Cybersecurity

Module 19 Challenge Submission File

Let's Go Splunking!

Make a copy of this document to work in, and then respond to each question below the prompt. Save and submit this completed file as your Challenge deliverable.

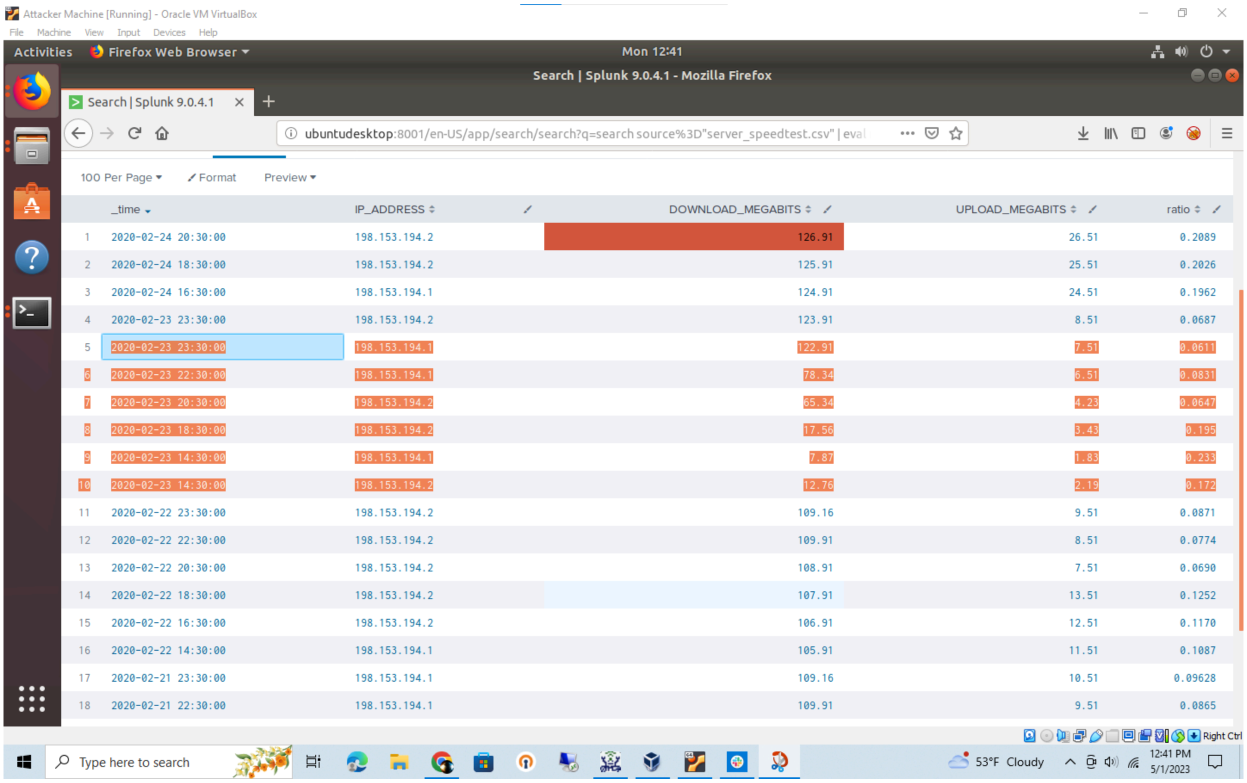
Step 1: The Need for Speed

1. Based on the report you created, what is the approximate date and time of the attack?

```
The date was February, 23 2020 from 14:30 to 22:30 or about 8 hours.
```

2. How long did it take your systems to recover?

```
After the last attack at 22:30 the system recovery took about an hour.
```



