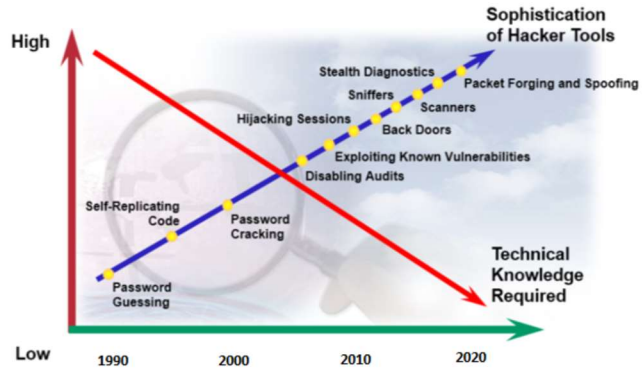
Part 1: Conceptual

Q1.- Define Cybersecurity and enumerate its importance.

Q2.- Briefly explain the main theme in below diagram: -



Q3. Define following terminologies: -

a. Vulnerability
b. Exploit
c. Daisy Chaining
d. Zero-Day
e. Hack Value
f. Payload
g. Bot

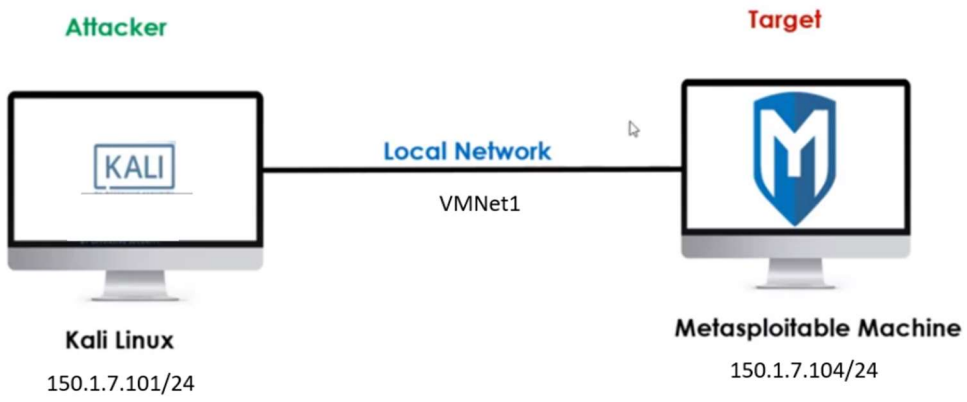
Q4 – Briefly explain the difference between Hacking, Ethical Hacking and Penetration testing.

Part 2: Lab

Marks: 80

Q5. Buildup your lab setup based on the provided network diagram, which includes a Kali Linux attacker machine and a Metasploitable target machine connected via a

local network (VMNet1). Use the IP address scheme as reflected. Ensure that Target machine is reachable from Kali Linux.



Part 1 Answer

Answer 1:

Cybersecurity is the practice that protects system, networks & data from unauthorized access, attack or damage. Its purpose is to secure sensitive information, detect cyber threats & prevent them.

Important of Cybersecurity:

1. **Data Protection:** Protects personal & business data from unauthorized access.
2. **Prevention of Cyber Attacks:** Protects systems from Malware, hacking attacks, Phishing.
3. **Privacy Protection:** Users personal & confidential information is kept secure.
4. **National Security:** Government & military data are protected by cyber warfare.

Answer 2:

1. **Sophistication of Hacker Tools (Blue Line - Increasing):**
    a. Earlier hacking techniques were simple, such as passwords guessing & self-replication codes.
    b. Gradually advanced techniques were introduced, such as Sniffer's, Hijacking Sessions & Exploiting known vulnerabilities.

    c. Today's modern attacks use complex methods such as Packet Forging, Spoofing & Stealth diagnostics.
2. **Technical Knowledge Required (Red Line - Decreasing):**
    a. In the 1990's Hacking required a lot of Technical Knowledge. Hackers had to manually find & Exploit vulnerabilities.

Answer 3:

1. **Vulnerability:** Weak point of system or software which an attacker can exploit.
2. **Exploit:** A technique or code which takes advantage of the vulnerability to hack the system.
3. **Daisy Chaining:** An attack method in which hacker attacks other connected systems by breaching one system.
4. **Zero-Day:** A vulnerability which is present in new system or software and has not been discovered yet. Attackers can attack by exploiting it.
5. **Hack Value:** Importance of a vulnerability or attack to the hacker community. The more unique or valuable it is, the higher its hack value.
6. **Payload:** Malicious code which is executed after being exploited, such as installing malware or taking control of the system.
7. **Bot:** Automated program that is under the control of a hacker and is used in cyber-attacks, like DDoS attacks.

