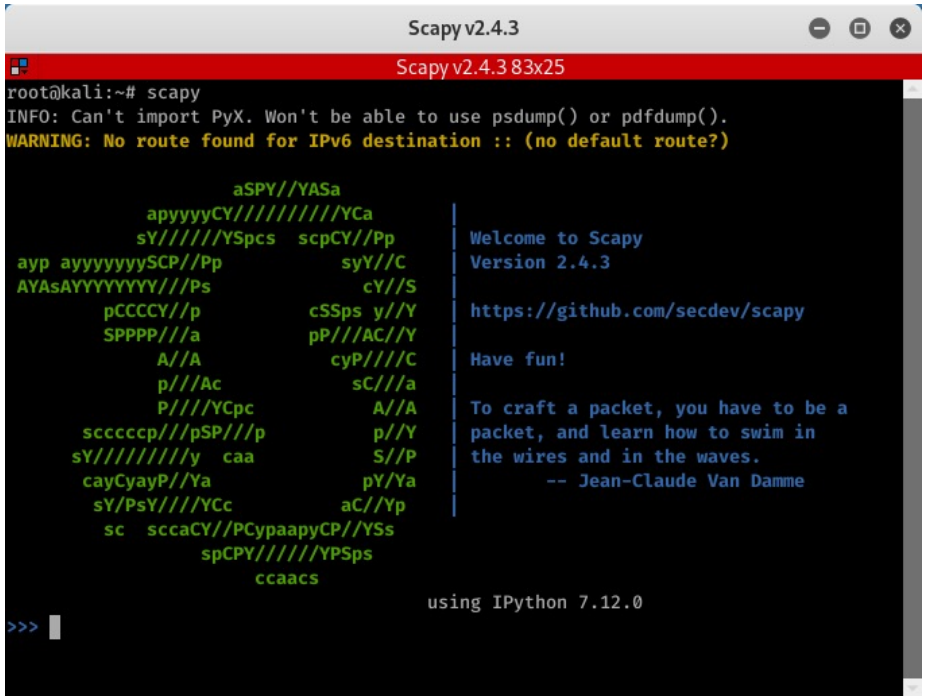
CyberSecPro

CC BY NC SA

SCAPY: Create/Send a Packet

Create packets on Scapy

- Start Scapy, and a Python command line within Scapy will open



- Assign the packet to a variable, say P.
  - >> **P = IP()**
- Define the IP Source (make it a fake IP, for example, a gateway IP address):
  - >> **P.src = "192.168.122.1"**
- Define the IP Target (victim machine):
  - >> **P.dst = "192.168.122.103"**
- Send the packet
  - **send(P)**

CyberSecPro
CC BY NC SA

Offensive Tools

NMAP

CyberSecPro

CC BY NC SA

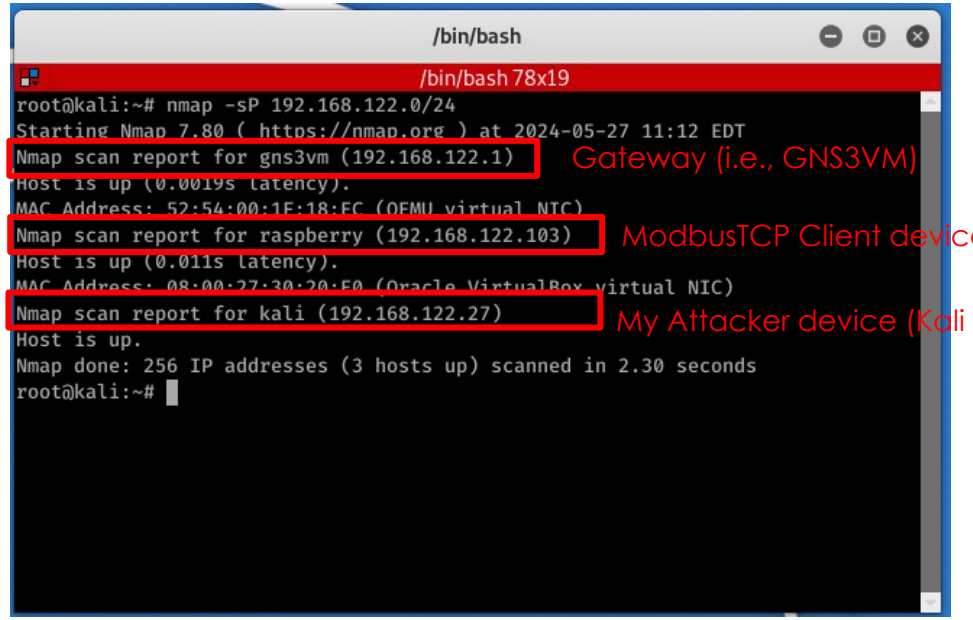
NMAP

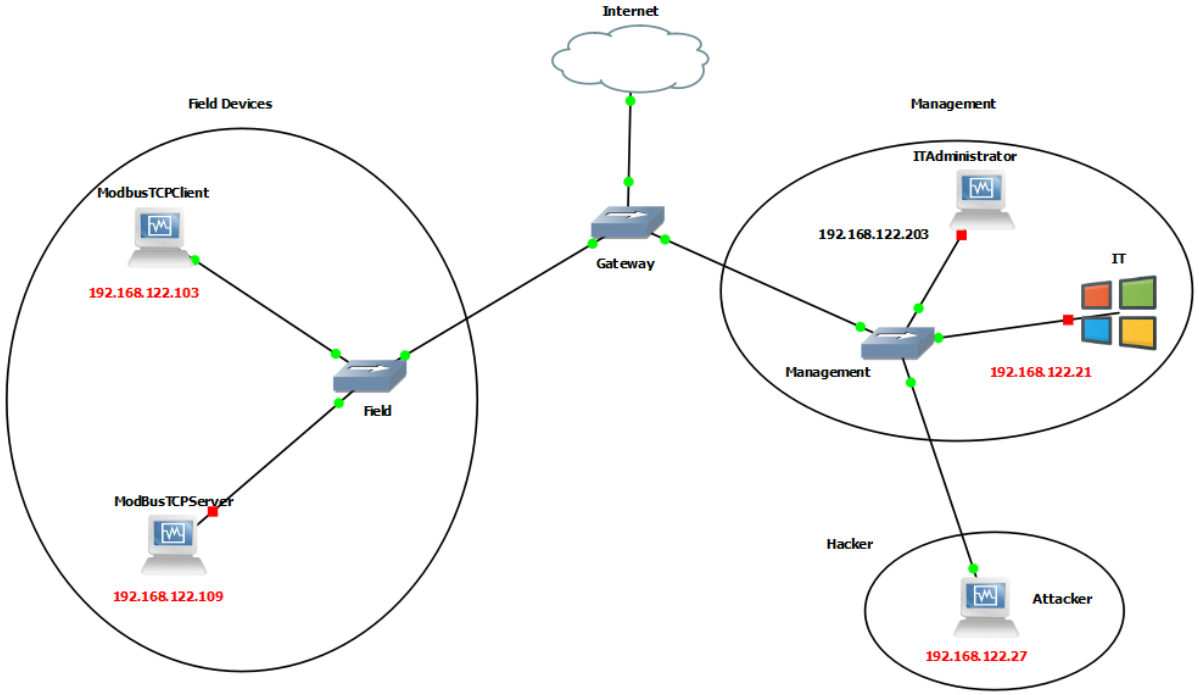
- It is a network tool used for network scanning and device discovery.
- It can also be used for **network management** and **security testing purposes**.
- The tool is capable of **exploiting** network **devices**, **detecting open ports**, and **identifying** available **services**.
- Additionally,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

CyberSecPro
CC BY NC SA

NMAP

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

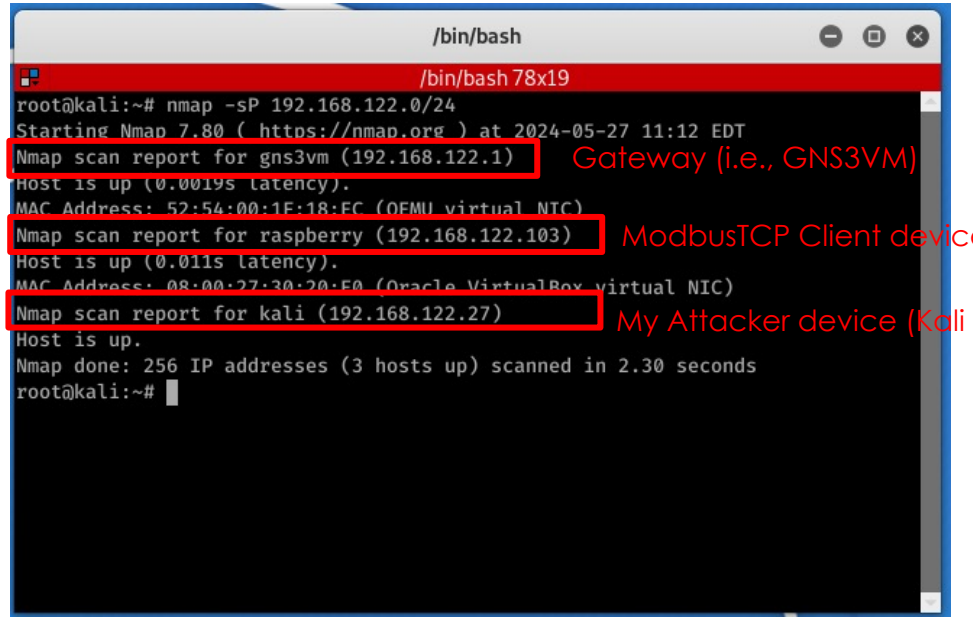


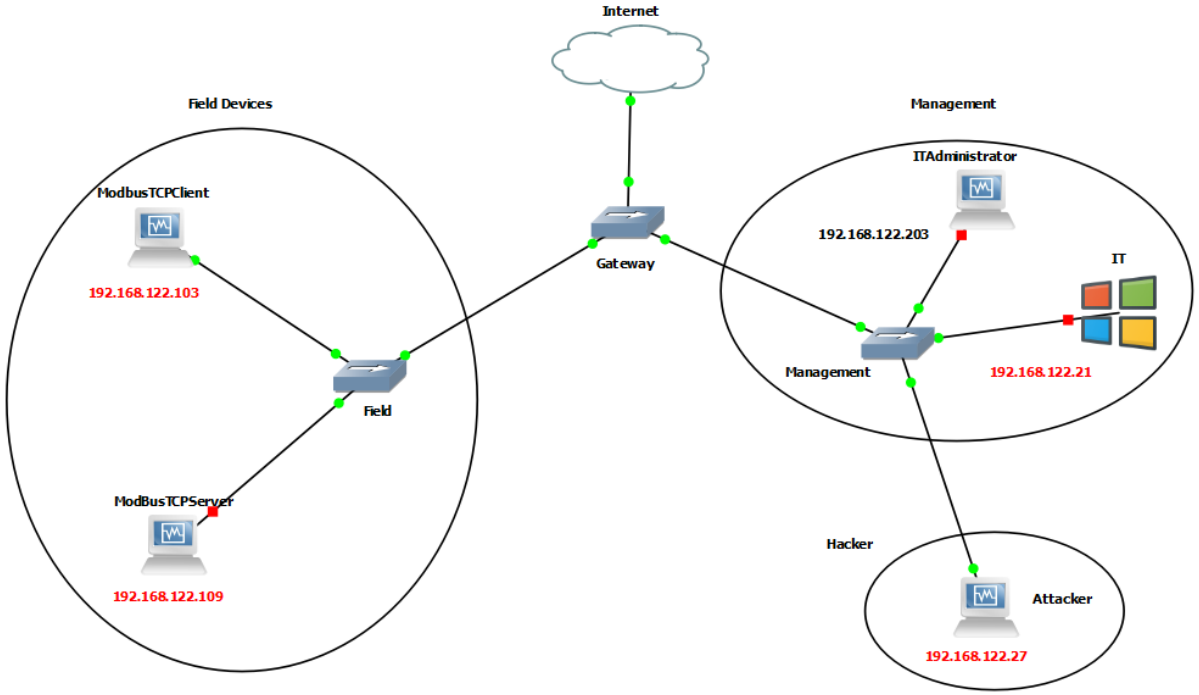


CyberSecPro
CC BY NC SA

NMAP

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



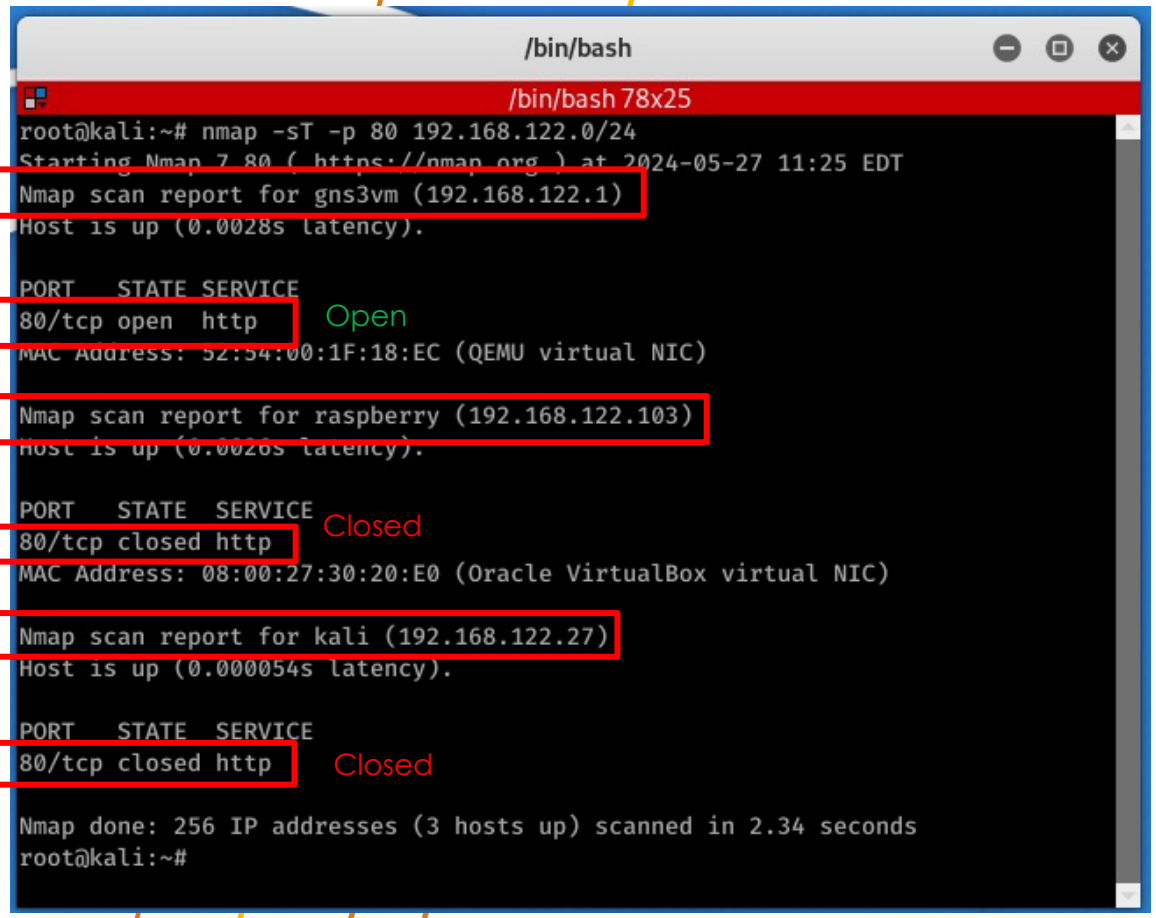


CyberSecPro
CC BY NC SA

NMAP

- Scan all all open ports in the network/a particular device:
  - Sudo Namp –sT -p <portnumbers> <network>

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



CyberSecPro
BY NC SA

Connect with CyberSecPro:
How to register and other practical information

1. Website: www.cybersecpro-project.eu
2. X (Twitter): https://twitter.com/CyberSecPro_eu
3. LinkedIn: https://www.linkedin.com/company/cybersecpro-euproject/

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

Thank you

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

CyberSecPro

CC BY NC SA