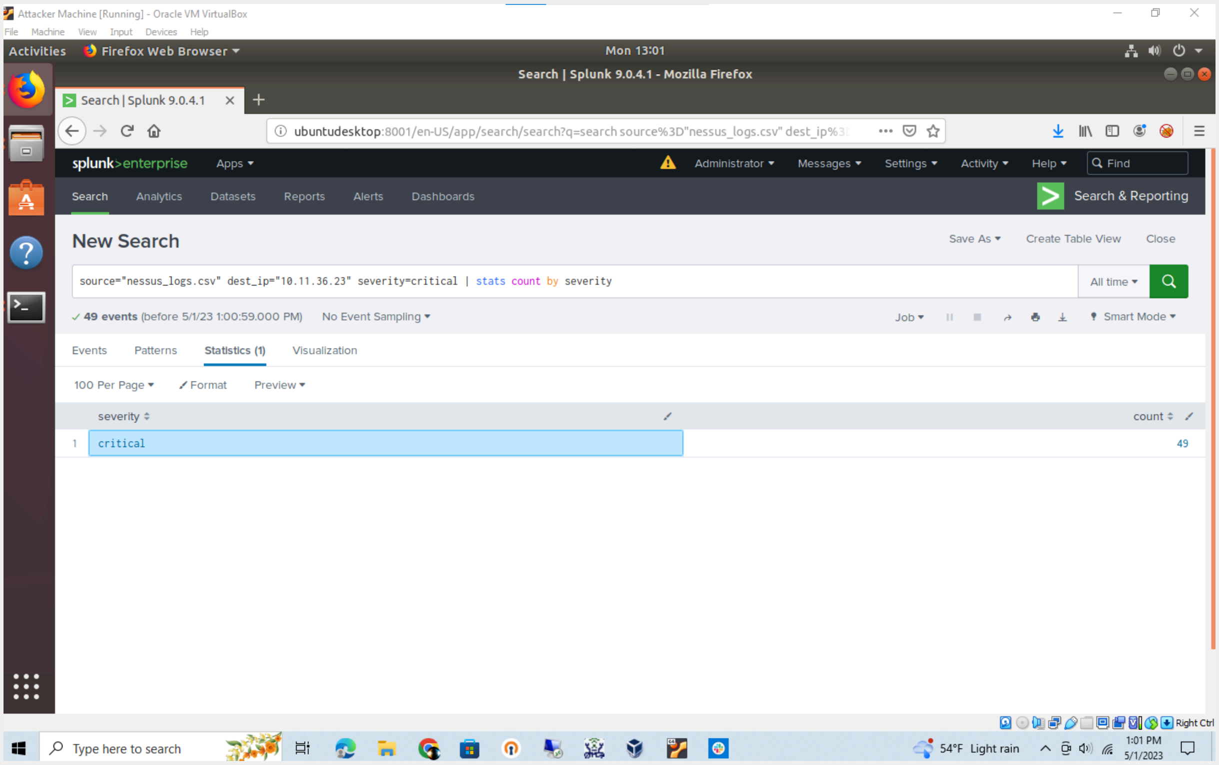
Attacker Machine [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
Mon 12:41
Search | Splunk 9.0.4.1 - Mozilla Firefox
Search | Splunk 9.0.4.1
ubuntudesktop:8001/en-US/app/search/search?q=search source%3D"server_speedtest.csv" | eval
100 Per Page
Format
Preview
Right Ctrl
Type here to search
53°F Cloudy
12:41 PM
5/1/2023

	_time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio
1	2020-02-24 20:30:00	198.153.194.2	126.91	26.51	0.2089
2	2020-02-24 18:30:00	198.153.194.2	125.91	25.51	0.2026
3	2020-02-24 16:30:00	198.153.194.1	124.91	24.51	0.1962
4	2020-02-23 23:30:00	198.153.194.2	123.91	8.51	0.0687
5	2020-02-23 23:30:00	198.153.194.1	122.91	7.51	0.0611
6	2020-02-23 22:30:00	198.153.194.1	78.34	6.51	0.0831
7	2020-02-23 20:30:00	198.153.194.2	65.34	4.23	0.0647
8	2020-02-23 18:30:00	198.153.194.2	17.56	3.43	0.195
9	2020-02-23 14:30:00	198.153.194.1	7.87	1.83	0.233
10	2020-02-23 14:30:00	198.153.194.2	12.76	2.19	0.172
11	2020-02-22 23:30:00	198.153.194.2	109.16	9.51	0.0871
12	2020-02-22 22:30:00	198.153.194.2	109.91	8.51	0.0774
13	2020-02-22 20:30:00	198.153.194.2	108.91	7.51	0.0690
14	2020-02-22 18:30:00	198.153.194.2	107.91	13.51	0.1252
15	2020-02-22 16:30:00	198.153.194.2	106.91	12.51	0.1170
16	2020-02-22 14:30:00	198.153.194.1	105.91	11.51	0.1087
17	2020-02-21 23:30:00	198.153.194.1	109.16	10.51	0.09628
18	2020-02-21 22:30:00	198.153.194.1	109.91	9.51	0.0865

Step 2: Are We Vulnerable?

