

Betito, Bernice Marie M.

NSSECUC2 – S12

TEST OUTPUTS

1. ScanPydia.py -h

Student

```
student@vm-ubuntu: ~/labtainer/labtainer-student$ sudo python3 ScanPydia.py -h
Welcome to ScanPydia!

Created by: Bernice Marie M. Betito NSSECUC2 - S12

-----

To use ScanPydia, use the following format:

sudo python3 scanpydia.py -<?> <positional args>

Wherein -<?> and <positional args> are any of the following:

To do an ICMP Echo Request:
-l - Start an ICMP Echo Request
-c <#> - Number of packets to send to the Target Host
IP - (Positional argument) IP address of the Target Host

To do a TCP Scan:
-p <#> - The port number to scan
-t - Do a TCP Connect Scan
-s - Do a TCP SYN (Half-Open) Scan
-x - Do an Xmas Scan
-f - Do a FIN Scan
-n - Do a Null Scan
-a - Do an ACK Scan
-ALL - Do all TCP Scans available
IP - (Positional argument) IP address of the Target Host

Other options:
-v - Know more about ScanPydia
-T - Find out how much time ScanPydia spent executing
-l - See a full list and details of all the scans available
-h - See a complete guide on how to use ScanPydia

student@vm-ubuntu: ~/labtainer/labtainer-student$
```

Client

```
ubuntu@client:~$ sudo python3 ScanPydia.py -h
Welcome to ScanPydia!

Created by: Bernice Marie M. Betito NSSECUC2 - S12

-----

To use ScanPydia, use the following format:

sudo python3 scanpydia.py -<?> <positional args>

Wherein -<?> and <positional args> are any of the following:

To do an ICMP Echo Request:
-l - Start an ICMP Echo Request
-c <#> - Number of packets to send to the Target Host
IP - (Positional argument) IP address of the Target Host

To do a TCP Scan:
-p <#> - The port number to scan
-t - Do a TCP Connect Scan
-s - Do a TCP SYN (Half-Open) Scan
-x - Do an Xmas Scan
-f - Do a FIN Scan
-n - Do a Null Scan
-a - Do an ACK Scan
-ALL - Do all TCP Scans available
IP - (Positional argument) IP address of the Target Host

Other options:
-v - Know more about ScanPydia
-T - Find out how much time ScanPydia spent executing
-l - See a full list and details of all the scans available
-h - See a complete guide on how to use ScanPydia

ubuntu@client:~$
```

2. ScanPydia.py -v

Student

```
student@vm-ubuntu: ~/labtainer/labtainer-student$ sudo python3 ScanPydia.py -v
ScanPydia

Created by: Bernice Marie M. Betito NSSECUC2 - S12

-----

ScanPydia is a Network Scanning Tool created by Bernice Betito
in order to accomplish her requirements for Advanced and Offensive
Security (NSSECUC2). The name is a combination of three words, Scan,
Python, and Encyclopedia. Scan came from the project requirement, which
is a Network Scanning Tool, Python is the programming language to be
used, and lastly, Encyclopedia came from the idea that all the needed
information would be provided regarding the scanned hosts and ports.

The goal of ScanPydia is to be able to do Network Scanning. This
includes ICMP Echo Request, TCP Connect Scan, TCP SYN (Half-Open) Scan,
Xmas Scan, FIN Scan, Null Scan, and ACK Scan. In order to be able to do
so, an additional library/tool is utilized which is called Scapy. Scapy
is a powerful program and library which could be used when dealing with
network packets.

student@vm-ubuntu: ~/labtainer/labtainer-student$
```

Client

```
ubuntu@client:~$ sudo python3 ScanPydia.py -v
ScanPydia

Created by: Bernice Marie M. Betito NSSECUC2 - S12

-----

ScanPydia is a Network Scanning Tool created by Bernice Betito
in order to accomplish her requirements for Advanced and Offensive
Security (NSSECUC2). The name is a combination of three words, Scan,
Python, and Encyclopedia. Scan came from the project requirement, which
is a Network Scanning Tool, Python is the programming language to be
used, and lastly, Encyclopedia came from the idea that all the needed
information would be provided regarding the scanned hosts and ports.

The goal of ScanPydia is to be able to do Network Scanning. This
includes ICMP Echo Request, TCP Connect Scan, TCP SYN (Half-Open) Scan,
Xmas Scan, FIN Scan, Null Scan, and ACK Scan. In order to be able to do
so, an additional library/tool is utilized which is called Scapy. Scapy
is a powerful program and library which could be used when dealing with
network packets.

ubuntu@client:~$
```

3. ScanPydia.py -i 10.10.0.11 -c3

Student

```
student@vm-ubuntu:/labtainer/labtainer-student$ sudo python3 Scanpydla.py -t 10.10.8.11 -c3
```

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
ICMP ECHO REQUEST  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
  
-----  
1. Scapy Information  
Begin emission:  
.....Finished sending 3 packets.  
Received 9 packets, got 0 answers, remaining 3 packets  
Info Explained  
  
