

First Shift CTF Task 7: The Crown Jewel

Author: Ernest Nyabayo Osindo

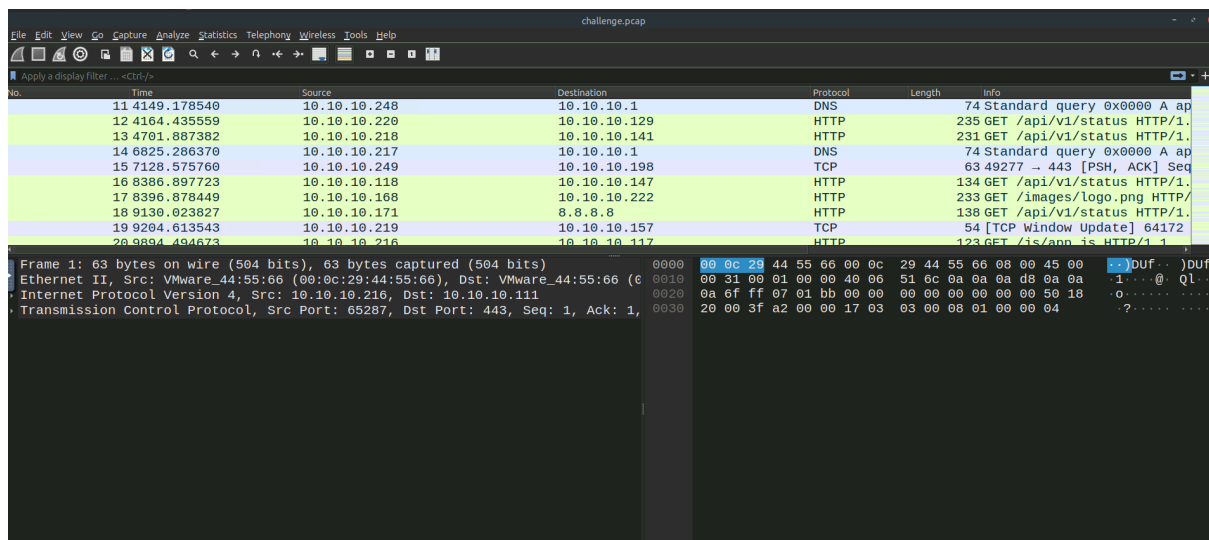
The Crown Jewel

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



index=network_logs

Search | Splunk 10.0.0

splunk>enterprise

Apps

Messages

Settings

Activity

Help

Find

SearchAnalyticsDatasetsReportsAlertsDashboards

Search & Reporting

New Search

Save AsCreate Table ViewClose

1indexnetwork_logsTime range: All time

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

Events (5,061)PatternsStatisticsVisualization

Timeline formatZoom OutZoom to SelectionDeselect1 day per column

FormatShow: 20 Per PageView: List

< Hide Fields

All Fields

SELECTED FIELDS

host 1

source 1

sourcetype 1

INTERESTING FIELDS

date_hour 24

date_mday 20

date_minute 60

date_month 1

date_second 60

date_wday 7

date_year 1

date_zone 1

eventagent 6

Time

Event

11/20/25 9:43:54.612 AM

[]

event: { []

host: router

log_type: netflow

sourcetype: network:netflow

time: 2025-11-20T23:35:36.775285Z

Show as raw text

host = lab source = network_traffic.json sourcetype = network_traffic

11/20/25 9:43:54.612 AM

[]

event: { []

host: jira

Search | Splunk 10.0.0

splunk>enterprise

Apps

Messages

Settings

Activity

Help

Find

SearchAnalyticsDatasetsReportsAlertsDashboards

Search & Reporting

New Search

Save AsCreate Table ViewClose

1eventquery "log_type=ids"Time range: All time

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

Events (1)PatternsStatisticsVisualization

Timeline formatZoom OutZoom to SelectionDeselect1 day per column

FormatShow: 20 Per PageView: List

< Hide Fields

All Fields

eventquery "log_type=ids"

event_type 4

eventcode 1

eventreferer 100+

eventresponse_time 7

eventsession 100+

eventsrc_ip 100+

eventstatus 6

eventtime_iso 100+

eventtimestamp 100+

eventurl 11

extracted_host 3

extracted_sourcetype 5

index 1

linecount 1

log_type 5

packet 2

splunk_server 1

time 100+

11 more fields

+ Extract New Fields

Time

Event

11/19/25 9:30:12.000 AM

[]

event: { []

host: jira

log_type: dns

sourcetype: network:dns

time: 2025-11-20T28:44:47.583147Z

Show as raw text

host = lab source = network_traffic.json sourcetype = network_traffic

log_type

5 Values, 100% of events

SelectedYesNo

Reports

Top values

Top values by time

Rare values

Events with this field

Values

Count

%

http

1,882

35.686%

dns

1,733

34.242%

netflow

1,435

28.354%

arp

98

1.778%

ids

1

0.02%

http://10.48.143.161:8000/en-US/app/search/search?q=search index=network_logs&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool=&earliest=0&latest=&sid=1769779834.7#