Provide a screenshot of your report:

```
[Place screenshot here]
```



New Search

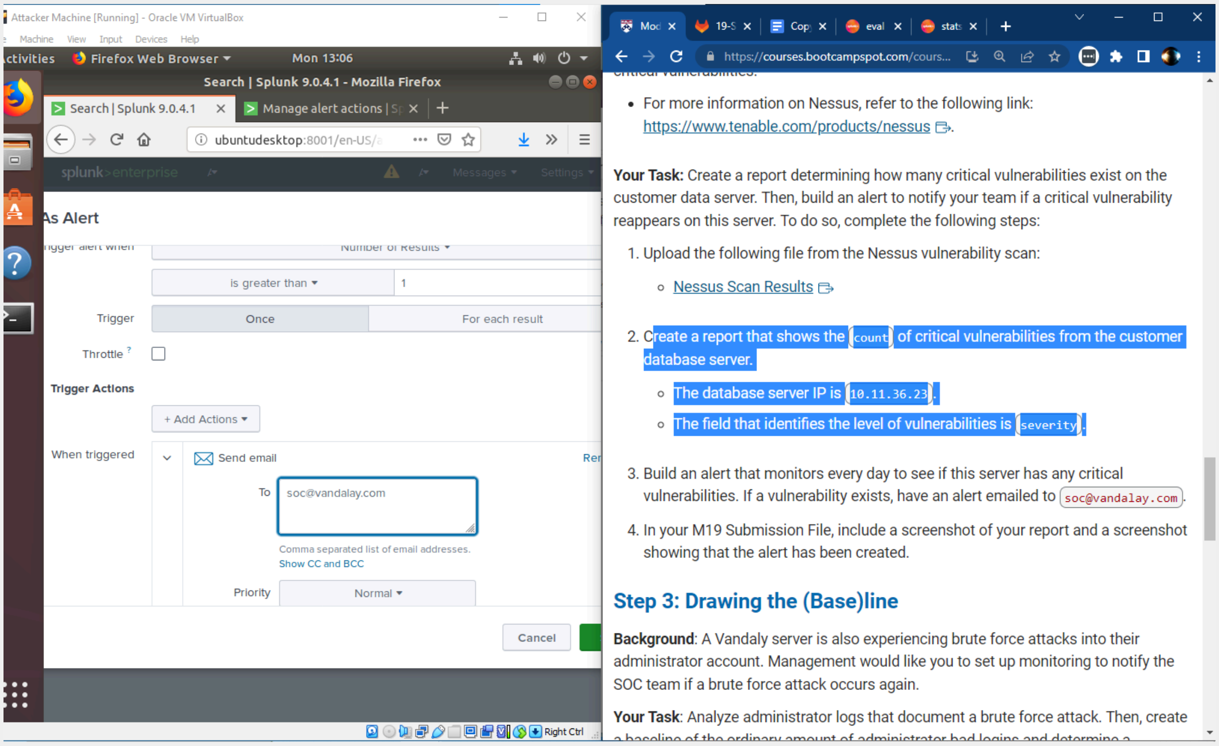
```
source="nessus_logs.csv" dest_ip="10.11.36.23" severity=critical | stats count by severity
```

✓ 49 events (before 5/1/23 1:00:59.000 PM)

	severity	count
1	critical	49

Provide a screenshot showing that the alert has been created:

[Place screenshot here]



As Alert

Trigger alert when: Number of Results ▾

is greater than ▾ 1

Trigger: Once | For each result

Throttle ☐

Trigger Actions

+ Add Actions ▾

When triggered: Send email

To: soc@vandalay.com

Comma separated list of email addresses.
Show CC and BCC

Priority: Normal ▾

Cancel

- For more information on Nessus, refer to the following link: https://www.tenable.com/products/nessus.

