Reconnaissance on IoT devices Report

Stage 3: Summary and Statistics

Total IP Address – Duplicate IP addresses =186

Total No of Responsive devices = 94

The name of the ioT set is **Foscam IP cameras**

Total No of Responsive devices is **94**

IP-ID Counter (ICMP)

Number of Zero IP ID counter (ICMP) =0

Number of random IP-ID counter (ICMP) = 57

Number of incremental IP-ID counter (ICMP) =37

Percentage	zero	Random	Incremental
Out of Total devices=186	0	30.64%	19.89%
Out of Responsive devices =96	**0**	**60.64%**	**39.36 %**

Thus, Percentage of devices with zero counter is 0%, random counter is 60.64% and incremental IP-ID counter is 39.36% in ICMP packets

Number of devices with port 80 open =18

Number of device with port 80 closed =76

Percentage of Responsive devices	Port 80 open
Out of Total devices=186	9.7%
Out of Responsive devices =96	**19.15%**

Thus, Percentage of devices with port 80 open (i.e., responsive) is 19.15%

Number of Zero IP ID counter (ICMP) =15

Number of random IP-ID counter (ICMP) = 0

Number of incremental IP-ID counter (ICMP) =3

Percentage	zero	Random	Incremental
Out of Total devices=186	8.06%	0	1.61%
Out of Responsive devices =96	15.625%	0	3.125%
Out of Responsive devices with port 80 open =18	**83.33%**	**0**	**16.67%**

Thus, Percentage of devices with zero counter is 83.33%, random counter is 0% and incremental IP-ID counter is 16.67% in TCP packets

Number of devices that deploy SYN cookies =17

Percentage	SYN cookies deployed
Out of Total devices=186	9.14%
Out of Responsive devices =96	17.71%
Out of Responsive devices with port 80 open =18	**94.44%**

Thus, Percentage of devices that deploys SYN cookies is 94.44%

TTL value range	Window Size	Outcome =OS	Number of devices with OS=outcome
64	Not Available	Likely Linux	74
64	5720	Customized Linux	9
64	5840	Linux 2.4 and 2.6	1
64	65535	MAC or Free BSD	5
64	Available but not in range	Other	3
255	Not Available	Other	2
			Total =94

Number of Windows operating system =**0**

Number of Linux operating system =74+9+1=**84**

Number of Linux devices with port 80 open =10 (Percentage =10/18 = 55.555)

(Other refers to OS such as Open BSD, AIX, CISCO, Solaris

Percentage	Linux OS	Windows OS
Out of Total devices=186	45.16%	0%
Out of Responsive devices =96	**89.36%**	**0%**
Out of Responsive devices with port 80 open =18	55.55%	0%

Thus, Percentage of devices with Linux operating system is 89.36% and Windows OS is 0%

(Additional instructions for testing stage 1 and stage 2 on 4482scappy.py file)

Stage 1:

Enter choice 1 and Enter the IP address needs to be tested. For example "73.142.73.94" or www.google.ca .

(Sample output)

```
C:\Users\User\4482_scapy\venv\Scripts\python.exe C:/Users/User/4482_scapy/main.py
Press 1 to enter an IP address
Press 2 to Enter file name containing IP address
1
Enter a IP addresses
217.121.154.149
Checking 217.121.154.149.....
Yes, the device is responsive
The device deploys incremental IP-ID counter (ICMP)
Yes, Port 80 on device is open
The device deploys zero IP-ID counter (TCP)
ttl: 53, Window size: 5840, OS: Linux 2.4 and Linux 2.6



Process finished with exit code 0
```

Stage 2:

Enter choice 2 to run a file containing shodan data (list of IP addresses). Please read the instructions on input screen before testing the program for stage 2. Pandas library must be installed on operating system, and input must be a csv file and contained in the same folder as the program.

