

ITA1443-Ethical Hacking For Legal Systems

Model Practical Examination

Name: R. Surya

RegNo: 192011244

Slot: D

Qus3:

The image displays two side-by-side screenshots from a Windows desktop. The left screenshot shows a Wi-Fi network traffic capture in Wireshark. The right screenshot shows a web browser displaying the login page of Saveetha University.

Wireshark Traffic Capture:

No.	Time	Source	Destination	Protocol	Length	Info
4432	124.362648	49.44.116.238	192.168.239.110	HTTP	233	HTTP/1.1 200 OK (1
7303	340.512973	206.221.176.14	192.168.239.110	HTTP	363	HTTP/1.1 400 Bad Re
7387	352.990482	192.168.239.110	23.92.17.15	HTTP	405	GET /announce?info
7408	355.868502	23.92.17.15	192.168.239.110	HTTP	1422	HTTP/1.1 200 OK (1
8466	419.175324	192.168.239.110	13.107.4.52	HTTP	208	GET /connecttest.t
8469	419.189358	2409:4072:58e:a746::	2a01:111:2003::52	HTTP	229	GET /connecttest.t
8478	419.560041	13.107.4.52	192.168.239.110	HTTP	593	HTTP/1.1 200 OK (1
8483	419.567065	2a01:111:2003::52	2409:4072:58e:a746::	HTTP	613	HTTP/1.1 200 OK (1
11775	611.360494	199.127.63.144	192.168.239.110	HTTP	381	HTTP/1.1 400 Bad Re
13099	730.743021	192.168.239.110	49.44.116.238	HTTP	178	GET /ncsi.txt HTTP
13103	730.946073	49.44.116.238	192.168.239.110	HTTP	233	HTTP/1.1 200 OK (1
15311	864.281115	206.221.176.14	192.168.239.110	HTTP	363	HTTP/1.1 400 Bad Re
15408	869.584993	103.195.100.93	192.168.239.110	HTTP	363	HTTP/1.1 400 Bad Re
18439	1117.516507	206.221.176.14	192.168.239.110	HTTP	363	HTTP/1.1 400 Bad Re
18868	1141.276672	172.96.140.32	192.168.239.110	HTTP	363	HTTP/1.1 400 Bad Re

Web Browser (Saveetha University):

The browser shows the login page of Saveetha University. The URL bar displays <https://arms.sse.saveetha.com/L...>. The page features the Saveetha School of Engineering logo and a "Sign In" button. Below the logo, there is a login form with fields for "Username" (containing "192011244") and "Password" (containing "*****"). A red error message below the form states: "The username and password you entered is invalid". A green "LOGIN" button is visible at the bottom of the form.

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
4432	124.362648	49.44.116.238	192.168.239.110	HTTP	233	HTTP/1.1 200 OK (text/html)
7303	340.512973	206.221.176.14	192.168.239.110	HTTP	363	HTTP/1.1 400 Bad Request
7307	352.990462	192.168.239.110	23.92.17.15	HTTP	405	GET /announce?info=
7408	355.868502	23.92.17.15	192.168.239.110	HTTP	1422	HTTP/1.1 200 OK (text/html)
8466	419.175324	192.168.239.110	13.107.4.52	HTTP	208	GET /connecttest.txt
8469	419.189358	2409:4072:58e:a746::	2a01:111:2003::52	HTTP	229	GET /connecttest.txt
8478	419.560041	13.107.4.52	192.168.239.110	HTTP	593	HTTP/1.1 200 OK (text/html)
8483	419.567065	2a01:111:2003::52	2409:4072:58e:a746::	HTTP	613	HTTP/1.1 200 OK (text/html)
11775	611.360494	199.127.63.144	192.168.239.110	HTTP	381	HTTP/1.1 400 Bad Request
13099	730.743821	192.168.239.110	49.44.116.238	HTTP	178	GET /ncsi.txt HTTP/1.1
13103	730.946073	49.44.116.238	192.168.239.110	HTTP	233	HTTP/1.1 200 OK (text/html)
15311	864.281115	206.221.176.14	192.168.239.110	HTTP	363	HTTP/1.1 400 Bad Request
15408	869.584993	103.195.100.93	192.168.239.110	HTTP	363	HTTP/1.1 400 Bad Request
18439	1117.516507	206.221.176.14	192.168.239.110	HTTP	363	HTTP/1.1 400 Bad Request
18868	1141.276672	172.96.140.32	192.168.239.110	HTTP	363	HTTP/1.1 400 Bad Request

[Window size scaling factor: 128]
Checksum: 0x2aa5 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> [Timestamps]
> [SEQ/ACK analysis]
TCP payload (309 bytes)
Hypertext Transfer Protocol
> [Expert Info (Warning/Security): Unencrypted]
> HTTP/1.1 400 Bad Request\r\nServer: nginx/1.22.1\r\nDate: Mon, 13 Feb 2023 08:24:43 GMT\r\nContent-Type: text/html\r\nContent-Length: 157\r\nConnection: close\r\n\r\n

