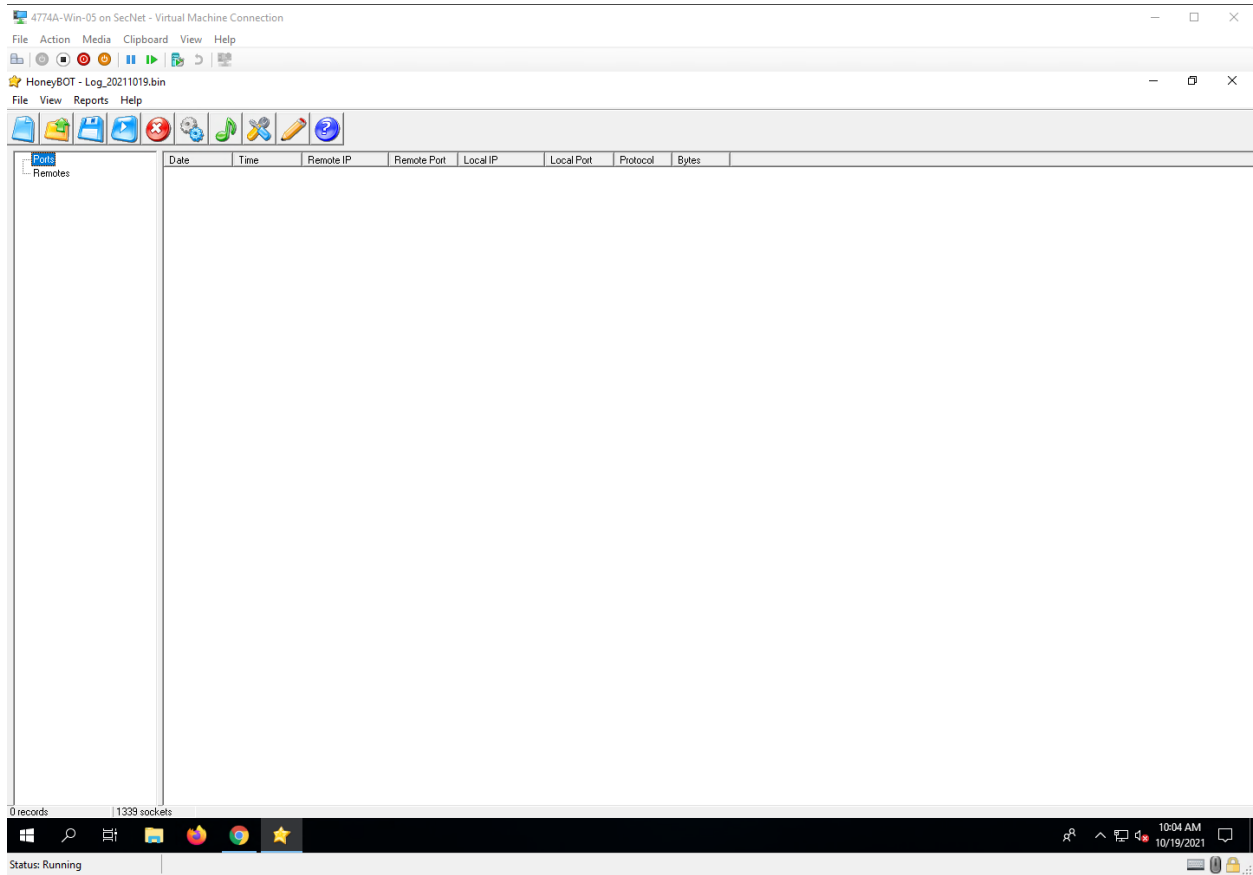


Jamel Douglas
JED18C
Lab 6 – Keylogger and Spyware
10/19/2021

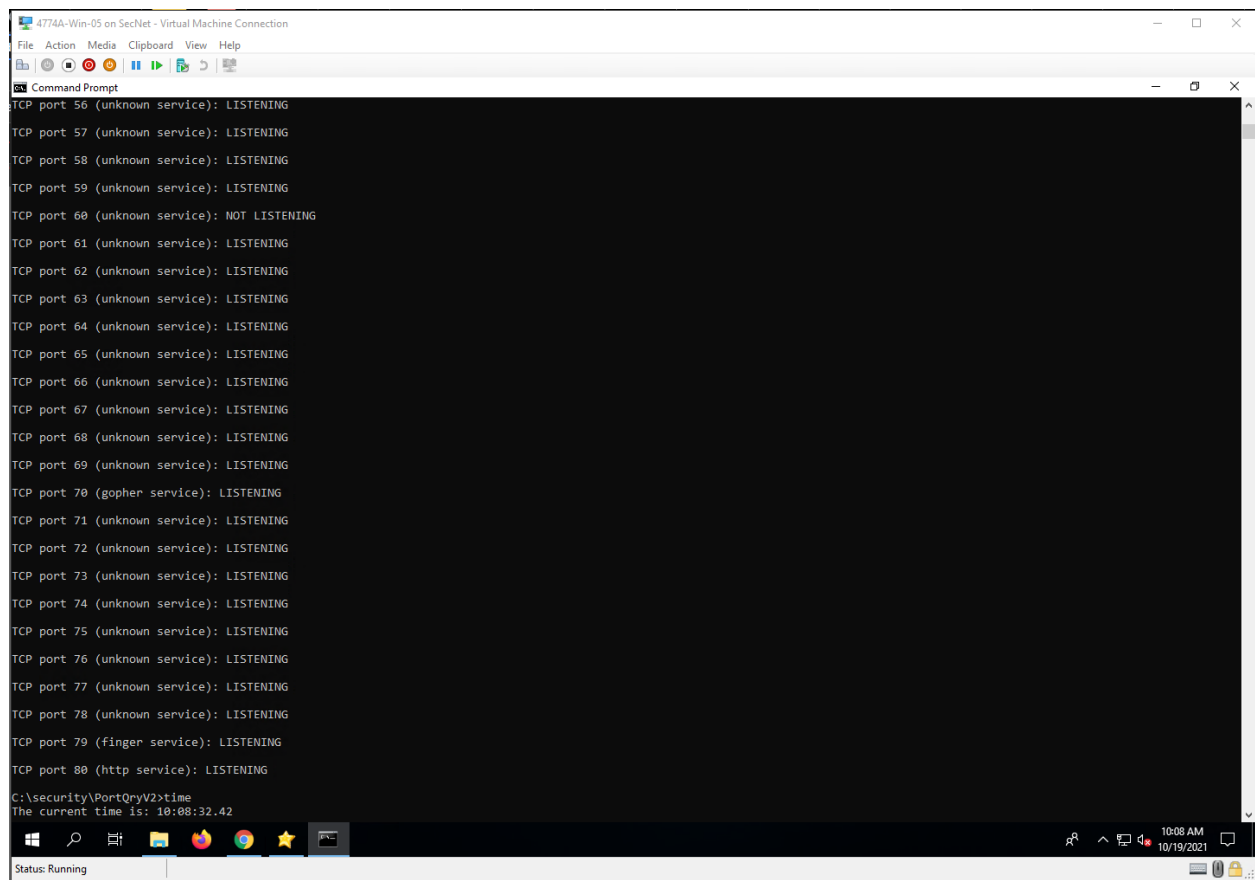
1 HoneyBot

Screenshots

Step 14



Step 27



```
4774A-Win-05 on SecNet - Virtual Machine Connection
File Action Media Clipboard View Help
Command Prompt
TCP port 56 (unknown service): LISTENING
TCP port 57 (unknown service): LISTENING
TCP port 58 (unknown service): LISTENING
TCP port 59 (unknown service): LISTENING
TCP port 60 (unknown service): NOT LISTENING
TCP port 61 (unknown service): LISTENING
TCP port 62 (unknown service): LISTENING
TCP port 63 (unknown service): LISTENING
TCP port 64 (unknown service): LISTENING
TCP port 65 (unknown service): LISTENING
TCP port 66 (unknown service): LISTENING
TCP port 67 (unknown service): LISTENING
TCP port 68 (unknown service): LISTENING
TCP port 69 (unknown service): LISTENING
TCP port 70 (gopher service): LISTENING
TCP port 71 (unknown service): LISTENING
TCP port 72 (unknown service): LISTENING
TCP port 73 (unknown service): LISTENING
TCP port 74 (unknown service): LISTENING
TCP port 75 (unknown service): LISTENING
TCP port 76 (unknown service): LISTENING
TCP port 77 (unknown service): LISTENING
TCP port 78 (unknown service): LISTENING
TCP port 79 (finger service): LISTENING
TCP port 80 (http service): LISTENING
C:\security\PortQryV2>time
The current time is: 10:08:22.42
Status: Running
10:08 AM
10/19/2021
```