Target Host = IP Address Entered  
Number of Packets = Total # of packets sent to the target host  
Response to Echo Request (*) = # of packets containing Echo-Reply of the target host  
No Response = Packets unanswered by the target host  
  
-----  
|          | Number    |           |             |  
| Target   | of        | Response  |              |  
| Host     | Packets   | to Echo   |              |  
|          |           | Request   |              |  
|          |           | (* )      |              |  
+-----+-----+-----+-----+  
| 10.10.0.11 | 3       |         0 |         3     |  
+-----+-----+-----+-----+
```

```
-----  
2. Packets Details  
Sending Packets  
  
Packet/s were sent with the following details:  
-----  
|          | Number    |           |            |  
| Target   | of        | Packets   | Type       |  
| Host     |           |           |            |  
+-----+-----+-----+-----+  
| 10.10.0.11 | 3       |         8 | ICMP Echo Request |  
+-----+-----+-----+-----+
```

```
Receiving Packets
```

Client

```

ubuntu@client:~
-----
1. Scapy Information
Begin emission:
Finished sending 3 packets.
***
Received 4 packets, got 3 answers, remaining 0 packets

Info Explained

Target Host = IP Address Entered

Number of Packets = Total # of packets sent to the target host

Response to Echo Request (*) = # of packets containing Echo-Reply of the target host

No Response = Packets unanswered by the target host
-----


| Target Host | Number of Packets | Response to Echo Requests (*) | Packets without Response |
|-------------|-------------------|-------------------------------|--------------------------|
| 10.10.0.11  | 3                 | 3                             | 0                        |


-----
2. Packets Details

Sending Packets

Packets/s were sent with the following details:



| Target Host | Number of Packets | Type                  |
|-------------|-------------------|-----------------------|
| 10.10.0.11  | 3                 | 8 - ICMP Echo Request |



Receiving Packets

Packets/s were received with the following details:



| Target Host | Number of Packets | Type                |
|-------------|-------------------|---------------------|
| 10.10.0.11  | 3                 | 0 - ICMP Echo Reply |


ubuntu@client:~$

```

```

student@vm-ubuntu: ~/labtainer/labtainer-students
-----
1. Scapy Information
-----
Begin emission:
.....Finished sending 3 packets.

Received 9 packets, got 0 answers, remaining 3 packets

Info Explained
-----
Target Host = IP Address Entered

Number of Packets = Total # of packets sent to the target host

Response to Echo Request (*) = # of packets containing Echo-Reply of the target host

No Response = Packets unanswered by the target host

-----


| Target Host | Number of Packets | Response to Echo Request (*) | Packets without Response |
|-------------|-------------------|------------------------------|--------------------------|
| 10.10.0.11  | 3                 | 0                            | 3                        |


-----
2. Packets Details
-----
Sending Packets
-----
Packets/s were sent with the following details:
-----


| Target Host | Number of Packets | Type                  |
|-------------|-------------------|-----------------------|
| 10.10.0.11  | 3                 | 8 - ICMP Echo Request |


-----
Receiving Packets
-----
Packets/s were received with the following details:
-----


| Target Host | Number of Packets | Type                |
|-------------|-------------------|---------------------|
| 10.10.0.11  | 0                 | 0 - ICMP Echo Reply |


-----
student@vm-ubuntu:~/labtainer/labtainer-students

```

4. ScanPydia.py -p 22 -ALL 10.10.0.11

Student

```
student@vm-ubuntu: ~/labtainer/labtainer-student$ sudo python3 ScanPydia.py -p 22 -ALL 10.10.0.11
=====
ALL TCP SCANS
=====
Target IP: 10.10.0.11
Port Number: 22
=====
1. Scapy Information
=====
Begin emission:
....Finished sending 1 packets.
Received 5 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
...
Received 1 packets, got 1 answers, remaining 0 packets
Sent 1 packets.
Begin emission:
Finished sending 1 packets.
....
Received 4 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
...
Received 3 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
...
Received 3 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
...
Received 3 packets, got 1 answers, remaining 0 packets
=====
Info Explained
=====
TCP Scan = Type of TCP Scan
First Packet = Flag Received with the First Packet
Second Packet = Flag Received with the Second Packet
Third Packet = Flag Received with the Third Packet
***
```

Client

```
ubuntu@client: ~$ sudo python3 ScanPydia.py -p 22 -ALL 10.10.0.11
=====
ALL TCP SCANS
=====
Target IP: 10.10.0.11
Port Number: 22
=====
1. Scapy Information
=====
Begin emission:
Finished sending 1 packets.
...
Received 2 packets, got 1 answers, remaining 0 packets
Sent 1 packets.
Begin emission:
Finished sending 1 packets.
...
Received 1 packets, got 1 answers, remaining 0 packets
Sent 1 packets.
Begin emission:
Finished sending 1 packets.
Received 0 packets, got 0 answers, remaining 1 packets
Finished sending 1 packets.
Received 0 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
Received 0 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
Received 0 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
=====
Info Explained
=====
TCP Scan = Type of TCP Scan
First Packet = Flag Received with the First Packet
Second Packet = Flag Received with the Second Packet
***
```

