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

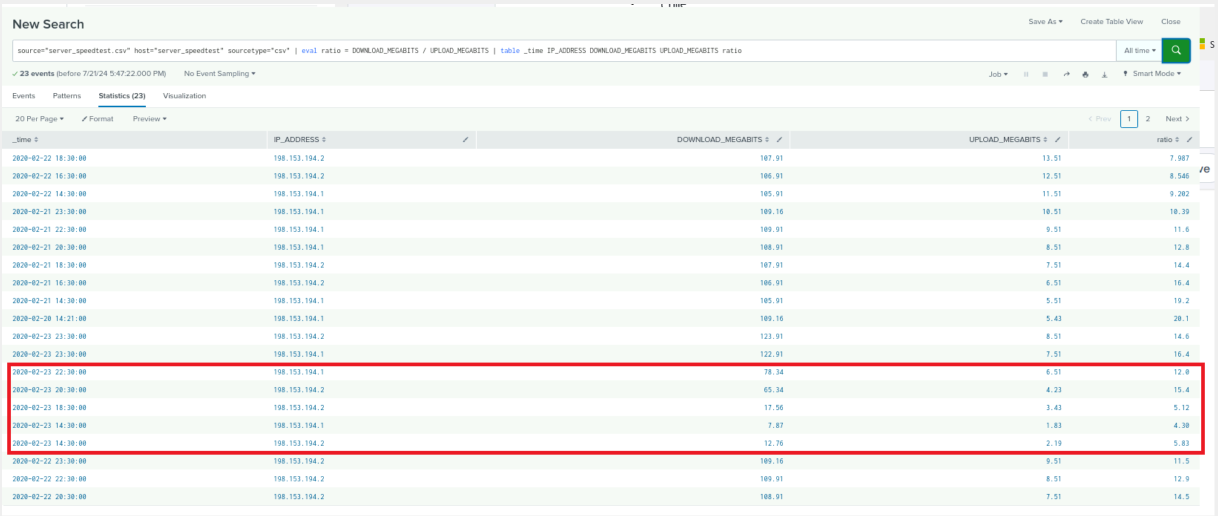
1. Based on the report you created, what is the approximate date and time of the attack?

```
Approximate date and time of the attack is February 23, 2020, 2:30pm
```

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

```
About 8 to 9 hours (approximate from 2:30pm through 10:30pm)
```

Provide a screenshot of your report:

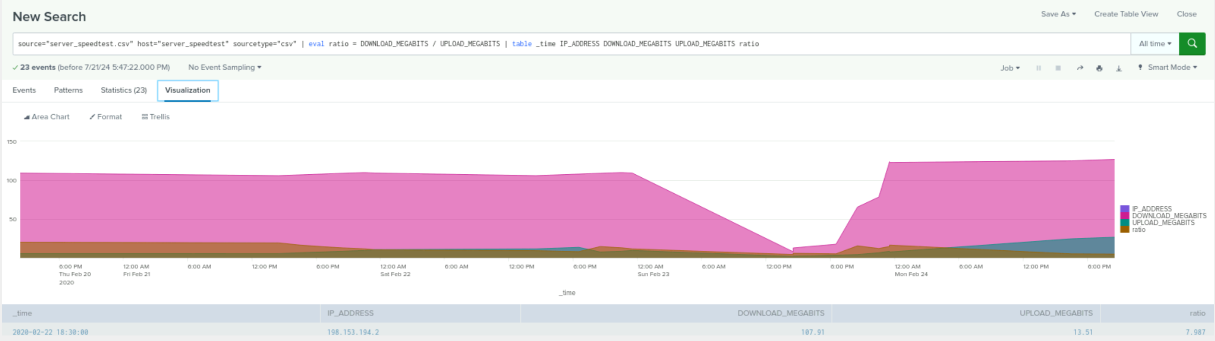


```
source="server_speedtest.csv" host="server_speedtest" sourcetype="csv" | eval ratio = DOWNLOAD_MEGABITS / UPLOAD_MEGABITS | table _time IP_ADDRESS DOWNLOAD_MEGABITS UPLOAD_MEGABITS ratio
```

