

ITA1443-Ethical Hacking For Legal Systems

Name: R.Surya

Reg.No:192011244

Slot: D

Exercise No 10: WireShark sniffer

The screenshot displays the Wireshark Network Analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. The main window is divided into several panes:

- Welcome to Wireshark**: A section with an "Open" button and a list of recent files: C:\Users\hp\Documents\3.pcapng (128 KB), C:\Users\hp\Documents\2.pcapng (215 KB), and C:\Users\hp\Documents\1.pcapng (6950 KB).
- Capture**: A section with a "Capture" button and a list of network interfaces. The "Wi-Fi" interface is selected, and the "Adapter for loopback traffic capture" is also visible.
- Learn**: A section with links to "User's Guide", "Wiki", "Questions and Answers", "Mailing Lists", "SharkFest", "Wireshark Discard", and "Donate".

The bottom pane shows the "Ready to load or capture" status. The "No Packets" indicator is present. The "Profile: Default" is selected. The "Capturing from Wi-Fi" status is shown. The "Apply a display filter" field is empty. The "Packets: 341 - Displayed: 341 (100.0%)" indicator is present.

The packet list pane shows the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
326	6.466587	10.200.48.219	239.255.255.250	SSDP	164	M-SEARCH * HTTP/1.1
327	6.466584	10.200.51.05	10.200.51.255	NBNS	92	Name query NB BALU2027<1c>
328	6.469299	10.200.48.219	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
329	6.529048	10.200.50.205	224.0.0.251	MDNS	103	Standard query 0x0012 PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM"
330	6.531756	10.200.50.190	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
331	6.558766	10.200.51.40	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
332	6.632317	ee:53:24:c7:62:29	CloudNet_b3:01:0f	ARP	56	Who has 10.200.48.1? Tell 10.200.51.60
333	6.660998	10.200.49.25	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
334	6.704525	10.200.51.39	224.0.0.251	MDNS	103	Standard query 0x0016 PTR _B4C3FAD4._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM"
335	6.800425	10.200.50.24	224.0.0.251	MDNS	291	Standard query response 0x0000 PTR, cache flush Android-58.local PTR, cache flush Android-58.local A, cache flu...
336	6.800821	fe80::dc09:c3ff:fe4...	ff02::fb	MDNS	311	Standard query response 0x0000 PTR, cache flush Android-58.local PTR, cache flush Android-58.local A, cache flu...
337	6.856961	10.200.51.40	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
338	6.872794	10.200.51.98	23.44.11.248	TCP	55	[TCP Retransmission] 61002 -> 443 [ACK] Seq=0 Ack=1 Win=513 Len=1
339	6.878269	23.44.11.248	10.200.51.98	TCP	56	443 -> 61002 [ACK] Seq=1 Ack=1 Win=501 Len=0
340	6.895606	10.200.50.236	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
341	7.079483	10.200.51.98	88.235.206.159	UDP	62	43725 -> 49328 Len=20

The packet details pane shows the following information for the selected packet (Frame 1):

- Frame 1: 167 bytes on wire (1336 bits), 167 bytes captured (1336 bits) on interface \Device\NPF...
- Ethernet II, Src: 26:35:3d:a0:7a:a3 (26:35:3d:a0:7a:a3), Dst: CloudNet_b3:01:0f (90:0f:0c:b3:01:0f)
- Internet Protocol Version 4, Src: 10.200.48.110, Dst: 239.255.255.250
- User Datagram Protocol, Src Port: 48508, Dst Port: 1900
- Simple Service Discovery Protocol

The packet bytes pane shows the raw data of the packet, including the Ethernet II header, IP header, and SSDP payload.