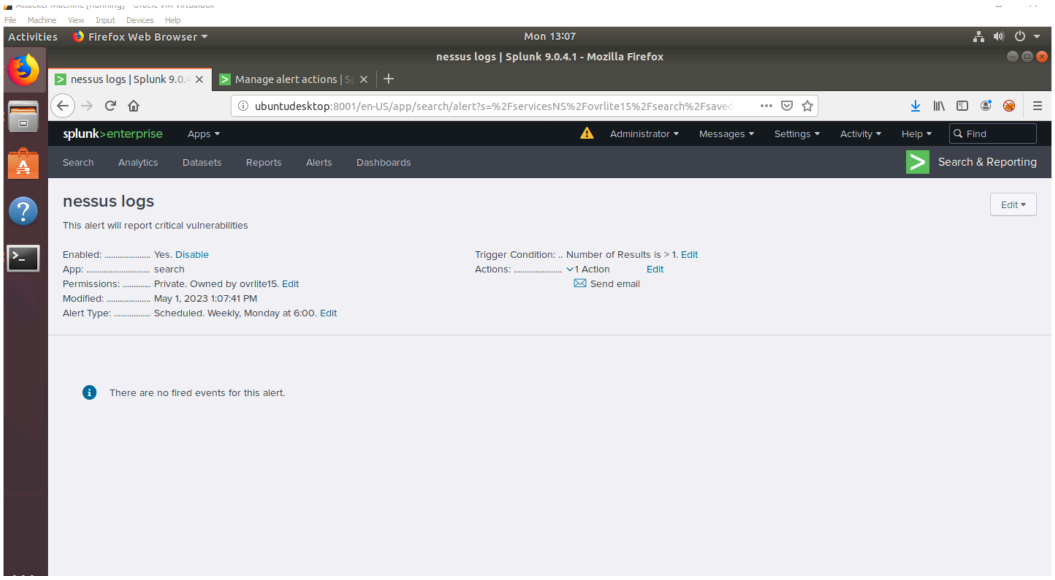
Your Task: Create a report determining how many critical vulnerabilities exist on the customer data server. Then, build an alert to notify your team if a critical vulnerability reappears on this server. To do so, complete the following steps:

1. Upload the following file from the Nessus vulnerability scan:
   - Nessus Scan Results
2. Create a report that shows the `count` of critical vulnerabilities from the customer database server.
   - The database server IP is `10.11.36.23`.
   - The field that identifies the level of vulnerabilities is `severity`.
3. Build an alert that monitors every day to see if this server has any critical vulnerabilities. If a vulnerability exists, have an alert emailed to `soc@vandalay.com`.
4. In your M19 Submission File, include a screenshot of your report and a screenshot showing that the alert has been created.

Step 3: Drawing the (Base)line

Background: A Vandaly server is also experiencing brute force attacks into their administrator account. Management would like you to set up monitoring to notify the SOC team if a brute force attack occurs again.

Your Task: Analyze administrator logs that document a brute force attack. Then, create



nessus logs

This alert will report critical vulnerabilities

Enabled: Yes. Disable
App: search
Permissions: Private. Owned by ovrlite15. Edit
Modified: May 1, 2023 1:07:41 PM
Alert Type: Scheduled. Weekly, Monday at 6:00. Edit

Trigger Condition: Number of Results is > 1. Edit
Actions: 1 Action Edit
Send email

There are no fired events for this alert.