✓ 23 events (before 7/21/24 5:47:22.000 PM) No Event Sampling

_time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio
2020-02-22 18:30:00	198.153.194.2	107.91	13.51	7.987
2020-02-22 16:30:00	198.153.194.2	106.91	12.51	8.546
2020-02-22 14:30:00	198.153.194.1	105.91	11.51	9.202
2020-02-21 23:30:00	198.153.194.1	109.16	10.51	10.39
2020-02-21 22:30:00	198.153.194.1	109.91	9.51	11.6
2020-02-21 20:30:00	198.153.194.1	108.91	8.51	12.8
2020-02-21 18:30:00	198.153.194.2	107.91	7.51	14.4
2020-02-21 16:30:00	198.153.194.2	106.91	6.51	16.4
2020-02-21 14:30:00	198.153.194.1	105.91	5.51	19.2
2020-02-20 14:21:00	198.153.194.1	109.16	5.43	20.1
2020-02-23 23:30:00	198.153.194.2	123.91	8.51	14.6
2020-02-23 23:30:00	198.153.194.1	122.91	7.51	16.4
2020-02-23 22:30:00	198.153.194.1	78.34	6.51	12.0
2020-02-23 20:30:00	198.153.194.2	65.34	4.23	15.4
2020-02-23 18:30:00	198.153.194.2	17.56	3.43	5.12
2020-02-23 14:30:00	198.153.194.1	7.87	1.83	4.30
2020-02-23 14:30:00	198.153.194.2	12.76	2.19	5.83
2020-02-22 23:30:00	198.153.194.2	109.16	9.51	11.5
2020-02-22 22:30:00	198.153.194.2	109.91	8.51	12.9
2020-02-22 20:30:00	198.153.194.2	108.91	7.51	14.5

Another way to view the date and time of the attack:



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

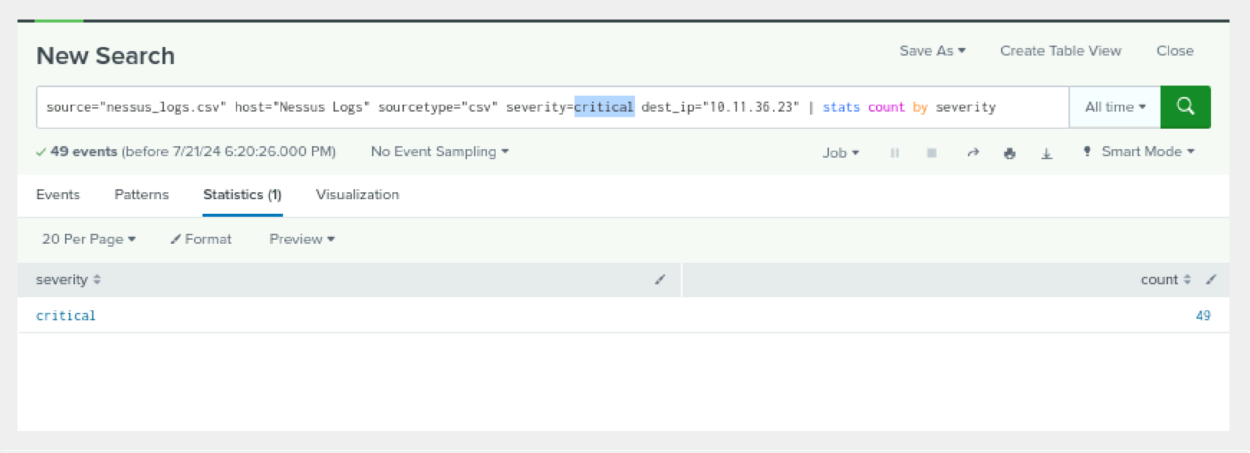
✓ 23 events (before 7/21/24 5:47:22.000 PM) No Event Sampling

_time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio
2020-02-22 18:30:00	198.153.194.2	107.91	13.51	7.987

Step 2: Are We Vulnerable?