New Search

Save AsCreate Table ViewClose

1indexnetwork_logs_log_type=idsTime range: All time

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

Events (1)PatternsStatisticsVisualization

Timeline formatZoom OutZoom to SelectionDeselect1 day per column

FormatShow: 20 Per PageView: List

< Hide Fields

All Fields

+ Extract New Fields

Time

Event

11/19/25 9:30:12.000 AM

[]

event: { []

host: jira

log_type: ids

sourcetype: network:ids

time: 2025-11-30T09:38:12.000000Z

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 index=network_logs_log_type=ids&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool=&earliest=0&latest=&sid=1769779998.10#

Search | Splunk 10.0.0

New Search

1 index=network_logs log_type=ids

Time range: All time

1 event (before 1/30/25 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: Row

Event

[{"time": "2025-11-30T09:30:12.000000Z", "log_type": "ids", "sourcetype": "network:ids", "host": "jira", "event": {"timestamp": "1764495012.0", "severity": "High", "src_ip": "10.10.100", "dest_ip": "1.1.1.1", "dest_port": "8080", "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

Time host source sourcetype

11/30/25 9:30:12.000 AM lab network_traffic.json network_traffic 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": "10.10.100", "dest_ip": "1.1.1.1", "dest_port": "8080", "proto": "TCP", "msg": "Reverse Shell Outbound Connection Detected", "sid": "SID:2100498", "time_iso": "2025-11-30T09:30:12.000000Z"}}]

Event Actions

Type	Field	Value	Actions
Selected	host	lab	
	source	network_traffic.json	
	sourcetype	network_traffic	
Event	event.dest_ip	1.1.1.1	
	event.dest_port	8080	
	event.msg	Reverse Shell Outbound Connection Detected	
	event.proto	TCP	
	event.severity	High	
	event.sid	SID:2100498	
	event.src_ip	10.10.100	
	event.time_iso	2025-11-30T09:30:12.000000Z	
	event.timestamp	1764495012.0	
	extracted_host	jira	
	extracted_sourcetype	network:ids	
	log_type	ids	
	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

Time host source sourcetype

11/30/25 9:30:12.000 AM lab network_traffic.json network_traffic 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": "10.10.100", "dest_ip": "1.1.1.1", "dest_port": "8080", "proto": "TCP", "msg": "Reverse Shell Outbound Connection Detected", "sid": "SID:2100498", "time_iso": "2025-11-30T09:30:12.000000Z"}}]

Event Actions

Type	Field	Value	Actions
Selected	host	lab	
	source	network_traffic.json	
	sourcetype	network_traffic	
Event	event.dest_ip	1.1.1.1	
	event.dest_port	8080	
	event.msg	Reverse Shell Outbound Connection Detected	
	event.proto	TCP	
	event.severity	High	
	event.sid	SID:2100498	
	event.src_ip	10.10.100	
	event.time_iso	2025-11-30T09:30:12.000000Z	
	event.timestamp	1764495012.0	
	extracted_host	jira	
	extracted_sourcetype	network:ids	
	log_type	ids	
	time	2025-11-30T09:30:12.000000Z	

Time 0 _time 2025-11-30T09:30:12.000+00:00

Default 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

log_type

5 Values, 100% of events

Reports

Top values

Values	Count	%
http	1,892	35.686%
dns	1,733	34.242%
netFlow	1,435	28.354%
arp	90	1.778%
ids	1	0.02%

Selected Yes No

Source type: 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

Search | Splunk 10.0.0

New Search

1 index=* log_type=arp
2 | table _time event.sender_ip event.sender_mac event.op event.target_ip event.target_ip event.target_mac

Time range: All time

90 events (before 1/30/26 1:48:17:000 PM) No Event Sampling

Statistics (90)

_time	event.sender_ip	event.sender_mac	event.op	event.target_ip	event.target_mac
2025-11-19 09:33:44.200	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 09:33:44.000	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 09:33:43.200	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 09:33:43.000	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

eventAgent

6 Values, 100% of events

Reports

Top values

Values	Count	%
curl/7.68.0	393	21.889%
Mozilla/5.0 (Windows NT 10.0; Win64; x64)	363	20.144%
AppleWebKit/537.36 (KHTML, like Gecko)	360	19.578%
Chrome/108.0.4896.75 Safari/537.36	358	19.423%
Python-requests/2.25.1	335	18.59%
Go-http-client/1.1	1	0.055%
CIE-2024-EXPLOIT	1	0.055%

