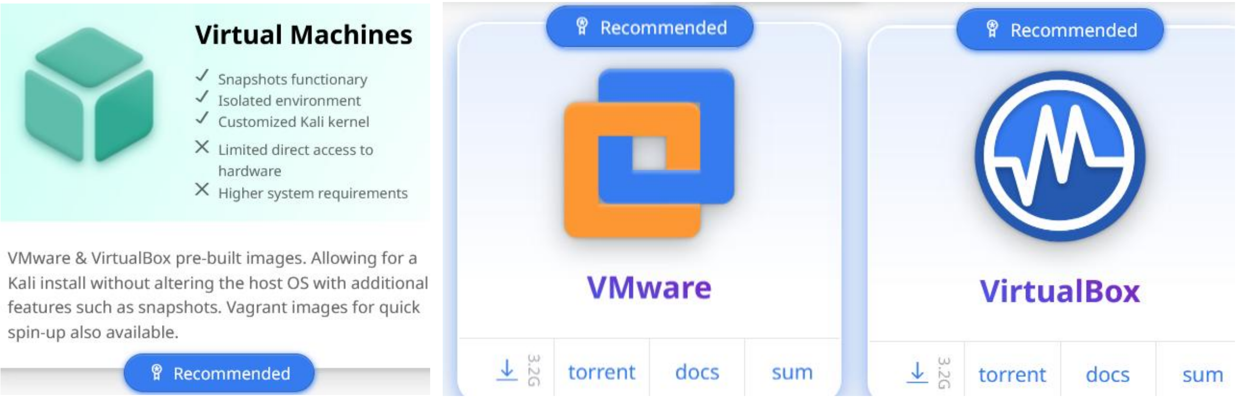
Lab #01: Set Up Penetration Testing Environment

Description: In this lab, we will set up our Pen Test lab environment, use a few tools for scanning the network and systems. I am using VMware Workstation Player and Kali Linux for this Lab course.

Step 1: To set up our own hacking environment, we need Intel i5 CPU, 8GB RAM, 500GB SSD, Wifi adapter.

Step 2: Download and install VMware Workstation Player or Oracle VirtualBox on your Windows 10 laptop. This serves as the virtualization application (Hypervisor) to run virtual machines, which use your laptop's hardware resources. Within VMware or VirtualBox we will set up a few virtual machines.

Step 3: The first VM is the attacker's machine. Download Kali Linux as Virtual Machine for VMware from https://www.kali.org/get-kali/#kali-virtual-machines which is a pre-built Kali VMware VM.



Virtual Machines

✓ Snapshots functionary
✓ Isolated environment
✓ Customized Kali kernel
✕ Limited direct access to hardware
✕ Higher system requirements

VMware & VirtualBox pre-built images. Allowing for a Kali install without altering the host OS with additional features such as snapshots. Vagrant images for quick spin-up also available.

Kali Linux is an open-source, Debian-based Linux distribution specifically designed for penetration testing, ethical hacking, and cybersecurity-related tasks. Developed and maintained by Offensive Security, Kali Linux is a highly versatile platform widely used by security professionals, researchers, and enthusiasts to test system vulnerabilities and strengthen defenses.

Key Features of Kali Linux:

- **Extensive Toolset**: Comes preloaded with over 600 security tools, including popular ones for:
  - Penetration testing (e.g., Metasploit, Burp Suite).
  - Network analysis (e.g., Wireshark, Nmap).
  - Digital forensics (e.g., Autopsy, Sleuth Kit).
  - Web application security (e.g., Nikto, Hydra, OWASP ZAP).
  - Password cracking (e.g., John the Ripper, Hashcat).
- **Customizable and Modular**:
  - Users can tailor the distribution to their needs by adding or removing tools.
  - Lightweight versions are available, or full installations for comprehensive environments.
- **Multiplatform Support:**
  - Available for a variety of platforms, including x86, x64, ARM, and virtualized environments.
  - Versions exist for smartphones (NetHunter for Android) and Raspberry Pi.

Useful for Use Cases:

- **Penetration Testing**: Simulating real-world attacks to identify vulnerabilities in systems.
- **Vulnerability Assessment**: Scanning and reporting security weaknesses in networks and applications.
- **Forensics and Incident Response**: Investigating breaches and analyzing data.
- **Wireless Security**: Testing the security of Wi-Fi networks and protocols.
- **Malware Analysis**: Analyzing malicious software to understand its behavior.

