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.

Kevin Cendana
CSC 154
Spring 2024

splunk>

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

Windows | Linux | Mac OS

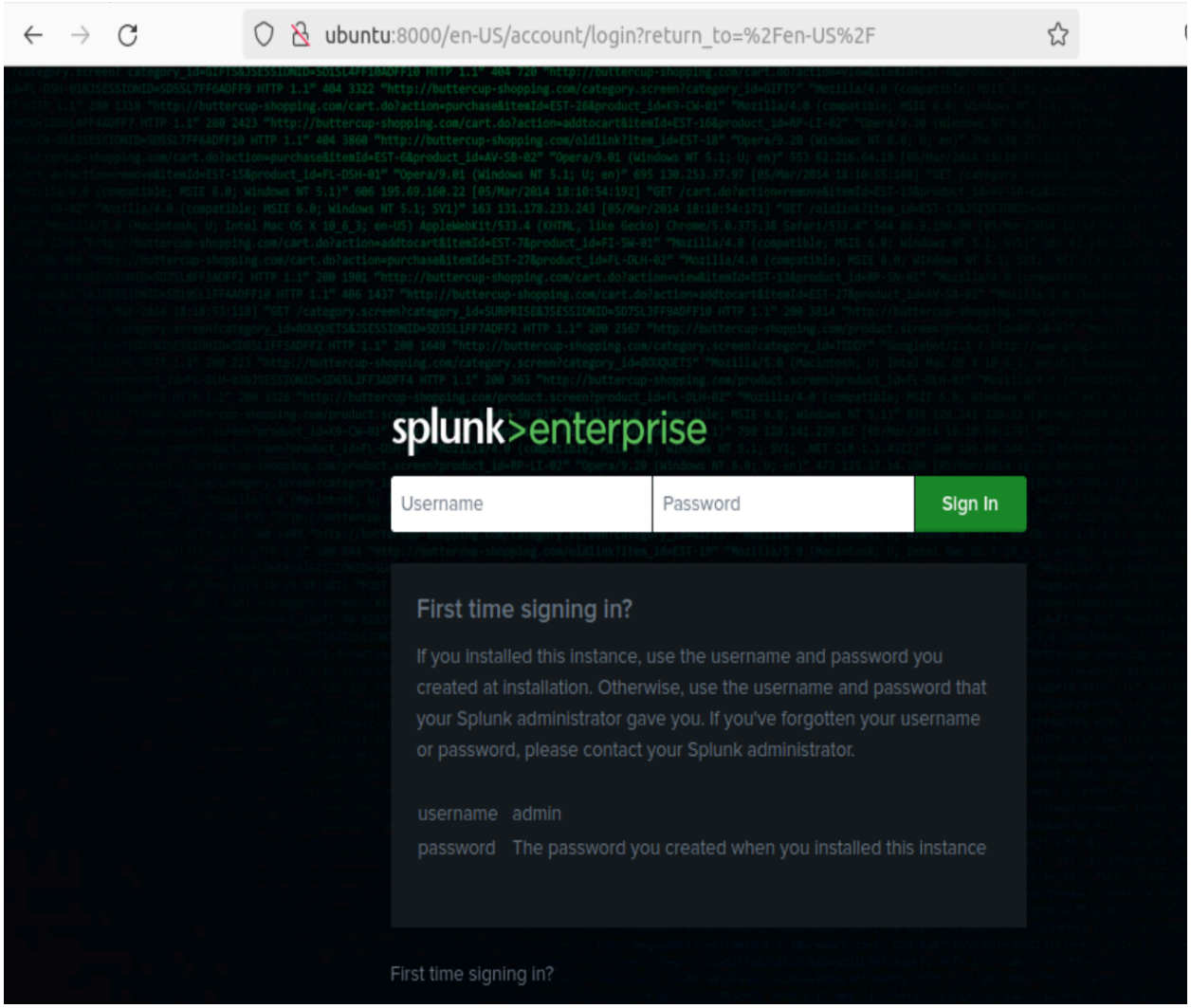
64-bit	3.x+, 4.x+, or 5.4.x kernel Linux distributions	.deb	520.37 MB	Download Now	Copy wget link	More
		.tgz	679.42 MB	Download Now	Copy wget link	More