```
student@vm-ubuntu: ~/labtainer/labtainer-student$ sudo python3 ScanPydia.py -p 22 -ALL 10.10.0.11
=====
Begin emission:
Finished sending 1 packets.
...
Received 3 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
...
Received 3 packets, got 1 answers, remaining 0 packets
=====
Info Explained
=====
TCP Scan = Type of TCP Scan
First Packet = Flag Received with the First Packet
Second Packet = Flag Received with the Second Packet
Third Packet = Flag Received with the Third Packet
=====
TCP Scan | First Packet | Second Packet | Third Packet
-----|-----|-----|-----
Connect | 1 - S | 0 - No Response | No Packet
SYN | 1 - S | 1 - SA | 1 - R
Xmas | 1 - FPU | 0 - No Response | No Packet
FIN | 1 - F | 0 - No Response | No Packet
Null | 1 - Null | 0 - No Response | No Packet
ACK | 1 - A | 1 - R | No Packet
=====
2. Packets Details
=====
TCP Scan | First Packet | Second Packet | Third Packet
-----|-----|-----|-----
Connect | SYN: Initiating Connect | Filtered | No Packet
SYN | SYN: Initiating Syn | Port is Open | R: RST
Xmas | FPU: Initiate Xmas | Open/Filtered | No Packet
FIN | F: Initiate Fin | Open/Filtered | No Packet
Null | Null: Initiate Null | Open/Filtered | No Packet
ACK | ACK: Initiate Ack | Unfiltered | No Packet
=====
student@vm-ubuntu:~/labtainer/labtainer-student$
```

```
ubuntu@client: ~$ sudo python3 ScanPydia.py -p 22 -ALL 10.10.0.11
=====
Begin emission:
Finished sending 1 packets.
...
Received 0 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
...
Received 0 packets, got 0 answers, remaining 1 packets
=====
Info Explained
=====
TCP Scan = Type of TCP Scan
First Packet = Flag Received with the First Packet
Second Packet = Flag Received with the Second Packet
Third Packet = Flag Received with the Third Packet
=====
TCP Scan | First Packet | Second Packet | Third Packet
-----|-----|-----|-----
Connect | 1 - S | 1 - SA | 1 - RA
SYN | 1 - S | 1 - SA | 1 - R
Xmas | 1 - FPU | 0 - No Response | No Packet
FIN | 1 - F | 0 - No Response | No Packet
Null | 1 - Null | 0 - No Response | No Packet
ACK | 1 - A | 0 - No Response | No Packet
=====
2. Packets Details
=====
TCP Scan | First Packet | Second Packet | Third Packet
-----|-----|-----|-----
Connect | SYN: Initiating Connect | Port is Open | RA: RST and ACK
SYN | SYN: Initiating Syn | Port is Open | R: RST
Xmas | FPU: Initiate Xmas | Open/Filtered | No Packet
FIN | F: Initiate Fin | Open/Filtered | No Packet
Null | Null: Initiate Null | Open/Filtered | No Packet
ACK | ACK: Initiate Ack | Filtered | No Packet
=====
ubuntu@client:~$
```


5. ScanPydia.py -p 25 -ALL 10.10.0.11

Student

```
student@vm-ubuntu: ~/labtainer/labtainer-student
student@vm-ubuntu:~/labtainer/labtainer-student$ sudo python3 ScanPydia.py -p 25 -ALL 10.10.0.11
=====
ALL TCP SCANS
=====
Target IP: 10.10.0.11
Port Number: 25
=====
1. Scapy Information
Begin emission:
....Finished sending 1 packets.
Received 5 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
Received 1 packets, got 1 answers, remaining 0 packets
Begin emission:
Finished sending 1 packets.
Received 1 packets, got 1 answers, remaining 0 packets
Begin emission:
Finished sending 1 packets.
Received 1 packets, got 1 answers, remaining 0 packets
Begin emission:
Finished sending 1 packets.
Received 1 packets, got 1 answers, remaining 0 packets
Begin emission:
Finished sending 1 packets.
Received 1 packets, got 1 answers, remaining 0 packets
Begin emission:
Finished sending 1 packets.
Info Explained
TCP Scan = Type of TCP Scan
First Packet = Flag Received with the First Packet
Second Packet = Flag Received with the Second Packet
Third Packet = Flag Received with the Third Packet
=====
TCP Scan | First Packet | Second Packet | Third Packet
-----|-----|-----|-----
Connect | 1 - S | 0 - No Response | No Packet
SYN | 1 - S | 1 - RA | No Packet
RST | 1 - RPU | 0 - No Response | No Packet
FIN | 1 - F | 1 - RA | No Packet
Null | 1 - Null | 1 - RA | No Packet
ACK | 1 - A | 1 - R | No Packet
=====
```

