

## Report: Week 2: Exploitation, Web Application Testing, and Advanced Networking

### Lab 7: Practical Use Cases for Wireshark in Real-World Scenarios.

Report Summary of the incident.

Timeline of events: 12 November 2024

Exercise 1:

- Describe the overall network traffic during the incident. Are there any noticeable spikes or anomalies? What potential indicators of compromise did you identify?

As the incident response team, a network traffics were analysis on both suspect IP address 192.168.60.208, source port 33632 and destination port 80. No suspicious activities were found, and no potential compromise was identified while analyzing the packet.

The screenshot displays the Wireshark interface with a packet capture of 'incident\_response.pcapng'. The filter 'ip.addr == 192.168.60.208' is applied. The packet list shows a series of DNS queries and responses between 192.168.60.208 and 10.0.2.15. Packet 3506 is selected, showing a DNS standard query response for 'c.amazon-adsystem.com CNAME d1y...'. The packet details pane shows the DNS structure, including the question section for 'c.amazon-adsystem.com. type A class IN' and the answer section. The packet bytes pane shows the raw data in hexadecimal and ASCII. The status bar at the bottom indicates 8934 packets displayed, with 626 (7.0%) displayed and 0 (0.0%) dropped.

No.	Time	Source	Destination	Protocol	Length	Info
3452	313.576644351	192.168.60.208	10.0.2.15	DNS	128	Standard query response 0x2bd9 AAAA web.facebook.com CNAME star...
3490	314.249202017	10.0.2.15	192.168.60.208	DNS	76	Standard query 0xb5d1 A unagi.amazon.com
3491	314.253995187	10.0.2.15	192.168.60.208	DNS	76	Standard query 0x40dd AAAA unagi.amazon.com
3492	314.289235652	192.168.60.208	10.0.2.15	DNS	174	Standard query response 0x40dd AAAA unagi.amazon.com CNAME unagi...
3493	314.298585626	192.168.60.208	10.0.2.15	DNS	364	Standard query response 0xb5d1 A unagi.amazon.com CNAME unagi-na...
3499	314.308905637	10.0.2.15	192.168.60.208	DNS	81	Standard query 0xc62b A c.amazon-adsystem.com
3500	314.310093713	10.0.2.15	192.168.60.208	DNS	81	Standard query 0x5216 AAAA c.amazon-adsystem.com
3506	314.335325918	192.168.60.208	10.0.2.15	DNS	273	Standard query response 0xc62b A c.amazon-adsystem.com CNAME d1y...
3507	314.341171952	192.168.60.208	10.0.2.15	DNS	202	Standard query response 0x5216 AAAA c.amazon-adsystem.com CNAME ...
3649	315.163077952	10.0.2.15	192.168.60.208	DNS	79	Standard query 0xf3e7 A static.xx.fbcdn.net
3650	315.170486964	10.0.2.15	192.168.60.208	DNS	79	Standard query 0x7eed AAAA static.xx.fbcdn.net
3653	315.181851301	10.0.2.15	192.168.60.208	DNS	72	Standard query 0xeb4d A facebook.com
3654	315.182330867	10.0.2.15	192.168.60.208	DNS	72	Standard query 0x644f AAAA facebook.com

... .. = Truncated: Message is not truncated  
... .. = Recursion desired: Do query recursively  
... .. 1... .. = Recursion available: Server can do recursive queries  
... .. .0.. .. = Z: reserved (0)  
... .. .0. .... = Answer authenticated: Answer/authority portion was not authenticated by the  
... .. .0 .... = Non-authenticated data: Unacceptable  
... .. .0000 = Reply code: No error (0)  
Questions: 1  
Answer RRs: 2  
Authority RRs: 4  
Additional RRs: 0  
Queries  
c.amazon-adsystem.com. type A class IN

0030 00 02 00 04 00 00 01 63 0f 61 6d 61  
0040 61 64 73 79 73 74 65 6d 03 63 6f 6d  
0050 01 c0 0c 00 05 00 01 00 00 01 91 00  
0060 79 6b 66 30 37 65 37 35 77 37 73 73  
0070 75 64 66 72 6f 6e 74 03 6e 65 74 00  
0080 00 01 00 00 00 2b 00 04 6c 8b c4 7b  
0090 00 01 00 00 04 fe 00 17 07 6e 73 2d  
00a0 09 61 77 73 64 6e 73 2d 36 32 03 6f  
00b0 33 00 02 00 01 00 00 04 fe 00 19 07  
00c0 37 36 33 09 61 77 73 64 6e 73 2d 32  
00d0 02 75 6b 00 c0 33 00 02 00 01 00 00  
00e0 06 6e 73 2d 37 39 33 09 61 77 73 64

Text item (text), 27 bytes  
Packets: 8934 · Displayed: 626 (7.0%) · Dropped: 0 (0.0%) · Profile: Default