		.rpm	679.24 MB	Download Now	Copy wget link	More

Kevin Cendana
CSC 154
Spring 2024

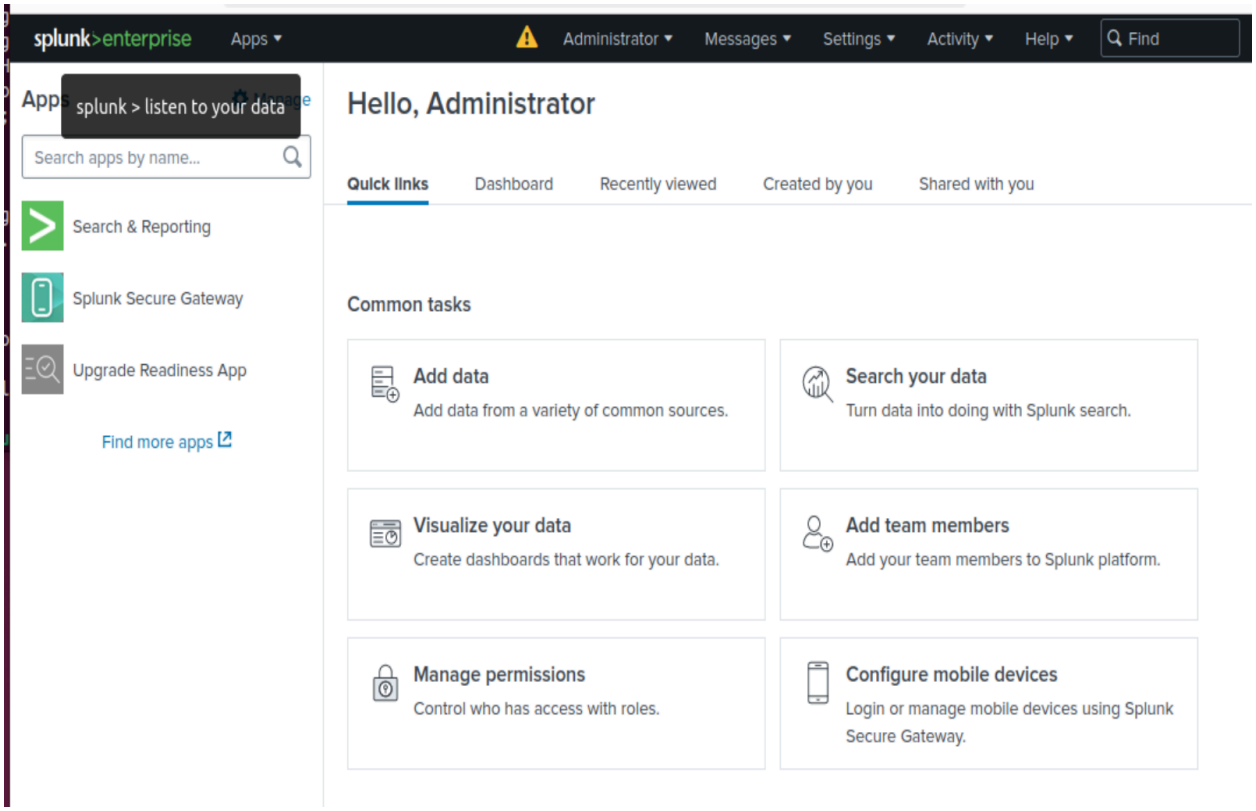
```
After this operation, 454 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libcurl4 amd6
4 7.81.0-1ubuntu1.16 [290 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 curl amd64 7.
81.0-1ubuntu1.16 [194 kB]
Fetched 484 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 valida
