

First Shift CTF Task 6: The Crown Jewel

Author: Ernest Nyabayo Osindo

The Crown Jewel

You are on a shift, looking at the new alert coming from Imperium Labs - a company under MSSP monitoring long before you joined the team. It's hard to say what the company's primary focus is, but it has a global presence and undoubtedly has secrets to protect, especially those on heavily secured GitLab and Jira servers which store proprietary source code and project data.

The Alert

The alert you are looking at is called Reverse Shell Outbound Connection Detected, not something you see every day. Fortunately, you were able to obtain the raw PCAPs and Splunk logs for this event. Can you analyze the network traffic and logs to reconstruct and stop a sophisticated attack aimed at stealing the "Crown Jewel" data?

- Detailed network traffic capture challenge.pcap that you can find on the network_traffic folder on the VM's Desktop
- Pre-ingested Splunk logs (index=network_logs), which can be accessed at 10.48.143.161:8000

No.	Time	Source	Destination	Protocol	Length	Info
11	4149.178540	10.10.10.248	10.10.10.1	DNS	74	Standard query 0x0000 A ap
12	4164.435559	10.10.10.220	10.10.10.129	HTTP	235	GET /api/v1/status HTTP/1.
13	4701.887382	10.10.10.218	10.10.10.141	HTTP	231	GET /api/v1/status HTTP/1.
14	6825.286370	10.10.10.217	10.10.10.1	DNS	74	Standard query 0x0000 A ap
15	7128.575760	10.10.10.249	10.10.10.198	TCP	63	49277 → 443 [PSH, ACK] Seq
16	8386.897723	10.10.10.118	10.10.10.147	HTTP	134	GET /api/v1/status HTTP/1.
17	8396.878449	10.10.10.168	10.10.10.222	HTTP	233	GET /images/logo.png HTTP/1.
18	9130.023827	10.10.10.171	8.8.8.8	HTTP	138	GET /api/v1/status HTTP/1.
19	9204.613543	10.10.10.219	10.10.10.157	TCP	54	[TCP Window Update] 64172
20	9894.494673	10.10.10.216	10.10.10.117	HTTP	123	GET /is/app_is HTTP/1.1 ,

Frame 1: 63 bytes on wire (504 bits), 63 bytes captured (504 bits)
Ethernet II, Src: VMware_44:55:66 (00:0c:29:44:55:66), Dst: VMware_44:55:66 (00:0c:31:00:01:00)
Internet Protocol Version 4, Src: 10.10.10.216, Dst: 10.10.10.111
Transmission Control Protocol, Src Port: 65287, Dst Port: 443, Seq: 1, Ack: 1, ,

index=network_logs

Search | Splunk 10.0.0

splunk-enterprise Apps

Search Analytics Datasets Reports Alerts Dashboards

New Search

1 index=network_logs

5,061 events (before 1/30/26 1:30:34.000 PM) No Event Sampling ▾

Events (5,061) Patterns Statistics Visualization

Timeline format ▾ — Zoom Out + Zoom to Selection × Deselect

Format Show: 20 Per Page ▾ View: List ▾

1 day per column

Time range: All time ▾

Save As ▾ Create Table View Close

1 2 3 4 5 6 7 8 ... Next >

Time	Event
11/20/25 9:43:54.612 AM	<pre>{ ... event: { ... } host: router log_type: netflow sourcetype: network:netflow time: 2025-11-20T23:35:36.7752852 } Show as raw text</pre>
11/20/25 9:43:54.612 AM	<pre>{ ... event: { ... } host: lab source = network_traffic.json sourcetype = network_traffic } host: jira log_type: http sourcetype: network:http time: 2025-11-20T23:30:41.1022692</pre>

Search | Splunk 10.0.0

splunk-enterprise Apps

Search Analytics Datasets Reports Alerts Dashboards

New Search

1 index=network_logs log_type=dns

5,061 events (before 1/30/26 1:30:34.000 PM) No Event Sampling ▾

Events (5,061) Patterns Statistics Visualization

Timeline format ▾ — Zoom Out + Zoom to Selection × Deselect

Format Show: 20 Per Page ▾ View: List ▾

1 2 3 4 5 6 7 8 ... Next >

Time	Event
11/20/25 9:43:54.612 AM	<pre>host: jira log_type: http sourcetype: network:http time: 2025-11-20T23:30:41.1022692</pre>