After running, wait for few minutes and the output file named **"Jaffar_result.csv"** will be automatically created in the folder

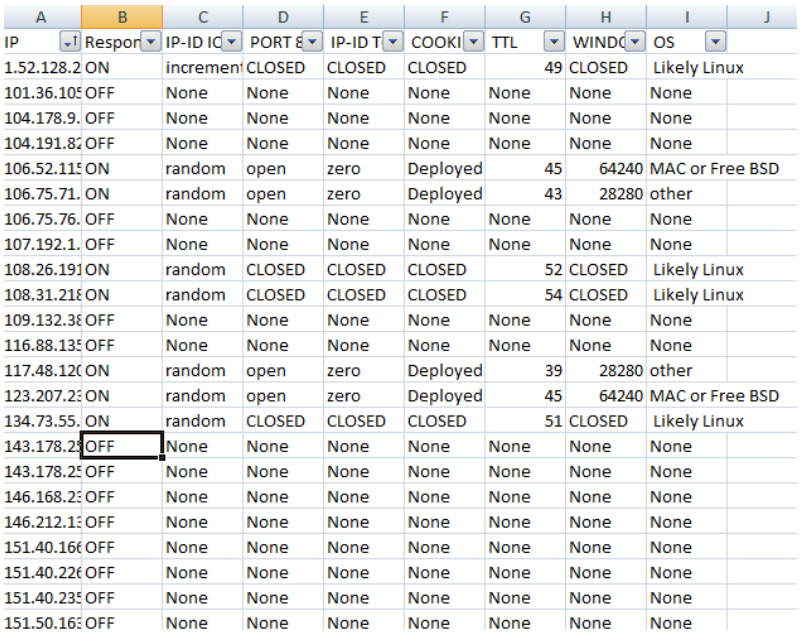
```
C:\Users\User\4482_scapy\venv\Scripts\python.exe C:/Users/User/4482_scapy/4482scappy.py
Press 1 to enter an IP address
Press 2 to Enter file name containing IP address
2
IMPORTANT: Before running
1.Make sure data file is in the same directory as program file or Enter a valid path
2.Only works with .csv files. For example, shodan_data.csv
3.To convert .xlsx file to .csv on Windows:
        Open .xlsx file--> Click File-->Save As--> save as type: CSV(comma delimited)-->Save
4.Make sure Pandas library is installed [Use: pip install pandas]
5.Uncomment import Pandas line at the beginning of the code

Enter the file name, for example shodan_data.csv
shodan_data.csv
Please wait for few minutes. Output file is being generated
Checking 151.51.92.117.....
151.51.92.117,OFF,None,None,None,None,None,None,None



Checking 24.51.165.132.....
24.51.165.132,OFF,None,None,None,None,None,None,None
```

After few minutes, Summary file called Jaffar_result.csv gets generated in the folder automatically after choosing option 2 in the program



A	B	C	D	E	F	G	H	I	J
IP	Respon	IP-ID IC	PORT 8	IP-ID T	COOKI	TTL	WINDC	OS	
1.52.128.2	ON	incremen	CLOSED	CLOSED	CLOSED	49	CLOSED	Likely Linux	
101.36.105	OFF	None	None	None	None	None	None	None	
104.178.9.	OFF	None	None	None	None	None	None	None	
104.191.8	OFF	None	None	None	None	None	None	None	
106.52.115	ON	random	open	zero	Deployed	45	64240	MAC or Free BSD	
106.75.71.	ON	random	open	zero	Deployed	43	28280	other	
106.75.76.	OFF	None	None	None	None	None	None	None	
107.192.1.	OFF	None	None	None	None	None	None	None	
108.26.191	ON	random	CLOSED	CLOSED	CLOSED	52	CLOSED	Likely Linux	
108.31.218	ON	random	CLOSED	CLOSED	CLOSED	54	CLOSED	Likely Linux	
109.132.38	OFF	None	None	None	None	None	None	None	
116.88.135	OFF	None	None	None	None	None	None	None	
117.48.120	ON	random	open	zero	Deployed	39	28280	other	
123.207.23	ON	random	open	zero	Deployed	45	64240	MAC or Free BSD	
134.73.55.	ON	random	CLOSED	CLOSED	CLOSED	51	CLOSED	Likely Linux	
143.178.28	OFF	None	None	None	None	None	None	None	
143.178.25	OFF	None	None	None	None	None	None	None	
146.168.23	OFF	None	None	None	None	None	None	None	
146.212.13	OFF	None	None	None	None	None	None	None	
151.40.166	OFF	None	None	None	None	None	None	None	
151.40.226	OFF	None	None	None	None	None	None	None	
151.40.235	OFF	None	None	None	None	None	None	None	
151.50.163	OFF	None	None	None	None	None	None	None	