tion for the httplib and urllib libraries shipped with the embedded Python inter
preter; 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.

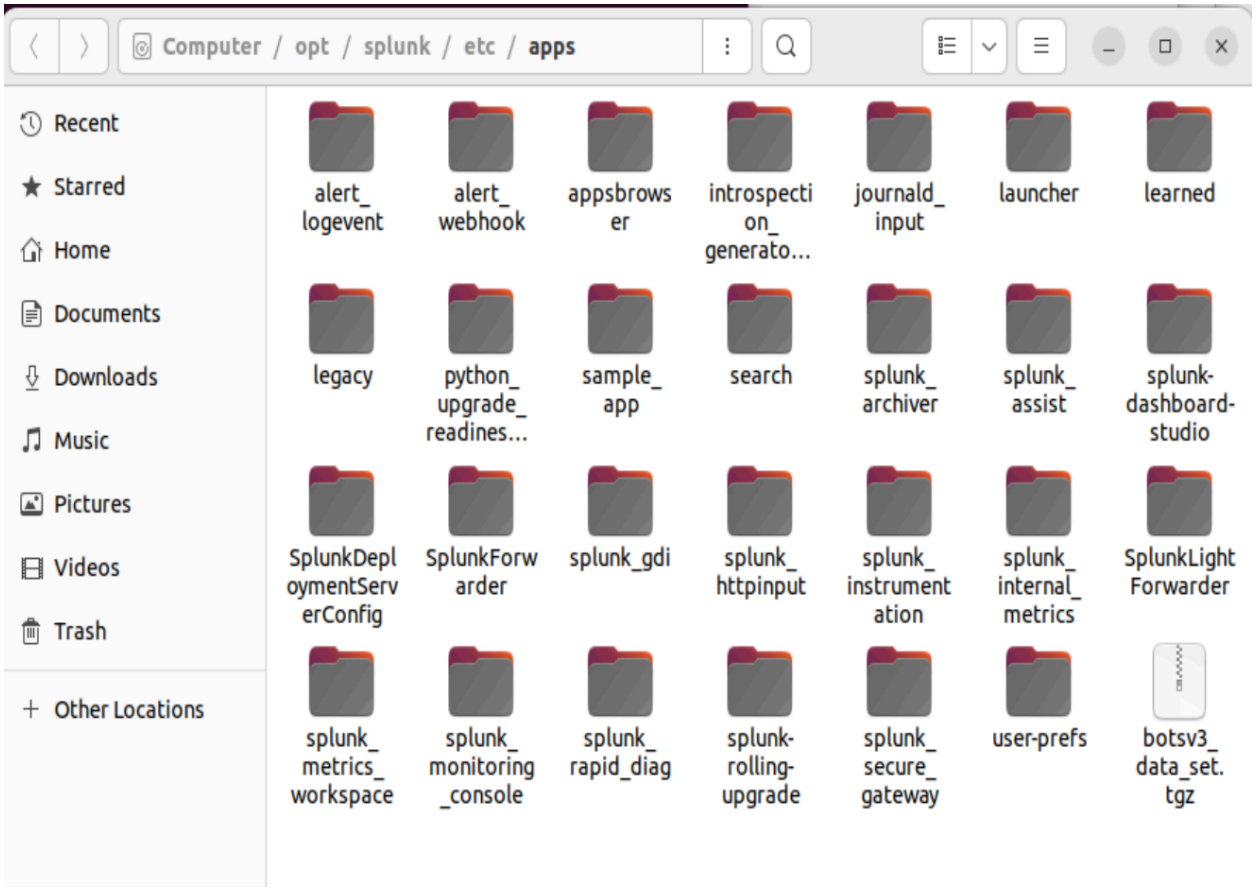


Kevin Cendana
CSC 154
Spring 2024

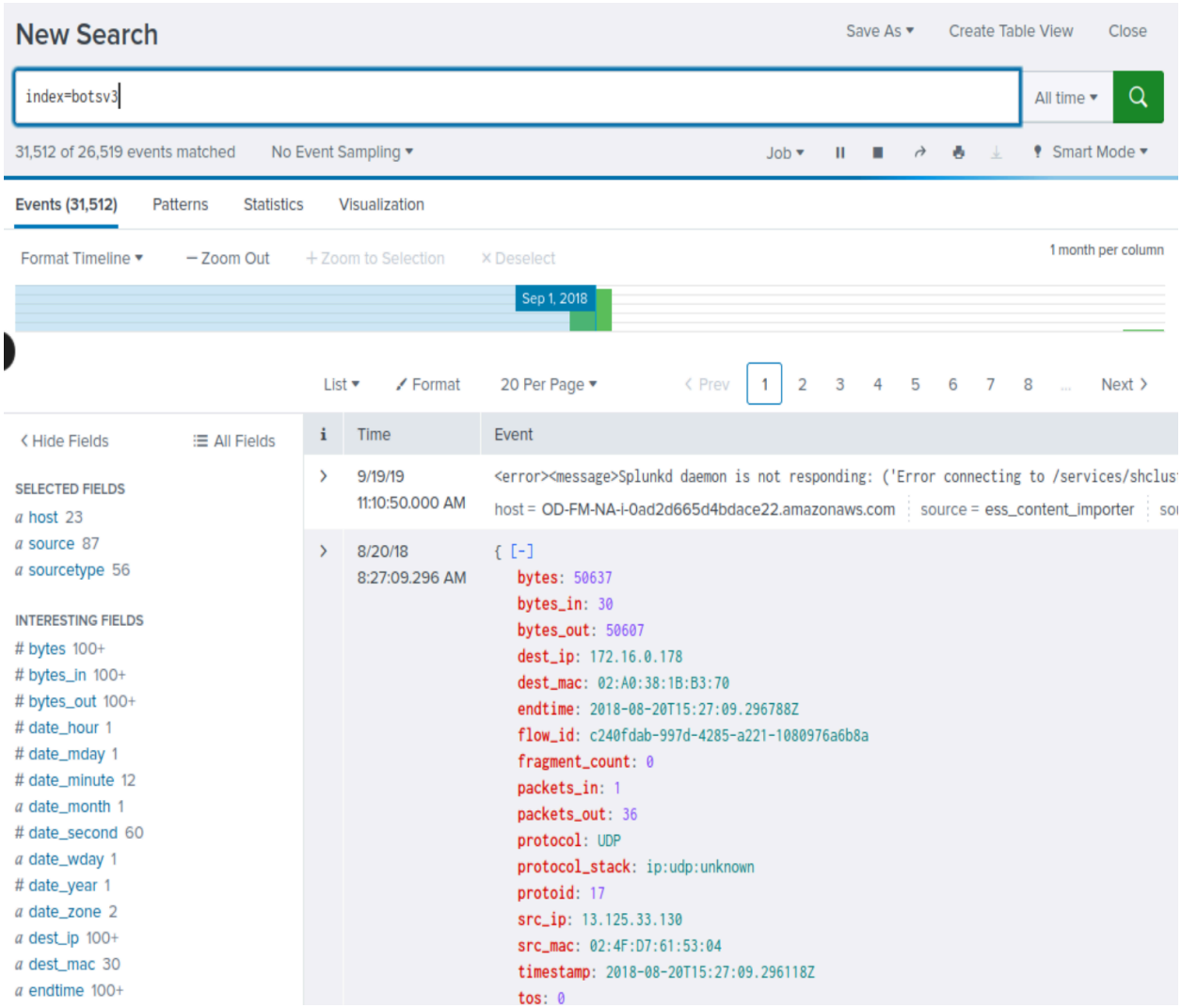


3) Loaded the BOTS V3 Dataset into Splunk and restarted the system to make the data available for queries.