Step 4: The second VM is Metasploitable 2 which will be our victim / target. Download this VM as a zip file from **https://sourceforge.net/projects/metasploitable/files/Metasploitable2/**

Metasploitable 2 is a deliberately vulnerable Linux virtual machine designed for penetration testing and security training. It is widely used by security professionals, ethical hackers, and students to practice identifying and exploiting vulnerabilities in a controlled environment.

Key Features of Metasploitable 2:

- **Purpose**: It serves as a safe, isolated platform for testing security tools and practicing exploitation techniques without affecting real-world systems.
- **Vulnerabilities**:
  - Includes many known vulnerabilities in apps and services like outdated versions of MySQL, Apache, PHP, and Tomcat.
  - Deliberate misconfigurations in services like FTP, SSH, and web applications (e.g., DVWA, Mutillidae).
  - Specific vulnerabilities for popular tools like the Metasploit Framework.
- **Pre-installed Services**:
  - Open ports with weak configurations.
  - Vulnerable apps such as TikiWiki, PHPMyAdmin, and vulnerable CGI scripts.
- **Legal and Ethical**: It is intended for use in secure, private lab environments and should never be exposed to the public internet, as its vulnerabilities are easily exploitable.

Step 5: The third VM → Kioptrix will be our next victim, download Kioptrix Level 2 from TCM → https://drive.google.com/drive/folders/1CsGWRsmyJm84TAU6U0-72o4Jnb5E9xvs OR https://download.vulnhub.com/kioptrix/archive/Kioptrix_Level_2-original.rar

Kioptrix VM is vulnerable virtual machine intentionally designed to help individuals practice penetration testing, ethical hacking, and vulnerability assessment in a controlled environment. This VM is widely used by cybersecurity professionals and students to enhance their skills in exploiting real-world vulnerabilities and learning various attack techniques.

- **Level 1**: Focuses on basic exploitation techniques like remote code execution.
- **Level 2-4**: Introduces advanced techniques - privilege escalation, web app exploitation, and chaining multiple vulnerabilities.
- **Level 5**: Tests advanced skills with complex scenarios.

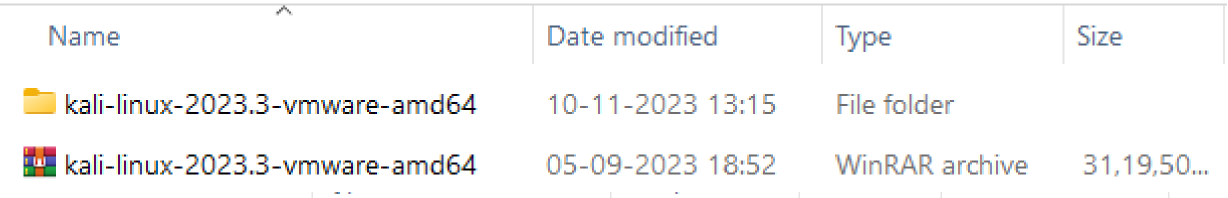
Key Features of Kioptrix VM:

- **Purpose**:
  - Created to mimic realistic scenarios with known vulnerabilities.
  - Ideal for practicing exploitation techniques on systems similar to real-world environments.
- **Focus on Realism:**
  - The VMs include commonly exploited vulnerabilities in Linux systems, web applications, and network services.
  - Challenges range in difficulty, making it suitable for beginners and intermediate users.
- **Common Vulnerabilities:**
  - Misconfigured services.
  - Outdated software versions.
  - SQL injection, command injection, and privilege escalation opportunities.
  - Weak file permissions and authentication mechanisms.
- **Usage:**
  - Used alongside tools like Metasploit, Nmap, Burp Suite, and other security utilities for reconnaissance, exploitation, and post-exploitation exercises.
  - Each VM in the series includes unique vulnerabilities and learning objectives.