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
26099	226.938066	180.235.121.242	10.200.51.98	HTTP	900	HTTP/1.1 200 OK (f
26276	230.436808	10.200.51.98	180.235.121.242	HTTP	218	POST / HTTP/1.1 (f
26280	230.534230	180.235.121.242	10.200.51.98	HTTP	900	HTTP/1.1 200 OK (f
27041	243.220412	10.200.51.98	180.235.121.242	HTTP	218	POST / HTTP/1.1 (f
27081	243.269707	180.235.121.242	10.200.51.98	HTTP	900	HTTP/1.1 200 OK (f
27726	256.505528	10.200.51.98	180.235.121.242	HTTP	224	POST / HTTP/1.1 (f
27736	256.554034	180.235.121.242	10.200.51.98	HTTP	900	HTTP/1.1 200 OK (f
28256	264.849773	10.200.51.98	180.235.121.242	HTTP	222	POST / HTTP/1.1 (f
28274	264.898031	180.235.121.242	10.200.51.98	HTTP	900	HTTP/1.1 200 OK (f
31649	327.799520	10.200.51.98	180.235.121.242	HTTP	224	POST / HTTP/1.1 (f
31669	327.849158	180.235.121.242	10.200.51.98	HTTP	900	HTTP/1.1 200 OK (f
35062	395.187408	10.200.51.98	180.235.121.242	HTTP	215	POST / HTTP/1.1 (f
35107	395.297999	180.235.121.242	10.200.51.98	HTTP	899	HTTP/1.1 200 OK (f
35328	402.035231	10.200.51.98	180.235.121.242	HTTP	211	POST / HTTP/1.1 (f
35343	402.132350	180.235.121.242	10.200.51.98	HTTP	899	HTTP/1.1 200 OK (f

Value: PHlo+yQ+EFGDxwF8zposiL+uukB18p
Form item: "_VIEWSTATEGENERATOR" = "C2EE
Key: _VIEWSTATEGENERATOR
Value: C2EE9A8B
Form item: "_EVENTVALIDATION" = "mmuH7gA
Key: _EVENTVALIDATION
Value: mmuH7gAr3QpPFuhzPk31RG6fQz9uU
Form item: "txtusername" = "admin"
Key: txtusername
Value: admin
Form item: "txtpassword" = "1234567890"
Key: txtpassword
Value: 1234567890
Form item: "btnlogin" = "Login"
Key: btnlogin
Value: Login

0390 4e 45 52 41 54 4f 52 3d 43 32 45 45 39
03a0 26 5f 5f 45 56 45 4e 54 56 41 4c 49 44
03b0 4f 4e 3d 6d 6d 75 4e 37 67 41 72 33 51
03c0 55 68 7a 58 6b 4a 31 52 47 36 66 6f 52
03d0 75 55 64 77 74 78 65 30 4d 61 53 68 61
03e0 44 37 45 7a 68 41 54 44 66 38 34 75 58
03f0 79 72 4a 57 4a 42 45 52 66 71 70 6f 48
0400 61 75 25 32 42 36 37 79 4b 34 47 66 48
0410 68 50 71 79 79 59 43 57 66 25 32 42 68
0420 6f 69 30 54 4f 63 66 54 75 36 53 52 52
0430 75 50 54 75 45 41 42 4a 59 67 73 7a 39
0440 48 54 49 30 67 6c 36 75 32 4d 4c 62 70
0450 6e 33 59 30 6d 31 35 46 68 77 43 56 6f
0460 7a 55 25 33 44 26 74 78 74 75 73 65 72
0470 65 3d 61 64 6d 69 6e 26 74 78 74 70 61
0480 6f 72 64 3d 31 32 33 34 35 36 37 38 39
0490 74 6e 6c 6f 67 69 6c 3d 4c 6f 67 69 6e

Frame (211 bytes) Reassembled TCP (1181 bytes)

Text item (text), 14 bytes

Packets: 38977 Displayed: 80 (0.2%) Profile: Default

86°F Sunny

Saveetha University

Not secure | http://ams.sse... | Paused

YUKTI-National Inn... OOAD GITHUB LIN... RSurya369/ITA1443...

SAVEETHA SCHOOL OF ENGINEERING

Sign In

admin

The username and password you entered is invalid

LOGIN

ENG IN 17:45 10-02-2023