

Splunk 2

Platform: tryhackme

Frome: Asem Reda

Diploma: Cybersecurity 87

Challenge link: <https://tryhackme.com/room/splunk2gcd5>

The screenshot shows the 'Splunk 2' challenge page on tryhackme. At the top, there's a navigation bar with 'Learn > Splunk 2'. Below it is a banner for 'Splunk 2' which is a 'Premium room'. The banner text says 'Part of the Blue Primer series. This room is based on version 2 of the Boss of the SOC (BOTS) competition by Splunk.' It also indicates a duration of '45 min' and has 29,280 views. Below the banner are several interaction buttons: 'Share your achievement', 'Start AttackBox', 'Save Room', '674 Recommend', and 'Options'. A progress bar at the bottom of the banner area shows 'Room completed (100%)'. The main content area is titled 'Task 1 Deploy' and shows a green checkmark indicating completion. Below it are six more tasks: 'Dive into the data', '100 series questions', '200 series questions', '300 series questions', '400 series questions', and 'Conclusion'. Each task has a green checkmark next to its name, signifying they have all been completed.

Task 1: Deploy!



Task 2: Dive into the data

In this exercise, you assume the persona of Alice Bluebird, the analyst who successfully assisted Wayne Enterprises and was recommended to Grace Hoppy at Frothly (a beer company) to assist them with their recent issues.

What Kinds of Events Do We Have?

The SPL (Splunk Search Processing Language) command metadata can be used to search for the same kind of information that is found in the Data Summary, with the bonus of being able to search within a specific index, if desired. All time-values are returned in EPOCH time, so to make the output user readable, the eval command should be used to provide more human-friendly formatting.

In this example, we will search the botsv2 index and return a listing of all the source types that can be found as well as a count of events and the first time and last time seen.

Resources:

- <http://docs.splunk.com/Documentation/Splunk/latest/SearchReference/Metadata>
- <https://www.splunk.com/blog/2017/07/31/metadata-metalore.html>

Metadata command:

```
| metadata type=sourcetypes index=botsv2 | eval firstTime=strftime(firstTime,"%Y-%m-%d %H:%M:%S") | eval lastTime=strftime(lastTime,"%Y-%m-%d %H:%M:%S") | eval recentTime=strftime(recentTime,"%Y-%m-%d %H:%M:%S") | sort - totalCount
```

Note: This information is from the Advanced Hunting APTs with Splunk app.

Task 3: 100 series questions

Amber Turing was hoping for Frothly to be acquired by a potential competitor which fell through, but visited their website to find contact information for their executive team. What is the website domain that she visited?

✓ Correct Answer

Amber found the executive contact information and sent him an email. What image file displayed the executive's contact information? Answer example: /path/image.ext

✓ Correct Answer

What is the CEO's name? Provide the first and last name.

✓ Correct Answer

What is the CEO's email address?

✓ Correct Answer

After the initial contact with the CEO, Amber contacted another employee at this competitor. What is that employee's email address?

✓ Correct Answer

What is the name of the file attachment that Amber sent to a contact at the competitor?

✓ Correct Answer

What is Amber's personal email address?

✓ Correct Answer ?

Solution method:

First, we need to get Amber's IP address. We'll do this by using the filter `index="botsv2" amber` , then going to the `src_ip` list. We'll find it there, and it's 10.0.2.101 , When you scroll down to the sender_email field, you will find her email address, which is aturing@froth.ly

First question:

We will use the filter [index="botsv2" 10.0.2.101 sourcetype="stream:HTTP" | dedup site | table site *wine*] to display the name of the site visited

The screenshot shows the Splunk Enterprise search interface. The top navigation bar includes links for Search, Analytics, Datasets, Reports, Alerts, and Dashboards. On the right, there are links for Message, Settings, Activity, Help, and Find, along with a "Search & Reporting" button. The main search bar contains the query: `index=_boxcar* host=19.8.2.181 sourcetype='strains:HTTP' | index site | table site _raw`. Below the search bar, it says "107 events (before 12/10/25 10:56:00 AM) No Event Sampling". The "Statistics (107)" tab is selected under the "Events, Patterns, Statistics (107), Visualization" menu. The results table has 20 items per page, with the first item being `site : www.vindale.com`. A context menu is open for this result, showing options: View events, Other events, Exclude from results, and New search. The "New search" option is highlighted with a blue border. The bottom status bar shows the URL `www.vindale.com`.