Step 29

4774A-Win-05 on SecNet - Virtual Machine Connection

File Action Media Clipboard View Help

HoneyBOT - Log_20211019.bin

File View Reports Help

(P) Ports	(R) Remotes	Date	Time	Remote IP	Remote Port	Local IP	Local Port	Protocol	Bytes
		10/19/2021	10:08:04 AM	192.168.72.54	24562	192.168.72.54	20	TCP	0
		10/19/2021	10:08:04 AM	192.168.72.54	24563	192.168.72.54	21	TCP	181
		10/19/2021	10:08:08 AM	192.168.72.54	24564	192.168.72.54	22	TCP	0
		10/19/2021	10:08:08 AM	192.168.72.54	24565	192.168.72.54	23	TCP	12
		10/19/2021	10:08:08 AM	192.168.72.54	24566	192.168.72.54	24	TCP	0
		10/19/2021	10:08:08 AM	192.168.72.54	24567	192.168.72.54	25	TCP	25
		10/19/2021	10:08:09 AM	192.168.72.54	24569	192.168.72.54	27	TCP	0
		10/19/2021	10:08:10 AM	192.168.72.54	24571	192.168.72.54	29	TCP	0
		10/19/2021	10:08:12 AM	192.168.72.54	24573	192.168.72.54	31	TCP	0
		10/19/2021	10:08:13 AM	192.168.72.54	24575	192.168.72.54	33	TCP	0
		10/19/2021	10:08:14 AM	192.168.72.54	24577	192.168.72.54	35	TCP	0
		10/19/2021	10:08:15 AM	192.168.72.54	24579	192.168.72.54	37	TCP	0
		10/19/2021	10:08:15 AM	192.168.72.54	24580	192.168.72.54	38	TCP	0
		10/19/2021	10:08:15 AM	192.168.72.54	24581	192.168.72.54	39	TCP	0
		10/19/2021	10:08:16 AM	192.168.72.54	24583	192.168.72.54	41	TCP	0
		10/19/2021	10:08:16 AM	192.168.72.54	24584	192.168.72.54	42	TCP	0
		10/19/2021	10:08:16 AM	192.168.72.54	24585	192.168.72.54	43	TCP	0
		10/19/2021	10:08:16 AM	192.168.72.54	24586	192.168.72.54	44	TCP	0
		10/19/2021	10:08:16 AM	192.168.72.54	24587	192.168.72.54	45	TCP	0
		10/19/2021	10:08:16 AM	192.168.72.54	24588	192.168.72.54	46	TCP	0
		10/19/2021	10:08:16 AM	192.168.72.54	24589	192.168.72.54	47	TCP	0
		10/19/2021	10:08:16 AM	192.168.72.54	24590	192.168.72.54	48	TCP	0
		10/19/2021	10:08:16 AM	192.168.72.54	24591	192.168.72.54	49	TCP	0
		10/19/2021	10:08:16 AM	192.168.72.54	24592	192.168.72.54	50	TCP	0
		10/19/2021	10:08:16 AM	192.168.72.54	24593	192.168.72.54	51	TCP	0
		10/19/2021	10:08:16 AM	192.168.72.54	24594	192.168.72.54	52	TCP	0
		10/19/2021	10:08:17 AM	192.168.72.54	24595	192.168.72.54	53	TCP	0
		10/19/2021	10:08:17 AM	192.168.72.54	24596	192.168.72.54	54	TCP	0
		10/19/2021	10:08:17 AM	192.168.72.54	24597	192.168.72.54	55	TCP	0
		10/19/2021	10:08:17 AM	192.168.72.54	24598	192.168.72.54	56	TCP	0
		10/19/2021	10:08:17 AM	192.168.72.54	24599	192.168.72.54	57	TCP	0
		10/19/2021	10:08:17 AM	192.168.72.54	24600	192.168.72.54	58	TCP	0
		10/19/2021	10:08:17 AM	192.168.72.54	24601	192.168.72.54	59	TCP	0
		10/19/2021	10:08:17 AM	192.168.72.54	24603	192.168.72.54	61	TCP	0
		10/19/2021	10:08:17 AM	192.168.72.54	24604	192.168.72.54	62	TCP	0
		10/19/2021	10:08:17 AM	192.168.72.54	24605	192.168.72.54	63	TCP	0
		10/19/2021	10:08:17 AM	192.168.72.54	24606	192.168.72.54	64	TCP	0
		10/19/2021	10:08:17 AM	192.168.72.54	24607	192.168.72.54	65	TCP	0
		10/19/2021	10:08:17 AM	192.168.72.54	24608	192.168.72.54	66	TCP	0
		10/19/2021	10:08:17 AM	192.168.72.54	24609	192.168.72.54	67	TCP	0
		10/19/2021	10:08:17 AM	192.168.72.54	24610	192.168.72.54	68	TCP	0
		10/19/2021	10:08:18 AM	192.168.72.54	24611	192.168.72.54	69	TCP	41
		10/19/2021	10:08:18 AM	192.168.72.54	24612	192.168.72.54	70	TCP	0
		10/19/2021	10:08:19 AM	192.168.72.54	24613	192.168.72.54	71	TCP	0
		10/19/2021	10:08:18 AM	192.168.72.54	24614	192.168.72.54	72	TCP	0
		10/19/2021	10:08:18 AM	192.168.72.54	24615	192.168.72.54	73	TCP	0
		10/19/2021	10:08:18 AM	192.168.72.54	24616	192.168.72.54	74	TCP	0
		10/19/2021	10:08:19 AM	192.168.72.54	24617	192.168.72.54	75	TCP	0
		10/19/2021	10:08:19 AM	192.168.72.54	24618	192.168.72.54	76	TCP	0
		10/19/2021	10:08:19 AM	192.168.72.54	24619	192.168.72.54	77	TCP	0
		10/19/2021	10:08:18 AM	192.168.72.54	24620	192.168.72.54	78	TCP	0