0030 01 f5 2a a5 00 00 48 54 54 50 2f 31 2e
0040 30 30 20 42 61 64 20 52 65 71 75 65 73
0050 53 65 72 76 65 72 3a 20 6e 67 69 6e 78
0060 32 32 2e 31 0d 0a 44 61 74 65 3a 20 4d
0070 20 31 33 20 46 65 62 20 32 30 32 33 20
0080 32 34 3a 34 33 20 47 4d 54 0d 0a 43 6f
0090 6e 74 2d 54 79 70 65 3a 20 74 65 78 74
00a0 6d 6c 0d 0a 43 6f 6e 74 65 6e 74 2d 4c
00b0 74 68 3a 20 31 35 37 0d 0a 43 6f 6e 6e
00c0 69 6f 6e 3a 20 63 6c 6f 73 65 0d 0a 0d
00d0 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c
00e0 6c 65 3e 34 30 30 20 42 61 64 20 52 65
00f0 73 74 3c 2f 74 69 74 6c 65 3e 3c 2f 68
0100 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63
0110 65 72 3e 3c 68 31 3e 34 30 30 20 42 61
0120 65 71 75 65 73 74 3c 2f 68 31 3e 3c 2f
0130 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65
0140 72 3e 6e 67 69 6e 78 2f 31 2e 32 32 2e
0150 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f
0160 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a

Hypertext Transfer Protocol (http), 152 bytes

Packets: 19198 - Displayed: 18 (0.1%) Profile: Default

90°F Sunny

Saveetha University

https://arms.sse.saveetha.com/L...

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

SAVEETHA SCHOOL OF ENGINEERING

Sign In

192011244

The username and password you entered is invalid

LOGIN

ENG IN 13:55 13-02-2023

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
4432	124.362648	49.44.116.238	192.168.239.110	HTTP	233	HTTP/1.1 200 OK (text/html)
7303	340.512973	206.221.176.14	192.168.239.110	HTTP	363	HTTP/1.1 400 Bad Request
7307	352.990462	192.168.239.110	23.92.17.15	HTTP	405	GET /announce?info=
7408	355.868502	23.92.17.15	192.168.239.110	HTTP	1422	HTTP/1.1 200 OK (text/html)
8466	419.175324	192.168.239.110	13.107.4.52	HTTP	208	GET /connecttest.txt
8469	419.189358	2409:4072:58e:a746::	2a01:111:2003::52	HTTP	229	GET /connecttest.txt
8478	419.560041	13.107.4.52	192.168.239.110	HTTP	593	HTTP/1.1 200 OK (text/html)
8483	419.567065	2a01:111:2003::52	2409:4072:58e:a746::	HTTP	613	HTTP/1.1 200 OK (text/html)
11775	611.360494	199.127.63.144	192.168.239.110	HTTP	381	HTTP/1.1 400 Bad Request
13099	730.743821	192.168.239.110	49.44.116.238	HTTP	178	GET /ncsi.txt HTTP/1.1
13103	730.946073	49.44.116.238	192.168.239.110	HTTP	233	HTTP/1.1 200 OK (text/html)
15311	864.281115	206.221.176.14	192.168.239.110	HTTP	363	HTTP/1.1 400 Bad Request
15408	869.584993	103.195.100.93	192.168.239.110	HTTP	363	HTTP/1.1 400 Bad Request
18439	1117.516507	206.221.176.14	192.168.239.110	HTTP	363	HTTP/1.1 400 Bad Request
18868	1141.276672	172.96.140.32	192.168.239.110	HTTP	363	HTTP/1.1 400 Bad Request

[Window size scaling factor: 128]
Checksum: 0x020b [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> [Timestamps]
> [SEQ/ACK analysis]
TCP payload (309 bytes)
Hypertext Transfer Protocol
> Line-based text data: text/html (7 lines)
<html>\r\n<head><title>400 Bad Request</title></head>\r\n<body>\r\n<center><h1>400 Bad Request</h1></center>\r\n<hr><center>nginx/1.22.1</center>\r\n</body>\r\n</html>\r\n

0050 53 65 72 76 65 72 3a 20 6e 67 69 6e 78
0060 32 32 2e 31 0d 0a 44 61 74 65 3a 20 4d
0070 20 31 33 20 46 65 62 20 32 30 32 33 20
0080 32 30 3a 30 36 20 47 4d 54 0d 0a 43 6f
0090 6e 74 2d 54 79 70 65 3a 20 74 65 78 74
00a0 6d 6c 0d 0a 43 6f 6e 74 65 6e 74 2d 4c
00b0 74 68 3a 20 31 35 37 0d 0a 43 6f 6e 6e
00c0 69 6f 6e 3a 20 63 6c 6f 73 65 0d 0a 0d
00d0 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c
00e0 6c 65 3e 34 30 30 20 42 61 64 20 52 65
00f0 73 74 3c 2f 74 69 74 6c 65 3e 3c 2f 68
0100 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63
0110 65 72 3e 3c 68 31 3e 34 30 30 20 42 61
0120 65 71 75 65 73 74 3c 2f 68 31 3e 3c 2f
0130 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65
0140 72 3e 6e 67 69 6e 78 2f 31 2e 32 32 2e
0150 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f
0160 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a

Line-based text data (data-text-lines), 157 bytes

Packets: 18987 - Displayed: 18 (0.1%) Profile: Default

90°F Sunny

Saveetha University

https://arms.sse.saveetha.com/L...

