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

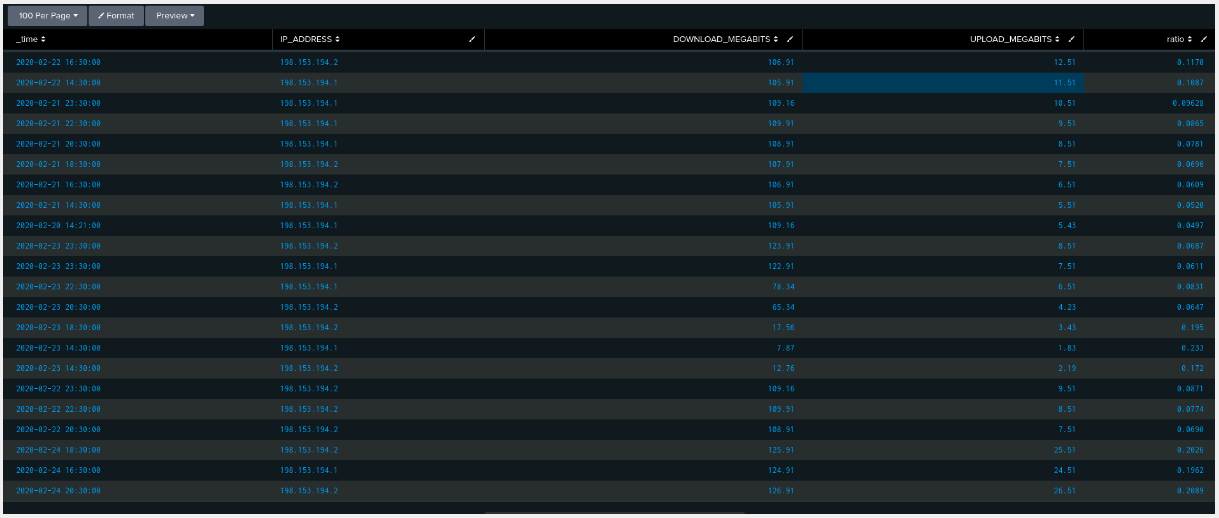
1. Based on the report you created, what is the approximate date and time of the attack?

```
2020-02-23 14:30:00
```

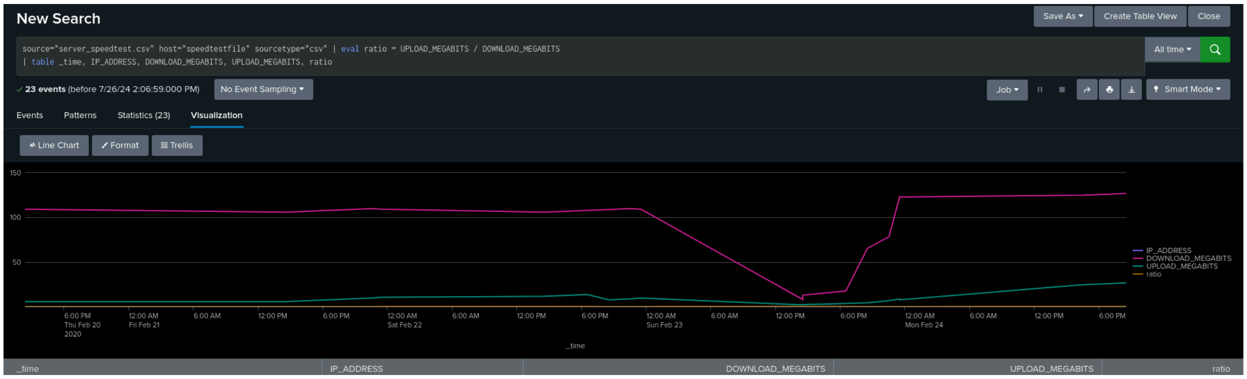
Y

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

```
2020-02-23 23:30:00 9 Hours
```