Kevin Cendana
CSC 154
Spring 2024

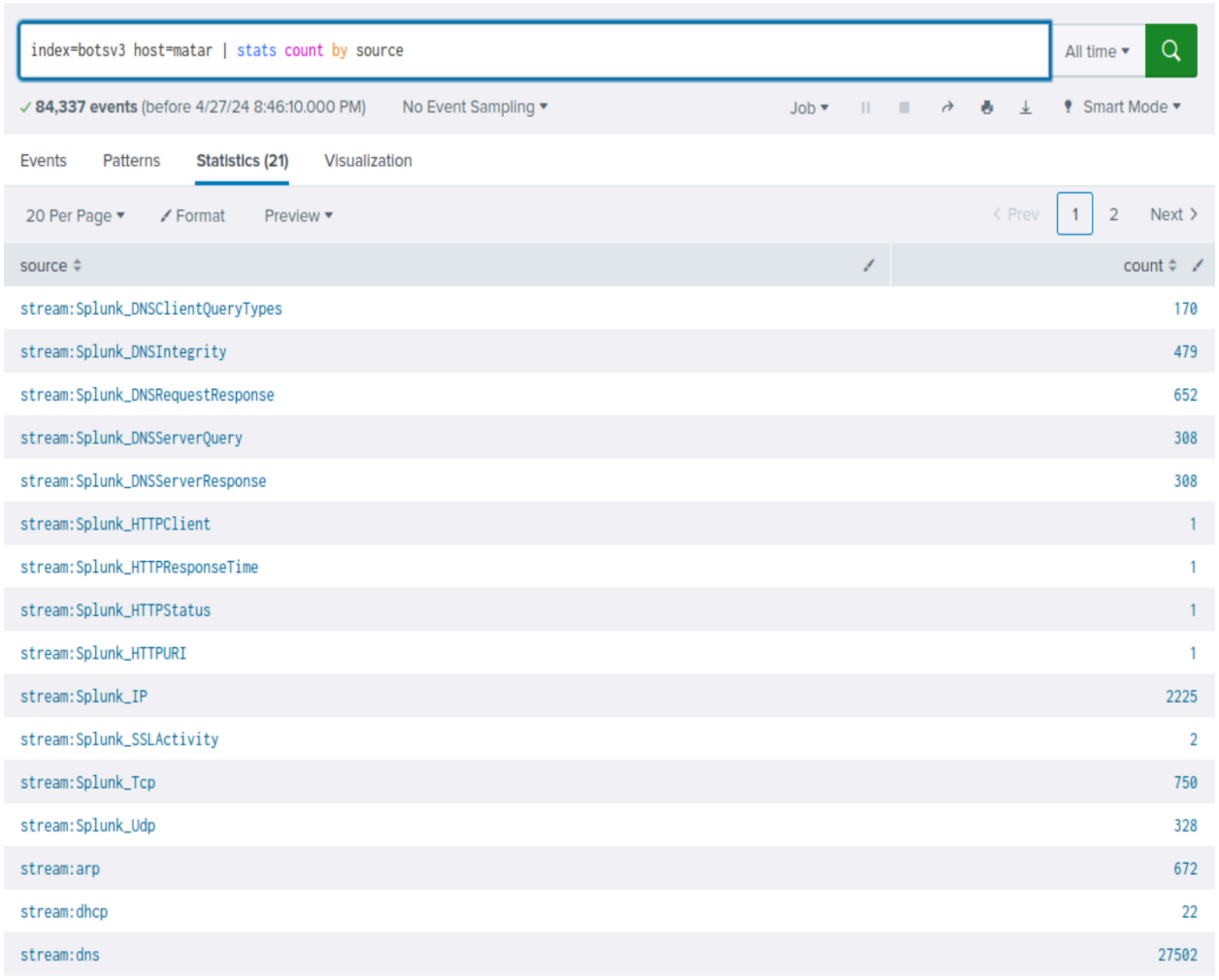


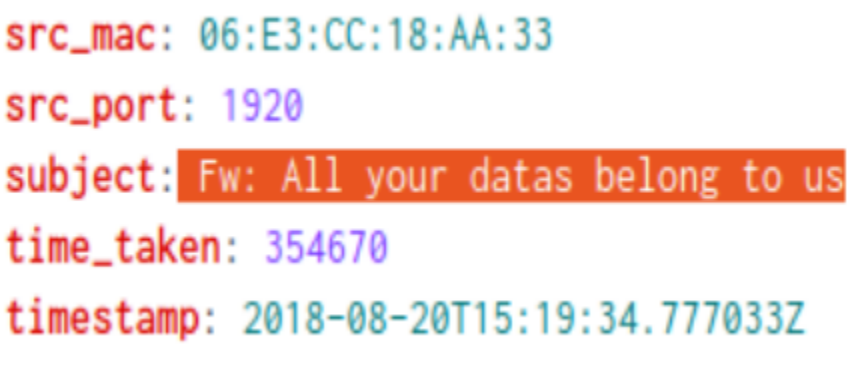
Kevin Cendana
CSC 154
