Python Final Project

Global Python Programming for Security V4

DEKSHINAMURTHY MEENAKSHI
5-12-2022

Contents

1. VMs, Environments

Attacking Machine: kali

Target: Kali Machine or Windows

The python program was written using Pycharm in Kali

2. Scope

The aim of this project is to develop a simple port scanner to identify a open ssh port and brute force it.

look for

1.a linux host which is alive and reachable as target

2. Scan for open ports

Source port from attacker Kali: chosen by Randshort()

Destination port: from 1 to 1023 well known ports

and make a list of ports open in the target linux machine

3. If ssh is enabled and port 22 is open in the target linux machine, aim to brute force ssh

to get the username / password details

3. Python Libraries Fundamentals

Python Libraries Need to be installed in the attacking Machine:

Scapy	**Python** program which allows user to send, sniff and dissect and forge network packets. So Using Scapy, we can Scan or Attack Networks! Scapy can be imported as an externam module into any python scipt.	from scapy.config import conf from scapy.layers.inet import TCP, IP, ICMP A layer is a subclass of the Packet class. All the logic behind layer manipulation is held by the Packet class and will be inherited. A simple layer is compounded by a list of fields that will be either concatenated when assembling the layer or dissected one by one when disassembling a string.

		from scapy.sendrecv import sr1, sr **sr()** • Sends packets and receiving answers. • sr() returns a two lists, first list contains stimulus-response couple(like a tuple), and teh second list contains the unanswered probes. sr1() Sends all the stimulus and records only the first response. from scapy.volatile import RandShort – Generates random numbers
Paramiko	Python Library that connects to a remote device using SSH.	Class SSHClient --A high-level representation of a session with an SSH server .**set_missing_host_key_policy**(*policytouse*) Policytouse = paramkio.AUtoadd policy() Set policy to use when connecting to servers without a known host key.
Socket	Python module is equivalent of BSD Socket interface. And supports networking applications	