_time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio
2020-02-22 16:30:00	198.153.194.2	106.91	12.51	0.1170
2020-02-22 14:30:00	198.153.194.1	105.91	11.51	0.1087
2020-02-21 23:30:00	198.153.194.1	109.16	10.51	0.09628
2020-02-21 22:30:00	198.153.194.1	109.91	9.51	0.0865
2020-02-21 20:30:00	198.153.194.1	108.91	8.51	0.0781
2020-02-21 18:30:00	198.153.194.2	107.91	7.51	0.0696
2020-02-21 16:30:00	198.153.194.2	106.91	6.51	0.0609
2020-02-21 14:30:00	198.153.194.1	105.91	5.51	0.0520
2020-02-20 14:21:00	198.153.194.1	109.16	5.43	0.0497
2020-02-23 23:30:00	198.153.194.2	123.91	8.51	0.0687
2020-02-23 23:30:00	198.153.194.1	122.91	7.51	0.0611
2020-02-23 22:30:00	198.153.194.1	78.34	6.51	0.0831
2020-02-23 20:30:00	198.153.194.2	65.34	4.23	0.0647
2020-02-23 18:30:00	198.153.194.2	17.56	3.43	0.195
2020-02-23 14:30:00	198.153.194.1	7.87	1.83	0.233
2020-02-23 14:30:00	198.153.194.2	12.76	2.19	0.172
2020-02-22 23:30:00	198.153.194.2	109.16	9.51	0.0871
2020-02-22 22:30:00	198.153.194.2	109.91	8.51	0.0774
2020-02-22 20:30:00	198.153.194.2	108.91	7.51	0.0690
2020-02-24 18:30:00	198.153.194.2	125.91	25.51	0.2026
2020-02-24 16:30:00	198.153.194.1	124.91	24.51	0.1962
2020-02-24 20:30:00	198.153.194.2	126.91	26.51	0.2089

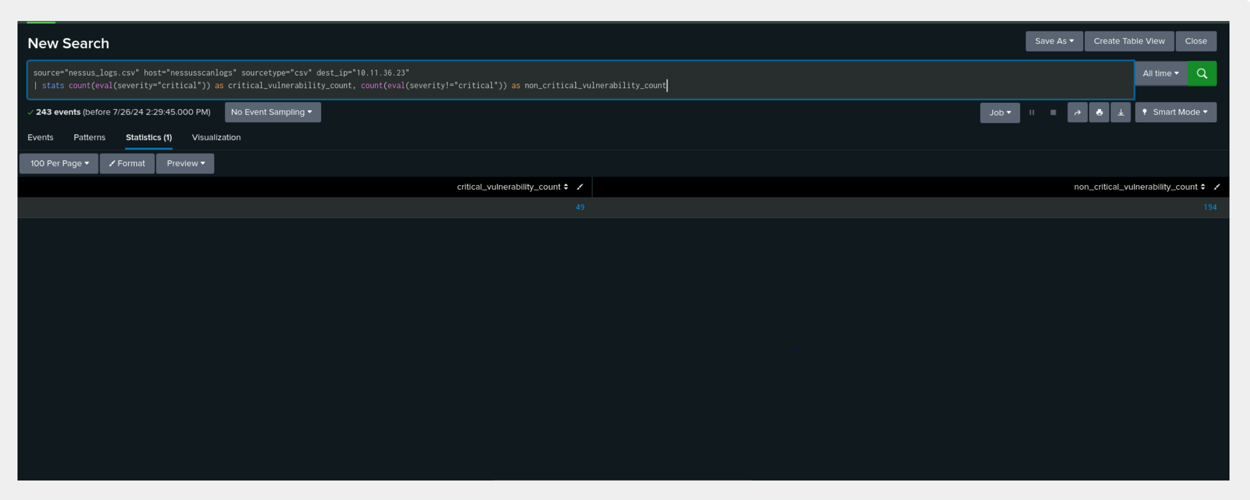


```
source="server_speedtest.csv" host="speedtestfile" sourcetype="csv" | eval ratio = UPLOAD_MEGABITS / DOWNLOAD_MEGABITS
| table _time, IP_ADDRESS, DOWNLOAD_MEGABITS, UPLOAD_MEGABITS, ratio
```

✓ **23 events** (before 7/26/24 2:06:59.000 PM) No Event Sampling

Step 2: Are We Vulnerable?

Provide a screenshot of your report:

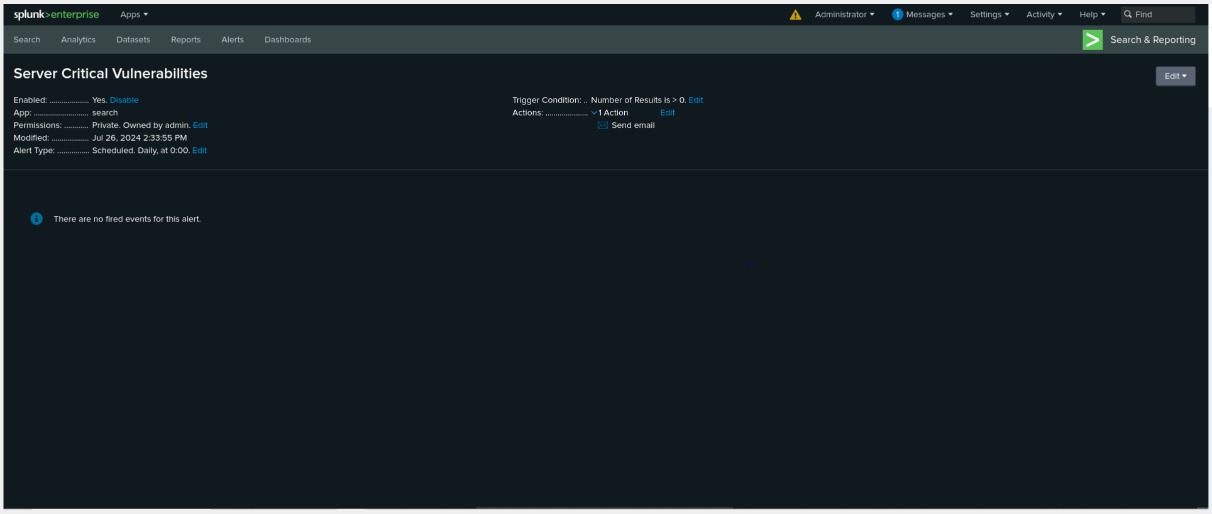


```
source="nessus_logs.csv" host="nessusscanlogs" sourcetype="csv" dest_ip="10.11.36.23"
| stats count(eval(severity="critical")) as critical_vulnerability_count, count(eval(severity!="critical")) as non_critical_vulnerability_count
```