Second question:

We will use this filter to find the image file [index="botsv2" 10.0.2.101 sourcetype="stream:http" www.berkbeer.com

|table uri_path]

We will find it is /images/ceoberk.png because this is what belongs to ceo

New Search	
1 index="botsv2" 10.0.2.101 sourcetype="stream:http" www.berkbeer.com 2 table uri_path	
 12 events (before 12/10/25 2:00:26.000 AM) No Event Sampling ▾	
Events Patterns Statistics (12) Visualization	
20 Per Page ▾	<input checked="" type="checkbox"/> Format <input type="checkbox"/> Preview ▾
uri_path ▾	
/images/socials02.png	
/images/socials03.png	
/images/socials01.png	
/images/img01.jpg	
/	
/favicon.ico	
/images/bgimg01.jpg	
/images/header-bg.jpg	
/images/ceoberk.png	

Third question:

We will use this filter to find the CEO's email address: index="botsv2" sourcetype="stream:smtp" berkbeer.com aturing@froth.ly. We will scroll down to sender_email and find it is mberk@berkbeer.com. Therefore, the CEO's name is Martin Berk

Fourth question:

Using the same steps, we will find the CEO's email address , mberk@berkbeer.com

sender: mberk@berkbeer.com
sender_email: mberk@berkbeer.com

Fifth question:

Using the same filter as the previous question, we will go down to receiver_email and find that the email address is hbernhard@berkbeer.com

```
]  
receiver_email: [ [-]  
    hbernhard@berkbeer.com  
]
```

Sixth question:

Using the same filter as the previous question, we will go to attach_disposition and find that the filename is Saccharomyces_cerevisiae_patent.docx

The screenshot shows a log entry from a botnet. The event details are as follows:

- Time: 8/30/17 3:08:00.075 PM
- Event type: [-]
- Content:

```
ack_packets_in: 0
ack_packets_out: 31
attach_content_decoded_md5_hash: [ [+]
]
attach_content_md5_hash: [ [+]
]
attach_disposition: [ [+]
]
attach_filename: [ [-]
    Saccharomyces_cerevisiae_patent.docx
]
```

Seventh question:

We will use the filter index="botsv2" amber, then scroll down to content_body, then take the base64 hash and go to a website to decode it, for example, <https://www.base64decode.org/>, then the email will appear

The screenshot shows a list of events with their content_body fields. One specific event is highlighted, showing a large amount of encoded data.

Below the log viewer, there is a "base64-decode.org" interface. It contains the following text:

Thanks for taking the time today. As discussed here is the document I was referring to. Probably better to take this offline. Email me from now on at ambersthebeast@weasiblebeast.com

From: hbernhard@berkbeer.com [mailto: hbernhard@berkbeer.com]

Sent: Friday, August 11, 2017 9:08 AM

To: Amber Turing <aturing@froth.ly>

Subject: Heinz Bernhard Contact Information

Heinz Bernhard,

Great talking with you today, here is my contact information. Do you have a personal email I can reach you at as well?