Wireshark · Follow TCP Stream (tcp.stream eq 3) · incident Response.pcapng

```

POST /wr2 HTTP/1.1
Host: o.pki.goog
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/ocsp-request
Content-Length: 84
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache

0R0P0N0L0J0 ...+.....SB.....Mw|. #1.{5.....y..>7$.!..49mB.0.....).4.....1...QHTTP/1
.1 200 OK
Content-Type: application/ocsp-response
Date: Tue, 12 Nov 2024 10:52:32 GMT
Cache-Control: public, max-age=14400
Server: ocsp_responder
Content-Length: 472
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN

0...
.....0..... +.....0.....0.....0.....y..>7$.!..49mB.0..20241111124441Z0t0r0J0 ...+....
.....SB.....Mw|. #1.{5.....y..>7$.!..49mB.0.....).4.....1...Q.....20241111124441Z....20241118
114440Z0

```

Packet 465. 7 client pkts, 7 server pkts, 13 turns. Click to select.

Entire conversation (8,212 bytes) Show data as ASCII Stream 3

Find: Find Next

incident Response.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 3

No.	Time	Source	Destination	Protocol	Length	Info
444	279.847538892	10.0.2.15	142.250.184.163	TCP	74	33632 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=...
460	279.855163115	142.250.184.163	10.0.2.15	TCP	60	80 → 33632 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
461	279.855233778	10.0.2.15	142.250.184.163	TCP	54	33632 → 80 [ACK] Seq=1 Ack=1 Win=32120 Len=0
465	279.859928966	10.0.2.15	142.250.184.163	OCSP	467	Request
466	279.860824445	142.250.184.163	10.0.2.15	TCP	60	80 → 33632 [ACK] Seq=1 Ack=414 Win=65535 Len=0
487	279.413023935	142.250.184.163	10.0.2.15	OCSP	756	Response
488	279.413057756	10.0.2.15	142.250.184.163	TCP	54	33632 → 80 [ACK] Seq=414 Ack=703 Win=31590 Len=0
621	280.340414534	10.0.2.15	142.250.184.163	OCSP	466	Request
622	280.341147676	142.250.184.163	10.0.2.15	TCP	60	80 → 33632 [ACK] Seq=703 Ack=826 Win=65535 Len=0
650	280.644526529	142.250.184.163	10.0.2.15	OCSP	755	Response
653	280.644696318	10.0.2.15	142.250.184.163	TCP	54	33632 → 80 [ACK] Seq=826 Ack=1404 Win=31590 Len=0
663	280.686051866	10.0.2.15	142.250.184.163	OCSP	467	Request
664	280.687574949	142.250.184.163	10.0.2.15	TCP	60	80 → 33632 [ACK] Seq=1404 Ack=1239 Win=65535 Len=0

Frame 444: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0

Ethernet II, Src: PCSSystemtec\_d2:48:cb (08:00:27:d2:48:cb), Dst: 52:54:00:12:35:02 (52:54:00:12:35:02)

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 142.250.184.163

Transmission Control Protocol, Src Port: 33632, Dst Port: 80, Seq: 0, Len: 0

Source Port: 33632

Destination Port: 80

[Stream index: 3]

[Conversation completeness: Incomplete, DATA (15)]

[TCP Segment Len: 0]

Sequence Number: 0 (relative sequence number)

Sequence Number (raw): 3362228696

[Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 0

## Exercise 2:

- Identify a specific packet that raises suspicion. Provide details about the packet, including source and destination IPs, ports, and protocol. What makes this packet suspicious?

A failed login attempts on Facebook.com source IP 192.168.60.208, and destination IP is 10.0.2.15, the source and destination ports are 53 and 50339, the protocol is DNS. The reason for suspicion is because of the login failure

The image shows a Wireshark packet capture of DNS traffic. The top pane displays a list of DNS packets. The bottom pane shows the details of a selected packet (No. 34), which is a DNS query response for 'facebook.com'.

No.	Time	Source	Destination	Protocol	Length	Info
168	7.871605023	10.0.2.15	192.168.60.208	DNS	97	Standard query 0x6ed0 AAAA firefox.settings.services.mozilla.com
215	9.371153459	10.0.2.15	192.168.60.208	DNS	104	Standard query 0xa367 A firefox-settings-attachments.cdn.mozilla...
13	2.268664293	192.168.60.208	10.0.2.15	DNS	241	Standard query response 0x885b A contile.services.mozilla.com A ...
14	2.275954462	192.168.60.208	10.0.2.15	DNS	169	Standard query response 0x1f46 AAAA contile.services.mozilla.com...
31	6.383800241	192.168.60.208	10.0.2.15	DNS	118	Standard query response 0x25b0 A static.xx.fbcdn.net CNAME scont...
32	6.400712393	192.168.60.208	10.0.2.15	DNS	130	Standard query response 0x2db4 AAAA static.xx.fbcdn.net CNAME sc...
33	6.400712830	192.168.60.208	10.0.2.15	DNS	100	Standard query response 0x93a0 AAAA facebook.com AAAA 2a03:2880:...
34	6.401702242	192.168.60.208	10.0.2.15	DNS	88	Standard query response 0x60db A facebook.com A 102.132.101.35
52	6.579547612	192.168.60.208	10.0.2.15	DNS	116	Standard query response 0x2940 A web.facebook.com CNAME star.c10...
53	6.582410692	192.168.60.208	10.0.2.15	DNS	128	Standard query response 0x3b44 AAAA web.facebook.com CNAME star...
145	7.665435216	192.168.60.208	10.0.2.15	DNS	130	Standard query response 0x3229 A static.xx.fbcdn.net CNAME scont...
147	7.691216788	192.168.60.208	10.0.2.15	DNS	142	Standard query response 0xe42c AAAA static.xx.fbcdn.net CNAME sc...
167	7.867587534	192.168.60.208	10.0.2.15	DNS	175	Standard query response 0xe4df A firefox.settings.services.mozil...