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
http	1,882	35.66%
dns	1,733	34.24%
netflow	1,435	28.35%
arp	98	1.77%
dns	1	0.02%

Show as raw text

host = lab
source = network_traffic.json
sourcetype = network_traffic

http://10.48.143.161:8000/en-US/app/search/search?q=search%20index%3Dnetwork_logs%20log_type%3Ddns&dispatch.sample_ratio%3D1&workload_pool%3D0&earliest%3D0&latest%3D0&sid%3D1769779934.7#

Search | Splunk 10.0.0

splunk-enterprise Apps

Search Analytics Datasets Reports Alerts Dashboards

New Search

1 index=network_logs log_type=ids

1 event (before 1/30/26 1:33:18.000 PM) No Event Sampling ▾

Events (1) Patterns Statistics Visualization

Timeline format ▾ — Zoom Out + Zoom to Selection × Deselect

Format Show: 20 Per Page ▾ View: List ▾

1 day per column

Time range: All time ▾

Save As ▾ Create Table View Close

1 2 3 4 5 6 7 8 ... Next >

Time	Event
11/19/25 9:30:12.000 AM	<pre> Raw { ... event: [...] host: jira log_type: ids sourcetype: network:ids time: 2025-11-19T09:30:12.0000002 } Show as raw text</pre>

host = lab
source = network_traffic.json
sourcetype = network_traffic

http://10.48.143.161:8000/en-US/app/search/search?q=search%20index%3Dnetwork_logs%20log_type%3Did%26display.page.search.mode%3Dsmart%26dispatch.sample_ratio%3D1%26workload_pool%3D0%26earliest%3D0%26latest%3D0%26sid%3D1769779998.10#

Search | Splunk 10.0.0

New Search

1 event (before 1/30/26 13:18:000 PM) No Event Sampling ▾

Events (1) Patterns Statistics Visualization

Timeline format ▾ Zoom Out + Zoom to Selection × Deselect

Format Show: 20 Per Page ▾ View: Raw ▾

< Hide Fields All Fields + Extract New Fields

i Event

> {"time": "2025-11-30T09:30:12.000000Z", "log_type": "ids", "sourcetype": "network:ids", "host": "jira", "event": {"timestamp": 1764495012.0, "severity": "High", "src_ip": "10.10.10.100", "dest_ip": "1.1.1.1", "dest_port": "8088", "proto": "TCP", "msg": "Reverse Shell Outbound Connection Detected", "sid": "SID:2100498", "time_iso": "2025-11-30T09:30:12.000000Z"}
Show syntax highlighted

1. From which internal IP did the suspicious connection originate?

index=network_logs log_type=ids

View table

Search | Splunk 10.0.0

Format Show: 20 Per Page ▾ View: Table ▾

< Hide Fields All Fields + Extract New Fields

	_time	host	source	sourcetype
>	11/19/25 9:30:12.000 AM	lab	network_traffic.json	network_traffic
("time": "2025-11-30T09:30:12.000000Z", "log_type": "ids", "sourcetype": "network:ids", "host": "jira", "event": {"timestamp": 1764495012.0, "severity": "High", "src_ip": "10.10.10.100", "dest_ip": "1.1.1.1", "dest_port": "8088", "proto": "TCP", "msg": "Reverse Shell Outbound Connection Detected", "sid": "SID:2100498", "time_iso": "2025-11-30T09:30:12.000000Z"})				
Event Actions				
Type	<input checked="" type="checkbox"/> Field	Value	Actions	
Selected	<input checked="" type="checkbox"/> host	lab	▼	
	<input checked="" type="checkbox"/> source	network_traffic.json	▼	
	<input checked="" type="checkbox"/> sourcetype	network_traffic	▼	
Event	<input type="checkbox"/> event.dest_ip	1.1.1.1	▼	
	<input type="checkbox"/> event.dest_port	8088	▼	
	<input type="checkbox"/> event.msg	Reverse Shell Outbound Connection Detected	▼	
	<input type="checkbox"/> event.proto	TCP	▼	
	<input type="checkbox"/> event.severity	High	▼	
	<input type="checkbox"/> event.sid	SID:2100498	▼	
	<input type="checkbox"/> event.src_ip	10.10.10.100	▼	
	<input type="checkbox"/> event.time_iso	2025-11-30T09:30:12.000000Z	▼	
	<input type="checkbox"/> event.timestamp	1764495012.0	▼	
	<input type="checkbox"/> extracted_host	jira	▼	
	<input type="checkbox"/> extracted_sourcetype	network:ids	▼	
	<input type="checkbox"/> log_type	ids	▼	
	<input type="checkbox"/> time	2025-11-30T09:30:12.000000Z	▼	

