

Kevin Cendana
CSC 154
Spring 2024

Lab 08-2 - Incident Response and Threat Hunting

Task 1

- 1) Installed Splunk on Ubuntu VM using the `deb` installer downloaded from Splunk's official site.



A verification email has been sent to you

Check your inbox and verify your email address to get started. If you don't see it, please check your spam folder.

Choose Your Installation Package



| 64-bit | 3.x+, 4.x+, or 5.4.x kernel Linux distributions | .deb | 520.37 MB | Download Now | Copy wget link | More ▾ |
|--------|---|------|-----------|------------------------------|--------------------------------|--------|
| | | .tgz | 679.42 MB | Download Now | Copy wget link | More ▾ |
| | | .rpm | 679.24 MB | Download Now | Copy wget link | More ▾ |

```
After this operation, 454 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libcurl4 amd64 7.81.0-1ubuntu1.16 [290 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 curl amd64 7.81.0-1ubuntu1.16 [194 kB]
Fetched 484 kB in 2s (206 kB/s)
(Reading database ... 231696 files and directories currently installed.)
Preparing to unpack .../libcurl4_7.81.0-1ubuntu1.16_amd64.deb ...
Unpacking libcurl4:amd64 (7.81.0-1ubuntu1.16) over (7.81.0-1ubuntu1.13) ...
Selecting previously unselected package curl.
Preparing to unpack .../curl_7.81.0-1ubuntu1.16_amd64.deb ...
Unpacking curl (7.81.0-1ubuntu1.16) ...
Setting up libcurl4:amd64 (7.81.0-1ubuntu1.16) ...
Setting up curl (7.81.0-1ubuntu1.16) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
kevin@ubuntu:~$ sudo dpkg -i ~/Downloads/splunk*.deb
Selecting previously unselected package splunk.
(Reading database ... 231703 files and directories currently installed.)
Preparing to unpack .../splunk-9.2.1-78803f08aabb-linux-2.6-amd64.deb ...
Unpacking splunk (9.2.1+78803f08aabb) ...
Setting up splunk (9.2.1+78803f08aabb) ...
complete
kevin@ubuntu:~$
```