68 records | 1339 sockets

Status: Running

10:08 AM 10/19/2021

Step 34

4774A-Win-05 on SecNet - Virtual Machine Connection

File Action Media Clipboard View Help

HoneyBOT - Log_20211019.bin

File View Reports Help

IP	Date	Time	Remote IP	Remote Port	Local IP	Local Port	Protocol	Bytes
Remotes	10/19/2021	10:13:12 AM	192.168.72.54	13471	192.168.72.54	21	TCP	144
	10/19/2021	10:13:12 AM	192.168.72.54	13472	192.168.72.54	21	TCP	144
	10/19/2021	10:13:24 AM	192.168.72.54	13473	192.168.72.54	21	TCP	132
	10/19/2021	10:13:25 AM	192.168.72.54	13474	192.168.72.54	21	TCP	132

4 records

Status: Running

10:13 AM
10/19/2021

Mozilla Firefox

Firefox

Step 36

4774A-Win-05 on SecNet - Virtual Machine Connection

File Action Media Clipboard View Help

HoneyBOT - Log_20211019.bin

File View Reports Help

Ports Remotes

Packet Log (ftp)

Connection Details:

Date: 10/19/2021
Time: 10:13:24 AM
Timezone: -4:00
Source IP: 192.168.72.54
Source Port: 13473
Server IP: 192.168.72.54
Server Port: 21 (ftp)
Protocol: TCP
Bytes Sent: 106
Bytes Received: 26

Packet History

Time	Direction	Bytes	Data
10:13:24 AM	RX	0	SYN
10:13:24 AM	TX	41	220 PUBLIC08 FTP Service (Version 5.0)
10:13:24 AM	RX	12	USER Jamel
10:13:24 AM	TX	34	331 Password required for Jamel
10:13:24 AM	RX	14	PASS Douglas
10:13:25 AM	TX	31	530 User Jamel cannot log in.
10:13:25 AM	RX	0	FIN

Packet Data:

View as ☒ text ☐ hex

<< < > >>

Start 1339 sockets

Status: Running

10:14 AM
10/19/2021

Step 41

4774A-Win-05 on SecNet - Virtual Machine Connection

File Action Media Clipboard View Help

Zenmap

Scan Tools Profile Help

Target: 192.168.72.54 Profile: Scan Cancel

Command: nmap -T4 -A -v 192.168.72.54

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

nmap -T4 -A -v 192.168.72.54

Discovered open port 5001/tcp on 192.168.72.54

Discovered open port 4000/tcp on 192.168.72.54

Discovered open port 4567/tcp on 192.168.72.54

Discovered open port 7201/tcp on 192.168.72.54

Discovered open port 2604/tcp on 192.168.72.54

Discovered open port 31337/tcp on 192.168.72.54

Discovered open port 4045/tcp on 192.168.72.54

Discovered open port 6007/tcp on 192.168.72.54

Discovered open port 179/tcp on 192.168.72.54

Discovered open port 444/tcp on 192.168.72.54

Discovered open port 427/tcp on 192.168.72.54

Discovered open port 4321/tcp on 192.168.72.54

Discovered open port 1000/tcp on 192.168.72.54

Discovered open port 1063/tcp on 192.168.72.54

Discovered open port 7100/tcp on 192.168.72.54

Discovered open port 1029/tcp on 192.168.72.54

Discovered open port 89/tcp on 192.168.72.54

Discovered open port 515/tcp on 192.168.72.54

Discovered open port 911/tcp on 192.168.72.54

Discovered open port 2020/tcp on 192.168.72.54

Discovered open port 9076/tcp on 192.168.72.54

Discovered open port 6005/tcp on 192.168.72.54

Discovered open port 88/tcp on 192.168.72.54

Discovered open port 7200/tcp on 192.168.72.54

Discovered open port 83/tcp on 192.168.72.54

Discovered open port 1001/tcp on 192.168.72.54

Discovered open port 4/tcp on 192.168.72.54

Discovered open port 1112/tcp on 192.168.72.54

Discovered open port 1002/tcp on 192.168.72.54

Discovered open port 2038/tcp on 192.168.72.54

Discovered open port 7001/tcp on 192.168.72.54

Discovered open port 1494/tcp on 192.168.72.54

Completed SYN Stealth Scan at 10:19, 0.25s elapsed (1000 total ports)

Initiating Service scan at 10:19

Scanning 248 services on 4774a-win-05.secnet.local (192.168.72.54)

Service scan Timing: About 4.82% done; ETC: 10:32 (0:12:11 remaining)

Service scan Timing: About 8.84% done; ETC: 10:32 (0:11:31 remaining)

Service scan Timing: About 12.45% done; ETC: 10:34 (0:13:22 remaining)

Service scan Timing: About 26.10% done; ETC: 10:30 (0:08:24 remaining)

Service scan Timing: About 33.33% done; ETC: 10:29 (0:06:56 remaining)

Service scan Timing: About 42.97% done; ETC: 10:28 (0:05:16 remaining)

Service scan Timing: About 55.42% done; ETC: 10:27 (0:03:47 remaining)

Service scan Timing: About 75.10% done; ETC: 10:26 (0:01:43 remaining)

Completed Service scan at 10:27, 500.07s elapsed (249 services on 1 host)

Initiating OS detection (try #1) against 4774a-win-05.secnet.local (192.168.72.54)

NSE: Script scanning 192.168.72.54.

Initiating NSE at 10:27

Filter Hosts

Status: Running

10:29 AM
10/19/2021

Step 43

4774A-Win-05 on SecNet - Virtual Machine Connection

File Action Media Clipboard View Help

HoneyBOT - Log_20211019.bin

File View Reports Help

Date	Time	Remote IP	Remote Port	Local IP	Local Port	Protocol	Bytes
10/19/2021	10:29:19 AM	192.168.72.54	15043	192.168.72.54	2002	TCP	0
10/19/2021	10:29:19 AM	192.168.72.54	15048	192.168.72.54	2968	TCP	0
10/19/2021	10:29:19 AM	192.168.72.54	15050	192.168.72.54	2049	TCP	0
10/19/2021	10:29:20 AM	192.168.72.54	15051	192.168.72.54	163	TCP	0
10/19/2021	10:29:20 AM	192.168.72.54	15057	192.168.72.54	995	TCP	54
10/19/2021	10:29:21 AM	192.168.72.54	15059	192.168.72.54	8000	TCP	517
10/19/2021	10:29:21 AM	192.168.72.54	15062	192.168.72.54	5800	TCP	821
10/19/2021	10:29:21 AM	192.168.72.54	15068	192.168.72.54	8008	TCP	0
10/19/2021	10:29:21 AM	192.168.72.54	15065	192.168.72.54	8080	TCP	555
10/19/2021	10:29:22 AM	192.168.72.54	723	192.168.72.54	179	TCP	110
10/19/2021	10:29:22 AM	192.168.72.54	15073	192.168.72.54	113	TCP	36
10/19/2021	10:29:22 AM	192.168.72.54	15075	192.168.72.54	3306	TCP	51
10/19/2021	10:29:22 AM	192.168.72.54	793	192.168.72.54	7	TCP	0
10/19/2021	10:29:23 AM	192.168.72.54	15076	192.168.72.54	199	TCP	0
10/19/2021	10:29:23 AM	192.168.72.54	15078	192.168.72.54	6	TCP	0
10/19/2021	10:29:23 AM	192.168.72.54	15081	192.168.72.54	2035	TCP	0
10/19/2021	10:29:23 AM	192.168.72.54	15082	192.168.72.54	7007	TCP	0
10/19/2021	10:29:23 AM	192.168.72.54	15086	192.168.72.54	5950	TCP	18
10/19/2021	10:29:24 AM	192.168.72.54	15088	192.168.72.54	8000	TCP	0
10/19/2021	10:29:24 AM	192.168.72.54	15105	192.168.72.54	1011	TCP	18
10/19/2021	10:29:25 AM	192.168.72.54	15107	192.168.72.54	5800	TCP	496
10/19/2021	10:29:25 AM	192.168.72.54	15102	192.168.72.54	8008	TCP	634
10/19/2021	10:29:25 AM	192.168.72.54	15108	192.168.72.54	6668	TCP	49
10/19/2021	10:29:25 AM	192.168.72.54	636	192.168.72.54	6080	TCP	426
10/19/2021	10:29:25 AM	192.168.72.54	15114	192.168.72.54	113	TCP	48
10/19/2021	10:29:26 AM	192.168.72.54	793	192.168.72.54	2525	TCP	82
10/19/2021	10:29:26 AM	192.168.72.54	15117	192.168.72.54	1080	TCP	0
10/19/2021	10:29:26 AM	192.168.72.54	15120	192.168.72.54	2106	TCP	0
10/19/2021	10:29:26 AM	192.168.72.54	15121	192.168.72.54	2042	TCP	0
10/19/2021	10:29:27 AM	192.168.72.54	15122	192.168.72.54	545	TCP	0
10/19/2021	10:29:28 AM	192.168.72.54	15119	192.168.72.54	8000	TCP	0
10/19/2021	10:29:28 AM	192.168.72.54	15131	192.168.72.54	5800	TCP	821
10/19/2021	10:29:29 AM	192.168.72.54	15132	192.168.72.54	8008	TCP	517
10/19/2021	10:29:30 AM	192.168.72.54	15134	192.168.72.54	179	TCP	0
10/19/2021	10:29:30 AM	192.168.72.54	15141	192.168.72.54	10082	TCP	110
10/19/2021	10:29:30 AM	192.168.72.54	15140	192.168.72.54	5800	TCP	821
10/19/2021	10:29:30 AM	192.168.72.54	15142	192.168.72.54	8000	TCP	231
10/19/2021	10:29:31 AM	192.168.72.54	15144	192.168.72.54	5800	TCP	0
10/19/2021	10:29:32 AM	192.168.72.54	15145	192.168.72.54	6668	TCP	517
10/19/2021	10:29:32 AM	192.168.72.54	15146	192.168.72.54	8000	TCP	517
10/19/2021	10:29:33 AM	192.168.72.54	15147	192.168.72.54	8000	TCP	233
10/19/2021	10:29:33 AM	192.168.72.54	15149	192.168.72.54	8000	TCP	517
10/19/2021	10:29:34 AM	192.168.72.54	15150	192.168.72.54	8000	TCP	233
10/19/2021	10:29:34 AM	192.168.72.54	15152	192.168.72.54	8443	TCP	517
10/19/2021	10:29:35 AM	192.168.72.54	15153	192.168.72.54	8000	TCP	517
10/19/2021	10:29:35 AM	192.168.72.54	15155	192.168.72.54	8000	TCP	231
10/19/2021	10:29:36 AM	192.168.72.54	793	192.168.72.54	143	TCP	114
10/19/2021	10:29:36 AM	192.168.72.54	15156	192.168.72.54	8000	TCP	517
10/19/2021	10:29:37 AM	192.168.72.54	15157	192.168.72.54	10082	TCP	88
10/19/2021	10:29:43 AM	192.168.72.54	15159	192.168.72.54	110	TCP	71
10/19/2021	10:29:44 AM	192.168.72.54	15160	192.168.72.54	13722	TCP	110
10/19/2021	10:29:52 AM	192.168.72.54	15162	192.168.72.54	13722	TCP	88