Task 4: 200 series questions

The screenshot shows a series of 8 questions from a challenge interface:

- What version of TOR Browser did Amber install to obfuscate her web browsing? Answer guidance: Numeric with one or more delimiter.
Answer: 7.0.4
Status: ✓ Correct Answer
- What is the public IPv4 address of the server running www.brewertalk.com?
Answer: 52.42.208.228
Status: ✓ Correct Answer
- Provide the IP address of the system used to run a web vulnerability scan against www.brewertalk.com.
Answer: 45.77.65.311
Status: ✓ Correct Answer
- The IP address from Q3 is also being used by a likely different piece of software to attack a URI path. What is the URI path? Answer guidance: Include the leading forward slash in your answer. Do not include the query string or other parts of the URL. Answer example: /phpinfo.php
Answer: /member.php
Status: ✓ Correct Answer
- What SQL function is being abused on the URI path from the previous question?
Answer: updateuri
Status: ✓ Correct Answer
- What was the value of the cookie that Kevin's browser transmitted to the malicious URL as part of an XSS attack? Answer guidance: All digits. Not the cookie name or symbols like an equal sign.
Answer: 1502408189
Status: ✓ Correct Answer
- What brewertalk.com username was maliciously created by a spear phishing attack?
Answer: klagerfeld
Status: ✓ Correct Answer

First question:

We will use the filter `index="botsv2" amber tor`, then we will go to the app field in Interesting Fields. We will find the version number, which is 7.0.4

The screenshot shows the Splunk interface with the following search command:

```
1 index="botsv2" amber tor
```

Results: 325 events (before 12/10/25 3:35:25.000 AM) No Event Sampling ▾

Events (325) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect

app

4 Values, 43.692% of events Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
C:\Users\amber_turing\Downloads\torbrowser-Install-7.0.4.en-US.exe	124	87.324%

Second question:

We will use the filter `index="botsv2" sourcetype="stream:HTTP" "brewertalk.com"`

`|table dest_ip, site, uri_path` to find the IP address, and it will be the first one:
52.42.208.228

The screenshot shows the Splunk interface with the following search command:

```
1 index="botsv2" sourcetype="stream:HTTP" "brewertalk.com"
2 |table dest_ip, site, uri_path
```

✓ 11,082 events (before 12/10/25 3:48:07.000 AM) No Event Sampling ▾

Events Patterns Statistics (11,082) Visualization

20 Per Page ▾ Format Preview ▾

dest_ip	site
52.42.208.228	www.brewertalk.com

Third question:

We will use the filter index="botsv2" sourcetype="stream:HTTP" "brewertalk.com"

Then we will go to Selected Fields and open src_ip. We will find that the IP address is 45.77.65.211

The screenshot shows a Splunk search interface with the following details:

- New Search:** index="botsv2" sourcetype="stream:HTTP" "brewertalk.com"
- Events (11,082):** 11,082 events (before 12/10/25 3:56:44.000 AM) No Event Sampling
- Selected Fields:** src_ip
- Reports:** Top values, Top values by time, Rare values
- Events with this field:** 8 Values, 89.848% of events
- Values Table:**

Values	Count	%
45.77.65.211	8,966	90.047%
52.40.10.231	317	3.184%
172.31.10.10	383	3.043%
71.39.18.125	133	1.336%
174.289.13.154	125	1.255%
10.0.2.189	98	0.904%
136.0.2.138	17	0.171%
136.0.0.125	6	0.06%

Fourth question:

We will use the filter index="botsv2" sourcetype="stream:HTTP" 45.77.65.211. Then we go to the Interesting Fields list and scroll down to uri_path. We will find that

/member.php

The screenshot shows a Splunk search interface with the following details:

- New Search:** index="botsv2" sourcetype="stream:HTTP" 45.77.65.211
- Events (11,082):** 11,082 events (before 12/10/25 3:56:44.000 AM) No Event Sampling
- Interesting Fields:** uri_path
- Reports:** Top values, Top values by time, Rare values
- Events with this field:** >100 Values, 92.329% of events
- Top 10 Values Table:**