Provide a screenshot of your report:

This report determines how many critical vulnerabilities exist on the customer data server.

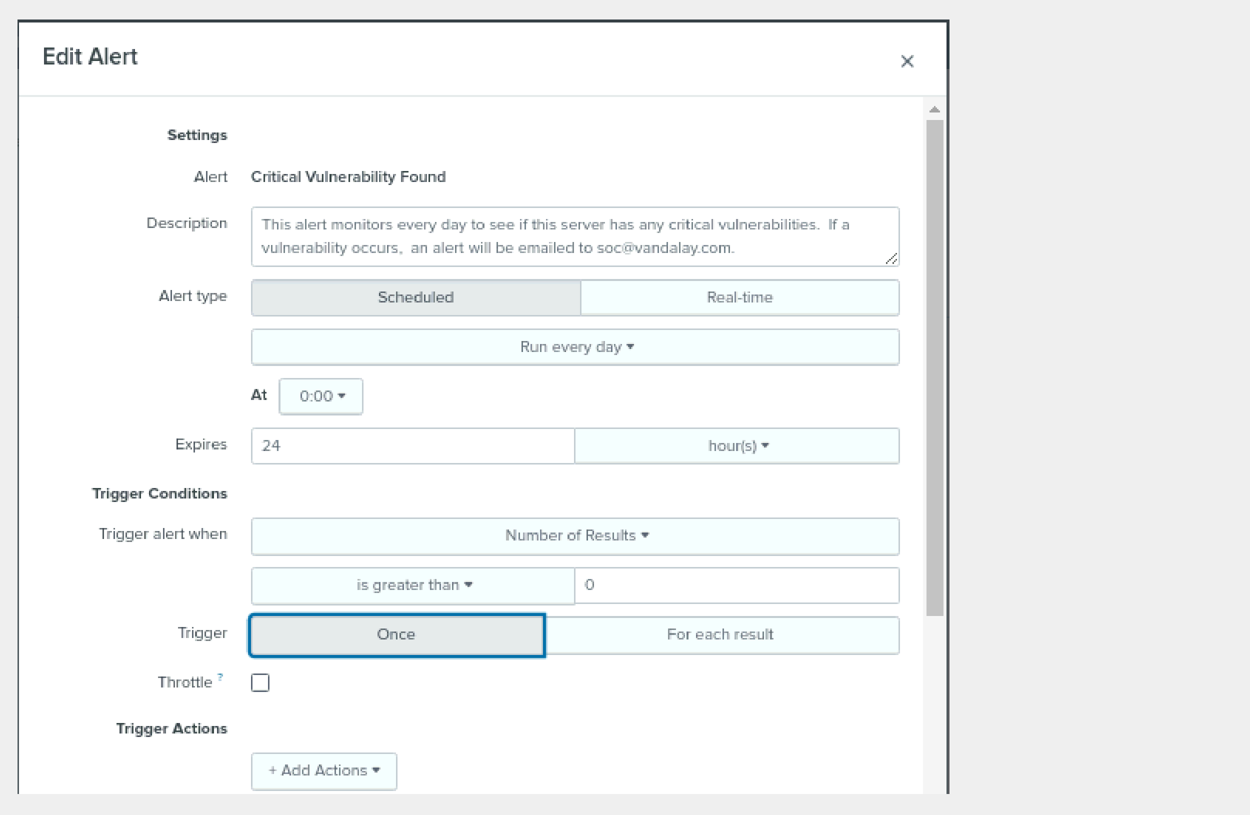


```
source="nessus_logs.csv" host="Nessus Logs" sourcetype="csv" severity=critical dest_ip="10.11.36.23" | stats count by severity
```

✓ **49 events** (before 7/21/24 6:20:26.000 PM)

severity	count
critical	49

Provide a screenshot showing that the alert has been created:



Settings

Alert: Critical Vulnerability Found

Description: This alert monitors every day to see if this server has any critical vulnerabilities. If a vulnerability occurs, an alert will be emailed to soc@vandalay.com.