Step 3: Drawing the (Base)line

1. When did the brute force attack occur?

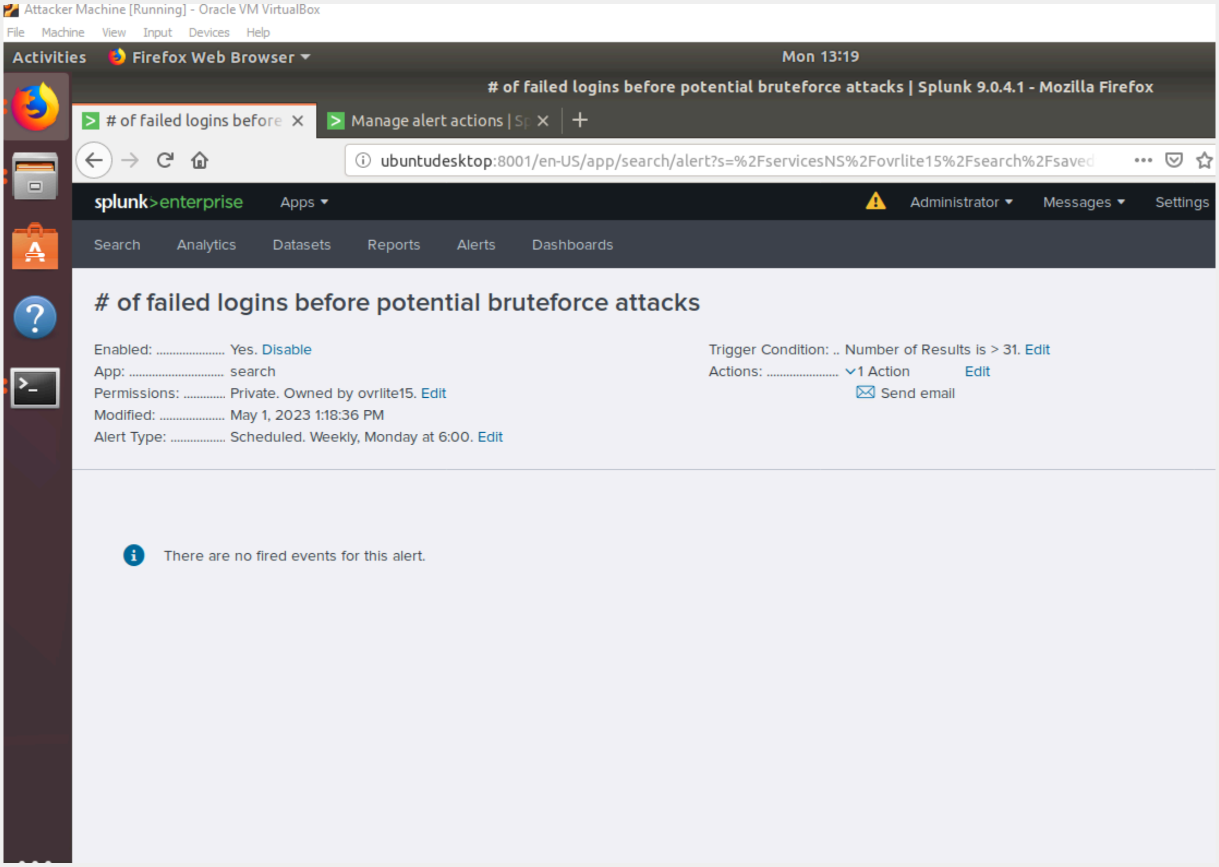
```
The brute force attack started at 9:00 am and ended at 2:00 pm with levels
tapering off.
```

2. Determine a baseline of normal activity and a threshold that would alert if a brute force attack is occurring:

```
My baseline is about 15 failed logins per hour with a high of 32 being the
threshold of it being a potential brute force attack.
```

3. Provide a screenshot showing that the alert has been created:

[Place scr


Attacker Machine [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Activities
Firefox Web Browser
Mon 13:19
# of failed logins before potential bruteforce attacks | Splunk 9.0.4.1 - Mozilla Firefox
# of failed logins before
Manage alert actions | Sp
ubuntudesktop:8001/en-US/app/search/alert?s=%2FservicesNS%2Fovrlite15%2Fsearch%2Fsaved
splunk>enterprise
Apps
Administrator
Messages
Settings
Search
Analytics
Datasets
Reports
Alerts
Dashboards

# of failed logins before potential bruteforce attacks

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by ovrlite15. Edit
Modified: .... May 1, 2023 1:18:36 PM
Alert Type: .... Scheduled. Weekly, Monday at 6:00. Edit

Trigger Condition: .. Number of Results is > 31. Edit
Actions: .... 1 Action Edit
Send email

There are no fired events for this alert.

eenshot here]