Answer 4:

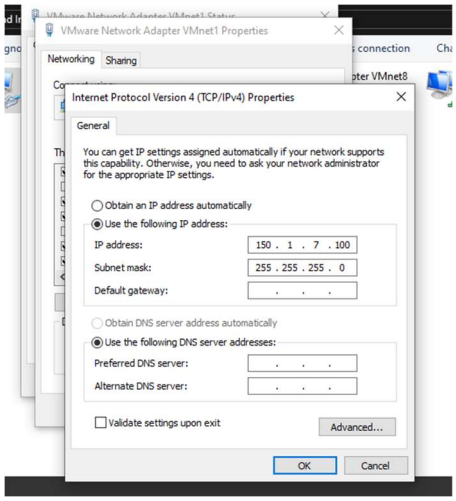
Term	Definition	Purpose
Hacking	Gaining unauthorized access to a system or network. Used for malicious activities, data theft, or damage.	This is because of malicious activities, data theft, or damage.
Ethical Hacking	Authorized hacking done to find and fix security vulnerabilities. To improve the security of the organization.	To improve the security of the organization.
Penetration Testing	An ethical hacking process that tests the security of a system in real-world attack scenarios. To analyze and fix security weaknesses.	To analyze and fix security weaknesses.

Part 2 Answer

Answer 5:

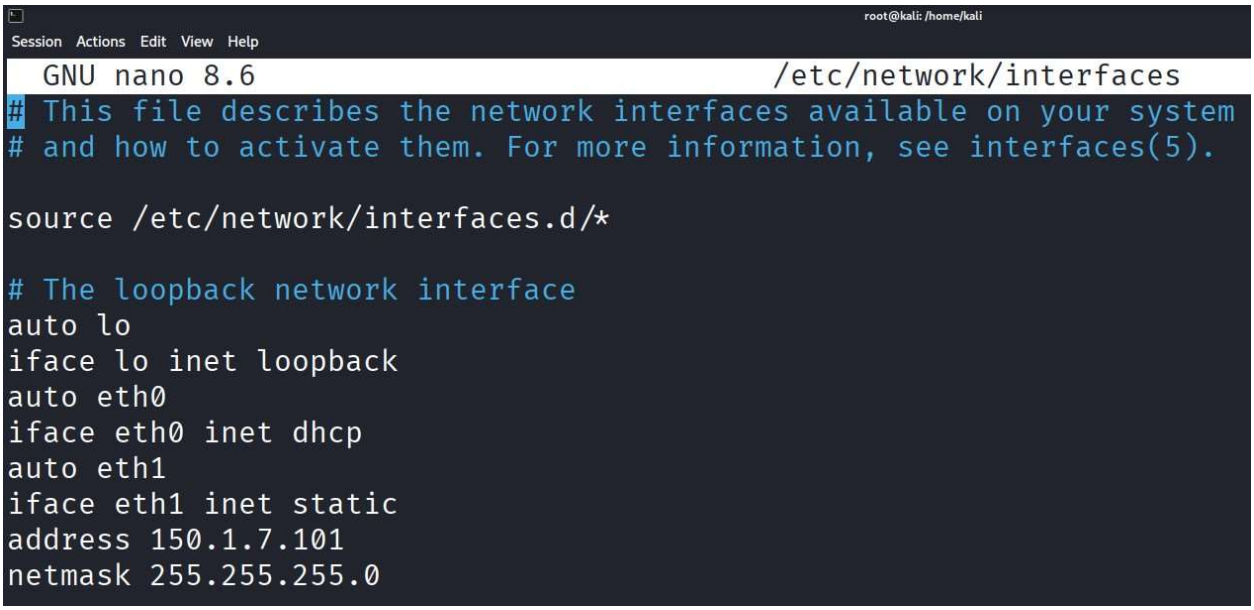
VM Adapter Setting:

Directory: Control Panel\Network and Internet\Network Connections



Accessing the /etc/network/interfaces file to add the VmNet1 configurations Kali Linux Machine (Attacker):

Nano and adding Configurations Kali Linux Machine (Attacker):