Alert type: [✓ Scheduled] Real-time

Run every day ▾

At 0:00 ▾

Expires: 24 hour(s) ▾

Trigger Conditions

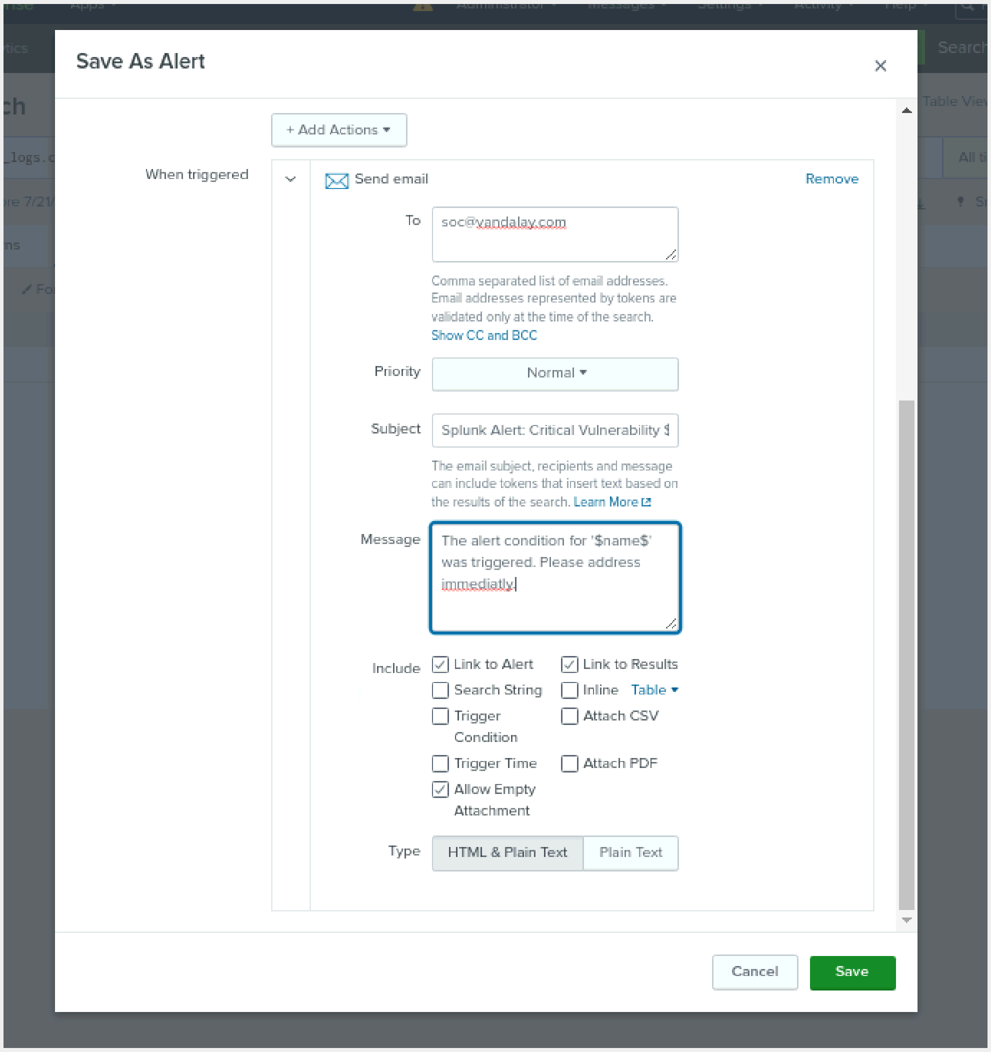
Trigger alert when: Number of Results ▾

is greater than ▾ 0

Trigger: [✓ Once] For each result

Throttle ? □

Trigger Actions



Save As Alert

When triggered

Send email

To: soc@vandalay.com

Comma separated list of email addresses. Email addresses represented by tokens are validated only at the time of the search.