Top 10 Values	Count	%
/member.php	662	7.383%
/search.php	164	1.829%
/	47	0.524%
/admin/	6	0.067%
/Debian-exim/	4	0.045%
/GekBd.html	4	0.045%
/apache/	4	0.045%
/archive/	4	0.045%
/backup/	4	0.045%
/cache/	4	0.045%

Fifth question:

We will use the filter index="botsv2" sourcetype="stream:HTTP" 45.77.65.211 "uri_path="/member.php"

```
|dedup form_data
```

```
|table form_data
```

And we will find that the SQL function being abused on the URI path is **updatexml**

Sixth question:

We will use the filter `index="botsv2"` Kevin /member.php

|dedup cookie

|table cookie

Then we will find the

value of the cookie

which will be: 1502408189

Seventh question:

We will use the filter index="botsv2" brewertalk.com sourcetype="stream:http" | table form_data uri

Then we will search for the username and find it is klagerfield

Why did we use `form_data`? Because the username only appears in

`'form_data'`

Because creating a new user is done through a registration form

New Search	
Index: "botvizi" _sourceType:"stream http" _id:_id form_data_id	
1,082 events (before 12/10/25 5:35:40:000 AM) No Event Sampling ▾	
Events	Patterns
Statistics (1,082)	Visualization
20 Per Page ▾	Format ▾
Preview ▾	1 / 1000
form_data * action=activate&id=452253E3Ccr1pt53E&er1t53E&er1t5279385AC54NE03B#Pf359327t3C5z2fscript3E action=activate&id=452253E3Ccr1pt53E&document,location:30822t3p3A3f2P45,-77.65,-21153A99993#MicrosoftUserFeedbackService3fmetric3t0822529328526document.cookie:J83X3C32fscript3E action=activate&id=452253E3Ccr1pt53E&document,location:30822t3p3A3f2P45,-77.65,-21153A99993#MicrosoftUserFeedbackService3fmetric3t0822529328526document.cookie:J83X3C32fscript3E action=activate&id=452253E3Ccr1pt53E&document,location:30822t3p3A3f2P45,-77.65,-21153A99993#MicrosoftUserFeedbackService3fmetric3t0822529328526document.cookie:J83X3C32fscript3E action=activate&id=452253E3Ccr1pt53E&document,location:30822t3p3A3f2P45,-77.65,-21153A99993#MicrosoftUserFeedbackService3fmetric3t0822529328526document.cookie:J83X3C32fscript3E action=activate&id=452253E3Ccr1pt53E&document,location:30822t3p3A3f2P45,-77.65,-21153A99993#MicrosoftUserFeedbackService3fmetric3t0822529328526document.cookie:J83X3C32fscript3E action=activate&id=452253E3Ccr1pt53E&document,location:30822t3p3A3f2P45,-77.65,-21153A99993#MicrosoftUserFeedbackService3fmetric3t0822529328526document.cookie:J83X3C32fscript3E action=_nologin@http://www.botvizi.com/_nouser.read.php?tid=1&logick_login=1&logick_username=franklin01&logick_password=bertha&logick_remember=yes&subtab1=login action=_nologin@http://www.botvizi.com/_nouser.read.php?tid=1&logick_login=1&logick_username=franklin01&logick_password=bertha&logick_remember=yes&subtab1=login action=_nologin@http://www.botvizi.com/_api/login?logick_login=1&logick_username=franklin01&logick_password=bertha_1zulzq101&remember=yes&subtab1=login action=_nologin@http://www.botvizi.com/_api/login?logick_login=1&logick_username=franklin01&logick_password=bertha_1zulzq101&remember=yes&subtab1=login	