✓ **243 events** (before 7/26/24 2:29:45.000 PM) No Event Sampling

critical_vulnerability_count	non_critical_vulnerability_count
49	194

Provide a screenshot showing that the alert has been created:



Server Critical Vulnerabilities

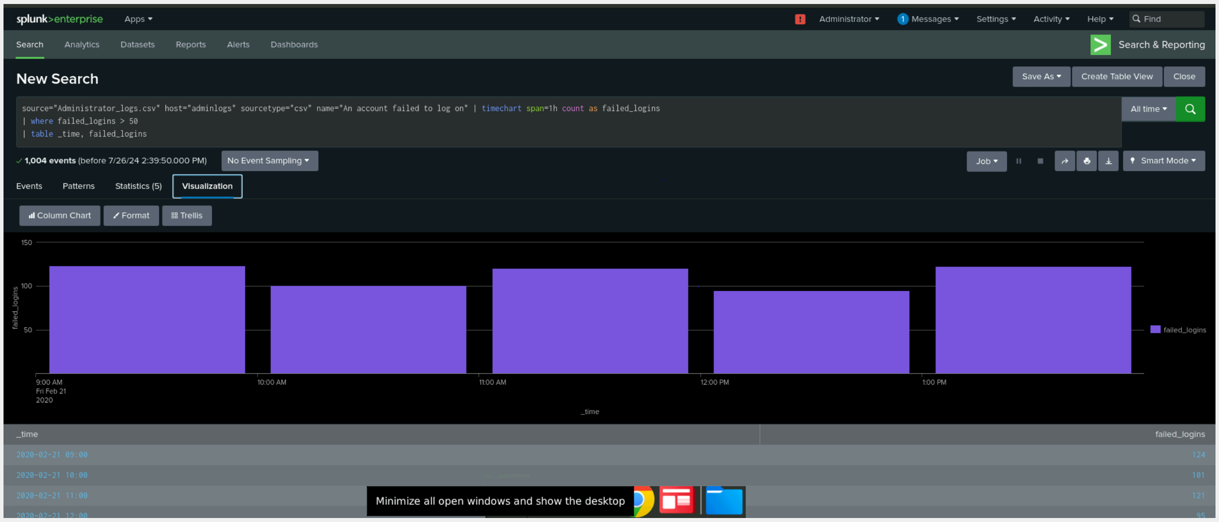
Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Jul 26, 2024 2:33:55 PM
Alert Type: .... Scheduled. Daily, at 0:00. Edit

Trigger Condition: .. Number of Results is > 0. 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?