Spring 2024



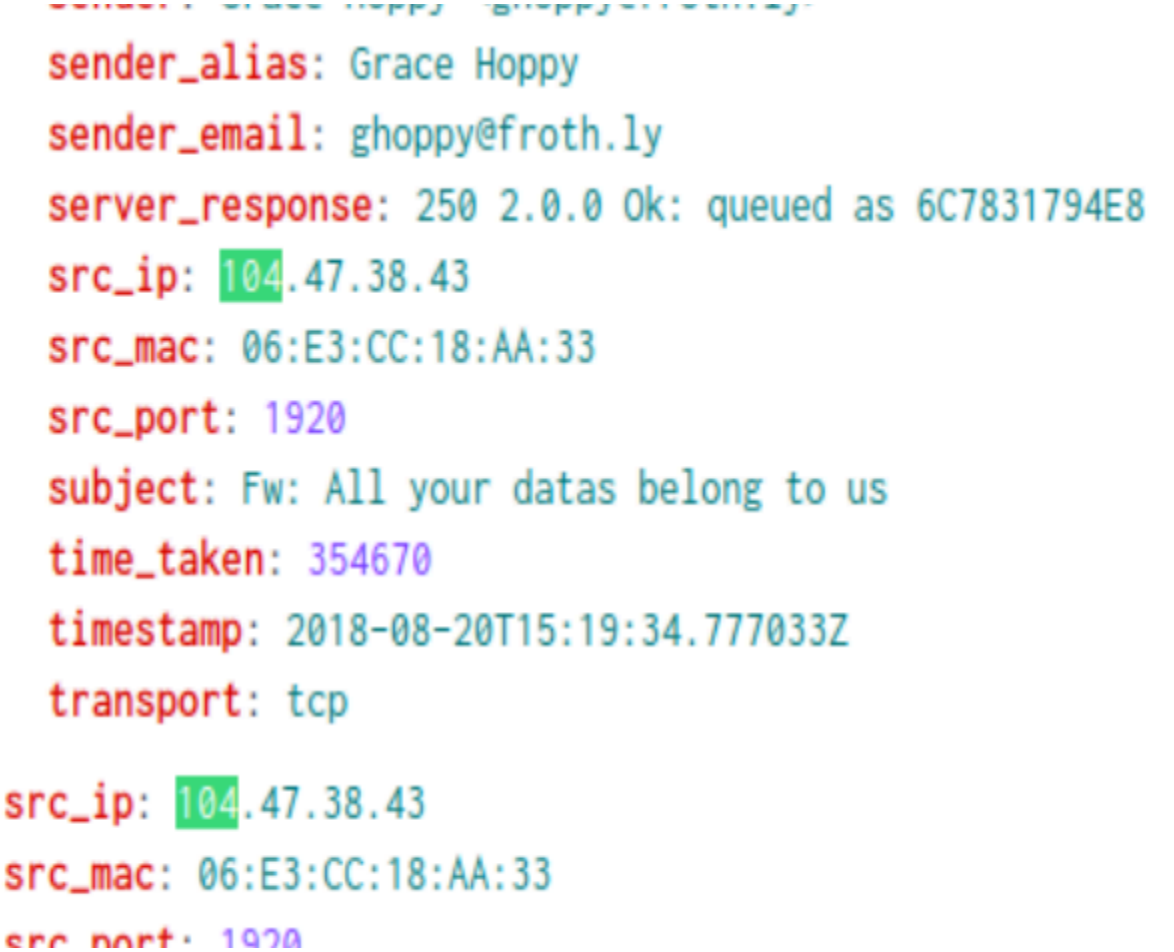
4) Used SPL to filter and count events from the "matar" host within the BOTSv3 index.