Answer: 10.10.10.100

2. What outbound connection was detected as a C2 channel? (Answer example: 1.2.3.4:9996)

Search | Splunk 10.0.0

Format Show: 20 Per Page ▾ View: Table ▾

< Hide Fields All Fields + Extract New Fields

	_time	host	source	sourcetype
>	11/19/25 9:30:12.000 AM	lab	network_traffic.json	network_traffic
("time": "2025-11-30T09:30:12.000000Z", "log_type": "ids", "sourcetype": "network:ids", "host": "jira", "event": {"timestamp": 1764495012.0, "severity": "High", "src_ip": "10.10.10.100", "dest_ip": "1.1.1.1", "dest_port": "8088", "proto": "TCP", "msg": "Reverse Shell Outbound Connection Detected", "sid": "SID:2100498", "time_iso": "2025-11-30T09:30:12.000000Z"})				
Event Actions				
Type	<input checked="" type="checkbox"/> Field	Value	Actions	
Selected	<input checked="" type="checkbox"/> host	lab	▼	
	<input checked="" type="checkbox"/> source	network_traffic.json	▼	
	<input checked="" type="checkbox"/> sourcetype	network_traffic	▼	
Event	<input type="checkbox"/> event.dest_ip	1.1.1.1	▼	
	<input type="checkbox"/> event.dest_port	8080	▼	
	<input type="checkbox"/> event.msg	Reverse Shell Outbound Connection Detected	▼	
	<input type="checkbox"/> event.proto	TCP	▼	
	<input type="checkbox"/> event.severity	High	▼	
	<input type="checkbox"/> event.sid	SID:2100498	▼	
	<input type="checkbox"/> event.src_ip	10.10.10.100	▼	
	<input type="checkbox"/> event.time_iso	2025-11-30T09:30:12.000000Z	▼	
	<input type="checkbox"/> event.timestamp	1764495012.0	▼	
	<input type="checkbox"/> extracted_host	jira	▼	
	<input type="checkbox"/> extracted_sourcetype	network:ids	▼	
	<input type="checkbox"/> log_type	ids	▼	
	<input type="checkbox"/> time	2025-11-30T09:30:12.000000Z	▼	
Time	<input checked="" type="checkbox"/> _time	2025-11-19T09:30:12.000+00:00	▼	
Default	<input type="checkbox"/> Index	network_logs	▼	

Answer: 1.1.1.1:8080

3. Which MAC address is impersonating the gateway 10.10.10.1?

Search | Splunk 10.0.0

Hide Fields All Fields Format Show: 20 Per Page View: Table

< Prev 1 2 3 4 5 6 7 8 ... Next >

log_type	Selected	sourceType	
5 Values, 100% of events	Yes No	network_traffic	
Reports			
Top values	Top values by time	Rare values	
Events with this field			
Values	Count	%	
http	1,882	35.696%	network_traffic
dns	1,733	34.242%	network_traffic
netflow	1,435	28.354%	network_traffic
arp	90	1.778%	network_traffic
ids	1	0.02%	

11 more fields + Extract New Fields

11/20/25 lab network_traffic.json network_traffic

index=* log_type=arp

```
| table _time event.sender_ip event.sender_mac event.op event.target_ip  
event.target_ip event.target_mac
```

The screenshot shows the Splunk Enterprise search interface. At the top, there's a navigation bar with links for Search, Analytics, Datasets, Reports, Alerts, Dashboards, and a search bar. Below the navigation is a "New Search" section with a search bar containing the query: `index=_* log_type=arp 2 | table _time event.sender_ip event.sender_mac event.op event.target_ip event.target_mac`. The results pane shows 90 events from November 19, 2025, at 09:33:44.000. The table has columns for _time, event.sender_ip, event.sender_mac, event.op, event.target_ip, and event.target_mac. The event.op column contains values like "is-at" and "is-not-at". The event.target_ip and event.target_mac columns show IP addresses and MAC addresses respectively. The interface includes a "Save As" dropdown, "Create Table View" button, and a "Time range: All time" selector. The bottom of the screen shows a toolbar with various icons and a footer with page numbers (1-5).

