# Python for Pentesters

Start AttackBox | Show Split View | Cloud Details | Awards | Help

Python is probably the most widely used and most convenient scripting language in cybersecurity. This room covers real examples of Python scripts including hash cracking, key logging, enumeration and scanning.

✕

Chart | Scoreboard | Discuss | Writeups | More

Difficulty: Easy

Active Machine Information

| Title | IP Address | Expires | |
|---|---|---|---|
| Py4PT2 | 10.10.96.99 | 1h 41m 01s | ? Add 1 hour Terminate |

41%

Task 1 ✓ Introduction

Task 2 ✓ Subdomain Enumeration

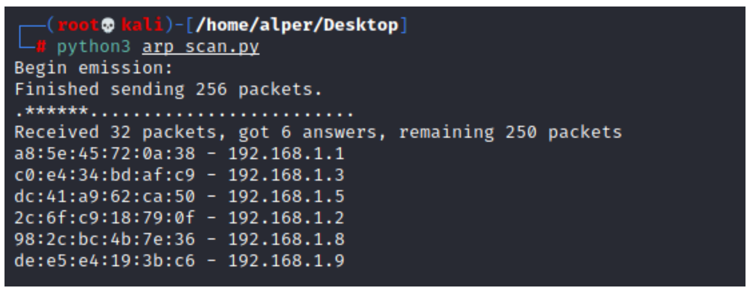
Task 3 ✓ Directory Enumeration

Task 4 ✓ Network Scanner

Python can be used to build a simple ICMP (Internet Control Message Protocol) scanner to identify potential targets on the network. However, ICMP packets can be monitored or blocked as the target organization would not expect a regular user to "ping a server". On the other hand, systems can be configured to not respond to ICMP requests. These are the main reasons why using the ARP (Address Resolution Protocol) to identify targets on the local network is more effective.

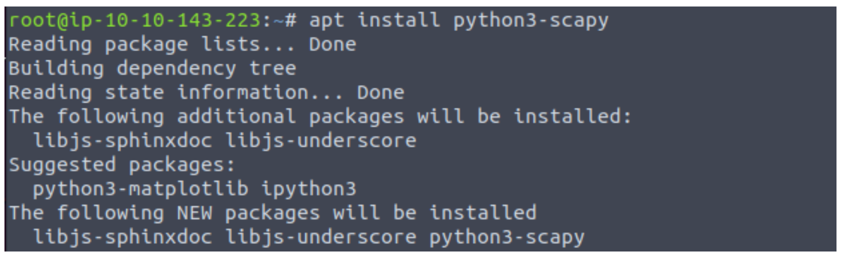
The code:

```
from scapy.all import *

interface = "eth0"
ip_range = "10.10.X.X/24"
broadcastMac = "ff:ff:ff:ff:ff:ff"

packet = Ether(dst=broadcastMac)/ARP(pdst = ip_range)

ans, unans = srp(packet, timeout =2, iface=interface, inter=0.1)

for send,receive in ans:
        print (receive.sprintf(r"%Ether.src% - %ARP.psrc%"))
```



```
┌──(root💀kali)-[/home/alper/Desktop]
└─# python3 arp_scan.py
Begin emission:
Finished sending 256 packets.
.******.........................
Received 32 packets, got 6 answers, remaining 250 packets
a8:5e:45:72:0a:38 - 192.168.1.1
c0:e4:34:bd:af:c9 - 192.168.1.3
dc:41:a9:62:ca:50 - 192.168.1.5
2c:6f:c9:18:79:0f - 192.168.1.2
98:2c:bc:4b:7e:36 - 192.168.1.8
de:e5:e4:19:3b:c6 - 192.168.1.9
```

If you are using the AttackBox, you will need to install Scapy first. This can easily be done using the " `apt install python3-scapy` " command.



```
root@ip-10-10-143-223:~# apt install python3-scapy
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libjs-sphinxdoc libjs-underscore
Suggested packages:
  python3-matplotlib ipython3
The following NEW packages will be installed
  libjs-sphinxdoc libjs-underscore python3-scapy
```

Answer the questions below

What module was used to create the ARP request packets?

scapy

Correct Answer

Hint

Which variable would you need to change according to your local IP block?

ip_range

Correct Answer

Hint

What variable would you change to run this code on a system with the network interface named ens33?

interface

Correct Answer

Task 5 ○ Port Scanner

Task 6 ○ File Downloader

Task 7 ○ Hash Cracker

Task 8 ○ Keyloggers

Task 9 ○ SSH Brute Forcing

Task 10 ○ Extra challenges

Created by

tryhackme

Only subscribers can deploy virtual machines in this room! Go to your profile page to subscribe (if you have not already). 20121 users are in here and this room is 594 days old.