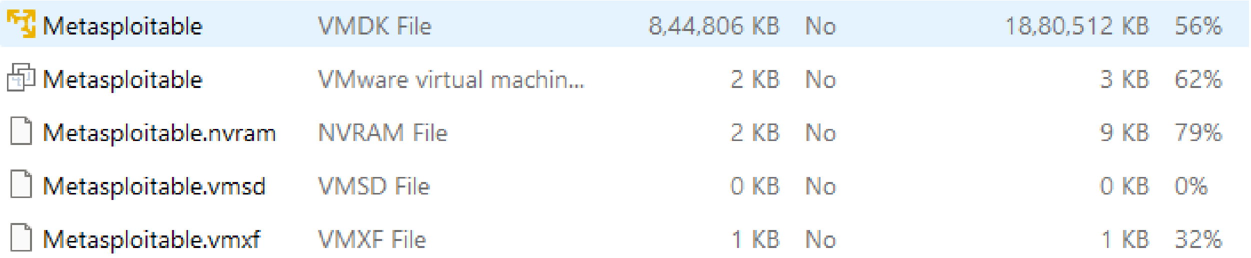
Benefits for using such VMs:

- Hands-on Experience: Gain practical skills in identifying, exploiting, and mitigating vulnerabilities.
- Controlled Environment: Ideal for beginners and advanced users to test techniques safely.
- Skill Development: Helps understand exploiting vulnerabilities and secure real-world systems.
- These victim VM are standalone target systems, run on hypervisors like VirtualBox or VMware which simulate real-world systems for security testing without impacting production networks.
- Helps learners understand how attackers identify and exploit vulnerabilities.
- Teaches defensive techniques by highlighting system weaknesses.

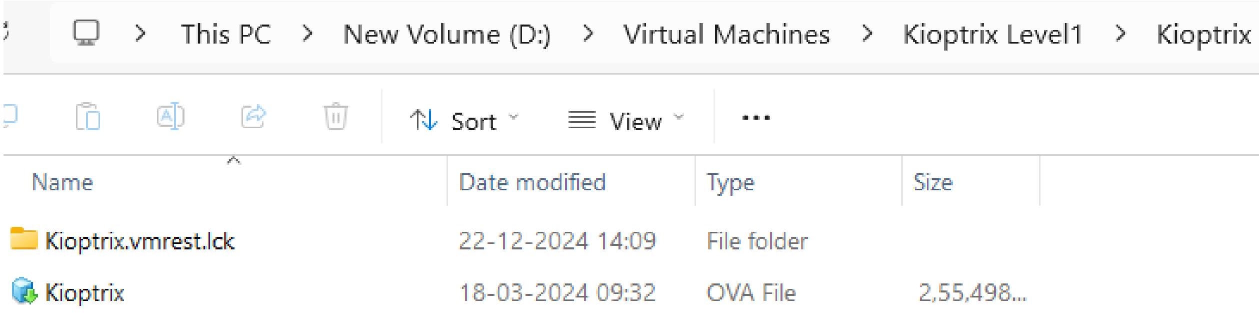
Step 6: Unzip the downloaded files into separate folders.



Name	Date modified	Type	Size
kali-linux-2023.3-vmware-amd64	10-11-2023 13:15	File folder	
kali-linux-2023.3-vmware-amd64	05-09-2023 18:52	WinRAR archive	31,19,50...



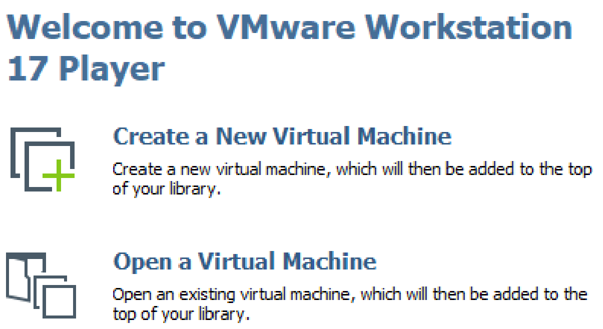
Metasploitable	VMDK File	8,44,806 KB	No	18,80,512 KB	56%
Metasploitable	VMware virtual machin...	2 KB	No	3 KB	62%
Metasploitable.nvram	NVRAM File	2 KB	No	9 KB	79%
Metasploitable.vmsd	VMSD File	0 KB	No	0 KB	0%
Metasploitable.vmxf	VMXF File	1 KB	No	1 KB	32%



This PC > New Volume (D:) > Virtual Machines > Kioptrix Level1 > Kioptrix

Name	Date modified	Type	Size
Kioptrix.vmrest.lck	22-12-2024 14:09	File folder	
Kioptrix	18-03-2024 09:32	OVA File	2,55,498...

Step 7: Use Hypervisor to 'Open a Virtual Machine' from the unzipped files - OWA/VMDK as add as VMs.