_time	event.sender_ip	event.sender_mac	event.op	event.target_ip	event.target_mac
2025-11-19 09:33:44.000	10.10.10.150	00:0c:29:11:22:33	is-at	10.10.10.1	ff:ff:ff:ff:ff:ff
2025-11-19 09:33:44.000	10.10.10.1	00:0c:29:11:22:33	is-at	10.10.10.150	ff:ff:ff:ff:ff:ff
2025-11-19 09:33:43.100	10.10.10.150	00:0c:29:11:22:33	is-at	10.10.10.1	ff:ff:ff:ff:ff:ff
2025-11-19 09:33:43.000	10.10.10.1	00:0c:29:11:22:33	is-at	10.10.10.150	ff:ff:ff:ff:ff:ff
2025-11-19 09:33:42.200	10.10.10.150	00:0c:29:11:22:33	is-at	10.10.10.1	ff:ff:ff:ff:ff:ff
2025-11-19 09:33:42.000	10.10.10.1	00:0c:29:11:22:33	is-at	10.10.10.150	ff:ff:ff:ff:ff:ff
2025-11-19 09:33:41.200	10.10.10.150	00:0c:29:11:22:33	is-at	10.10.10.1	ff:ff:ff:ff:ff:ff
2025-11-19 09:33:41.000	10.10.10.1	00:0c:29:11:22:33	is-at	10.10.10.150	ff:ff:ff:ff:ff:ff
2025-11-19 09:33:40.200	10.10.10.150	00:0c:29:11:22:33	is-at	10.10.10.1	ff:ff:ff:ff:ff:ff
2025-11-19 09:33:40.000	10.10.10.1	00:0c:29:11:22:33	is-at	10.10.10.150	ff:ff:ff:ff:ff:ff
2025-11-19 09:33:39.200	10.10.10.150	00:0c:29:11:22:33	is-at	10.10.10.1	ff:ff:ff:ff:ff:ff

Answer: 00:0c:29:11:22:33

5. What is the non-standard User-Agent hitting the Jira instance?

index=* log_type=http

Search | Splunk 10.0.0

INTERESTING FIELDS

Type	Field	Value	Actions
Selected	<input checked="" type="checkbox"/> host	lab	
	<input checked="" type="checkbox"/> source	network_traffic.json	
	<input checked="" type="checkbox"/> sourcetype	network_traffic	
Event	<input type="checkbox"/> event.agent	CVE-202X-EXPLOIT	
	<input type="checkbox"/> event.bytes	512	
	<input type="checkbox"/> event.c2_port	8080	
	<input type="checkbox"/> event.clientip	11.11.11.11	
	<input type="checkbox"/> event.method	POST	
	<input type="checkbox"/> event.status	404	
	<input type="checkbox"/> event.time_iso	2025-11-30T09:30:10.000000Z	
	<input type="checkbox"/> event.timestamp	1764495010.0	
	<input type="checkbox"/> event.uri	/vulnerable_endpoint?cmd=RCE	
	<input type="checkbox"/> extracted_host	jira	
	<input type="checkbox"/> extracted_sourcetype	networkhttp	
	<input type="checkbox"/> log_type	http	
	<input type="checkbox"/> time	2025-11-30T09:30:10.000000Z	
Time	<input type="checkbox"/> _time	2025-11-30T09:30:10.000+00:00	
Default	<input type="checkbox"/> index	network_logs	
	<input type="checkbox"/> linecount	1	
	<input type="checkbox"/> punct	[...]	
	<input type="checkbox"/> splunk_server	tryhackme	