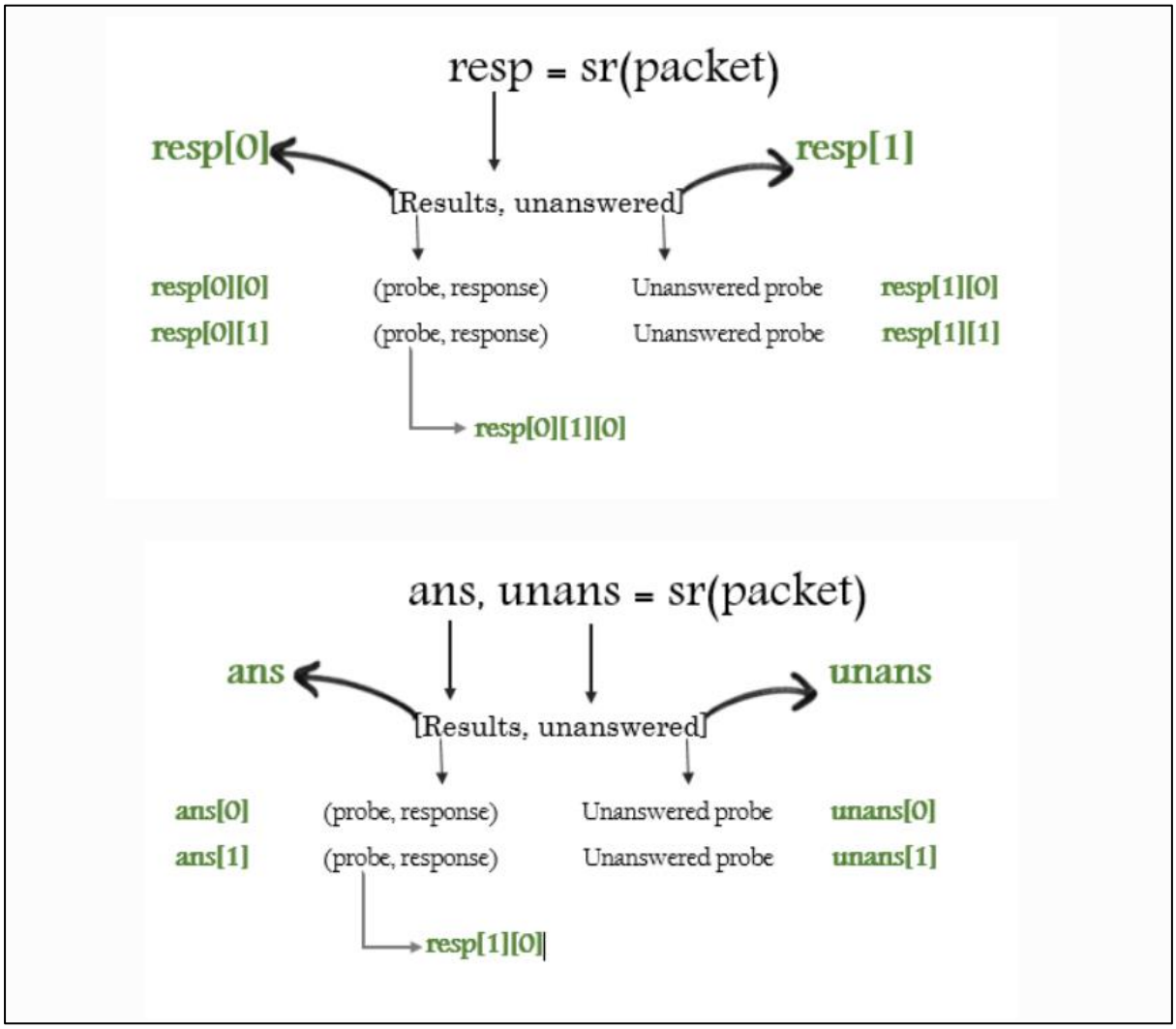
To install scapy

```
PS C:\Users\meena\Downloads\myvscproj> pip install scapy
Collecting scapy
  Downloading scapy-2.4.5.tar.gz (1.1 MB)
     ---------------------------------------- 1.1/1.1 MB 3.2 MB/s eta 0:00:00
  Preparing metadata (setup.py) ... done
Using legacy 'setup.py install' for scapy, since package 'wheel' is not installed.
Installing collected packages: scapy
  Running setup.py install for scapy ...
```

Scapy uses Python dictionaries as the data structure for packets.

Send and receive packets (sr)

The sr() function is for sending packets and receiving answers. The function returns **a couple of packet and answers, and the unanswered packets**. The function sr1() is a variant that only returns one packet that answered the packet (or the packet set) sent.



4. Program Outline

Input_sanity() – The Function checks for a valid Ip address Format using the Ip_address python inbuilt function

