# Lab - Packet Crafting with Scapy

# Objectives

In this lab, you will use Scapy, a Python-based packet manipulation tool, to craft custom packets. These custom packets will be used to perform reconnaissance on a target system.

- Part 1: Investigate the Scapy Tool.
- Part 2: Use Scapy to Sniff Network Traffic.
- Part 3: Create and Send an ICMP Packet.
- Part 4: Create and Send TCP SYN Packets.

# Background / Scenario

Penetration testers and ethical hackers often use specially-crafted packets to discover and/or exploit vulnerabilities in clients' infrastructure and systems. You have used Nmap to scan and analyze vulnerabilities in a computer attached to the local network.

In this lab, you will perform further reconnaissance on the same computer using custom ICMP and TCP packets.

# Required Resources

- Kali VM customized for Ethical Hacker course
- Internet Access

# Instructions

## Part 1: Investigate the Scapy Tool

Scapy is a multi-purpose tool originally written by Philippe Biondi. In this part, you will load the Scapy tool and explore some of its capabilities. Tools like Scapy should only be used to scan or communicate with machines that you own or have written permission to access.

### Step 1: Investigate Scapy documentation and resources.

Scapy can be run interactively from the Python shell or can be incorporated into Python programs by importing the python-scapy module. The Scapy tool has extensive documentation online at https://scapy.readthedocs.io/en/latest/introduction.html. This customized Kali Linux is distributed with both Python and Scapy pre-installed.

a. Start the Kali VM and login.
b. Open the Firefox browser and navigate to https://scapy.readthedocs.io/en/latest/introduction.html. Read the Introduction page written by the Scapy creator, Philippe Biondi.

How does the author describe the capabilities of Scapy in the first paragraph of the page?

Answer Area

<!----><!---->

## Step 2: Use Scapy interactive command mode.

Enter the **scapy** command in a terminal window to load the Python interpreter. By using this command, the interpreter runs pre-loaded with the Scapy classes and objects. You will enter Scapy commands interactively and receive the output. Scapy commands can also be embedded in a Python script.

a. The commands to craft and send packets require root privileges to run. Use the **sudo su** command to obtain root privileges before starting Scapy. If prompted for a password, enter **kali**.

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─#
```

b. Load the Scapy tool using the **scapy** command. The interactive Python interpreter will load and present a screen image similar to that shown.

```
┌──(root㉿kali)-[/home/kali]
└─# scapy
INFO: Can't import PyX. Won't be able to use psdump() or pdfdump().


                     aSPY//YASa
             apyyyyCY//////////YCa       |
            sY//////YSpcs  scpCY//Pp     | Welcome to Scapy
 ayp ayyyyyyySCP//Pp           syY//C    | Version 2.5.0
 AYAsAYYYYYYYY///Ps              cY//S   |
         pCCCCY//p          cSSps y//Y   | https://github.com/secdev/scapy
         SPPPP///a          pP///AC//Y   |
              A//A            cyP////C   | Have fun!
              p///Ac            sC///a   |
              P////YCpc           A//A   | What is dead may never die!
       scccccp///pSP///p          p//Y   |                     -- Python 2
      sY/////////y  caa           S//P   |
       cayCyayP//Ya              pY/Ya
```

```
            sY/PsY////YCc           aC//Yp

             sc  sccaCY//PCypaapyCP//YSs

                      spCPY//////YPSps

                           ccaacs

                                          using IPython 8.5.0

>>>
```

c. At the >>> prompt within the Scapy shell, enter the **ls()** function to list all of the available default formats and protocols included with the tool. The list is quite extensive and will fill multiple screens.

```
>>> ls()
```

TFTP is a protocol used to send and receive files on a LAN segment. It is commonly used to back up configuration files on networking devices. Scroll up to view the available TFTP packet formats.

How many types of TFTP packet formats are listed?

Answer Area

<!----><!---->

## Step 3: Examine the fields in an IPv4 packet header.

a. It is important to understand the structure of an IP packet before creating and sending custom packets over the network. Each IP packet has an associated header that provides information about the structure of the packet. Review this information before continuing with the lab.

**IPv4 Packet Header Fields**

The binary values of each field identify various settings of the IP packet. Protocol header diagrams, which are read left to right, and top down, provide a visual to refer to when discussing protocol fields. The IP protocol header diagram in the figure identifies the fields of an IPv4 packet.

Significant fields in the IPv4 header include the following:

**Version -** Contains a 4-bit binary value set to 0100 that identifies this as an IPv4 packet.

**Differentiated Services or DiffServ (DS) -** Formerly called the type of service (ToS) field, the DS field is an 8-bit field used to determine the priority of each packet. The six most significant bits of the DiffServ field are the differentiated services code point (DSCP) bits and the last two bits are the explicit congestion notification (ECN) bits.

**Time to Live (TTL) –** TTL contains an 8-bit binary value that is used to limit the lifetime of a packet. The packet source device sets the initial TTL value. It is decreased by one each time the packet is processed by a router. If the TTL field decrements to zero, the router discards the packet and sends an Internet Control Message Protocol (ICMP) Time Exceeded message to the source IP address. Because the router decrements the TTL of each packet, the router must also recalculate the Header Checksum.

**Protocol –** This field is used to identify the next level protocol. This 8-bit binary value indicates the data payload type that the packet is carrying, which enables the network layer to pass the data to the appropriate upper-layer protocol. Common values include ICMP (1), TCP (6), and UDP (17).

**Header Checksum –** This is used to detect corruption in the IPv4 header.

**Source IPv4 Address –** This contains a 32-bit binary value that represents the source IPv4 address of the packet. The source IPv4 address is always a unicast address.

**Destination IPv4 Address –** This contains a 32-bit binary value that represents the destination IPv4 address of the packet. The destination IPv4 address is a unicast, multicast, or broadcast address.

b. The **ls()** function can also be used to list details of the fields and options available in each protocol header. The syntax to use a function in Scapy is ***function_name(arguments).*** Use the **ls(IP)** function to list the available fields in an IP packet header.

```
>>> ls(IP)
version    : BitField  (4 bits)                = ('4')
ihl        : BitField  (4 bits)                = ('None')
tos        : XByteField                        = ('0')
len        : ShortField                        = ('None')
id         : ShortField                        = ('1')
flags      : FlagsField                        = ('<Flag 0 ()>')
frag       : BitField  (13 bits)               = ('0')
ttl        : ByteField                         = ('64')
proto      : ByteEnumField                     = ('0')
chksum     : XShortField                       = ('None')
src        : SourceIPField                     = ('None')
dst        : DestIPField                       = ('None')
options    : PacketListField                   = ('[]')
```

Compare the fields in the IP detail on Scapy with the packet header described in Step 3a. Are there any differences between the two?

Answer Area

<!----><!---->

Which field do you think you would change to create a packet that would generate a reply to a target machine, rather than the machine that actually sent the packet?

Answer Area

<!----><!---->

# Part 2: Use Scapy to Sniff Network Traffic

Scapy can be used to capture and display network traffic, similar to a tcpdump or tshark packet collection.

## Step 1: Use the sniff() function.

a. Use the **sniff()** function to collect traffic using the default eth0 interface of your VM. Start the capture with the **sniff()** function without specifying any arguments.

```
>>> sniff()
```

b. Open a second terminal window and **ping** an internet address, such as **www.cisco.com**. Remember to specify the count using the **-c** argument.

```
┌──(kali㉿kali)-[~]
└─$ ping -c 5 www.cisco.com
```

c. Return to the terminal window that is running the Scapy tool. Press **CTRL-C** to stop the capture. You should receive output similar to what is shown here:

```
^C<Sniffed: TCP:75 UDP:42 ICMP:32 Other:2>
```

d. View the captured traffic using the **summary()** function. The **a=_** assigns the variable **a** to hold the output of the **sniff()** function. The underscore ( _ ) in Python is used to temporarily hold the output of the last function executed.

```
>>> a=_
>>> a.summary()
```

The output of this command can be extensive, depending on the applications running on the network.

## Step 2: Capture and save traffic on a specific interface.

In this step, you will capture traffic to and from a device connected to a virtual network in your Kali Linux VM.

a. Open a new terminal window. Use the **ifconfig** command to determine the name of the interface that is assigned the IP address **10.6.6.1**. This is the default gateway address for one of the virtual networks running inside Kali. Note the name of interface.

b. Return to the terminal window that is running the Scapy tool. Use the syntax **sniff(iface="***interface name***")** to begin the capture on the **br-internal** virtual interface.

```
>>> sniff(iface="br-internal")
```

c. Open Firefox and navigate to the URL **http://10.6.6.23/**. When the Gravemind home page opens, return to the terminal window that is running the Scapy tool. Press **CTRL-C**. You should receive output similar to:

```
^C<Sniffed: TCP:112 UDP:0 ICMP:0 Other:2>
```

d. View the captured traffic as you did in Step 1d.

```
>>> a=_
>>> a.summary()
```

## Step 3: Examine the collected packets.

In this step, you will filter the collected traffic to include only ICMP traffic, limit the number of packets being collected, and view the individual packet details.

a. Use interface ID associated with 10.6.6.1 (br-internal) to capture ten ICMP packets sent and received on the internal virtual network. The syntax is **sniff(iface="***interface name***", filter = "***protocol***", count =** *integer***)**.