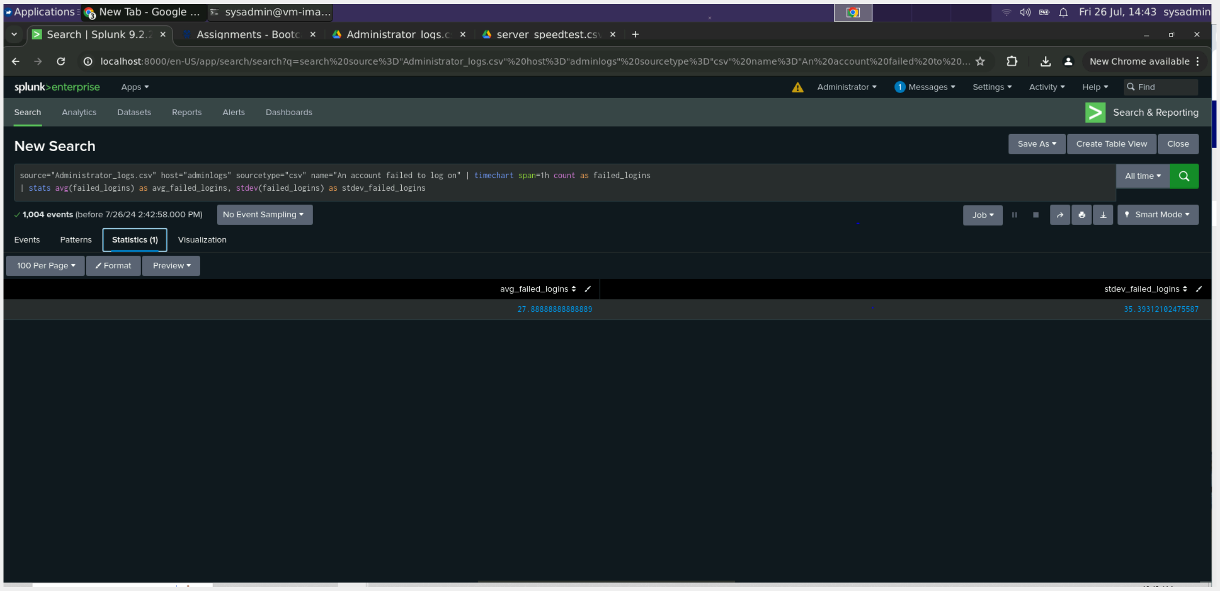
```
source="Administrator_logs.csv" host="adminlogs" sourcetype="csv" name="An account failed to log on" | timechart span=1h count as failed_logins
| where failed_logins > 50
| table _time, failed_logins
```

✓ 1,004 events (before 7/26/24 2:39:50.000 PM)

_time	failed_logins
2020-02-21 09:00	124
2020-02-21 10:00	101
2020-02-21 11:00	121
2020-02-21 12:00	95

2020-02-21 09:00am - 2020-02-21 13:00pm

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



New Search

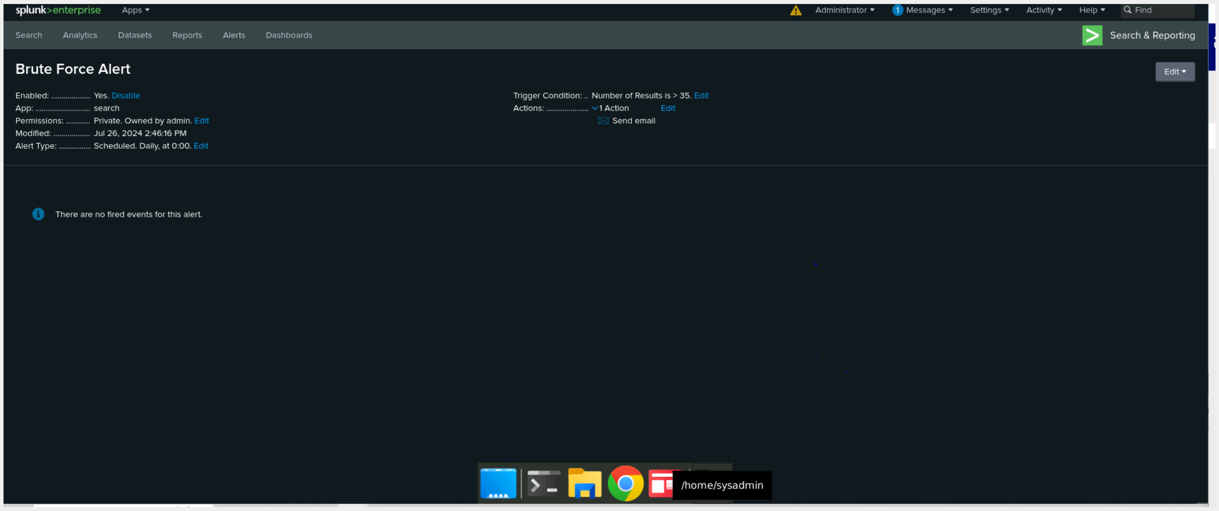
```
source="Administrator_logs.csv" host="adminlogs" sourcetype="csv" name="An account failed to log on" | timechart span=1h count as failed_logins
| stats avg(failed_logins) as avg_failed_logins, stdev(failed_logins) as stdev_failed_logins
```

✓ 1,004 events (before 7/26/24 2:42:58.000 PM)

avg_failed_logins	stdev_failed_logins
27.88888888888889	35.39312102475587

The baseline is 27 and the threshold is 35

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



Brute Force Alert

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Jul 26, 2024 2:46:16 PM
Alert Type: .... Scheduled. Daily, at 0:00. Edit

Trigger Condition: .. Number of Results is > 35. Edit
Actions: .... 1 Action Edit
Send email

There are no fired events for this alert.