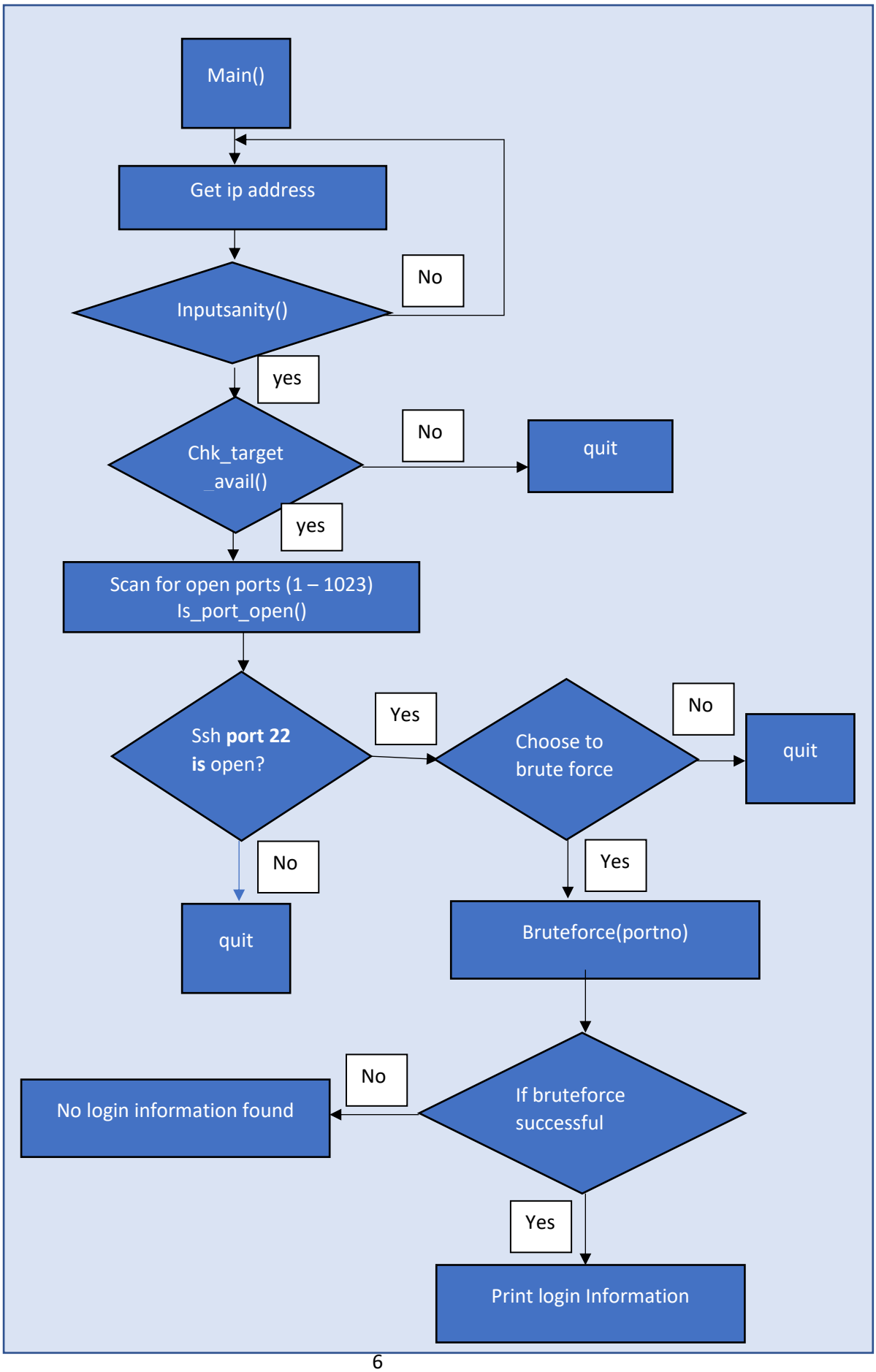
Any valid class of ip address is acceptable

Chk_target_avail() – The Function is used to check if the target is up and running and reachable from the attacker machine

Is_port_open() – scans all ports from 1 to 1023 to check if they are open. If open, the port will be added to a list of open_ports.

Bruteforce(portno) – digs the ssh password using bruteforce, if the user wants to brute force the ssh login for the given username, using the password wordlist provided.

Ssh_connect() – uses paramiko and creates SSH session if the username and password are given


Main()
Get ip address
Inputsanity()
No
yes
Chk_target
_avail()
No
quit
yes
Scan for open ports (1 – 1023)
Is_port_open()
Ssh port 22
is open?
Yes
Choose to
brute force
No
quit
No
quit
Yes
Bruteforce(portno)
If bruteforce
successful
No
No login information found
Yes
Print login Information

5.The Program Execution:

Attacker: kali – 10.0.2.19

Victim: beebox – 10.0.2.15

The output: