

9/8/24

Experiment - 5

Packet Capture Tool

Aim:
 Experiments on packet capture tools wire shark

Packet sniffer:

Sniffs messages being sent / received from / by your computer store and display the contents of the various protocol fields in the message

Passive program
never sends packets its self
no packet addressed to it
receives a copy of packets
(sent / received)

Packet Sniffer structure Diagnostic Tools

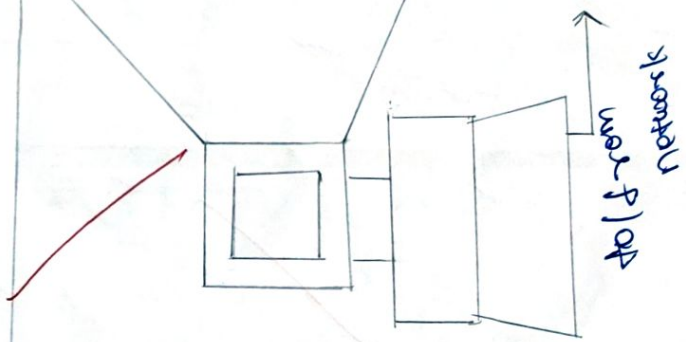
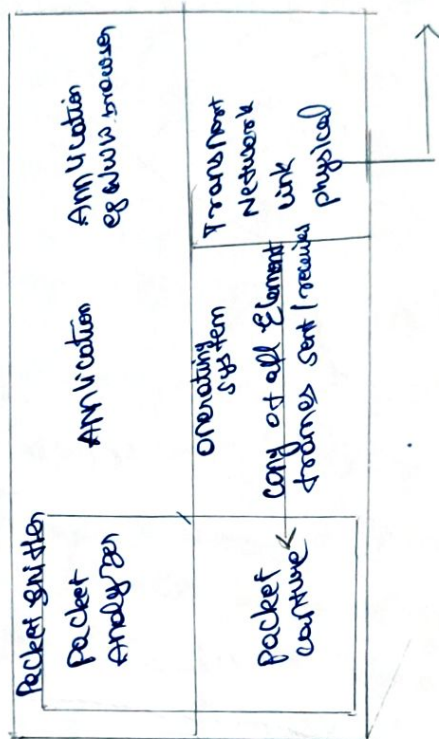
Tcp dump:

Eg: Apcdump - exe host

10.129.41.2-W

Wire Shark

wire shark - r exe 3 - out



Section	Range	County	Acres	Value
1	10	Clark	100	100.00
2	10	Clark	100	100.00
3	10	Clark	100	100.00
4	10	Clark	100	100.00
5	10	Clark	100	100.00
6	10	Clark	100	100.00
7	10	Clark	100	100.00
8	10	Clark	100	100.00
9	10	Clark	100	100.00
10	10	Clark	100	100.00
11	10	Clark	100	100.00
12	10	Clark	100	100.00
13	10	Clark	100	100.00
14	10	Clark	100	100.00
15	10	Clark	100	100.00
16	10	Clark	100	100.00
17	10	Clark	100	100.00
18	10	Clark	100	100.00
19	10	Clark	100	100.00
20	10	Clark	100	100.00
21	10	Clark	100	100.00
22	10	Clark	100	100.00
23	10	Clark	100	100.00
24	10	Clark	100	100.00
25	10	Clark	100	100.00
26	10	Clark	100	100.00
27	10	Clark	100	100.00
28	10	Clark	100	100.00
29	10	Clark	100	100.00
30	10	Clark	100	100.00
31	10	Clark	100	100.00
32	10	Clark	100	100.00
33	10	Clark	100	100.00
34	10	Clark	100	100.00
35	10	Clark	100	100.00
36	10	Clark	100	100.00
37	10	Clark	100	100.00
38	10	Clark	100	100.00
39	10	Clark	100	100.00
40	10	Clark	100	100.00
41	10	Clark	100	100.00
42	10	Clark	100	100.00
43	10	Clark	100	100.00
44	10	Clark	100	100.00
45	10	Clark	100	100.00
46	10	Clark	100	100.00
47	10	Clark	100	100.00
48	10	Clark	100	100.00
49	10	Clark	100	100.00
50	10	Clark	100	100.00
51	10	Clark	100	100.00
52	10	Clark	100	100.00
53	10	Clark	100	100.00
54	10	Clark	100	100.00
55	10	Clark	100	100.00
56	10	Clark	100	100.00
57	10	Clark	100	100.00
58	10	Clark	100	100.00
59	10	Clark	100	100.00
60	10	Clark	100	100.00
61	10	Clark	100	100.00
62	10	Clark	100	100.00
63	10	Clark	100	100.00
64	10	Clark	100	100.00
65	10	Clark	100	100.00
66	10	Clark	100	100.00
67	10	Clark	100	100.00
68	10	Clark	100	100.00
69	10	Clark	100	100.00
70	10	Clark	100	100.00
71	10	Clark	100	100.00
72	10	Clark	100	100.00
73	10	Clark	100	100.00
74	10	Clark	100	100.00
75	10	Clark	100	100.00
76	10	Clark	100	100.00
77	10	Clark	100	100.00
78	10	Clark	100	100.00
79	10	Clark	100	100.00
80	10	Clark	100	100.00
81	10	Clark	100	100.00
82	10	Clark	100	100.00
83	10	Clark	100	100.00
84	10	Clark	100	100.00
85	10	Clark	100	100.00
86	10	Clark	100	100.00
87	10	Clark	100	100.00
88	10	Clark	100	100.00
89	10	Clark	100	100.00
90	10	Clark	100	100.00
91	10	Clark	100	100.00
92	10	Clark	100	100.00
93	10	Clark	100	100.00
94	10	Clark	100	100.00
95	10	Clark	100	100.00
96	10	Clark	100	100.00
97	10	Clark	100	100.00
98	10	Clark	100	100.00
99	10	Clark	100	100.00
100	10	Clark	100	100.00