Kevin Cendana
CSC 154
Spring 2024



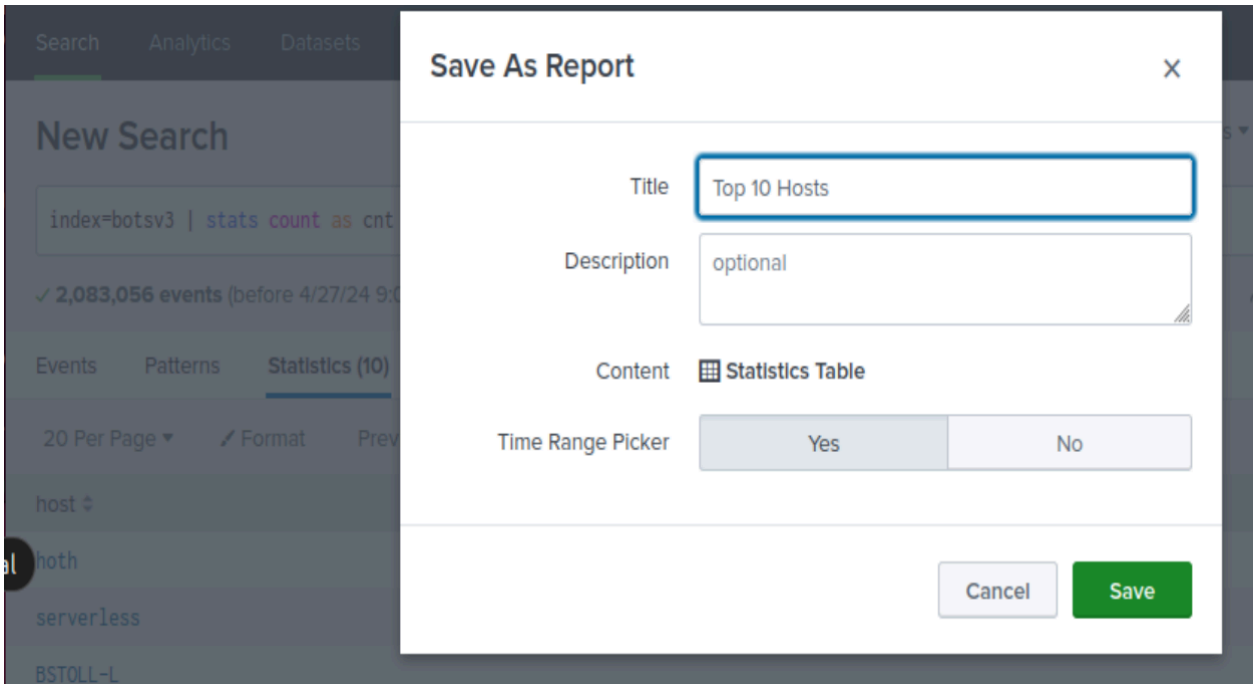


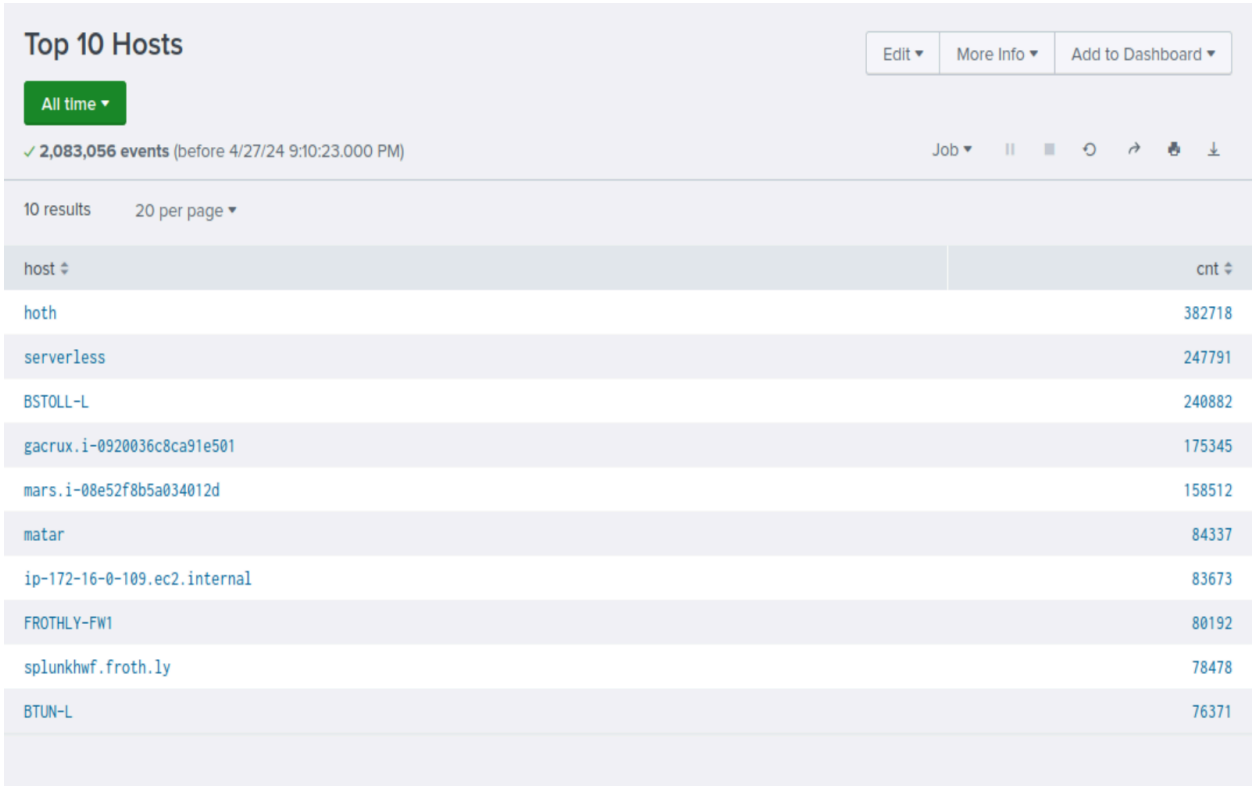
Kevin Cendana
CSC 154
Spring 2024



5) Created a report showing the top 10 source IP addresses in the BOTSv3 index and saved it for future reference.