```
student@vm-ubuntu:~/labtainer/labtainer-student$
Begin emission:
Finished sending 1 packets.
Received 1 packets, got 1 answers, remaining 0 packets
Begin emission:
Finished sending 1 packets.
Received 1 packets, got 1 answers, remaining 0 packets
Info Explained
TCP Scan = Type of TCP Scan
First Packet = Flag Received with the First Packet
Second Packet = Flag Received with the Second Packet
Third Packet = Flag Received with the Third Packet
=====
TCP Scan | First Packet | Second Packet | Third Packet
-----|-----|-----|-----
Connect | 1 - S | 0 - No Response | No Packet
SYN | 1 - S | 1 - RA | No Packet
RST | 1 - RPU | 0 - No Response | No Packet
FIN | 1 - F | 1 - RA | No Packet
Null | 1 - Null | 1 - RA | No Packet
ACK | 1 - A | 1 - R | No Packet
=====
2. Packets Details
=====
TCP Scan | First Packet | Second Packet | Third Packet
-----|-----|-----|-----
Connect | SYN: Initiating Connect | Filtered | No Packet
SYN | SYN: Initiating Syn | Port is Closed | No Packet
RST | RPU: Initiate Rst | Port is Closed | No Packet
FIN | F: Initiate Fin | Port is Closed | No Packet
Null | Null: Initiate Null | Port is Closed | No Packet
ACK | ACK: Initiate Ack | Unfiltered | No Packet
=====
```

Client

```
ubuntu@client: ~
ACK | ACK: Initiate Ack | Filtered | No Packet
=====
ubuntu@client:~$ clear
ubuntu@client:~$ sudo python3 ScanPydia.py -p 25 -ALL 10.10.0.11
=====
ALL TCP SCANS
=====
Target IP: 10.10.0.11
Port Number: 25
=====
1. Scapy Information
Begin emission:
Finished sending 1 packets.
Received 2 packets, got 1 answers, remaining 0 packets
Begin emission:
Finished sending 1 packets.
Received 1 packets, got 1 answers, remaining 0 packets
Begin emission:
Finished sending 1 packets.
Received 0 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
Received 0 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
Received 0 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
Info Explained
TCP Scan = Type of TCP Scan
First Packet = Flag Received with the First Packet
Second Packet = Flag Received with the Second Packet
Third Packet = Flag Received with the Third Packet
=====
```

```
ubuntu@client: ~
Begin emission:
Finished sending 1 packets.
Received 0 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
Received 1 packets, got 1 answers, remaining 0 packets
Info Explained
TCP Scan = Type of TCP Scan
First Packet = Flag Received with the First Packet
Second Packet = Flag Received with the Second Packet
Third Packet = Flag Received with the Third Packet
=====
TCP Scan | First Packet | Second Packet | Third Packet
-----|-----|-----|-----
Connect | 1 - S | 1 - RA | No Packet
SYN | 1 - S | 1 - RA | No Packet
RST | 1 - RPU | 0 - No Response | No Packet
FIN | 1 - F | 0 - No Response | No Packet
Null | 1 - Null | 0 - No Response | No Packet
ACK | 1 - A | 1 - R | No Packet
=====
2. Packets Details
=====
TCP Scan | First Packet | Second Packet | Third Packet
-----|-----|-----|-----
Connect | SYN: Initiating Connect | Port is Closed | No Packet
SYN | SYN: Initiating Syn | Port is Closed | No Packet
RST | RPU: Initiate Rst | Open/Filtered | No Packet
FIN | F: Initiate Fin | Open/Filtered | No Packet
Null | Null: Initiate Null | Open/Filtered | No Packet
ACK | ACK: Initiate ack | Unfiltered | No Packet
=====
```

6. ScanPydia.py -p 22 -ALL 10.10.10.1

Student

```
student@vm-ubuntu: ~/labtainer/labtainer-student$ sudo python3 ScanPydia.py -p 22 -ALL 10.10.10.1
=====
ALL TCP SCANS
=====
Target IP: 10.10.0.1
Port Number: 22

1. Scapy Information
-----
Begin emission:
.....Finished sending 1 packets.
Received 13 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
.....
Received 5 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
.....
Received 5 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
.....
Received 7 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
.....
Received 5 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
.....
Received 2 packets, got 0 answers, remaining 1 packets
-----
Info Explained
-----
TCP Scan = Type of TCP Scan
First Packet = Flag Received with the First Packet
Second Packet = Flag Received with the Second Packet
Third Packet = Flag Received with the Third Packet
-----
TCP Scan | First Packet | Second Packet | Third Packet
-----
```