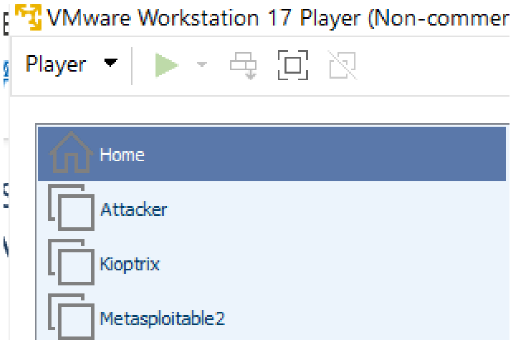
Welcome to VMware Workstation 17 Player

Create a New Virtual Machine

Create a new virtual machine, which will then be added to the top of your library.

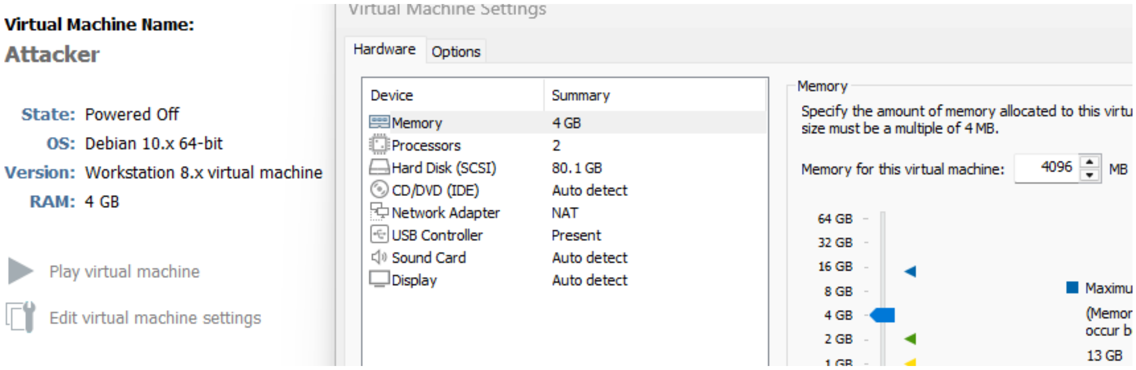
Open a Virtual Machine

Open an existing virtual machine, which will then be added to the top of your library.



VMware Workstation 17 Player (Non-commer

Step 8: Click the VM → 'Edit Settings' to change the hardware (for Kali: RAM 2→ 4GB, Processor →2 & Network → NAT), other VMs can run on 512MB or 1GB only. BUT ensure all VMs are using NAT network.



Virtual Machine Name:
Attacker

State: Powered Off
OS: Debian 10.x 64-bit
Version: Workstation 8.x virtual machine
RAM: 4 GB

Device	Summary
Memory	4 GB
Processors	2
Hard Disk (SCSI)	80.1 GB
CD/DVD (IDE)	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Memory