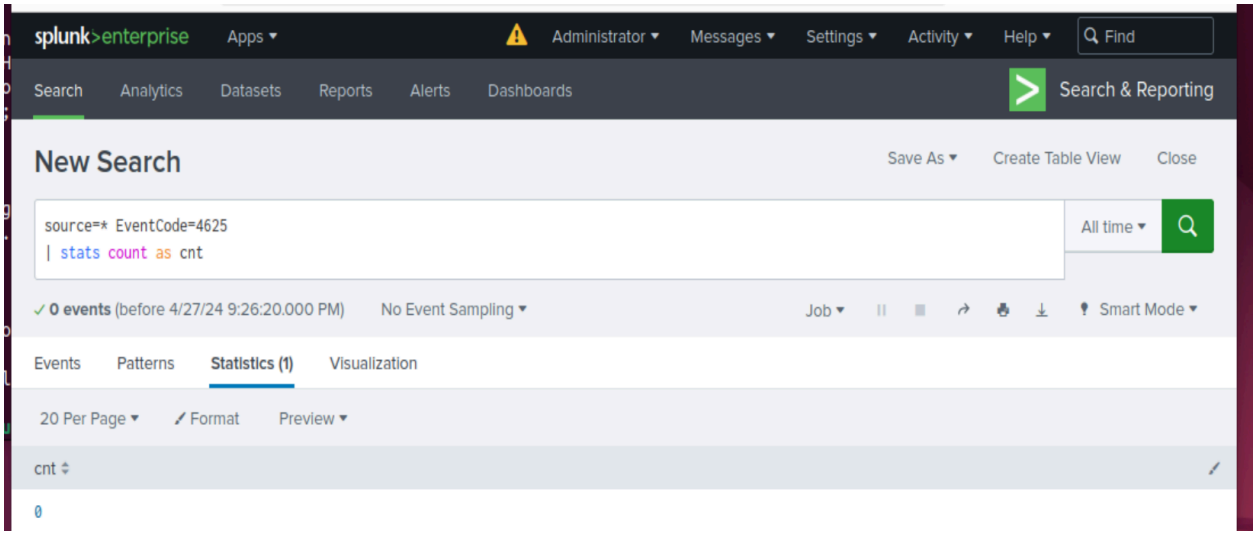
Kevin Cendana
CSC 154
Spring 2024





host	cnt
hoth	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
splunkhwf.froth.ly	78478
BTUN-L	76371

Kevin Cendana
CSC 154
Spring 2024
6) Got stuck here, 0 results from the query 😕

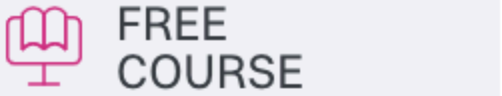


7)

Task 2