Task 5: 300 series questions

Answer the questions below	
Mallory's critical PowerPoint presentation on her MacBook gets encrypted by ransomware on August 18. What is the name of this file after it was encrypted?	<input type="text"/> fronty_marketing_campaign_Q117.pptx.crypt ✓ Correct Answer
There is a Games of Thrones movie file that was encrypted as well. What season and episode is it?	<input type="text"/> S07E02 ✓ Correct Answer 0
Kevin Lagerfeld used a USB drive to move malware onto kutekitten, Mallory's personal MacBook. She ran the malware, which obfuscates itself during execution. Provide the vendor name of the USB drive Kevin likely used. Answer Guidance: Use time correlation to identify the USB drive.	<input type="text"/> Alcor Micro Corp. ✓ Correct Answer
What programming language is at least part of the malware from the question above written in?	<input type="text"/> Perl ✓ Correct Answer
When was this malware first seen in the wild? Answer Guidance: YYYY-MM-DD	<input type="text"/> 2017-01-17 ✓ Correct Answer
The malware infecting kutekitten uses dynamic DNS destinations to communicate with two C&C servers shortly after installation. What is the fully-qualified domain name (FQDN) of the first (alphabetically) of these destinations?	<input type="text"/> elk4.duckdns.org ✓ Correct Answer
From the question above, what is the fully-qualified domain name (FQDN) of the second (alphabetically) contacted C&C server?	<input type="text"/> elk5.hopto.org ✓ Correct Answer

First question:

Initially, we will use the filter index="botsv2" host="MACLORY-AIR13" (*.ppt OR *.pptx)

Then, the name of the critical presentation file will appear on the first line.

_Frothly_marketing_campaign_Q317.pptx.crypt

The screenshot shows the Splunk search interface with the following details:

- Search Bar:** index=_internal host=*.mcdriven.com [Aug 10, 2017 - Aug 11, 2017]
- Time Range:** 7 events (before 10/10/25 00:00:00,000 AM) - No Event Sampling
- Event Count:** 2
- Event Preview:** (Zoom Out) ▾ (Zoom In) ▾ (Details)
- List View:** List ▾ Format 20 Per Page
- Fields:** _Host, _Index, _Time, _Event
- Selected Fields:** _Host, _Index, _Time, _Event, source, sourcetype
- Interesting Fields:** _Host, _Index, _Time, _Event, source, sourcetype
- Time Range:** 12:40:02 02/08/2017, 9:50:43 03/08/2017

The search results table shows two events:

Time	Event
12:40:02 02/08/2017	[{"_source": "kraemson_marketing", "host": "128.111.128.247", "sourcetype": "log", "type": "MACD�WRS", "value": "2017-08-10T12:40:02Z"}, {"_source": "kraemson_marketing", "host": "128.111.128.247", "sourcetype": "log", "type": "MACD�WRS", "value": "2017-08-10T12:40:02Z"}]
9:50:43 03/08/2017	[{"_source": "kraemson_marketing", "host": "128.111.128.247", "sourcetype": "log", "type": "MACD�WRS", "value": "2017-08-10T09:50:43Z"}, {"_source": "kraemson_marketing", "host": "128.111.128.247", "sourcetype": "log", "type": "MACD�WRS", "value": "2017-08-10T09:50:43Z"}]

Second question:

First, we'll use the filter index="botsv2" host="MACLORY-AIR13" *.crypt. Then we'll see the season and episode, which will be S07E02

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** Under "New Search", the query is: `index=_internal host=MACLOR#42813 +crypt`.
- Event Count:** 1,003 events (before 12/05/2015 08:54:00 AM) - No Event Sampling.
- Events (1,003):** Patterns, Statistics, Visualization.
- Format Timeline:** Zoom Out, Zoom In Selection, Selected.
- Event List:**
 - Fields:** Hide Fields, All Fields.
 - Event 1:**
 - Time:** 8/19/17 8:46:10 AM
 - Event:** {
 - action:** added
 - createdTime:** Sat Aug 19 08:46:10 2017 UTC
 - decoration:** { ... }
 - host:** MACLOR#42813.local
 - hostId:** 1001
 - lastUpdate:** 1503521918
 - source:** /var/log/cryptd.log
 - time:** 8/19/17 8:46:10 AM
 - Show as raw text:** host=MACLOR#42813 source=/var/log/cryptd.log sourcetype=crypt_results
 - Event 2:**
 - Time:** 8/19/17 8:46:10 AM
 - Event:** {
 - host:** MACLOR#42813
 - source:** p4
 - sourcetype:** p4