Priority: Normal ▾

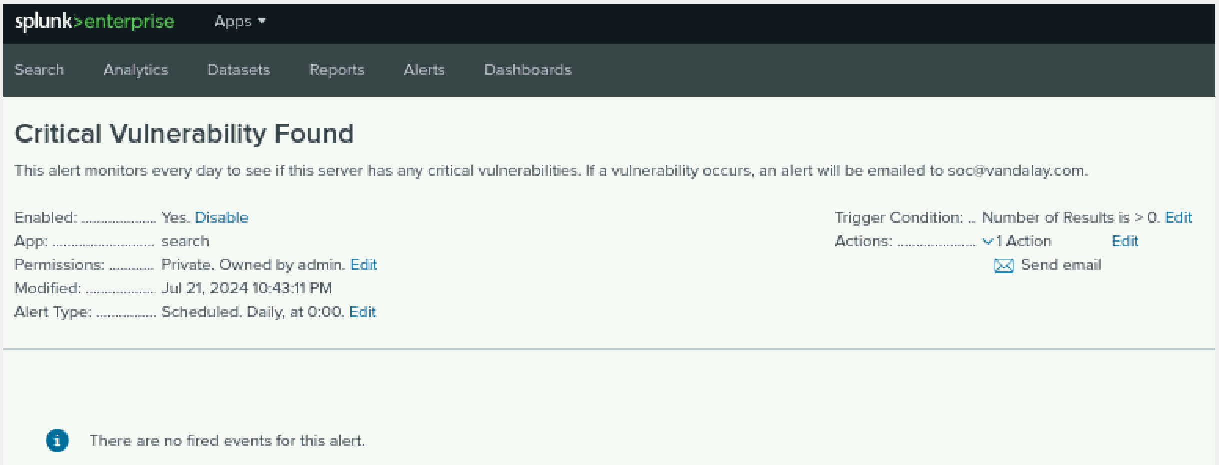
Subject: Splunk Alert: Critical Vulnerability $

The email subject, recipients and message can include tokens that insert text based on the results of the search. Learn More

Message: The alert condition for '$name$' was triggered. Please address immediatly

Include:
- ☑ Link to Alert
- ☑ Link to Results
- ☐ Search String
- ☐ Inline Table ▾
- ☐ Trigger Condition
- ☐ Attach CSV
- ☐ Trigger Time
- ☐ Attach PDF
- ☑ Allow Empty Attachment

Type: [✓ HTML & Plain Text] Plain Text



Critical Vulnerability Found

This alert monitors every day to see if this server has any critical vulnerabilities. If a vulnerability occurs, an alert will be emailed to soc@vandalay.com.

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Jul 21, 2024 10:43:11 PM
Alert Type: .... Scheduled. Daily, at 0:00. Edit

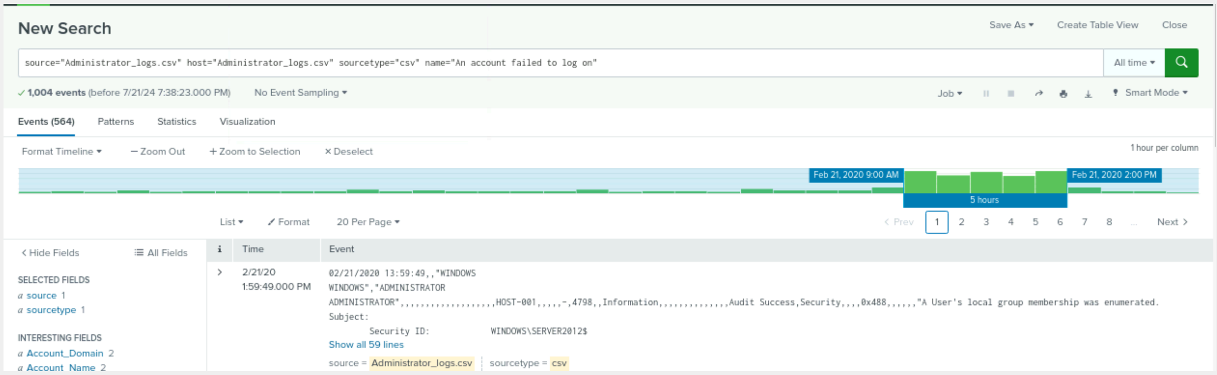
Trigger Condition: .. Number of Results is > 0. Edit
Actions: .... 1 Action Edit
Send email

There are no fired events for this alert.

Step 3: Drawing the (Base)line

1. When did the brute force attack occur?

The system experienced a brute force attack lasting five hours (or more) from 9:00 AM to 2:00 PM on February 21, 2020.



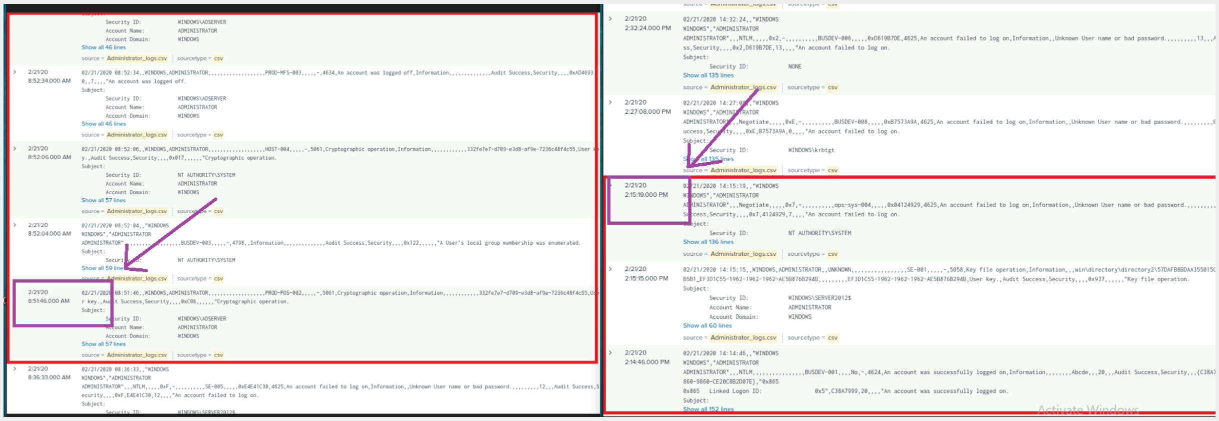
```
source="Administrator_logs.csv" host="Administrator_logs.csv" sourcetype="csv" name="An account failed to log on"
```

✓ 1,004 events (before 7/21/24 7:38:23.000 PM)   No Event Sampling ▾

```
>  2/21/20            02/21/2020 13:59:49,,"WINDOWS
   1:59:49.000 PM     WINDOWS","ADMINISTRATOR
                      ADMINISTRATOR",,,,,,,,,,,,,,,,,,HOST-001,,,,,-,4798,,Information,,,,,,,,,,,,,,Audit Success,Security,,,,0x488,,,,,,"A User's local group membership was enumerated.
                      Subject:
                              Security ID:            WINDOWS\SERVER2012$
                      Show all 59 lines
                      source = Administrator_logs.csv  |  sourcetype = csv
```

Because the number of events between 8 AM - 9AM and 1PM - 2 PM was significantly higher than the baseline for normal activity (34 events), I decided to conduct a deep analysis of the logs. I discovered that the attack began at 8:51:46 AM and ended at 2:15:19 PM.