+ Extract New Fields

Answer: CVE-202X-EXPLOIT

6. How many ARP spoofing attacks were observed in the PCAP?

index=* log_type=arp

splunk>enterprise Apps ▾

Search Analytics Datasets Reports Alerts Dashboards

New Search

1 index** log_type=arp

events (before 1/30/26 2:03:05.000 PM) No Event Sampling

Events (90) Patterns Statistics Visualization

Timeline format ▾ Zoom Out + Zoom to Selection X Deselect

Format ▾ Show: 20 Per Page ▾ View: Table ▾

No.	_time	host	source	sourcetype
>	1/19/25 9:33:44.000 AM	lab	network_traffic.json	network_traffic
>	1/19/25 9:33:44.000 AM	lab	network_traffic.json	network_traffic
>	1/19/25 9:33:43.200 AM	lab	network_traffic.json	network_traffic
>	1/19/25 9:33:43.000 AM	lab	network_traffic.json	network_traffic

Also

arp.opcode == 2

File Edit View Go Capture Analyze statistics Telephony Wireless Tools Help

challenge.pcap

arp.opcode == 2

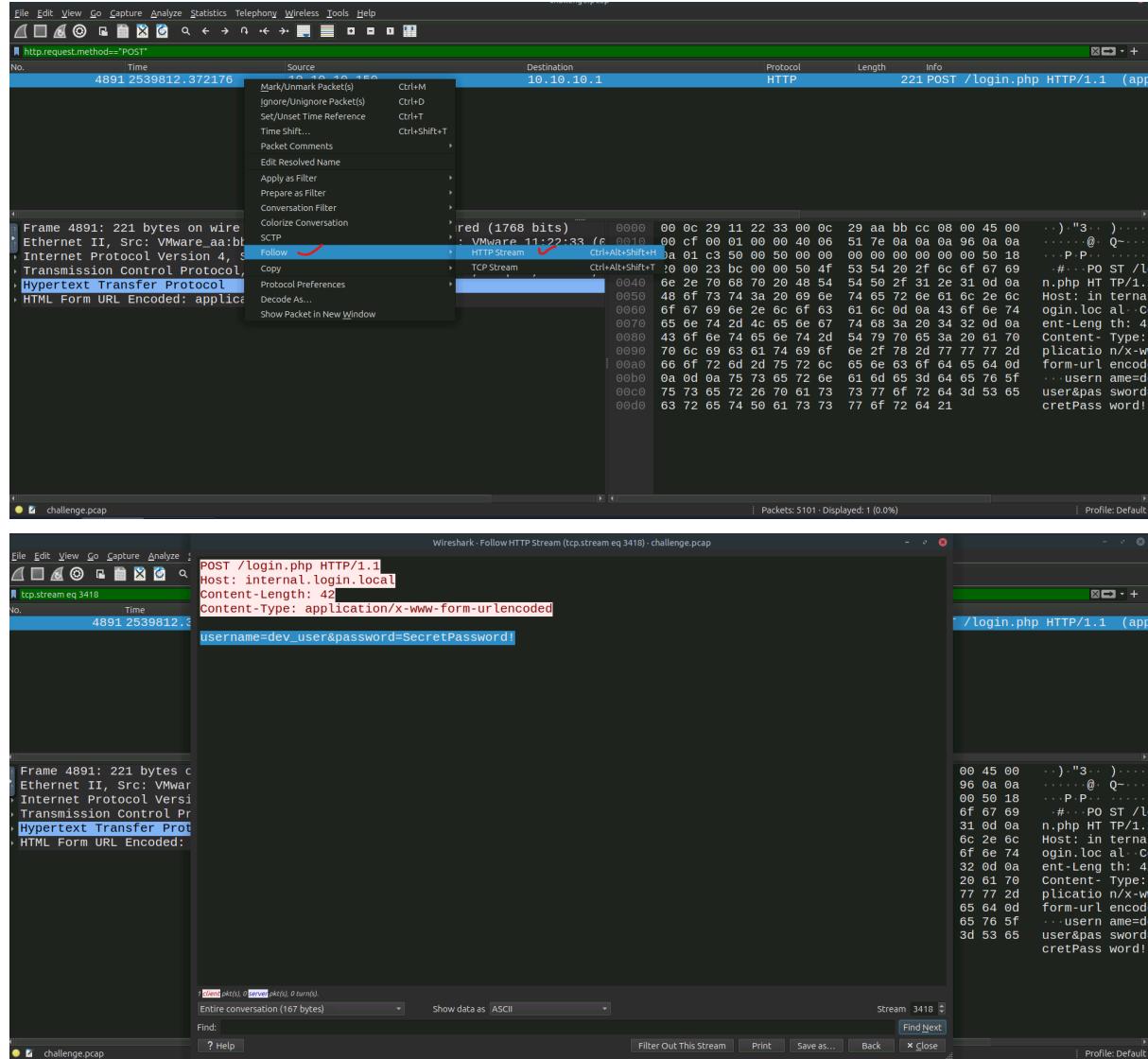
No.	Source	Destination	Protocol	Length	Info
29west_2dpalrifec_5.39807.372176	VMware_11:22:33	Broadcast	ARP	42	10.10.10.1 is at 00:0c:29:11:22:33 (oui Unknown) > Broadcast on interface VMware_11:22:33 (eth0) [ethertype IPv4 (0x0800), length 42] (no route to host)
4881 2539807.572176	VMware_11:22:33	Broadcast	ARP	42	10.10.10.150 is at 00:0c:29:11:22:33 (oui Unknown) > Broadcast on interface VMware_11:22:33 (eth0) [ethertype IPv4 (0x0800), length 42] (no route to host)
4882 2539808.572176	VMware_11:22:33	Broadcast	ARP	42	10.10.10.1 is at 00:0c:29:11:22:33 (oui Unknown) > Broadcast on interface VMware_11:22:33 (eth0) [ethertype IPv4 (0x0800), length 42] (no route to host)
4883 2539808.572176	VMware_11:22:33	Broadcast	ARP	42	10.10.10.150 is at 00:0c:29:11:22:33 (oui Unknown) > Broadcast on interface VMware_11:22:33 (eth0) [ethertype IPv4 (0x0800), length 42] (no route to host)
