Introduction to Scapy

1 Objective

Python/SCAPY is a Python module that provides detailed support for networking protocols as well as some common functions for network diagnosis. This lab will introduce you to scapy and to write a scapy script to perform a traceroute and a SYN Flood attack.

2 Intro to SCAPY

Use your Kali VM. To run SCAPY, first type python at the command prompt, then:

```
import sys
from scapy.all import *
```

At this point you have access to all the features of Python as well as *scapy*. Try out some of the features shown in scapy.pdf to get familiar with *scapy*. If you need information on Python look at https://www.python.org/. There are many books on Python as well as many examples that can be found using Google as well as many additional modules.

Your program should work with input given from the command line. One method to do this is to use the raw_input function, as follows:

```
IP_input = raw_input("Please enter an IP address: ")
print "You entered", IP_input
```

Example: Build the following packet by stacking the following layers and give the screen-shots of the constructed packets after running on scapy. Use show() to see the fields of the packets.

Ethernet, IP, TCP

Answer: You can build the packet with the following commands:

```
l3=IP(dst=IP_input)/TCP()
l2=Ether()/l3
l2.show()
```

The full answer to the example would be the seven lines of code in order. Using a text editor in Linux (e.g., pico, gedit, vim), create a file called example.py, and put the seven lines into the file. Save it, and run the program by putting `python example.py` into the command prompt.

Questions:

1. [20 pts] Generate a set of packets for any given IP address and its subnet (example: 10.20.111.2/30) and assign each of the generated packets the TCP destination port numbers [80, 53]. Give the screenshots of the packets generated. Your generated packets must conform to IP standards, e.g., for the example subnet 10.20.111.2/30, 10.20.111.3 is not a valid address because it's the broadcast address. Your program must work with any normal IP address.
2. [15 pts] Send an ICMP packet from the Kali machine to a specified IP address and get the reply. Give the screenshots of the packets generated and the replies.

3. [25 pts] Implement TCP traceroute to a specified IP address using scapy. Do **NOT** use the build-in *traceroute* function. Give the screenshots of the packets generated. You should test your program with the internal Linux machine, 10.20.111.2.

What to submit:

For each question:
(1) Provide the source code required to construct each program named ***<name>-<question#>.py***. You may combine the three questions into a single program.
(2) Include screen shots of the results of the program. All screenshots must be the entire screen of the VM.
(3) Provide a report with descriptions and explanations of the code.

3 SYN Flood Attack

Definition:

A SYN flood creates massive numbers of TCP SYN packets from spoofed source addresses and directs them toward a particular TCP server. The goal is to overwhelm the server by forcing the targeted TCP stack to commit all of its resources to sending out SYN/ACK packets and wait around for ACK packets that will never come**.**

Objective:

1. Write a Python script to create a SYN flood attack from the BackTrack 5 machine to an IP address specified from the command line.
2. This script should implement a many to one SYN flood attack, i.e., many ports from the BackTrack5 IP address sending SYN messages. You should test your program by sending packets to the NetBIOS service running on port **139** on the Windows XP machine.

Setup:

For this assignment we will need one prerequisite setup task. By default the Linux kernel sends an RST in response to a SYN-ACK received from the server. This is because of a lack of communication between SCAPY and the kernel. For this reason an IPTABLES rule needs to be created in the BackTrack5 machine to block any outgoing RST packets. To do this, open up a command prompt in the BackTrack5 machine and run the following code:

```
sudo iptables -A OUTPUT -p tcp -s [IPADDRESSofKali] --tcp-flags RST RST -j DROP
```

Next verify that the command is in the output chain. To do this, use the command:

```
sudo iptables -L
```

If you don't see the command listed under the OUTPUT chain then it wasn't entered properly. **Note that this command will only last until you restart your BackTrack5 machine, as it is a temporary command in iptables.

What to submit:

[20 pts] The Python script named ***<name>-Q4.py***, screenshots of the results, and a report with descriptions as to what the code is doing.

[20 pts] Screen-shots of the victim's machine, showing the SYN flood attack in action. For the Windows machine screenshot, open a command prompt (cmd.exe) and use the command '**netstat –a'** to show the '**syn_recv'** state next to the ½ open connections being made.

**Note that if the command prompt is taking a while to finish listing and becoming unresponsive you may want to open multiple and run multiple instances of that command.

** Note that all screenshots must be the entire screen of the VM.