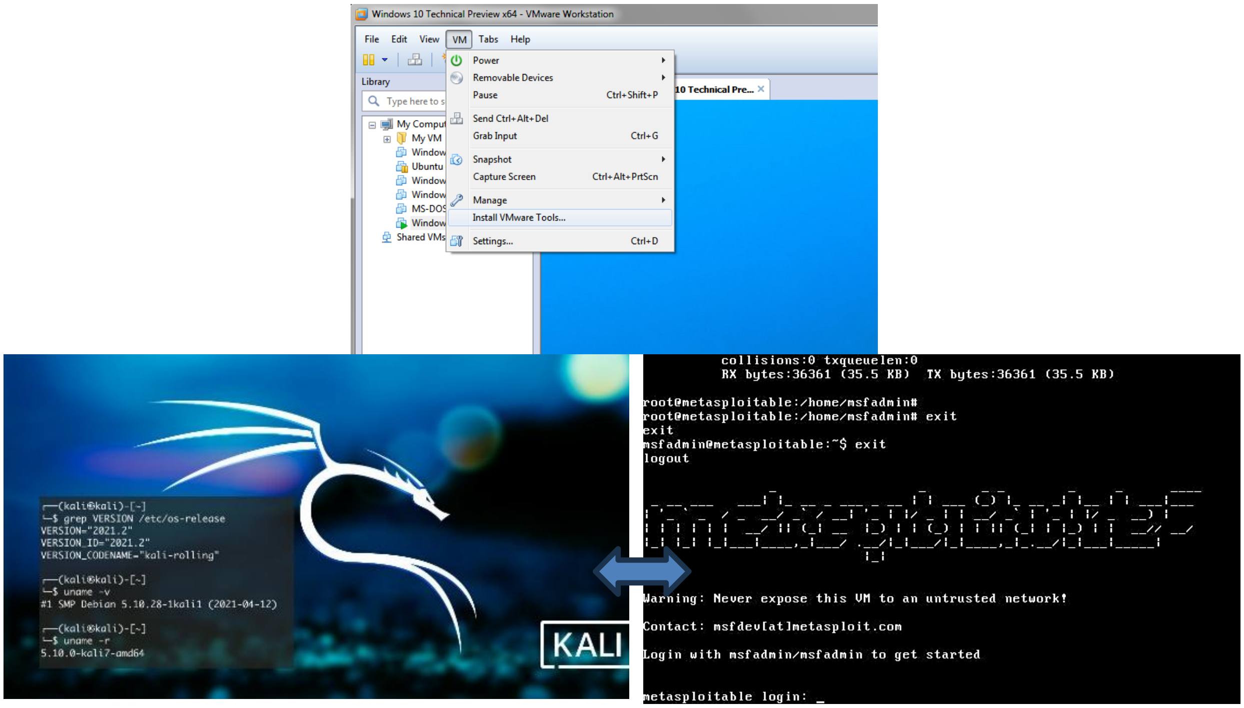
Specify the amount of memory allocated to this virtu size must be a multiple of 4 MB.

Memory for this virtual machine: 4096 MB

Why NAT?

Network Address Translation (NAT)	Bridged network
Gives a virtual machine access to network resources using the host computer's IP address.	Connects the virtual machine to a network using the host computer's Ethernet adapter.
Here the VM does not have its own IP address on the external network.	Here the VM is a full participant in the network - another system on LAN.
Instead, a separate private network is set up on the host system, controlled by the Hypervisor.	It has access to other machines on the network.
Your VMs get IP address on that network from the VMware virtual DHCP server.	Can be contacted by other machines on the network as if it is a physical system on that LAN.

Our Hacking Environment: This should look like our LAN running Kali, Metasploitable2 and Kioptrix.

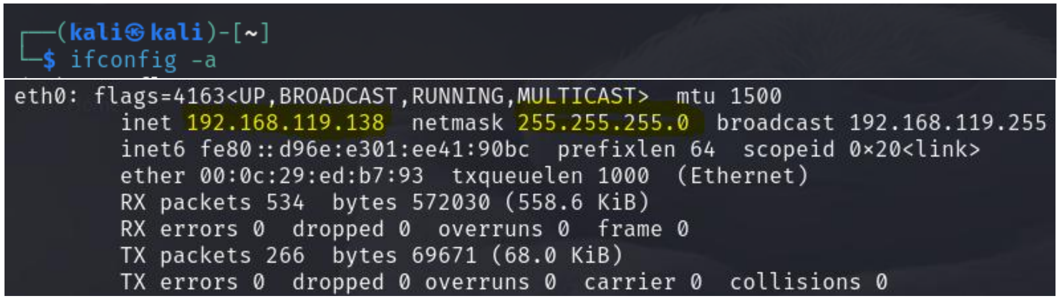


```
┌──(kali㉿kali)-[~]
└─$ grep VERSION /etc/os-release
VERSION="2021.2"
VERSION_ID="2021.2"
VERSION_CODENAME="kali-rolling"

┌──(kali㉿kali)-[~]
└─$ uname -v
#1 SMP Debian 5.10.28-1kali1 (2021-04-12)

┌──(kali㉿kali)-[~]
└─$ uname -r
5.10.0-kali7-amd64
```

```
          collisions:0 txqueuelen:0
          RX bytes:36361 (35.5 KB)  TX bytes:36361 (35.5 KB)

root@metasploitable:/home/msfadmin#
root@metasploitable:/home/msfadmin# exit
exit
msfadmin@metasploitable:~$ exit
logout


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: _
```

Step 8: Attacker is on the victim's network – BUT how do we confirm or interact with the victims? For this 'Power On' your attacker VM (Kali Linux), login as user 'kali' and password 'kali'.

Step 9: Now we need to find the attacker's IP Address to determine the network info, use **$ ifconfig -a**



```
┌──(kali㉿kali)-[~]
└─$ ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.119.138  netmask 255.255.255.0  broadcast 192.168.119.255
        inet6 fe80::d96e:e301:ee41:90bc  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:ed:b7:93  txqueuelen 1000  (Ethernet)
        RX packets 534  bytes 572030 (558.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 266  bytes 69671 (68.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

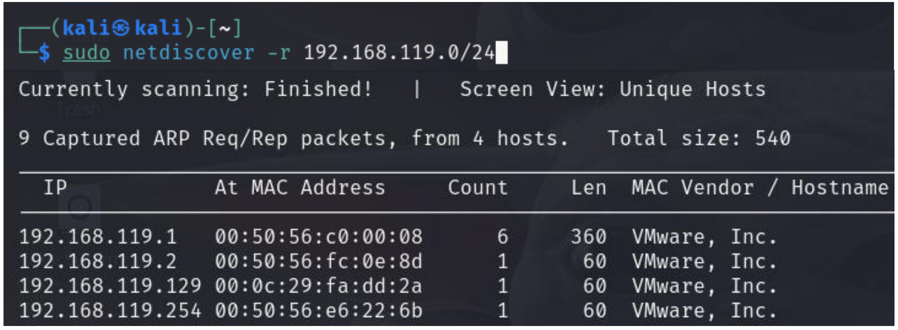
Step 10: Note the Virtual Ethernet card 0 (eth0) IP address which is assigned by VMware Hypervisor.

- VMware app runs DHCP Server → assigned Private IP address to Kali VM → 192.168.119.138
- Subnet mask: 255.255.255.0 → /24 → Possible IP addresses: 255
- 192.168.119.0 – identifies the network, not assigned to any device
- 192.168.119.255 – broadcast IP for sending data to all devices on this network
- Valid IP range 192.168.119.1 – 254 (254 hosts / systems / devices)

IP Address	VMware IP address allocations
192.168.119.1	Assigned to the physical host machine's virtual network adapter. Represents the Gateway for VMs within the VMware NAT network. Allows the host systems to communicate with VMs in the same virtual network.
192.168.119.2	Assigned to the VMware virtual DHCP server. Provides dynamic IP addresses to VMs added to VMware Hypervisor in the network. Ensures proper IP address allocation within the VMware virtual network.
192.168.119.254	Default gateway IP address for the NAT or Host-Only network. For NAT - routes traffic from VMs to external networks/internet) via host machine.

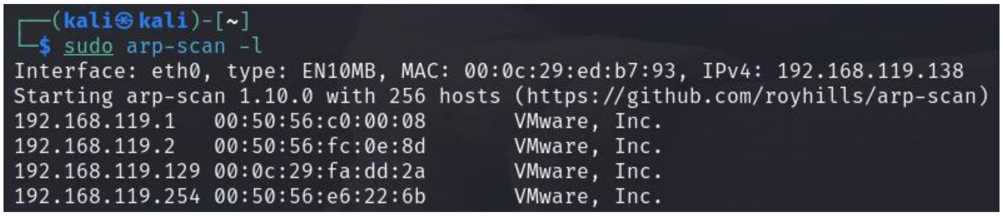
Step 11: Now we need to find the remaining IP address of other systems (victims / target) on this network.

- Use 'netdiscover' command to scan the entire network range



```
┌──(kali㉿kali)-[~]
└─$ sudo netdiscover -r 192.168.119.0/24
Currently scanning: Finished!   |   Screen View: Unique Hosts

9 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 540
 ____________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 --------------------------------------------------------------------
192.168.119.1   00:50:56:c0:00:08      6     360  VMware, Inc.
192.168.119.2   00:50:56:fc:0e:8d      1      60  VMware, Inc.
192.168.119.129 00:0c:29:fa:dd:2a      1      60  VMware, Inc.
192.168.119.254 00:50:56:e6:22:6b      1      60  VMware, Inc.
```

- OR use 'arp-scan' command which sends ARP packets to list all active systems and the MAC addresses on the local network.



```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:ed:b7:93, IPv4: 192.168.119.138
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.119.1   00:50:56:c0:00:08       VMware, Inc.
192.168.119.2   00:50:56:fc:0e:8d       VMware, Inc.
192.168.119.129 00:0c:29:fa:dd:2a       VMware, Inc.
192.168.119.254 00:50:56:e6:22:6b       VMware, Inc.
```

These commands reveal 'live' IP and MAC addresses as well as type of system. Your IPs may be different.

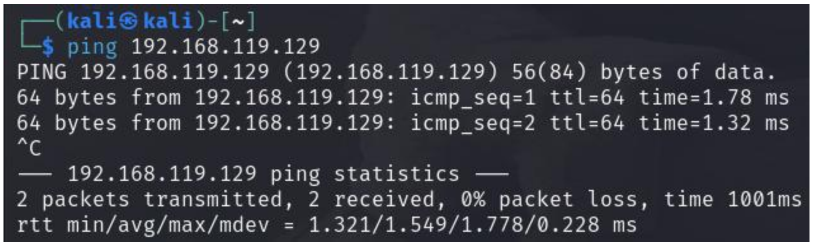
Step 12: Now we know the attacker's IP is 192.168.119.138, while the other IP address found (apart from VMware IPs) is 192.168.119.129. To verify this is correct, poke (PING) the victim IP from Kali machine.

PING (Packet Internet Groper) is a network utility that uses the ICMP (Internet Control Message Protocol) to test connectivity and measure the round-trip time (RTT) for messages sent from the source to a destination host.

- **ICMP Echo Request/Reply**:
    - PING sends **ICMP Echo Request** packets to the target host.
    - The target host responds with **ICMP Echo Reply** packets if reachable.
    - Each packet includes:
        - Source and destination IP addresses.
        - A unique identifier and sequence number.
        - 32 Kilo Bit Payload data for verifying data integrity.
- **Round-Trip Time (RTT)**:
    - The time taken for the Echo Request to reach the destination and the Echo Reply to return to the source.
    - PING calculates RTT for each packet (4 times for Windows OS, unlimited for Linux OS) for network performance evaluation.
- **Packet Loss**:
    - PING measures the number of packets sent versus received.
    - Packet loss indicates issues - congestion, routing problems, or firewalls dropping ICMP traffic.

Limitations of PING:

- **ICMP Restrictions**: Many modern firewalls and network devices block or limit ICMP traffic to mitigate reconnaissance. Some systems deprioritize responding to ICMP, causing false negatives.
- **Not Always Indicative of Service Availability**: A host might respond to PING but have critical services (e.g., HTTP, SSH) offline.
- **No Detailed Route Information**: PING only tests connectivity and RTT, offering no insight into intermediary hops (use traceroute for that).
- **Vulnerable to Spoofing**: ICMP packets can be forged, leading to trust issues in results.



```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.119.129
PING 192.168.119.129 (192.168.119.129) 56(84) bytes of data.
64 bytes from 192.168.119.129: icmp_seq=1 ttl=64 time=1.78 ms
64 bytes from 192.168.119.129: icmp_seq=2 ttl=64 time=1.32 ms
^C
—— 192.168.119.129 ping statistics ——
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.321/1.549/1.778/0.228 ms
```

Note:

- Time=1xxx seconds & 0% packet loss – indicates the network is fast and efficient – Virtual Network.
- TTL = 64 - this value determines how long data should be kept before being discarded.

TTL or Time To Live:

- Network Perspective: Each IP packet has a TTL field, which is an 8-bit value. As the packet traverses through routers, the TTL value is decreased by 1 each time it passes a router. If the TTL reaches zero before the packet reaches its destination, the packet is discarded. This prevents packets from circulating indefinitely on the network.
- Cybersecurity Perspective: TTL reveals the version/type of OS of the device.
    - TTL value for **Linux/Unix OS** is **64**
    - TTL value for **Windows 95/98/XP/ME OS** is **32**
    - TTL value for **Windows XP/7/8/10/11/2003/2009** is **128**.
    - TTL value for **Max OS X** is **64**.
    - TTL value for **Solaris OS** is **255**.

Lab Activities:

- **Perform steps to setup and access your targets from the attacker machine (Kali Linux):**
    - **Virtual Machines - Metasploitable2 and Kioptrix**
    - **External domains: Webscantest.com, Gbhackers.com, Scanme.nmap.org.**

Note:

- **Take clear snip/screenshots of your research, submit your lab file as WORD DOCX only.**
- **Do not copy experiments from others OR share your work with others.**
- **Those found copying or sharing their lab documents with others, their lab will be graded as ZERO.**