```
student@vm-ubuntu: ~/labtainer/labtainer-student$
Begin emission:
Finished sending 1 packets.
.....
Received 5 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
.....
Received 2 packets, got 0 answers, remaining 1 packets
-----
Info Explained
-----
TCP Scan = Type of TCP Scan
First Packet = Flag Received with the First Packet
Second Packet = Flag Received with the Second Packet
Third Packet = Flag Received with the Third Packet
-----
TCP Scan | First Packet | Second Packet | Third Packet
-----
Connect | 1 - S | 0 - No Response | No Packet
SYN | 1 - S | 0 - No Response | No Packet
Xmas | 1 - FPU | 0 - No Response | No Packet
FIN | 1 - F | 0 - No Response | No Packet
Null | 1 - Null | 0 - No Response | No Packet
ACK | 1 - A | 0 - No Response | No Packet
-----
2. Packets Details
-----
TCP Scan | First Packet | Second Packet | Third Packet
-----
Connect | SYN: Initiating Connect | Filtered | No Packet
SYN | SYN: Initiating Syn | Filtered | No Packet
Xmas | FPU: Initiate Xmas | Open/Filtered | No Packet
FIN | F: Initiate Fin | Open/Filtered | No Packet
Null | Null: Initiate Null | Open/Filtered | No Packet
ACK | ACK: Initiate Ack | Filtered | No Packet
-----
student@vm-ubuntu:~/labtainer/labtainer-student$
```

Client

```
ubuntu@client:~$
Null | Null: Initiate Null | Open/Filtered | No Packet
ACK | ACK: Initiate Ack | Unfiltered | No Packet
-----
ALL TCP SCANS
=====
Target IP: 10.10.0.1
Port Number: 22

1. Scapy Information
-----
Begin emission:
Finished sending 1 packets.
Received 1 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
.....
Received 0 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
.....
Received 0 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
.....
Received 0 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
.....
Received 0 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
.....
Received 0 packets, got 0 answers, remaining 1 packets
-----
Info Explained
-----
TCP Scan = Type of TCP Scan
First Packet = Flag Received with the First Packet
Second Packet = Flag Received with the Second Packet
Third Packet = Flag Received with the Third Packet
-----
```

```
ubuntu@client:~$
Begin emission:
Finished sending 1 packets.
.....
Received 0 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
.....
Received 0 packets, got 0 answers, remaining 1 packets
-----
Info Explained
-----
TCP Scan = Type of TCP Scan
First Packet = Flag Received with the First Packet
Second Packet = Flag Received with the Second Packet
Third Packet = Flag Received with the Third Packet
-----
TCP Scan | First Packet | Second Packet | Third Packet
-----
Connect | 1 - S | 0 - No Response | No Packet
SYN | 1 - S | 0 - No Response | No Packet
Xmas | 1 - FPU | 0 - No Response | No Packet
FIN | 1 - F | 0 - No Response | No Packet
Null | 1 - Null | 0 - No Response | No Packet
ACK | 1 - A | 0 - No Response | No Packet
-----
2. Packets Details
-----
TCP Scan | First Packet | Second Packet | Third Packet
-----
Connect | SYN: Initiating Connect | Filtered | No Packet
SYN | SYN: Initiating Syn | Filtered | No Packet
Xmas | FPU: Initiate Xmas | Open/Filtered | No Packet
FIN | F: Initiate Fin | Open/Filtered | No Packet
Null | Null: Initiate Null | Open/Filtered | No Packet
ACK | ACK: Initiate Ack | Filtered | No Packet
-----
ubuntu@client:~$
```

7. ScanPydia.py -p 445 -ALL 10.10.10.1

Student

```
student@vm-ubuntu:~/labtainer/labtainer-student$ sudo python3 ScanPydia.py -p 445 -ALL 10.10.10.1
=====
ALL TCP SCANS
=====
Target IP: 10.10.0.1
Port Number: 445
=====
1. Scapy Information
-----
Begin emission:
.....Finished sending 1 packets.
Received 7 packets, got 0 answers, remaining 1 packets
Begin emission:
.....Finished sending 1 packets.
Received 9 packets, got 0 answers, remaining 1 packets
Begin emission:
.....Finished sending 1 packets.
Received 7 packets, got 0 answers, remaining 1 packets
Begin emission:
.....Finished sending 1 packets.
Received 15 packets, got 0 answers, remaining 1 packets
Begin emission:
.....Finished sending 1 packets.
Received 6 packets, got 0 answers, remaining 1 packets
Begin emission:
.....Finished sending 1 packets.
Received 18 packets, got 0 answers, remaining 1 packets
=====
Info Explained
-----
TCP Scan = Type of TCP Scan
First Packet = Flag Received with the First Packet
Second Packet = Flag Received with the Second Packet
Third Packet = Flag Received with the Third Packet
=====
TCP Scan | First Packet | Second Packet | Third Packet
-----|-----|-----|-----
Connect | 1 - S | 0 - No Response | No Packet
```

Client