Selected Yes No

Source type: network_traffic

Search | Splunk 10.0.0

INTERESTING FIELDS

- # date_hour 1
- # date_minute 1
- # date_month 1
- # date_second 1
- # date_wday 1
- # date_year 1
- # date_zone 1
- # event_agent 1
- # event_bytes 1
- # event_c2_port 1
- # event_clientip 1
- # event_method 1
- # event_status 1
- # event_time_iso 1
- # event_timestamp 1
- # event_uri 1
- # extracted_host 1
- # extracted_sourcetype 1
- # index 1
- # linecount 1
- # log_type 1
- # punct 1
- # splunk_server 1
- # time 1

+ Extract New Fields

Type	Field	Value	Actions
Selected	host	lab	
	source	network_traffic.json	
	sourcetype	network_traffic	
Event	event_agent	CVE-202X-EXPLOIT	
	event_bytes	512	
	event_c2_port	8080	
	event_clientip	1111	
	event_method	POST	
	event_status	404	
	event_time_iso	2025-11-30T09:30:10.000000Z	
	event_timestamp	1764495010.0	
	event_uri	/vulnerable_endpoint/cmd-RCE	
	extracted_host	jira	
	extracted_sourcetype	networkhttp	
	log_type	http	
	time	2025-11-30T09:30:10.000000Z	
Time	_time	2025-11-19T09:30:10.000+00:00	
Default	index	network_logs	
	linecount	1	
	punct	[{"ts": "2025-11-30T09:30:10.000000Z", "type": "http", "value": "404"}]	
	splunk_server	tryhackme	

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

Search & Reporting

New Search

1 index=* log_type=arp

Time range: All time

Events (90)

Timeline format Zoom Out Zoom to Selection Deselect

1 second per column

_time	host	source	sourcetype
11/19/25 9:33:44.200 AM	lab	network_traffic.json	network_traffic
11/19/25 9:33:44.000 AM	lab	network_traffic.json	network_traffic
11/19/25 9:33:43.200 AM	lab	network_traffic.json	network_traffic
11/19/25 9:33:43.000 AM	lab	network_traffic.json	network_traffic

Also

arp.opcode == 2

challenge.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp.opcode == 2

No.	Source	Destination	Protocol	Length	Info
4881	2539807.572176 VMware_11:22:33	Broadcast	ARP	42	10.10.10.1 is at 00:0c:29:11:22:33
4882	2539808.372176 VMware_11:22:33	Broadcast	ARP	42	10.10.10.150 is at 00:0c:29:11:22:33
4883	2539808.372176 VMware_11:22:33	Broadcast	ARP	42	10.10.10.150 is at 00:0c:29:11:22:33
4884	2539809.372176 VMware_11:22:33	Broadcast	ARP	42	10.10.10.150 is at 00:0c:29:11:22:33
4885	2539809.372176 VMware_11:22:33	Broadcast	ARP	42	10.10.10.150 is at 00:0c:29:11:22:33
4886	2539810.372176 VMware_11:22:33	Broadcast	ARP	42	10.10.10.150 is at 00:0c:29:11:22:33
4887	2539810.372176 VMware_11:22:33	Broadcast	ARP	42	10.10.10.150 is at 00:0c:29:11:22:33
4888	2539811.372176 VMware_11:22:33	Broadcast	ARP	42	10.10.10.150 is at 00:0c:29:11:22:33

Frame 4880: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0

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)