1990

Process 1: 250 bytes on wire (2000 bps), 10 bytes captured (2000 bps) on interface Device001, packet 1
 Ethernet II, Src: IntelRealtek_00:0C:29:3A:2D:42, Dst: 00:0C:29:3A:2D:42 (00:0C:29:3A:2D:42)
 Internet Protocol Version 4, Src: 192.168.1.10, Dst: 12.34.5.67
 Transmission Control Protocol, Src Port: 8080, Dst Port: 443, Seq: 1, Ack: 407, Len: 259
 Hypertext Transfer Protocol

[illegible][illegible]

Flow graph:

GenBank record for the complete genome of a virus. The record shows a single contig of 12,176,326 bp. The sequence is annotated with various features, including ORFs, CDS, and protein-coding regions. The sequence is displayed in a table format with columns for coordinates, sequence, and annotations. The sequence is shown in a single line, with the coordinates and sequence wrapped around. The annotations are listed on the right side of the table.

No.	dns	Source	Destination	Protocol	Length	Info
	dnserver	192.168.101.41	192.168.101.84	DNS	90	STA
2	0.028851	48.218.107.40	192.168.101.41	TLSv1.2	482	App
3	0.028851	52.123.178.24	192.168.101.41	TLSv1.2	92	App
4	0.028851	52.123.178.24	192.168.101.41	TCP	54	562
5	0.028974	192.168.101.41	48.218.107.40	TLSv1.2	319	App
6	0.032513	192.168.101.41	48.218.107.40	TLSv1.2	110	App
7	0.032843	192.168.101.41	48.218.107.40	TLSv1.2	293	App
8	0.038276	64:ff9b::d6b:380	2409:408d:38d:33bc::	TLSv1.2	173	App
9	0.039494	192.168.101.41	52.123.178.24	TLSv1.2		

No.	Time	Source	Destination	Protocol	Length	Info
10	0.040000	192.168.101.41	192.168.101.84	DNS	90	STA
11	0.040000	192.168.101.41	192.168.101.84	DNS	90	STA
12	0.040000	192.168.101.41	192.168.101.84	DNS	90	STA
13	0.040000	192.168.101.41	192.168.101.84	DNS	90	STA
14	0.040000	192.168.101.41	192.168.101.84	DNS	90	STA
15	0.040000	192.168.101.41	192.168.101.84	DNS	90	STA
16	0.040000	192.168.101.41	192.168.101.84	DNS	90	STA
17	0.040000	192.168.101.41	192.168.101.84	DNS	90	STA
18	0.040000	192.168.101.41	192.168.101.84	DNS	90	STA
19	0.040000	192.168.101.41	192.168.101.84	DNS	90	STA
20	0.040000	192.168.101.41	192.168.101.84	DNS	90	STA

No.	Time	Source	Destination	Protocol	Length	Info
21	0.040000	192.168.101.41	192.168.101.84	DNS	90	STA
22	0.040000	192.168.101.41	192.168.101.84	DNS	90	STA
23	0.040000	192.168.101.41	192.168.101.84	DNS	90	STA
24	0.040000	192.168.101.41	192.168.101.84	DNS	90	STA
25	0.040000	192.168.101.41	192.168.101.84	DNS	90	STA
26	0.040000	192.168.101.41	192.168.101.84	DNS	90	STA
27	0.040000	192.168.101.41	192.168.101.84	DNS	90	STA
28	0.040000	192.168.101.41	192.168.101.84	DNS	90	STA
29	0.040000	192.168.101.41	192.168.101.84	DNS	90	STA
30	0.040000	192.168.101.41	192.168.101.84	DNS	90	STA

No.	Time	Source	Destination	Protocol	Length	Info
31	0.040000	192.168.101.41	192.168.101.84	DNS	90	STA
32	0.040000	192.168.101.41	192.168.101.84	DNS	90	STA
33	0.040000	192.168.101.41	192.168.101.84	DNS	90	STA
34	0.040000	192.168.101.41	192.168.101.84	DNS	90	STA
35	0.040000	192.168.101.41	192.168.101.84	DNS	90	STA
36	0.040000	192.168.101.41	192.168.101.84	DNS	90	STA
37	0.040000	192.168.101.41	192.168.101.84	DNS	90	STA
38	0.040000	192.168.101.41	192.168.101.84	DNS	90	STA
39	0.040000	192.168.101.41	192.168.101.84	DNS	90	STA
40	0.040000	192.168.101.41	192.168.101.84	DNS	90	STA

Students observation:

1) What is Promiscuous mode?
Promiscuous mode is a welcome interface card (NIC) setting that allows card to intercept and read all network packets on network segments.

2) Does ARP packets has transport layer header? Explain
No, ARP packets does not have transport layer header.

3) which transport layer protocol is used by DNS?

DNS (Domain name system) primarily uses UDP for its transport layer protocol.

4) What is the port number used http protocol?
HTTP protocol uses port number 80 by default.

5)

What is broadcast IP address?

It is a broadcast IP address which is used to send packets to all devices on a specific network segment.

Result:

Thus the packet capturing and flow graph are filtering and wire shark observed using.

~~8/18/24~~