```
ubuntu@client: ~$
=====
ALL TCP SCANS
=====
Target IP: 10.10.0.1
Port Number: 445
=====
1. Scapy Information
-----
Begin emission:
.....Finished sending 1 packets.
Received 1 packets, got 0 answers, remaining 1 packets
Begin emission:
.....Finished sending 1 packets.
Received 8 packets, got 0 answers, remaining 1 packets
Begin emission:
.....Finished sending 1 packets.
Received 8 packets, got 0 answers, remaining 1 packets
Begin emission:
.....Finished sending 1 packets.
Received 8 packets, got 0 answers, remaining 1 packets
Begin emission:
.....Finished sending 1 packets.
Received 8 packets, got 0 answers, remaining 1 packets
=====
Info Explained
-----
TCP Scan = Type of TCP Scan
First Packet = Flag Received with the First Packet
Second Packet = Flag Received with the Second Packet
Third Packet = Flag Received with the Third Packet
=====
TCP Scan | First Packet | Second Packet | Third Packet
-----|-----|-----|-----
Connect | 1 - S | 0 - No Response | No Packet
```

```
student@vm-ubuntu:~/labtainer/labtainer-student$
Begin emission:
.....Finished sending 1 packets.
Received 8 packets, got 0 answers, remaining 1 packets
Begin emission:
.....Finished sending 1 packets.
Received 18 packets, got 0 answers, remaining 1 packets
=====
Info Explained
-----
TCP Scan = Type of TCP Scan
First Packet = Flag Received with the First Packet
Second Packet = Flag Received with the Second Packet
Third Packet = Flag Received with the Third Packet
=====
TCP Scan | First Packet | Second Packet | Third Packet
-----|-----|-----|-----
Connect | 1 - S | 0 - No Response | No Packet
SYN | 1 - S | 0 - No Response | No Packet
Xmas | 1 - FPU | 0 - No Response | No Packet
FIN | 1 - F | 0 - No Response | No Packet
Null | 1 - Null | 0 - No Response | No Packet
ACK | 1 - A | 0 - No Response | No Packet
=====
2. Packets Details
-----
TCP Scan | First Packet | Second Packet | Third Packet
-----|-----|-----|-----
Connect | SYN: Initiating Connect | Filtered | No Packet
SYN | SYN: Initiating Syn | Filtered | No Packet
Xmas | FPU: Initiate Xmas | Open/Filtered | No Packet
FIN | F: Initiate Fin | Open/Filtered | No Packet
Null | Null: Initiate Null | Open/Filtered | No Packet
ACK | ACK: Initiate Ack | Filtered | No Packet
```

```
ubuntu@client: ~$
Begin emission:
.....Finished sending 1 packets.
Received 8 packets, got 0 answers, remaining 1 packets
Begin emission:
.....Finished sending 1 packets.
Received 8 packets, got 0 answers, remaining 1 packets
=====
Info Explained
-----
TCP Scan = Type of TCP Scan
First Packet = Flag Received with the First Packet
Second Packet = Flag Received with the Second Packet
Third Packet = Flag Received with the Third Packet
=====
TCP Scan | First Packet | Second Packet | Third Packet
-----|-----|-----|-----
Connect | 1 - S | 0 - No Response | No Packet
SYN | 1 - S | 0 - No Response | No Packet
Xmas | 1 - FPU | 0 - No Response | No Packet
FIN | 1 - F | 0 - No Response | No Packet
Null | 1 - Null | 0 - No Response | No Packet
ACK | 1 - A | 0 - No Response | No Packet
=====
2. Packets Details
-----
TCP Scan | First Packet | Second Packet | Third Packet
-----|-----|-----|-----
Connect | SYN: Initiating Connect | Filtered | No Packet
SYN | SYN: Initiating Syn | Filtered | No Packet
Xmas | FPU: Initiate Xmas | Open/Filtered | No Packet
FIN | F: Initiate Fin | Open/Filtered | No Packet
Null | Null: Initiate Null | Open/Filtered | No Packet
ACK | ACK: Initiate Ack | Filtered | No Packet
```


8. ScanPydia.py -p 22 -ALL 192.168.1.195

Student

```
student@vm-ubuntu: ~$ sudo python3 ScanPydia.py -p 22 -ALL 192.168.1.195
=====
ALL TCP SCANS
=====
Target IP: 192.168.1.195
Port Number: 22
=====
1. Scapy Information
=====
Begin emission:
.....Finished sending 1 packets.
Received 0 packets, got 0 answers, remaining 1 packets
Begin emission:
.....Finished sending 1 packets.
Received 1 packets, got 1 answers, remaining 0 packets
Sent 1 packets.
Begin emission:
.....Finished sending 1 packets.
Received 0 packets, got 0 answers, remaining 1 packets
Begin emission:
.....Finished sending 1 packets.
Received 7 packets, got 0 answers, remaining 1 packets
Begin emission:
.....Finished sending 1 packets.
Received 0 packets, got 0 answers, remaining 1 packets
Begin emission:
.....Finished sending 1 packets.
Received 1 packets, got 1 answers, remaining 0 packets
=====
Info Explained
=====
TCP Scan = Type of TCP Scan
First Packet = Flag Received with the First Packet
Second Packet = Flag Received with the Second Packet
Third Packet = Flag Received with the Third Packet
```

Client