2086 records | 1339 sockets

Status: Running

Step 54

4774A-Win-05 on SecNet - Virtual Machine Connection

File Action Media Clipboard View Help

HoneyBOT - Log_20211019.bin

File View Reports Help

(p) Ports	Date	Time	Remote IP	Remote Port	Local IP	Local Port	Protocol	Bytes
(d) Remotes	10/19/2021	11:19:26 AM	192.168.72.54	895	192.168.72.54	2035	TCP	44
	10/19/2021	11:19:27 AM	192.168.72.54	822	192.168.72.54	199	TCP	44
	10/19/2021	11:19:27 AM	192.168.72.54	856	192.168.72.54	31337	TCP	44
	10/19/2021	11:19:27 AM	192.168.72.54	691	192.168.72.54	6101	TCP	44
	10/19/2021	11:19:27 AM	192.168.72.54	654	192.168.72.54	555	TCP	44
	10/19/2021	11:19:28 AM	192.168.72.54	672	192.168.72.54	8081	TCP	44
	10/19/2021	11:19:28 AM	192.168.72.54	1001	192.168.72.54	5432	TCP	44
	10/19/2021	11:19:28 AM	192.168.72.54	846	192.168.72.54	5960	TCP	44
	10/19/2021	11:19:35 AM	192.168.72.54	1027	192.168.72.54	2525	TCP	25
	10/19/2021	11:19:37 AM	192.168.72.54	823	192.168.72.54	953	TCP	517
	10/19/2021	11:19:41 AM	192.168.72.54	33339	192.168.72.54	3306	TCP	51
	10/19/2021	11:19:47 AM	192.168.72.54	13727	192.168.72.54	5900	TCP	12
	10/19/2021	11:19:48 AM	192.168.72.54	561	192.168.72.54	3389	TCP	517
	10/19/2021	11:19:48 AM	192.168.72.54	14685	192.168.72.54	5900	TCP	24
	10/19/2021	11:19:53 AM	192.168.72.54	14686	192.168.72.54	8010	TCP	156
	10/19/2021	11:19:59 AM	192.168.72.54	30295	192.168.72.54	3306	TCP	51
	10/19/2021	11:19:59 AM	192.168.72.54	30256	192.168.72.54	2525	TCP	142
	10/19/2021	11:20:00 AM	192.168.72.54	823	192.168.72.54	389	TCP	31
	10/19/2021	11:20:14 AM	192.168.72.54	11982	192.168.72.54	8443	TCP	517
	10/19/2021	11:20:30 AM	192.168.72.54	823	192.168.72.54	1433	TCP	41
	10/19/2021	11:20:46 AM	192.168.72.54	561	192.168.72.54	5900	TCP	24
	10/19/2021	11:20:53 AM	192.168.72.54	19768	192.168.72.54	3306	TCP	51
	10/19/2021	11:20:56 AM	192.168.72.54	561	192.168.72.54	5432	TCP	8
	10/19/2021	11:21:03 AM	192.168.72.54	823	192.168.72.54	5432	TCP	517
	10/19/2021	11:21:09 AM	0.0.0.0	68	192.168.72.54	67	UDP	322
	10/19/2021	11:21:09 AM	192.168.72.7	67	192.168.72.54	68	UDP	301
	10/19/2021	11:21:34 AM	192.168.72.54	1036	192.168.72.54	8010	TCP	152
	10/19/2021	11:21:46 AM	192.168.72.54	1040	192.168.72.54	993	TCP	517
	10/19/2021	11:22:17 AM	192.168.72.54	561	192.168.72.54	3389	TCP	517
	10/19/2021	11:22:48 AM	192.168.72.54	1470	192.168.72.54	8443	TCP	517
	10/19/2021	11:23:19 AM	192.168.72.54	561	192.168.72.54	2525	TCP	142
	10/19/2021	11:23:20 AM	192.168.72.54	823	192.168.72.54	2525	TCP	542
	10/19/2021	11:23:20 AM	192.168.72.54	1036	192.168.72.54	465	TCP	517
	10/19/2021	11:23:51 AM	192.168.72.54	823	192.168.72.54	119	TCP	51
	10/19/2021	11:23:59 AM	192.168.72.54	561	192.168.72.54	119	TCP	552
	10/19/2021	11:23:59 AM	192.168.72.54	1035	192.168.72.54	25	TCP	142
	10/19/2021	11:24:01 AM	192.168.72.54	823	192.168.72.54	25	TCP	542
	10/19/2021	11:24:02 AM	192.168.72.54	561	192.168.72.54	465	TCP	517
	10/19/2021	11:24:33 AM	192.168.72.54	823	192.168.72.54	1433	TCP	41
	10/19/2021	11:25:05 AM	192.168.72.54	6444	192.168.72.54	443	TCP	517
	10/19/2021	11:25:36 AM	192.168.72.54	1036	192.168.72.54	443	TCP	517
	10/19/2021	11:26:07 AM	192.168.72.54	1041	192.168.72.54	21	TCP	102
	10/19/2021	11:26:08 AM	192.168.72.54	561	192.168.72.54	21	TCP	598
	10/19/2021	11:26:09 AM	192.168.72.54	1043	192.168.72.54	995	TCP	517
	10/19/2021	11:26:40 AM	192.168.72.54	561	192.168.72.54	143	TCP	114
	10/19/2021	11:26:41 AM	192.168.72.54	29717	192.168.72.54	143	TCP	614
	10/19/2021	11:26:42 AM	192.168.72.54	29718	192.168.72.54	143	TCP	189
	10/19/2021	11:26:42 AM	192.168.72.54	823	192.168.72.54	395	TCP	517
	10/19/2021	11:30:13 AM	0.0.0.0	68	192.168.72.54	67	UDP	322
	10/19/2021	11:30:13 AM	192.168.72.7	67	192.168.72.54	68	UDP	301
	10/19/2021	11:33:03 AM	0.0.0.0	68	192.168.72.54	67	UDP	322
	10/19/2021	11:33:03 AM	192.168.72.7	67	192.168.72.54	68	UDP	301