4884 2539809.572176	VMware_11:22:33	Broadcast	ARP	42	10.10.10.1 is at 00:0c:29:11:22:33 (oui Unknown) > Broadcast on interface VMware_11:22:33 (eth0) [ethertype IPv4 (0x0800), length 42] (no route to host)
4885 2539809.572176	VMware_11:22:33	Broadcast	ARP	42	10.10.10.150 is at 00:0c:29:11:22:33 (oui Unknown) > Broadcast on interface VMware_11:22:33 (eth0) [ethertype IPv4 (0x0800), length 42] (no route to host)
4886 2539810.572176	VMware_11:22:33	Broadcast	ARP	42	10.10.10.1 is at 00:0c:29:11:22:33 (oui Unknown) > Broadcast on interface VMware_11:22:33 (eth0) [ethertype IPv4 (0x0800), length 42] (no route to host)
4887 2539810.572176	VMware_11:22:33	Broadcast	ARP	42	10.10.10.150 is at 00:0c:29:11:22:33 (oui Unknown) > Broadcast on interface VMware_11:22:33 (eth0) [ethertype IPv4 (0x0800), length 42] (no route to host)
4888 2539811.572176	VMware_11:22:33	Broadcast	ARP	42	10.10.10.1 is at 00:0c:29:11:22:33 (oui Unknown) > Broadcast on interface VMware_11:22:33 (eth0) [ethertype IPv4 (0x0800), length 42] (no route to host)
4889 2539811.572176	VMware_11:22:33	Broadcast	ARP	42	10.10.10.150 is at 00:0c:29:11:22:33 (oui Unknown) > Broadcast on interface VMware_11:22:33 (eth0) [ethertype IPv4 (0x0800), length 42] (no route to host)

Frame 4880: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
 Ethernet II, Src: VMware_11:22:33 (00:0c:29:11:22:33), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 Address Resolution Protocol (reply)

Answer: 90

7. What's the payload containing the plaintext creds found in the POST request?

http.request.method=="POST"



Answer: username=dev_user&password=SecretPassword!

8. What domain, owned by the attacker, was used for data exfiltration?

Answer: exfil-domain.xyz

9. After examining the logs, which protocol was used for data exfiltration?

Answer: DNS