```
ubuntu@client: ~$ sudo python3 ScanPydia.py -p 22 -ALL 192.168.1.195
=====
ALL TCP SCANS
=====
Target IP: 192.168.1.195
Port Number: 22
=====
1. Scapy Information
=====
Begin emission:
.....Finished sending 1 packets.
Received 2 packets, got 1 answers, remaining 0 packets
Sent 1 packets.
Begin emission:
.....Finished sending 1 packets.
Received 1 packets, got 1 answers, remaining 0 packets
Sent 1 packets.
Begin emission:
.....Finished sending 1 packets.
Received 0 packets, got 0 answers, remaining 1 packets
Begin emission:
.....Finished sending 1 packets.
Received 0 packets, got 0 answers, remaining 1 packets
Begin emission:
.....Finished sending 1 packets.
Received 0 packets, got 0 answers, remaining 1 packets
Begin emission:
.....Finished sending 1 packets.
Received 0 packets, got 0 answers, remaining 1 packets
=====
Info Explained
=====
TCP Scan = Type of TCP Scan
First Packet = Flag Received with the First Packet
Second Packet = Flag Received with the Second Packet
```

```
student@vm-ubuntu: ~$ sudo python3 ScanPydia.py -p 22 -ALL 192.168.1.195
=====
ALL TCP SCANS
=====
Target IP: 192.168.1.195
Port Number: 22
=====
1. Scapy Information
=====
Begin emission:
.....Finished sending 1 packets.
Received 0 packets, got 0 answers, remaining 1 packets
Begin emission:
.....Finished sending 1 packets.
Received 1 packets, got 1 answers, remaining 0 packets
=====
Info Explained
=====
TCP Scan = Type of TCP Scan
First Packet = Flag Received with the First Packet
Second Packet = Flag Received with the Second Packet
Third Packet = Flag Received with the Third Packet
=====
TCP Scan | First Packet | Second Packet | Third Packet
-----|-----|-----|-----
Connect | 1 - S | 0 - No Response | No Packet
SYN | 1 - S | 1 - SA | 1 - R
Xmas | 1 - FPU | 0 - No Response | No Packet
FIN | 1 - F | 0 - No Response | No Packet
Null | 1 - Null | 0 - No Response | No Packet
ACK | 1 - A | 1 - R | No Packet
=====
2. Packets Details
=====
TCP Scan | First Packet | Second Packet | Third Packet
-----|-----|-----|-----
Connect | SYN: Initiating Connect | Filtered | No Packet
SYN | SYN: Initiating Syn | Port Is Open | R: RST
Xmas | FPU: Initiate Xmas | Open/Filtered | No Packet
FIN | F: Initiate Fin | Open/Filtered | No Packet
Null | Null: Initiate Null | Open/Filtered | No Packet
ACK | ACK: Initiate Ack | Unfiltered | No Packet
```

```
ubuntu@client: ~$ sudo python3 ScanPydia.py -p 22 -ALL 192.168.1.195
=====
ALL TCP SCANS
=====
Target IP: 192.168.1.195
Port Number: 22
=====
1. Scapy Information
=====
Begin emission:
.....Finished sending 1 packets.
Received 0 packets, got 0 answers, remaining 1 packets
Begin emission:
.....Finished sending 1 packets.
Received 0 packets, got 0 answers, remaining 1 packets
=====
Info Explained
=====
TCP Scan = Type of TCP Scan
First Packet = Flag Received with the First Packet
Second Packet = Flag Received with the Second Packet
Third Packet = Flag Received with the Third Packet
=====
TCP Scan | First Packet | Second Packet | Third Packet
-----|-----|-----|-----
Connect | 1 - S | 1 - SA | 1 - RA
SYN | 1 - S | 1 - SA | 1 - R
Xmas | 1 - FPU | 0 - No Response | No Packet
FIN | 1 - F | 0 - No Response | No Packet
Null | 1 - Null | 0 - No Response | No Packet
ACK | 1 - A | 0 - No Response | No Packet
=====
2. Packets Details
=====
TCP Scan | First Packet | Second Packet | Third Packet
-----|-----|-----|-----
Connect | SYN: Initiating Connect | Port Is Open | RA: RST and ACK
SYN | SYN: Initiating Syn | Port Is Open | R: RST
Xmas | FPU: Initiate Xmas | Open/Filtered | No Packet
FIN | F: Initiate Fin | Open/Filtered | No Packet
Null | Null: Initiate Null | Open/Filtered | No Packet
ACK | ACK: Initiate Ack | Filtered | No Packet
```

9. ScanPydia.py -p 25 -ALL 192.168.1.195

Student

```
student@vm-ubuntu: ~/labtainer/labtainer-student
student@vm-ubuntu:~/labtainer/labtainer-student$ sudo python3 ScanPydia.py -p 25 -ALL 192.168.1.195
=====
ALL TCP SCANS
=====
Target IP: 192.168.1.195
Port Number: 25