Third question:

First, we'll use the filter index="botsv2" kutekitten "\\\users\\mkraeuse", then go to Selected Fields and choose sourcetype

then osquery_results

New Search

1 index="botsv2" kutekitten "\\\users\\mkraeuse"

300 events (before 12/10/25 6:55:17.000 AM) No Event Sampling ▾

Events (300) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect

i	Time	Event
>	8/29/17 11:10:15.000 AM	{ [-] action: added

SOURCETYPE

1 Value, 100% of events

REPORTS

Top values Top values by time Events with this field

VALUES

osquery_results

Then we go to columns.target_path and select the first option

columns.target_path

1 Value, 1.667% of events Selected Yes No

REPORTS

Top values Top values by time Rare values

EVENTS WITH THIS FIELD

Values	Count	%
/Users/mkraeuse/Downloads/	5	100%

Then we go down to the last event, take the hash, and go to VirusTotal to verify it

36/58 security vendors flagged this file as malicious

bfa98fe488244c64db096522bfad73fd01ea8c4cd0323f1cbdee81ba008271

fpseud

Community Score 36 / 58

File size 13.18 KB

Last Analysis Date 3 months ago

Tags perl sets-process-name ssh detect-debug-environment malware checks-hostname ssh-communication checks-cpu-name exploit

First, we'll change the event time to the last minute. Then, we'll use the keyword "usb". Next, we'll take "model_id": "6387" and "vendor_id": "058f" and go to the DeviceHunt website to retrieve the USB name

Index="botsv2" kutekitten usb

2 events (8/3/17 6:18:07.000 PM to 8/3/17 6:20:07.000 PM) No Event Sampling ▾

Events (2) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect

i	Time	Event
>	8/3/17 6:18:10.000 PM	{ "name": "pack_hardware-monitoring_usb_devices", "hostIdentifier": "kutekitten.local", "calendarTime": "Thu Aug 03 18:18:18 2017 UTC", "unixTime": "1501784296", "decorations": { "host_id": "00000000-0000-1000-0000-000000000000", "host_label": "kutekitten.local", "host_ip": "110.10.10.10", "host_mac": "00:0C:29:6A:4C:57", "username": "mkraeuse"}, "columns": [{ "name": "model_id", "value": "6387" }, { "name": "product_id", "value": "058f" }, { "name": "serial_number", "value": "1" }] } host = kutekitten source = /var/log/osquery/osqueryd.results.log sourcetype = osquery_results
>	8/3/17 6:18:10.000 PM	{ "action": "removed", "calendarTime": "Thu Aug 03 18:18:18 2017 UTC", "host": "kutekitten", "source": "/var/log/osquery/osqueryd.results.log", "sourcetype": "osquery_results", "columns": [{ "name": "model_id", "value": "6387" }] }

Type	Vendor ID	Device ID
USB	058F	6387

Device Details

Flash Drive

Type	Information
ID	6387

Vendor Details

Alcor Micro Corp.

Fourth question:

Go back to VirusTotal, then go to Details, and you will find the answer. perl

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks

Fifth question:

You will find the answer in the same place as the previous question 2017-01-17

History	
First Seen In The Wild	2017-01-17 19:09:06 UTC
First Submission	2017-01-31 16:54:15 UTC
Last Submission	2025-03-17 23:18:35 UTC
Last Analysis	2025-09-09 08:44:27 UTC

Sixth question:

Go to the hybrid-analysis website. Then enter the hash and scroll down to Network Analysis. You will find the answer at eidk.duckdns.org



**H Y B R I D
A N A L Y S I S**

Sandbox • Quick details.