Start | Ports | 1339 sockets

Status: Running

11:37 AM 10/19/2021

Step 61

4774A-Win-05 on SecNet - Virtual Machine Connection

File Action Media Clipboard View Help

New Tab x New Tab x Nessus Essentials / Folders / View x +

Not secure | https://localhost:8834/#/scans/reports/15/hosts/2/vulnerabilities

nessus Essentials Scans Settings admin

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules

TENABLE

- Community
- Research
- Plugin Release Notes

JameIDouglasNessus / 192.168.72.54

Configure Audit Trail Launch Report Export

Vulnerabilities 34

Filter Search Vulnerabilities 34 Vulnerabilities

Sev	Name	Family	Count	
MIXED	4 Apache Httpd (Multiple Issues)	Web Servers	4	
CRITICAL	DameWare Mini Remote Control Pre-Authenticatio...	Windows	1	
CRITICAL	Kuang2 the Virus Detection	Backdoors	1	
CRITICAL	Symantec pcAnywhere Unsupported	Misc.	1	
MIXED	3 Mysql (Multiple Issues)	Databases	3	
HIGH	FakeBO NetBus Handling Code Remote Overflow	Gain a shell remotely	1	
HIGH	ISMail Multiple Command Domain Name Handling ...	SMTP problems	1	
HIGH	NetBus 1.x Software Detection	Backdoors	1	
	TP (Multiple Issues)	Web Servers	4	
	Print FireWall-1 Identification	Firewalls	3	
	Service Detection	Service detection	2	
	...ing not required	Misc.	1	

Host Details

IP: 192.168.72.54
DNS: DESKTOP-VLAFEF9.SECNET.local
OS: Windows
Start: Today at 10:32 AM
End: Today at 10:56 AM
Elapsed: 24 minutes
KB: Download

Vulnerabilities

3 Qualifications Cyber Safety Review Board Members...

Read More

Nessus Essentials / Folders / View Scan - Google Chrome

Nessus Essentials / Folders / Vie...

11:39 AM 10/19/2021

Status: Running

Project Questions

1. My IP address is 192.168.72.54.
2. Honey bot recorded 2086 events for the IP scan.
3. Honey bot recorded 1262 events for the Nessus scan.
4. I don't think that HoneyBot recorded any other IP addresses throughout my scans.

Thought Questions

1. Ports need to be open in order for them to be enticing to hackers, closed ports don't allow access, but open ports do.
2. It depends on the skill level of person who setup the honeypot, and the skills of the hacker accessing the honeypot. An experienced hacker probably would be able to tell if a basic or even intermediate honeypot is on the system.
3. I'm sure that there is some kind of honeypot that caters to blocking the harvesting of email addresses from sites
4. It is very much possible that law enforcement agencies in the US would use honeypots to track criminal behavior.