```
>>> sniff(iface="br-internal",filter = "icmp",count = 10)
```

b. Open a second terminal window and ping the host at 10.6.6.23.

```
┌──(kali㉿Kali)-[~]
└─$ ping -c 10 10.6.6.23
```

c. Return to the terminal window running the Scapy tool. The capture automatically stopped when 10 packets were sent or received. View the captured traffic with line numbers using the **nsummary()** function.

```
>>>  a=_
>>>  a.nsummary()
```

The summary should only contain 10 lines because the capture count is equal to 10.

What traffic is displayed in the output of the nsummary() function?

Answer Area

<!----><!---->

d. To view details about a specific packet in the series, refer to the blue line number of the packet. Do not include the leading zeros.

```
>>> a[2]
```

The detail output shows the layers of information about the protocol data units (PDUs) that make up the packet. The protocol layer names appear in red in the output. Examine the source (src) and destination (dst) addresses as well as the raw data (load=) portion of the collected packet.

Why are there two sets of source and destination fields?

Answer Area

<!----><!---->

e. Use the **wrpcap()** function to save the captured data to a pcap file that can be opened by Wireshark and other applications. The syntax is **wrpcap("***filename.pcap***"**, *variable name***),** in this example the variable that you stored the output is "**a**".

```
>>> wrpcap("capture1.pcap", a)
```

f. The .pcap file will be written to the default user directory. Use a different terminal window to verify the location of the **capture1.pcap** file using the Linux **ls** command.
g. Open the capture in Wireshark to view the file contents.

## Part 3: Create and Send an ICMP Packet.

ICMP is a protocol designed to send control messages between network devices for various purposes. There are many types of ICMP packets, with echo-request and echo-reply the most familiar to IT technicians. To see a list of the message types that can be sent and received using ICMP, navigate to https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml**.**

### Step 1: Use interactive mode to create and send a custom ICMP packet.

a. In a Scapy terminal window, enter the command to sniff traffic from the interface connected to the 10.6.6.0/24 network.

```
>>> sniff(iface="br-internal")
```

b. Open another terminal window, enter **sudo su** to perform packet crafting as root. Start a second instance of Scapy. Enter the **send**() function to send a packet to 10.6.6.23 with a modified ICMP payload.

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# scapy


>>> send(IP(dst="10.6.6.23")/ICMP()/"This is a test")


Response
Sent 1 packet
```

c. Return to the first terminal window and press **CTRL-C**. You should receive a response similar to this:

```
^C<Sniffed: TCP:0 UDP:0 ICMP:2 Other:0>
```

d. Enter the summary command to display the summary with packet numbers.

```
>>> a=_
>>> a.nsummary()
```

What type of packets are shown in the summary output?

Answer Area

<!----><!---->

### Step 2: View and compare the ICMP packet contents.

Use the packet numbers to view the individual ICMP Echo-request and Echo-reply packets. Compare those packets to the ones that you examined in Part 2, Step 3d.

```
>>> a[packet number]
```

What is different between the original ICMP packet conversation and the custom ICMP packet conversation?

Answer Area

<!----><!---->

## Part 4: Create and Send a TCP SYN Packet.

In this part, you will use Scapy to determine if port 445, a Microsoft Windows drive share port, is open on the target system at 10.6.6.23.

### Step 1: Start the packet capture on the internal interface.

a. In the original Scapy terminal window, begin a packet capture on the internal interface attached to the 10.6.6.0/24 network. Use the interface name that you obtained previously.
b. Navigate to the second terminal window. Create and send a TCP SYN packet using the command shown.

```
>>> send(IP(dst="10.6.6.23")/TCP(dport=445, flags="S"))

1 packet sent
```

This command sent an IP packet to the host with IP address 10.6.6.23. The packet is addressed to TCP port 445 and has the S (SYN) flag set.

c. Close the terminal window.

### Step 2: Review the captured packets.

a. In the original Scapy terminal window, stop the packet capture by pressing **CTRL-C**. The output should be similar to that shown.

```
^C<Sniffed: TCP:3 UDP:0 ICMP:0 Other:0>
```

b. View the captured TCP packets using the **nsummary()** function. Display the detail of the TCP packet that was returned from the target computer at 10.6.6.23.

```
>>> a[packet number]
```

What does the SA flag indicate in the packet returned from 10.6.6.23?

Answer Area

<!----><!---->

# Reflection Questions

1. How can crafting various TCP SYN packets be used to perform passive reconnaissance on a target host.?

Answer Area

<!----><!---->

2. How could creating an ICMP echo-request packet with a spoofed source address create a denial of service attack on against a target host?

Answer Area

<!----><!---->