Analysed 1 process in total.

 perl perl /tmp/befa9bfe4882.pl (PID: 1824)

Logged Script Calls	Logged Stdout	Extracted Streams	Memory
 Reduced Monitoring	 Network Activity	 Network Error	 Multi

Network Analysis

DNS Requests

Login to Download DNS Requests (CSV)

Domain

[e1dk.duckdns.org](#)



Seventh question:

In the same way as the previous question, you will find the answer below: eidk.hopto.org

The screenshot shows the Hybrid Analysis interface. At the top, there's a logo with three overlapping circles in red, green, and blue, followed by the text "HYBRID ANALYSIS". To the right are links for "Sandbox", "File", and "Quit". Below the logo is a green bar with the word "details." in white. The main content area has a title "Analysed 1 process in total." and a command line input field: "`perl perl /tmp/bef9bfe4882.pl` (PID: 1824)". Below this are several tabs: "Logged Script Calls", "Logged STDOUT", "Extracted Streams", "Reduced Monitoring" (which is selected), "Network Activity", and "Network Error". The "Reduced Monitoring" tab displays a table with two rows. The first row is for "elidk.duckdns.org" with status "DNSINT". The second row is for "elidk.hopto.org" with status "DNSINT". A "Domain" section is also present. At the bottom, there's a "Login to Download DNS Requests (CSV)" button.

Task 6: 400 series questions

A Federal law enforcement agency reports that Taedonggang often spear phishing its victims with zip files that have to be opened with a password. What is the name of the attachment sent to Frothly by a malicious Taedonggang actor?	invoice.zip	✓ Correct Answer
What is the password to open the zip file?	912345678	✓ Correct Answer
The Taedonggang APT group encrypts most of their traffic with SSL. What is the "SSL Issuer" that they use for the majority of their traffic? Answer guidance: Copy the field exactly, including spaces.	C = US	✓ Correct Answer
What unusual file (for an American company) does winsys32.dll cause to be downloaded into the Frothly environment?	나는_데이비드를_사랑한다.hwp	✓ Correct Answer
What is the first and last name of the poor innocent sap who was implicated in the metadata of the file that executed PowerShell Empire on the first victim's workstation? Answer example: John Smith	Ryan Kovar	✓ Correct Answer
Within the document, what kind of points is mentioned if you found the text?	CyberEastEgg	✓ Correct Answer
To maintain persistence in the Frothly network, Taedonggang APT configured several Scheduled Tasks to beacon back to their C2 server. What single webpage is most contacted by these Scheduled Tasks? Answer example: index.php or images.html	process.php	✓ Correct Answer

Question 1:

We will use the filter index="botsv2" sourcetype="stream:smtp" *.zip. Then we will go to the Selected Fields list, then to attach_filename{}, and then we will find the attachment name invoice.zip

New Search

1 index="totals" sourcetype="stream:setup" .zip

✓ 6 events (before 12/10/25 7:58:43 0000 AM) No Event Sampling *

Events (6) Patterns Statistics Visualization

Format Timeline ▾ Zoom Out ▾ Zoom In Selection ▾ Document

Format Timeline ▾ ▾ Zoom Out ▾ Zoom In Selection ▾ Document

List ▾ Format 20 Per Page ▾

◀ Hide Fields ▶ All Fields

Selected Fields

- ↳ field_1
- ↳ source_1
- ↳ sourcetype_1

Interesting Fields

- ↳ ack_packets_in_2
- ↳ ack_packets_out_5
- ↳ attach_disposition_1
- ↳ attach_size_1
- ↳ attach_size_decoded_1
- ↳ attach_size_1
- ↳ attach_transfer_encoding_1
- ↳ attach_type_1

Time ▾ Event

> 8:26:07 (-2)

attach_filename@

1 Value, 66.667% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values Count %

Value	Count	%
host-a.zip	4	100%

Question 2:

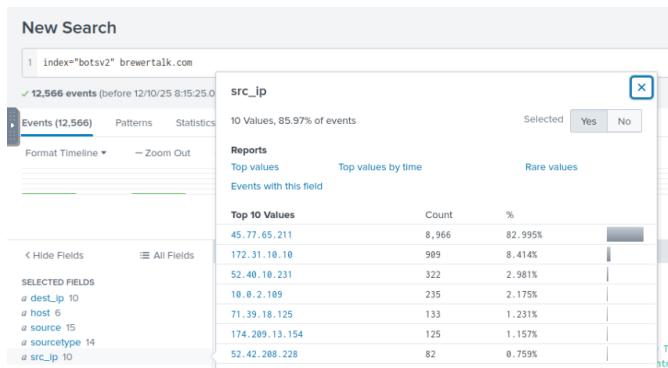
First, we'll use the filter index="botsv2" sourcetype="stream:smtp" *.zip
""attach_filename{}"="invoice.zip

Then, we'll click on "Show as raw text" at the end of the first event, and then we'll search for the password, which will be 912345678

Question 3:

First, we need to find the attacker's IP address. Remember, there was an IP address scanning brewertalk.com. We'll use the filter index="botsv2" brewertalk.com

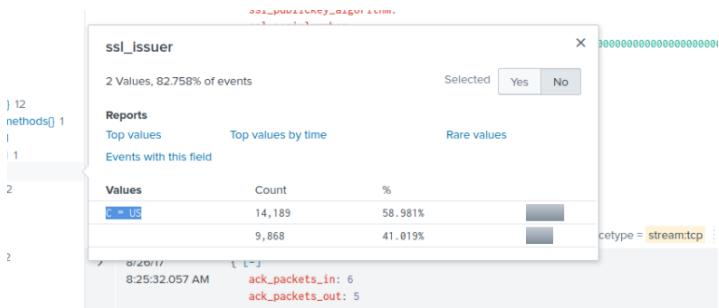
Then, we'll go to src_ip, and the IP address will be 45.77.65.211



Then we will use the filter index="botsv2" sourcetype="stream:tcp" 45.77.65.211

Then go down to ssl_issuer

After that you will find the answer $C = US$



Question 4:

First, we'll use the filter index="botsv2" sourcetype="stream:ftp"

Then we'll go to method and then RETR to narrow down the search

After that, we'll go to filename and then find the unusual filename

filename	x
7 Values, 100% of events	Selected Yes No
Reports	
Top values Top values by time Rare values	
Events with this field	
Values	Count %
dns.py	2 14.286%
nc.exe	2 14.286%
psexec.exe	2 14.286%
python-2.7.6.amd64.msi	2 14.286%
wget64.exe	2 14.286%
winsys64.dll	2 14.286%
나는_데이비드를_사랑한다_.hwp	2 14.286%

Question 5:

Using the hash of the malicious file, we will access the VirusTotal website and find the answer, which is Ryan Kovar

Question 6:

Go to app.any.run and you will find the answer CyberEastEgg

Question 7:

We will use the filter index="botsv2" HKLM\\Software\\Microsoft\\Network. Then we will go down to any event and look at the data. We will see that it is in base64 format. We will go to decompile it, and after that, the output will appear as process.php

Task 7: Conclusion

Task 7 Conclusion

In this room, you navigated through the [Splunk Boss of the Soc 2 \(BOTS2\)](#) competition dataset to increase our capabilities using Splunk.

The 500 series questions were intentionally omitted from this room as the questions didn't go with the theme of the APT hunt.

You're encouraged to download the dataset into a local Splunk instance and give it a go at the other questions within the dataset.

Below is additional data from the [Advanced Hunting APTs with Splunk](#) app under [Supplemental Material](#).

Taedonggang Diamond Model

What is the Diamond Model? Read more about this [here](#).