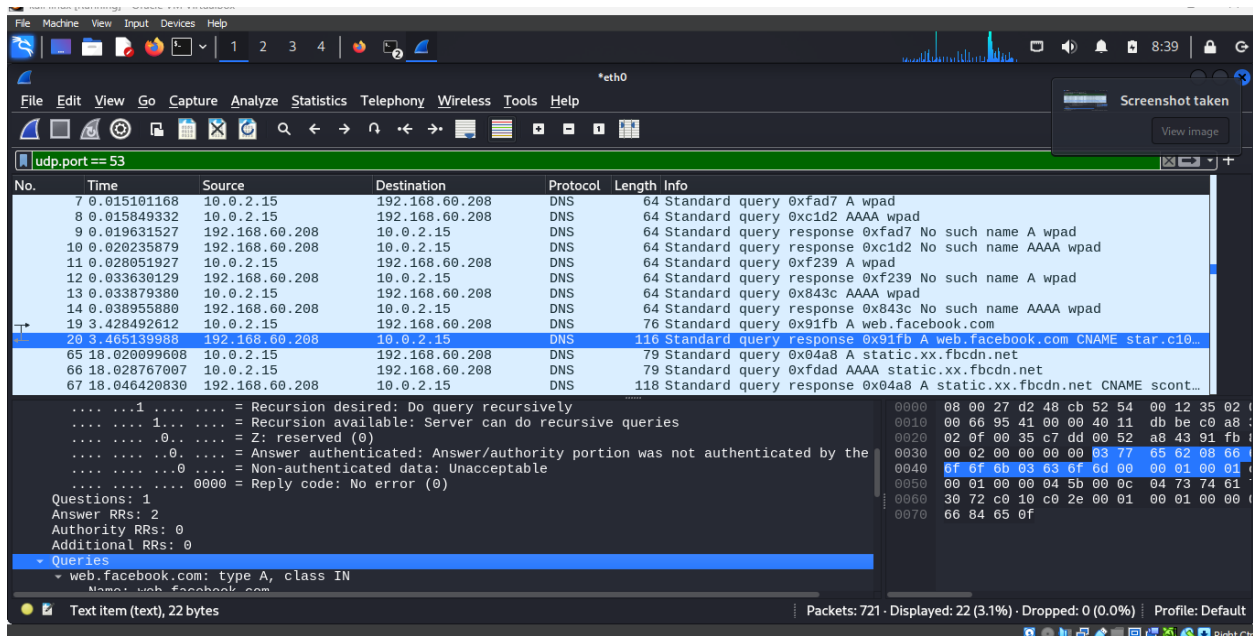
Frame 34: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface eth0, id 0  
 Ethernet II, Src: 52:54:00:12:35:02 (52:54:00:12:35:02), Dst: PCSSystemtec\_d2:48:cb (08:00:27:d2:48:cb)  
 Internet Protocol Version 4, Src: 192.168.60.208, Dst: 10.0.2.15  
 User Datagram Protocol, Src Port: 53, Dst Port: 46238  
 Domain Name System (response)  
 Transaction ID: 0x60db  
 Flags: 0x8180 Standard query response, No error  
 1... .. = Response: Message is a response  
 0000... .. = Opcode: Standard query (0)  
 ...0... .. = Authoritative: Server is not an authority for domain  
 ...0... .. = Truncated: Message is not truncated  
 ...1... .. = Recursion desired: Do query recursively  
 ...4... .. = Recursion available: Server can do recursive queries

On the flag, answer authentication: answer/authority portion was not authenticate by server.

### Exercise 3:

- Implement a capture filter to monitor DNS traffic. Analyze the captured packets and summarize any findings related to unusual queries or connections.

The packet captured was filter using `udp.port == 53` and there is no unusual queries or connections.



#### Exercise 4:

- Identify any DNS packets that may indicate a connection to a suspicious or malicious domain. Provide details about the domain queried and any associated IP addresses

The domain was examine carefully and no malicious domain. The queries are, web . facebook.com: type A, class IN, Name: web.Facebook.com, Name Length: 16, Label Count: 3, Type: A (1) (Host Address).

#### Exercise 5:

- Document any anomalous traffic patterns you discovered. What does this suggest about potential malicious activity?

No abnormality is discovered, and this suggests that the system is secure from potential malicious activities.