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

SAVEETHA SCHOOL OF ENGINEERING

Sign In

192011244

The username and password you entered is invalid

LOGIN

ENG IN 13:54 13-02-2023

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter -<Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
32545	2372.713444	192.168.239.110	154.6.88.149	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 64087 → 51413 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P...
32546	2372.722225	103.170.178.14	192.168.239.110	UDP	62	6881 → 43725 Len=20
32547	2372.728197	103.170.178.14	192.168.239.110	UDP	364	6881 → 43725 Len=322
32548	2372.728414	192.168.239.110	103.170.178.14	UDP	62	43725 → 6881 Len=20
32549	2372.728733	192.168.239.110	103.170.178.14	UDP	1480	43725 → 6881 Len=1438
32550	2372.932281	195.230.4.169	192.168.239.110	BT-DHT	331	BitTorrent DHT Protocol reply=0 nodes
32551	2372.932694	192.168.239.110	103.170.178.14	UDP	62	43725 → 6881 Len=20
32552	2373.125200	192.168.239.110	185.21.217.50	TCP	1424	[TCP Retransmission] 64073 → 58851 [PSH, ACK] Seq=187 Ack=384 Win=65280 Len=1370
32553	2373.241304	206.251.216.51	192.168.239.110	TCP	59	[TCP Window Full] [TCP Spurious Retransmission] 45077 → 64084 [PSH, ACK] Seq=318 Ack=183 Win=64256 Len=5
32554	2373.588446	192.168.239.110	136.35.216.144	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 64070 → 2099 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P...
32555	2373.588547	192.168.239.110	49.196.207.34	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 64071 → 47948 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P...
32556	2373.588570	192.168.239.110	176.241.44.212	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 64072 → 7352 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P...
32557	2373.589389	192.168.239.110	27.34.50.82	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 64075 → 44930 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P...
32558	2373.589463	192.168.239.110	223.65.130.103	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 64076 → 49160 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P...
32559	2373.877183	192.168.239.110	103.170.178.14	UDP	1480	43725 → 6881 Len=1438
32560	2374.564614	192.168.239.110	45.227.67.142	BT-DHT	145	BitTorrent DHT Protocol

> [Expert Info (Warning/Security): Unencrypted HTTP protocol detected over encrypted port, HTTP/1.1 400 Bad Request\r\n

> [Expert Info (Chat/Sequence): HTTP/1.1 400 Bad Request\r\n

Response Version: HTTP/1.1

Status Code: 400

[Status Code Description: Bad Request]

Response Phrase: Bad Request

Server: nginx/1.22.1\r\n

Date: Mon, 13 Feb 2023 08:24:43 GMT\r\n

Content-Type: text/html\r\n

Content-Length: 157\r\n

Connection: close\r\n

\r\n

[HTTP response 1/1]

File Data: 157 bytes

> Line-based text data: text/html (7 lines)

0040 30 30 20 42 61 64 20 52 65 71 75 65 73 74 0d 0a 00 Bad R equest:
0050 53 65 72 76 65 72 3a 20 6e 67 69 6e 78 2f 31 2e Server: nginx/1.
0060 32 32 2e 31 0d 0a 44 61 74 65 3a 20 4d 6f 6e 3c 22.1. Da te: Mon,
0070 20 31 33 20 46 65 62 20 32 30 32 33 20 30 38 3a 13 Feb 2023 08:
0080 32 34 3a 3a 33 20 47 4d 54 0d 0a 43 6f 6e 74 65 24:43 GM T: Conte
0090 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 68 74 nt-Type: text/ht
00a0 6d 6c 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 ml: Cont ent-Leng
00b0 74 68 3a 20 31 35 37 0d 0a 43 6f 6e 6e 65 63 74 th: 157 -Connect
00c0 69 6f 6e 3a 20 63 6c 6f 73 65 0d 0a 0d 0a 3c 68 ion: clo se -<ch
00d0 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 tml>-<h ead>tit
00e0 6c 65 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 le>400 B ad Reque
00f0 73 74 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 st</titl e></head
0100 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 >>>body >>><cent
0110 65 72 3e 3c 68 31 3e 34 30 30 20 42 61 64 20 52 er><h1>4 00 Bad R
0120 65 71 75 65 73 74 3c 2f 68 31 3e 3c 2f 63 65 6e equest</ h1></cen
0130 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 ter>>><h r><cente
0140 72 3e 6e 67 69 6e 78 2f 31 2e 32 2e 31 3c 2f r>nginx/ 1.22.1</
0150 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e cent>-</body>
0160 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a <</html> >>>

Line-based text data (data-text-lines), 157 bytes

Packets: 32560 · Displayed: 32560 (100.0%)

Profile: Default

90°F Sunny

Search

99%

ENG IN

14:15 13-02-2023