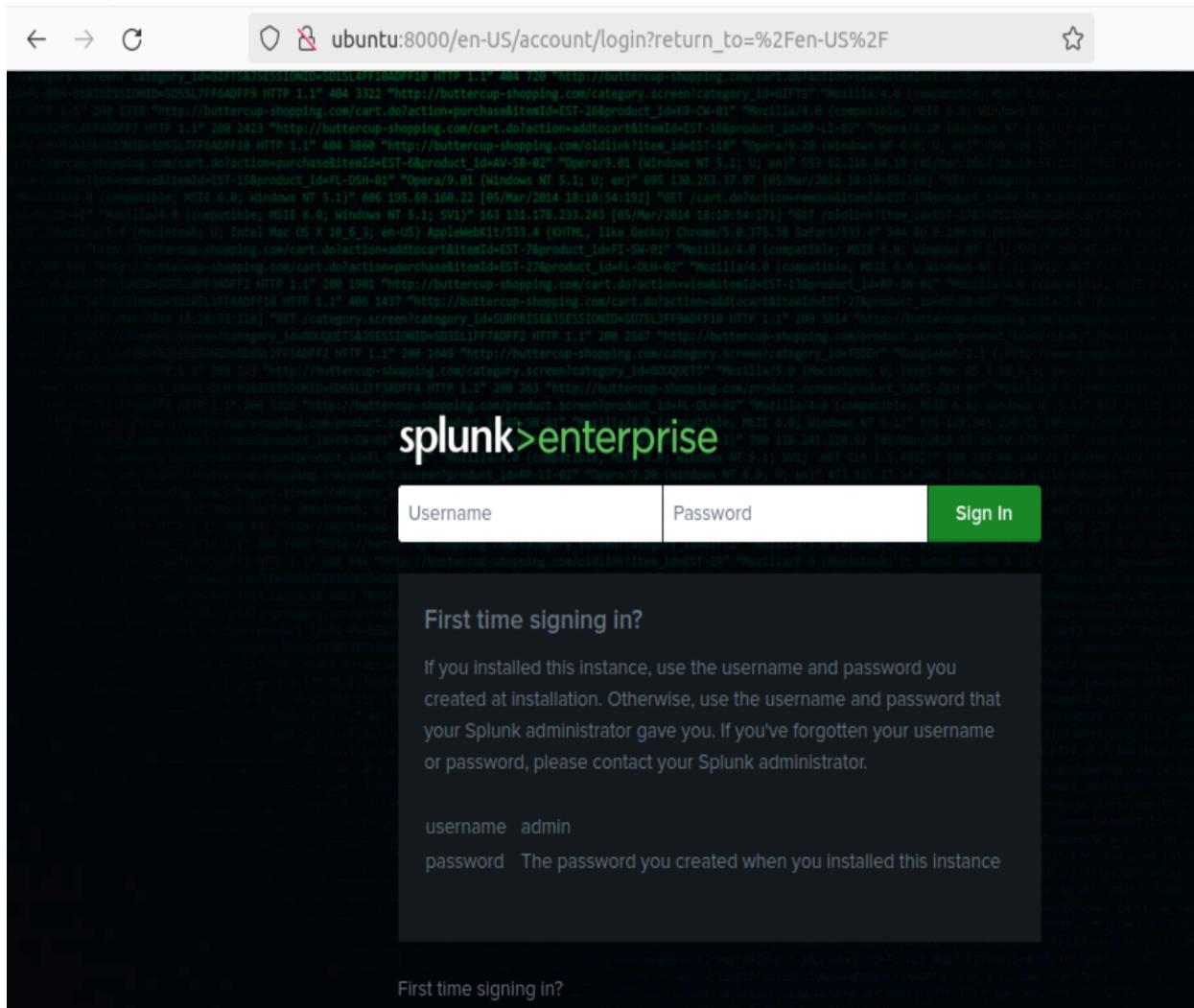
```
Done
All preliminary checks passed.
```

```
Starting splunk server daemon (splunkd)...
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'privKeySecure.pem'
-----
Signature ok
subject=/CN=ubuntu/O=SplunkUser
Getting CA Private Key
writing RSA key
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries shipped with the embedded Python interpreter; must be set to "1" for increased security
Done
```

```
Waiting for web server at http://127.0.0.1:8000 to be available....
```

Kevin Cendana
CSC 154
Spring 2024

2) Started Splunk and set up an account with a chosen username and password.



Kevin Cendana

CSC 154

Spring 2024

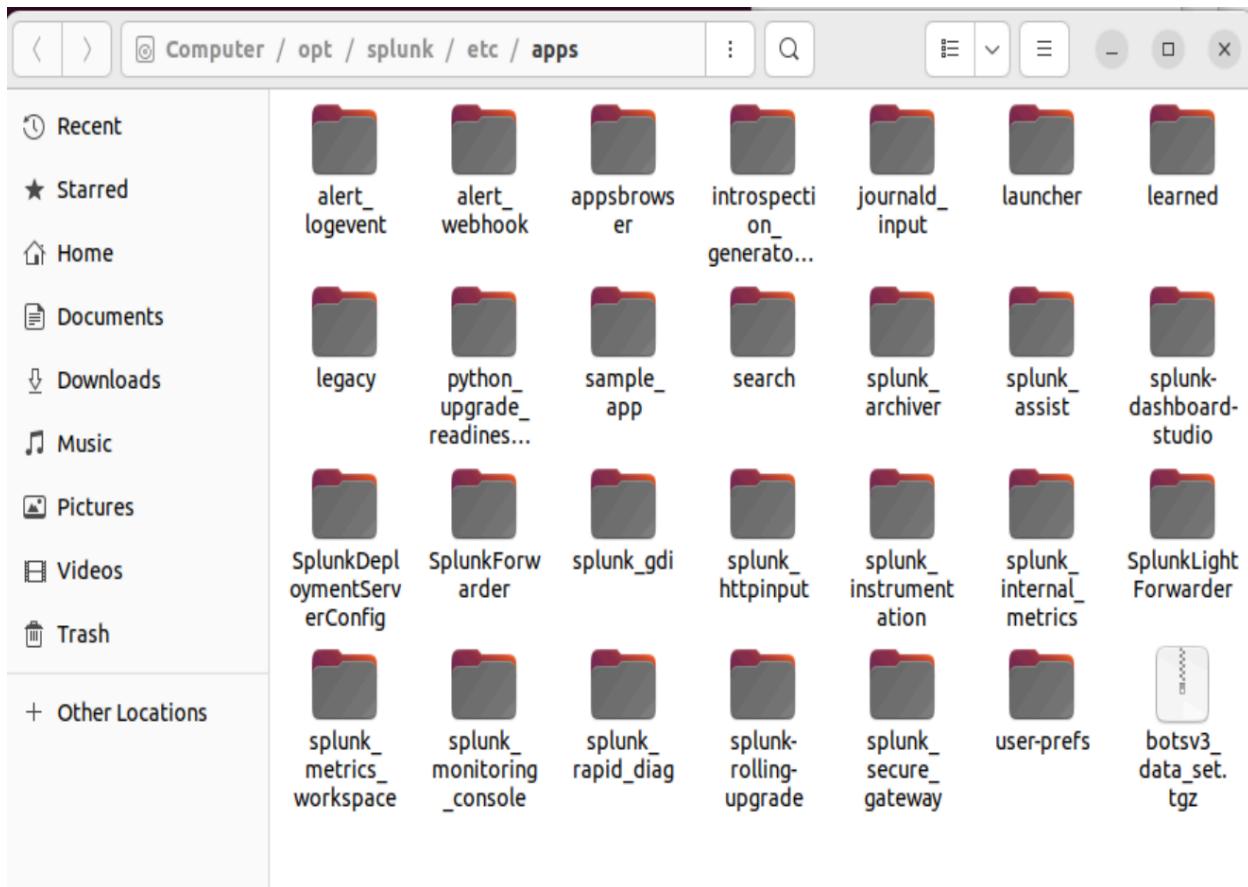
The screenshot shows the Splunk Enterprise interface. At the top, there is a navigation bar with the Splunk logo, a search bar, and links for 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a 'Find' button. Below the navigation bar, the main dashboard is titled 'Hello, Administrator'. On the left side, there is a sidebar titled 'splunk > listen to your data' with a search bar and a list of apps: 'Search & Reporting', 'Splunk Secure Gateway', and 'Upgrade Readiness App'. There is also a link to 'Find more apps'. The main content area is titled 'Common tasks' and contains six cards: 'Add data' (Add data from a variety of common sources), 'Search your data' (Turn data into doing with Splunk search), 'Visualize your data' (Create dashboards that work for your data), 'Add team members' (Add your team members to Splunk platform), 'Manage permissions' (Control who has access with roles), and 'Configure mobile devices' (Login or manage mobile devices using Splunk Secure Gateway).

- 3) Loaded the BOTS V3 Dataset into Splunk and restarted the system to make the data available for queries.

Kevin Cendana

CSC 154

Spring 2024



New Search

Save As ▾ Create Table View Close

index=botsv3 | All time ▾ 

31,512 of 26,519 events matched No Event Sampling ▾ Job ▾ II ■ ↗ ↓ Smart Mode ▾

Events (31,512) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 1 month per column

Sep 1, 2018

List ▾ Format 20 Per Page ▾ ◀ Prev 1 2 3 4 5 6 7 8 ... Next ▾

| i | Time | Event |
|---|----------------------------|--|
| > | 9/19/19 11:10:50.000 AM | <error><message>Splunkd daemon is not responding: ('Error connecting to /services/shclus: host = OD-FM-NA-I-0ad2d665d4bdace22.amazonaws.com source = ess_content_importer soi </error> |
| > | 8/20/18 8:27:09.296 AM | { [-] bytes: 50637 bytes_in: 30 bytes_out: 50607 dest_ip: 172.16.0.178 dest_mac: 02:A0:38:1B:B3:70 endtime: 2018-08-20T15:27:09.296788Z flow_id: c240fdab-997d-4285-a221-1080976a6b8a fragment_count: 0 packets_in: 1 packets_out: 36 protocol: UDP protocol_stack: ip:udp:unknown protoid: 17 src_ip: 13.125.33.130 src_mac: 02:4F:D7:61:53:04 timestamp: 2018-08-20T15:27:09.296118Z tos: 0 |

- 4) Used SPL to filter and count events from the "matar" host within the BOTSV3 index.

Kevin Cendana
CSC 154
Spring 2024

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

- Search Bar:** index=botsv3 host=matar | stats count by source
- Time Range:** All time
- Event Count:** 84,337 events (before 4/27/24 8:46:10.000 PM)
- Sampling:** No Event Sampling
- Job Status:** Job
- Mode:** Smart Mode

The results table displays 21 rows of data, ordered by count (descending). The columns are source and count.

| source | count |
|-----------------------------------|-------|
| stream:Splunk_DNSClientQueryTypes | 170 |
| stream:Splunk_DNSIntegrity | 479 |
| stream:Splunk_DNSRequestResponse | 652 |
| stream:Splunk_DNSServerQuery | 308 |
| stream:Splunk_DNSServerResponse | 308 |
| stream:Splunk_HTTPClient | 1 |
| stream:Splunk_HTTPResponseTime | 1 |
| stream:Splunk_HTTPStatus | 1 |
| stream:Splunk_HTTPURI | 1 |
| stream:Splunk_IP | 2225 |
| stream:Splunk_SSLActivity | 2 |
| stream:Splunk_Tcp | 750 |
| stream:Splunk_Udp | 328 |
| stream:arp | 672 |
| stream:dhcp | 22 |
| stream:dns | 27502 |

src_mac: 06:E3:CC:18:AA:33
src_port: 1920
subject: Fw: All your datas belong to us
time_taken: 354670
timestamp: 2018-08-20T15:19:34.777033Z

```
-----  
sender_alias: Grace Hoppy  
sender_email: ghoppy@froth.ly  
server_response: 250 2.0.0 Ok: queued as 6C7831794E8  
src_ip: 104.47.38.43  
src_mac: 06:E3:CC:18:AA:33  
src_port: 1920  
subject: Fw: All your datas belong to us  
time_taken: 354670  
timestamp: 2018-08-20T15:19:34.777033Z  
transport: tcp  
  
src_ip: 104.47.38.43  
src_mac: 06:E3:CC:18:AA:33  
src_port: 1920
```

- 5) Created a report showing the top 10 source IP addresses in the BOTSV3 index and saved it for future reference.

Search Analytics Datasets

New Search

```
index=botsv3 | stats count as cnt
```

✓ 2,083,056 events (before 4/27/24 9:01:23 PM)

Events Patterns Statistics (10) **Statistics Table**

20 Per Page ▾ Format Prev

host ↴

- host
- serverless
- BSTOLL-L

Save As Report

Title: Top 10 Hosts

Description: optional

Content: Statistics Table

Time Range Picker: Yes No

Cancel Save

Top 10 Hosts

All time ▾

✓ 2,083,056 events (before 4/27/24 9:10:23.000 PM)

Edit ▾ More Info ▾ Add to Dashboard ▾

Job ▾

| host ↴ | cnt ↴ |
|------------------------------|--------|
| host | 382718 |
| serverless | 247791 |
| BSTOLL-L | 240882 |
| gacrux.i-0920036c8ca91e501 | 175345 |
| mars.i-08e52f8b5a034012d | 158512 |
| matar | 84337 |
| ip-172-16-0-109.ec2.internal | 83673 |
| FROTHLY-FW1 | 80192 |
| splunkhlf.froth.ly | 78478 |
| BTUN-L | 76371 |

Kevin Cendana

CSC 154

Spring 2024

6) Got stuck here, 0 results from the query 😞

The screenshot shows the Splunk Enterprise search interface. The top navigation bar includes links for Apps, Administrator, Messages, Settings, Activity, Help, and a search bar labeled 'Find'. Below the navigation is a secondary menu with options: Search, Analytics, Datasets, Reports, Alerts, and Dashboards. A green button labeled 'Search & Reporting' is visible. The main search area is titled 'New Search' and contains the following query:

```
source==* EventCode=4625  
| stats count as cnt
```

Below the query, it displays '0 events (before 4/27/24 9:26:20.000 PM)' and 'No Event Sampling'. The search results pane is titled 'Statistics (1)' and shows a single row with 'cnt' and a value of '0'. The interface includes various buttons and dropdown menus for job management and visualization.