To be more precise: the brute force attack lasted 5 hours, 23 minutes, and 33 seconds.



```
                              Security ID:            WINDOWS\ADSERVER
                              Account Name:           ADMINISTRATOR
                              Account Domain:         WINDOWS
                      Show all 46 lines
                      source = Administrator_logs.csv  |  sourcetype = csv
>  2/21/20            02/21/2020 08:52:34,,WINDOWS,ADMINISTRATOR,,,,,,,,,,,,,,,,,,PROD-MFS-003,,,,,-,4634,An account was logged off,Information,,,,,,,,,,,,,,Audit Success,Security,,,,0xAD4693
   8:52:34.000 AM     0,,7,,,,"An account was logged off.
                      Subject:
                              Security ID:            WINDOWS\ADSERVER
                              Account Name:           ADMINISTRATOR
                              Account Domain:         WINDOWS
                      Show all 46 lines
                      source = Administrator_logs.csv  |  sourcetype = csv
>  2/21/20            02/21/2020 08:52:06,,WINDOWS,ADMINISTRATOR,,,,,,,,,,,,,,,,,,HOST-004,,,,,-,5061,Cryptographic operation,Information,,,,,,,,,,,,,332fe7e7-d709-e3d8-af9e-7236c48f4c55,User ke
   8:52:06.000 AM     y.,Audit Success,Security,,,,0x017,,,,,,"Cryptographic operation.
                      Subject:
                              Security ID:            NT AUTHORITY\SYSTEM
                              Account Name:           ADMINISTRATOR
                              Account Domain:         WINDOWS
                      Show all 57 lines
                      source = Administrator_logs.csv  |  sourcetype = csv
>  2/21/20            02/21/2020 08:52:04,,"WINDOWS
   8:52:04.000 AM     WINDOWS","ADMINISTRATOR
                      ADMINISTRATOR",,,,,,,,,,,,,,,,,,BUSDEV-003,,,,,-,4798,,Information,,,,,,,,,,,,,,Audit Success,Security,,,,0x122,,,,,,"A User's local group membership was enumerated.
                      Subject:
                              Security ID:            NT AUTHORITY\SYSTEM
                      Show all 59 lines
                      source = Administrator_logs.csv  |  sourcetype = csv
   2/21/20            02/21/2020 08:51:46,,WINDOWS,ADMINISTRATOR,,,,,,,,,,,,,,,,,,PROD-POS-002,,,,,-,5061,Cryptographic operation,Information,,,,,,,,,,,,,332fe7e7-d709-e3d8-af9e-7236c48f4c55,Use
   8:51:46.000 AM     r key.,Audit Success,Security,,,,0xC06,,,,,,"Cryptographic operation.
                      Subject:
                              Security ID:            WINDOWS\ADSERVER
                              Account Name:           ADMINISTRATOR
                              Account Domain:         WINDOWS
                      Show all 57 lines
                      source = Administrator_logs.csv  |  sourcetype = csv
>  2/21/20            02/21/2020 08:36:33,,"WINDOWS
   8:36:33.000 AM     WINDOWS","ADMINISTRATOR
                      ADMINISTRATOR",,,NTLM,,,,,0xF,-,,,,,,,,,,SE-005,,,,,0xE4E41C30,4625,An account failed to log on,Information,,Unknown User name or bad password.,,,,,,,,,,12,,,Audit Success,S
                      ecurity,,,,0xF,E4E41C30,12,,,,"An account failed to log on.
                      Subject:
                              Security ID:            WINDOWS\SERVER2012$
```