-----
1. Scapy Information
-----
Begin emission:
.....Finished sending 1 packets.
Received 0 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
Received 5 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
Received 5 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
Received 5 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
Received 5 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
Received 11 packets, got 0 answers, remaining 1 packets
-----
Info Explained
-----
TCP Scan = Type of TCP Scan
First Packet = Flag Received with the First Packet
Second Packet = Flag Received with the Second Packet
Third Packet = Flag Received with the Third Packet

TCP Scan | First Packet | Second Packet | Third Packet
-----
Connect | 1 - S | 0 - No Response | No Packet
```

```
student@vm-ubuntu:~/labtainer/labtainer-student$
Begin emission:
Finished sending 1 packets.
Received 5 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
Received 11 packets, got 0 answers, remaining 1 packets
-----
Info Explained
-----
TCP Scan = Type of TCP Scan
First Packet = Flag Received with the First Packet
Second Packet = Flag Received with the Second Packet
Third Packet = Flag Received with the Third Packet

TCP Scan | First Packet | Second Packet | Third Packet
-----
Connect | 1 - S | 0 - No Response | No Packet
SYN | 1 - S | 0 - No Response | No Packet
Xmas | 1 - FPU | 0 - No Response | No Packet
FIN | 1 - F | 0 - No Response | No Packet
Null | 1 - Null | 0 - No Response | No Packet
ACK | 1 - A | 0 - No Response | No Packet

-----
2. Packets Details
-----
TCP Scan | First Packet | Second Packet | Third Packet
-----
Connect | SYN: Initiating Connect | Filtered | No Packet
SYN | SYN: Initiating Syn | Filtered | No Packet
Xmas | FPU: Initiate Xmas | Open/Filtered | No Packet
FIN | F: Initiate Fin | Open/Filtered | No Packet
Null | Null: Initiate Null | Open/Filtered | No Packet
ACK | ACK: Initiate Ack | Filtered | No Packet
```

Client

```
ubuntu@client: ~
=====
ALL TCP SCANS
=====
Target IP: 192.168.1.195
Port Number: 25

-----
1. Scapy Information
-----
Begin emission:
Finished sending 1 packets.
Received 1 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
Received 0 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
Received 0 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
Received 0 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
Received 0 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
Received 0 packets, got 0 answers, remaining 1 packets
-----
Info Explained
-----
TCP Scan = Type of TCP Scan
First Packet = Flag Received with the First Packet
Second Packet = Flag Received with the Second Packet
Third Packet = Flag Received with the Third Packet

TCP Scan | First Packet | Second Packet | Third Packet
-----
Connect | 1 - S | 0 - No Response | No Packet
```

```
ubuntu@client: ~
Begin emission:
Finished sending 1 packets.
Received 0 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
Received 0 packets, got 0 answers, remaining 1 packets
-----
Info Explained
-----
TCP Scan = Type of TCP Scan
First Packet = Flag Received with the First Packet
Second Packet = Flag Received with the Second Packet
Third Packet = Flag Received with the Third Packet

TCP Scan | First Packet | Second Packet | Third Packet
-----
Connect | 1 - S | 0 - No Response | No Packet
SYN | 1 - S | 0 - No Response | No Packet
Xmas | 1 - FPU | 0 - No Response | No Packet
FIN | 1 - F | 0 - No Response | No Packet
Null | 1 - Null | 0 - No Response | No Packet
ACK | 1 - A | 0 - No Response | No Packet

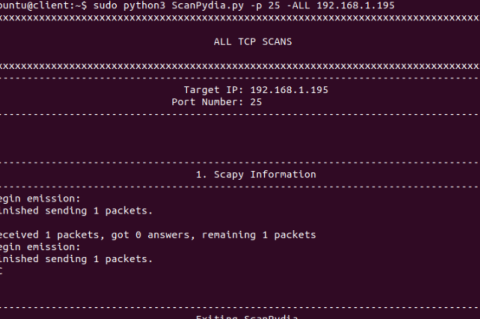
-----
2. Packets Details
-----
TCP Scan | First Packet | Second Packet | Third Packet
-----
Connect | SYN: Initiating Connect | Filtered | No Packet
SYN | SYN: Initiating Syn | Filtered | No Packet
Xmas | FPU: Initiate Xmas | Open/Filtered | No Packet
FIN | F: Initiate Fin | Open/Filtered | No Packet
Null | Null: Initiate Null | Open/Filtered | No Packet
ACK | ACK: Initiate Ack | Filtered | No Packet
```


10. ScanPydia.py -p 25 -ALL 192.168.1.195 (Press CTRL-C while running)

Student

[illegible]

Client



```

ubuntu@client:~$ python3 ScanPydia.py -p 25 -ALL 192.168.1.195
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
ALL TCP SCANS
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Target IP: 192.168.1.195
Port Number: 25
-----

1. Scapy Information
-----
Begin emission:
Finished sending 1 packets.
.
Received 1 packets, got 0 answers, remaining 1 packets
Begin emission:
Finished sending 1 packets.
^C

Exiting ScanPydia...

ubuntu@client:~$

```