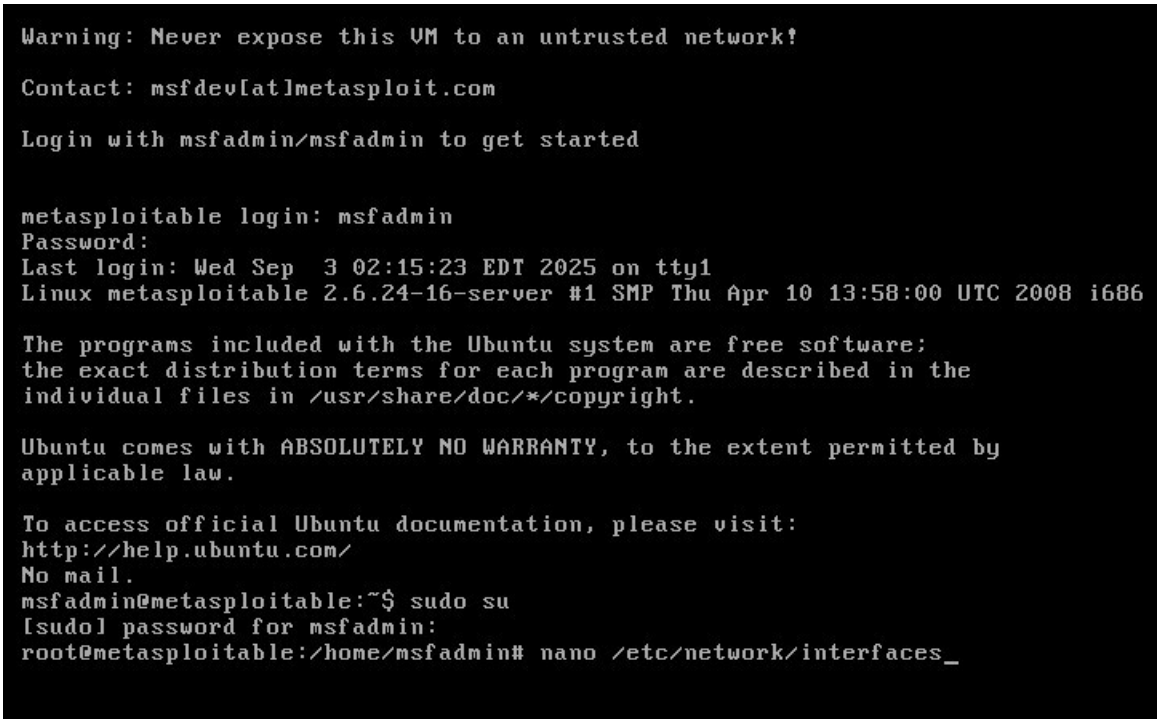
Checking the Network/Interfaces Configurations of Kali Linux Machine (Attacker):

```
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.84.130  netmask 255.255.255.0  broadcast 192.168.84.255
        inet6 fe80::2bb3:e9b0:121f:60b2  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:d1:09:b6  txqueuelen 1000  (Ethernet)
        RX packets 60  bytes 5341 (5.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 34  bytes 4248 (4.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 150.1.7.101  netmask 255.255.255.0  broadcast 150.1.7.255
        inet6 fe80::20c:29ff:fed1:9c0  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:d1:09:c0  txqueuelen 1000  (Ethernet)
        RX packets 2  bytes 529 (529.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 19  bytes 2634 (2.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 88  bytes 6960 (6.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 88  bytes 6960 (6.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

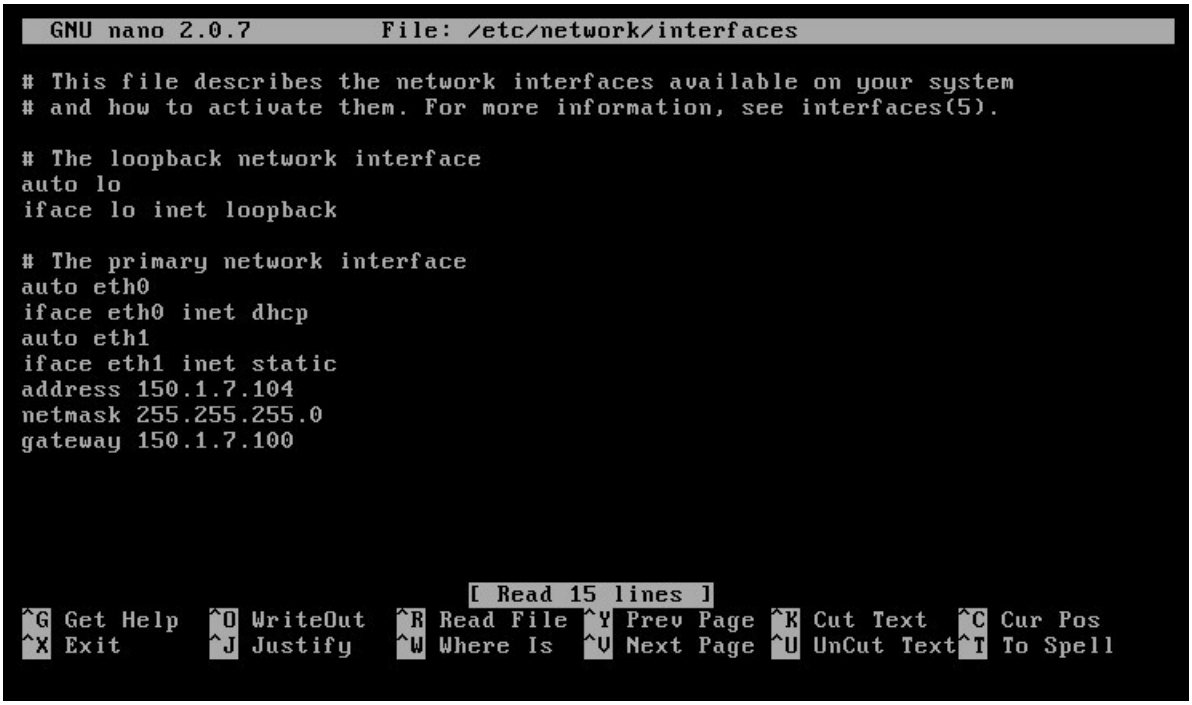
Now PING From kali (Attacker) to Metasploitable (Victim MS)

```
┌──(root㉿kali)-[/home/kali]
└─# ping 150.1.7.104
PING 150.1.7.104 (150.1.7.104) 56(84) bytes of data.
64 bytes from 150.1.7.104: icmp_seq=1 ttl=64 time=0.536 ms
64 bytes from 150.1.7.104: icmp_seq=2 ttl=64 time=0.574 ms
64 bytes from 150.1.7.104: icmp_seq=3 ttl=64 time=0.714 ms
64 bytes from 150.1.7.104: icmp_seq=4 ttl=64 time=0.690 ms
64 bytes from 150.1.7.104: icmp_seq=5 ttl=64 time=0.725 ms
64 bytes from 150.1.7.104: icmp_seq=6 ttl=64 time=0.647 ms
^C
── 150.1.7.104 ping statistics ──
6 packets transmitted, 6 received, 0% packet loss, time 5070ms
rtt min/avg/max/mdev = 0.536/0.647/0.725/0.070 ms
```

Accessing the /etc/network/interfaces file to add the VmNet1 configurations Metasploitable Machine (Victim):



Nano and adding Configurations Kali Linux Machine Metasploitable (Victim MS)



Checking the Network/Interfaces Configurations of Metasploitable (Victim MS)

```
eth1      Link encap:Ethernet  HWaddr 00:0c:29:a5:c3:bd
          inet addr:150.1.7.104  Bcast:150.1.7.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fea5:c3bd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:31 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:303 (303.0 B)  TX bytes:3642 (3.5 KB)
          Interrupt:18 Base address:0x2080

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:135 errors:0 dropped:0 overruns:0 frame:0
          TX packets:135 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:40109 (39.1 KB)  TX bytes:40109 (39.1 KB)
```

Now PING From Metasploitable (Victim MS) to Kali Linux (Attacker)

```
root@metasploitable:/home/msfadmin# ping 150.1.7.101
PING 150.1.7.101 (150.1.7.101) 56(84) bytes of data.
64 bytes from 150.1.7.101: icmp_seq=1 ttl=64 time=0.382 ms
64 bytes from 150.1.7.101: icmp_seq=2 ttl=64 time=0.601 ms
64 bytes from 150.1.7.101: icmp_seq=3 ttl=64 time=0.616 ms
64 bytes from 150.1.7.101: icmp_seq=4 ttl=64 time=0.664 ms
64 bytes from 150.1.7.101: icmp_seq=5 ttl=64 time=0.640 ms

64 bytes from 150.1.7.101: icmp_seq=6 ttl=64 time=0.787 ms
64 bytes from 150.1.7.101: icmp_seq=7 ttl=64 time=0.801 ms
64 bytes from 150.1.7.101: icmp_seq=8 ttl=64 time=0.656 ms

--- 150.1.7.101 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 6994ms
rtt min/avg/max/mdev = 0.382/0.643/0.801/0.122 ms
root@metasploitable:/home/msfadmin#
root@metasploitable:/home/msfadmin# _
```