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

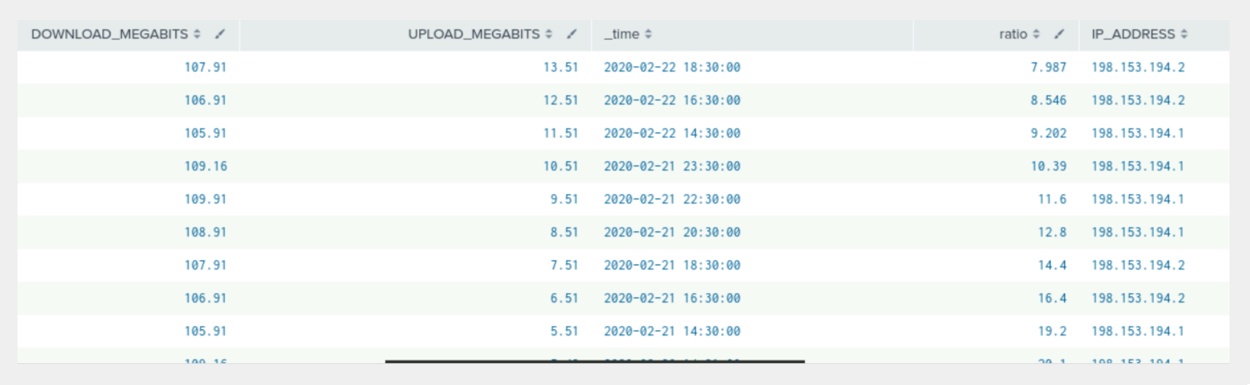
1. Based on the report you created, what is the approximate date and time of the attack?

```
2/23/20 2:30:00:0000 PM.
```

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

```
6 hours.
```

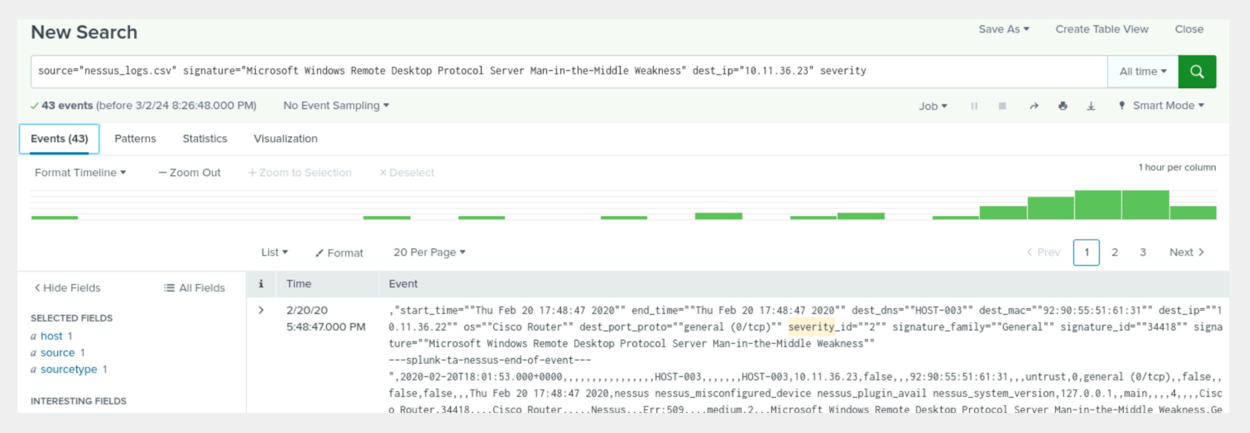
Provide a screenshot of your report:



DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	_time	ratio	IP_ADDRESS
107.91	13.51	2020-02-22 18:30:00	7.987	198.153.194.2
106.91	12.51	2020-02-22 16:30:00	8.546	198.153.194.2
105.91	11.51	2020-02-22 14:30:00	9.202	198.153.194.1
109.16	10.51	2020-02-21 23:30:00	10.39	198.153.194.1
109.91	9.51	2020-02-21 22:30:00	11.6	198.153.194.1
108.91	8.51	2020-02-21 20:30:00	12.8	198.153.194.1
107.91	7.51	2020-02-21 18:30:00	14.4	198.153.194.2
106.91	6.51	2020-02-21 16:30:00	16.4	198.153.194.2
105.91	5.51	2020-02-21 14:30:00	19.2	198.153.194.1

Step 2: Are We Vulnerable?

Provide a screenshot of your report:



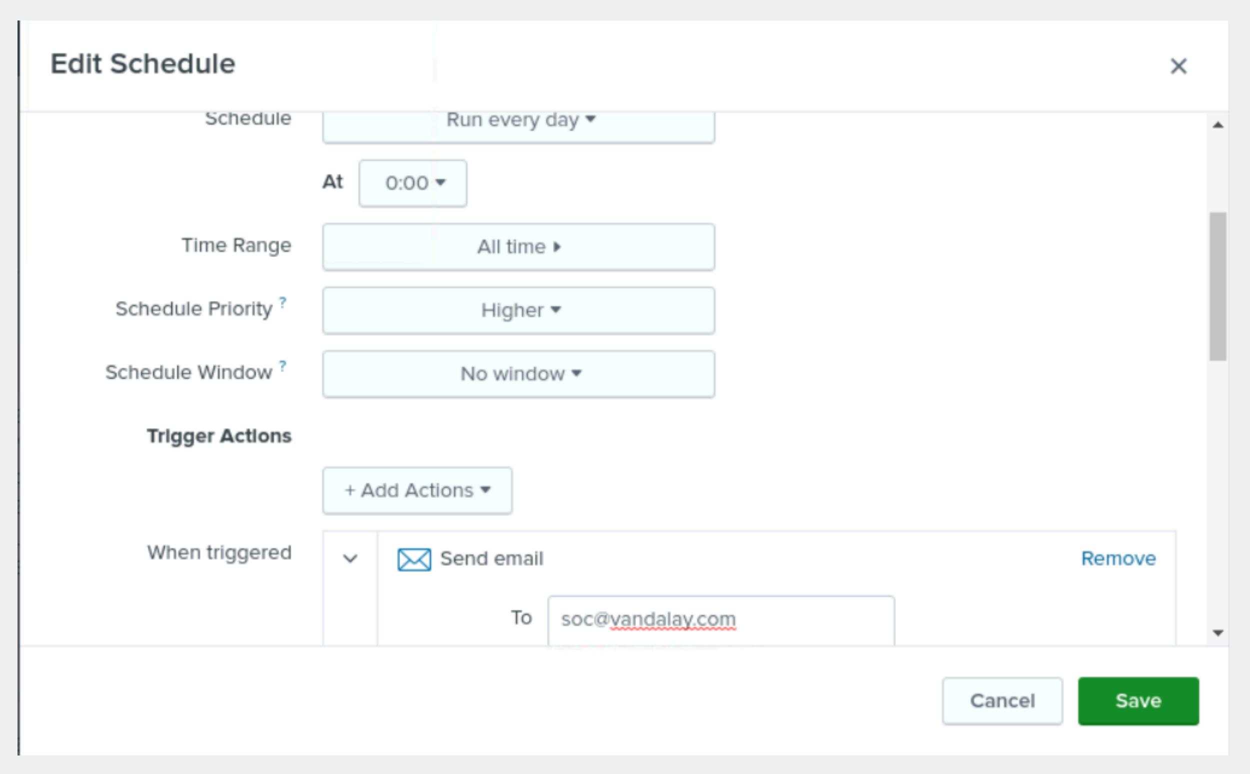
```
source="nessus_logs.csv" signature="Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness" dest_ip="10.11.36.23" severity
```

✓ 43 events (before 3/2/24 8:26:48.000 PM)   No Event Sampling ▾

2/20/20 5:48:47.000 PM

```
,"start_time=""Thu Feb 20 17:48:47 2020"" end_time=""Thu Feb 20 17:48:47 2020"" dest_dns=""HOST-003"" dest_mac=""92:90:55:51:61:31"" dest_ip=""1
0.11.36.22"" os=""Cisco Router"" dest_port_proto=""general (0/tcp)"" severity_id=""2"" signature_family=""General"" signature_id=""34418"" signa
ture=""Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness""
---splunk-ta-nessus-end-of-event---
",2020-02-20T18:01:53.000+0000,,,,,,,,,,,,,,,HOST-003,,,,,,HOST-003,10.11.36.23,false,,,92:90:55:51:61:31,,,untrust,0,general (0/tcp),,false,,
false,false,,,Thu Feb 20 17:48:47 2020,nessus nessus_misconfigured_device nessus_plugin_avail nessus_system_version,127.0.0.1,,main,,,,4,,,,Cisc
o Router,34418,...,Cisco Router,....,Nessus,..,Err:509,...,medium,2,..,Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness,Ge
```

Provide a screenshot showing that the alert has been created:



Schedule: Run every day ▾

At: 0:00 ▾

Time Range: All time ▸

Schedule Priority ?: Higher ▾

Schedule Window ?: No window ▾

When triggered: Send email

To: soc@vandalay.com

Step 3: Drawing the (Base)line

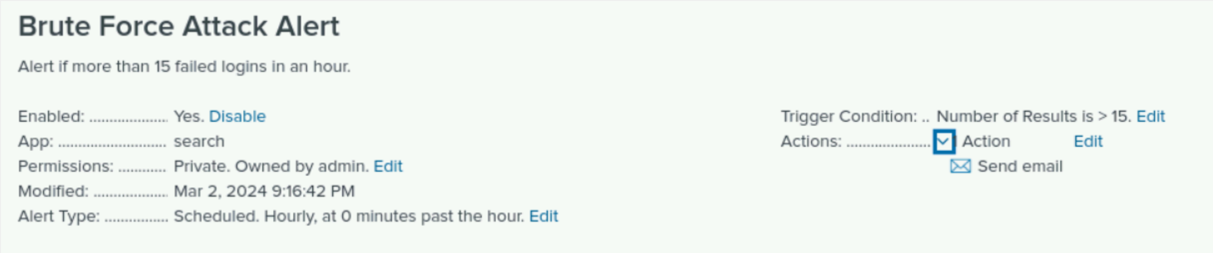
1. When did the brute force attack occur?

```
8 AM on Friday, February 21st, 2020.
```

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

```
Alert if more than 15 failed login attempts in an hour.
```

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



Brute Force Attack Alert

Alert if more than 15 failed logins in an hour.

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Mar 2, 2024 9:16:42 PM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 15. Edit
Actions: .... ☑ Action Edit
✉ Send email