7)

Task 2

1) Registered for and enrolled in the "Introduction to Enterprise Security" course on Splunk's training site.



FREE
COURSE

Introduction to Enterprise Security

Understand
the basics of
security
incidents and
how Enterprise
Security can
help identify,
combat and
prevent
threats.

Download

Kevin Cendana
CSC 154
Spring 2024



Thank you, Kevin Cendana

Thank you! We have received your payment information. The purchased learning items are available in your [My Plan](#). An email notification will be sent to you. You can also view your [Order history](#) and make changes or cancel your enrollment within the time limit specified for respective learning items.

Order: 0001100096

Status: Confirmed

28-APR-2024

Order Details

| Item Details | | |
|--|------------|-----------------------------|
| Learning | Unit Price | Total Price (USD) |
|  Introduction to Enterprise Security (eLearning) eLearning Duration: 00:40 Language: English | 0.00 | 0.00 |
| | | Sub Total 0.00 |
| | | Cost Total(USD) 0.00 |

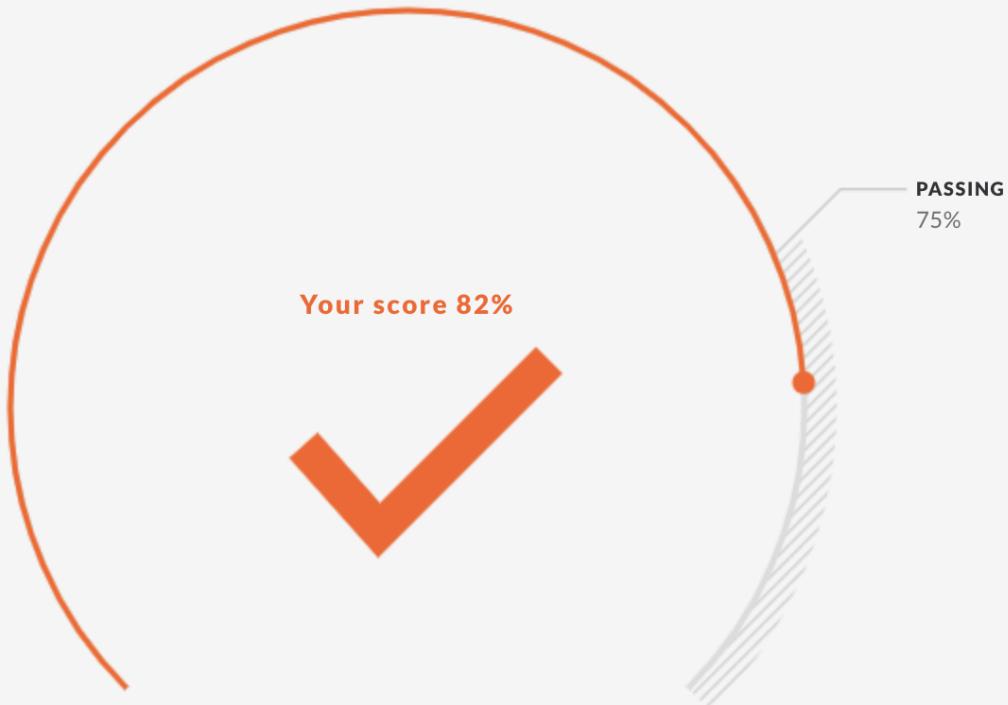
- 2) Watched the assigned video coursework, taking detailed notes for better understanding and future reference.
- 3) Completed the quiz associated with the course, achieving a score above the required 75% (82% in my case), and obtained a certificate of completion.

Kevin Cendana

CSC 154

Spring 2024

Quiz Results



TAKE AGAIN



Kevin Cendana
CSC 154
Spring 2024