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

Kevin Cendana
CSC 154
Spring 2024

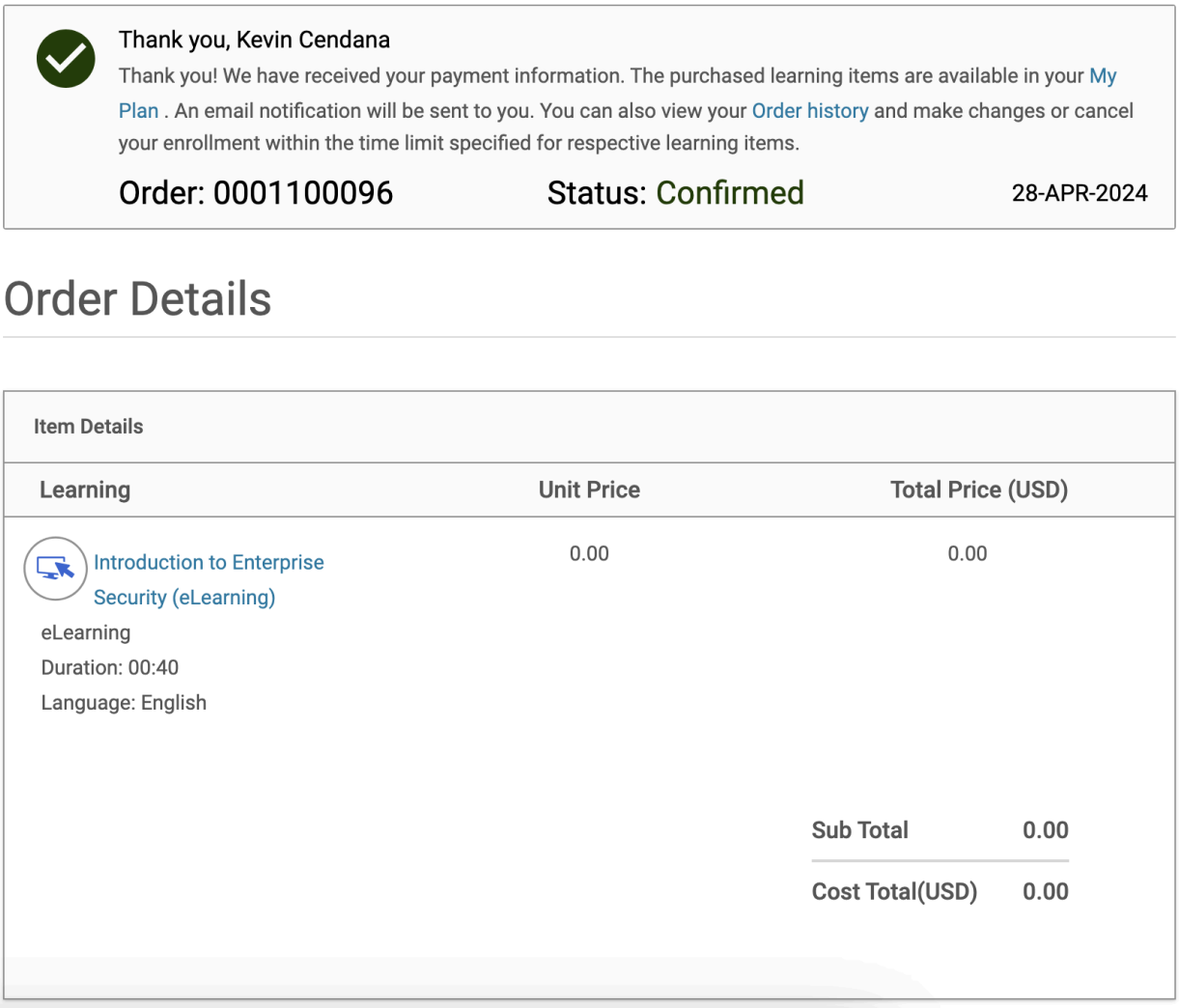


Introduction to Enterprise Security

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

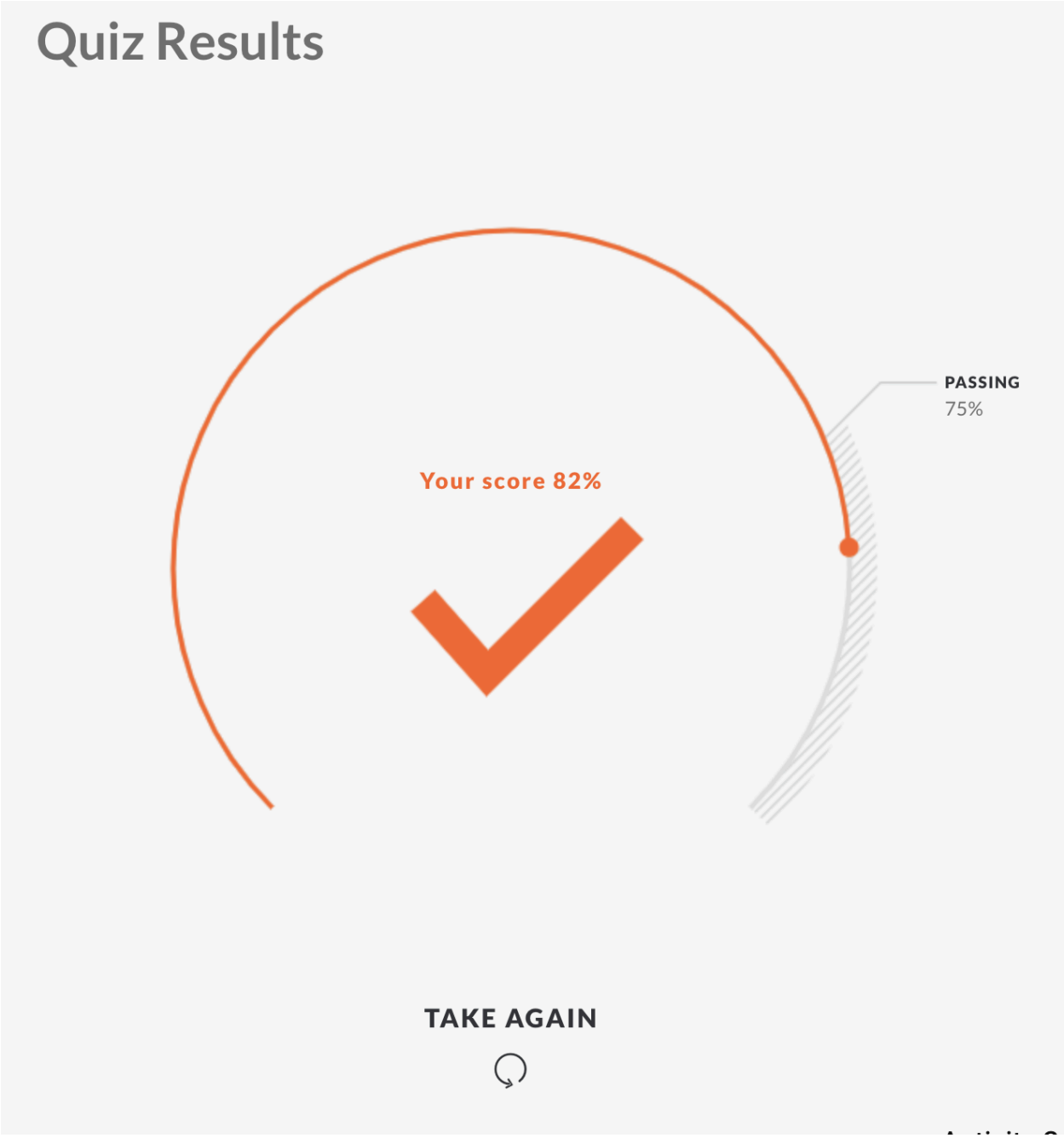
Item Details

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



Kevin Cendana
CSC 154
Spring 2024