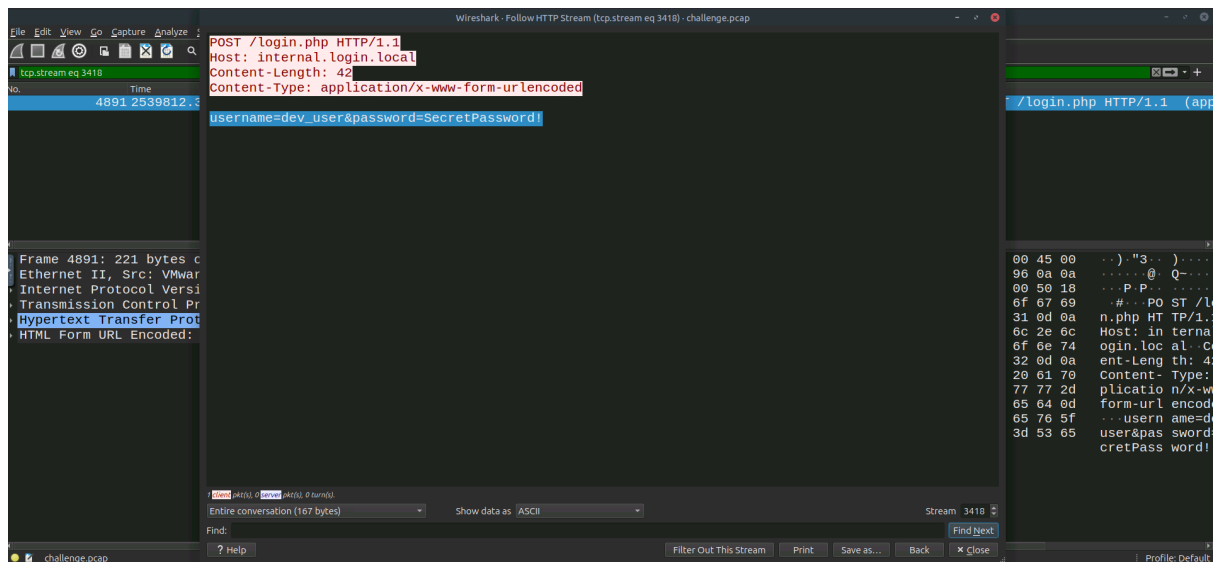
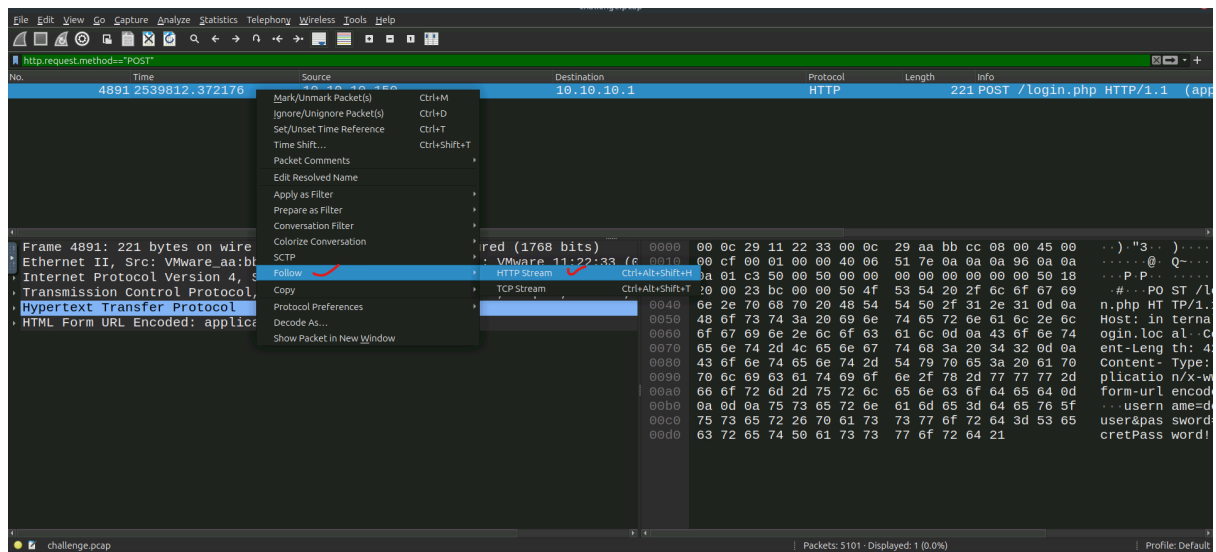
challenge.pcap

Packets: 5101 · Displayed: 90 (1.8%)

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?

Search | Splunk 10.0.0

Format Show: 20 Per Page View: Table

log_type

5 Values, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
http	1,882	35.68%
dns	1,733	34.24%
netflow	1,435	28.35%
arp	90	1.77%
ids	1	0.02%

_time	host	source	sourcetype
11/20/25 9:43:54.612 AM	lab	network_traffic.json	network_traffic
11/20/25 9:43:54.612 AM	lab	network_traffic.json	network_traffic
11/20/25 9:43:54.612 AM	lab	network_traffic.json	network_traffic

Search | Splunk 10.0.0

Format Show: 20 Per Page View: Table

event.domain

1 Value, 28.852% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
exfil-domain.xyz	500	100%

_time	host	source	sourcetype
11/20/25 9:43:54.612 AM	lab	network_traffic.json	network_traffic
11/20/25 9:43:54.612 AM	lab	network_traffic.json	network_traffic
11/20/25 9:43:54.612 AM	lab	network_traffic.json	network_traffic

Answer: exfil-domain.xyz

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

Answer: **DNS**