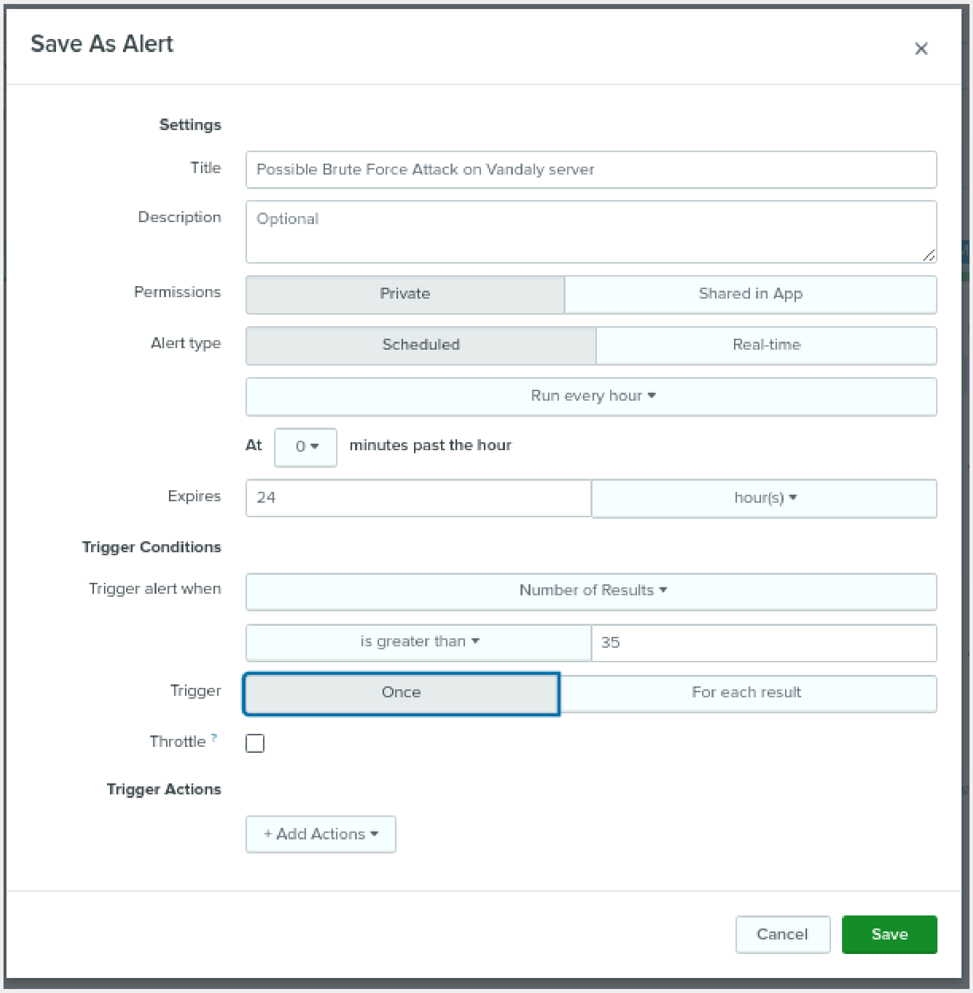
```
>  2/21/20            02/21/2020 14:32:24,,"WINDOWS
   2:32:24.000 PM     WINDOWS","ADMINISTRATOR
                      ADMINISTRATOR",,,NTLM,,,,,0x2,-,,,,,,,,,,BUSDEV-006,,,,,0xD619B7DE,4625,An account failed to log on,Information,,Unknown User name or bad password.,,,,,,,,,,13,,,A
                      ss,Security,,,,0x2,D619B7DE,13,,,,"An account failed to log on.
                      Subject:
                              Security ID:            NONE
                      Show all 135 lines
                      source = Administrator_logs.csv  |  sourcetype = csv
>  2/21/20            02/21/2020 14:27:08,,"WINDOWS
   2:27:08.000 PM     WINDOWS","ADMINISTRATOR
                      ADMINISTRATOR",,,Negotiate,,,,,0xE,-,,,,,,,,,,BUSDEV-008,,,,,0xB7573A9A,4625,An account failed to log on,Information,,Unknown User name or bad password.,,,,,,,,,,0
                      uccess,Security,,,,0xE,B7573A9A,0,,,,"An account failed to log on.
                      Subject:
                              Security ID:            WINDOWS\krbtgt
                      Show all 135 lines
                      source = Administrator_logs.csv  |  sourcetype = csv
>  2/21/20            02/21/2020 14:15:19,,"WINDOWS
   2:15:19.000 PM     WINDOWS","ADMINISTRATOR
                      ADMINISTRATOR",,,Negotiate,,,,,0x7,-,,,,,,,,,,ops-sys-004,,,,,0x04124929,4625,An account failed to log on,Information,,Unknown User name or bad password.,,,,,,,,,
                      Success,Security,,,,0x7,4124929,7,,,,"An account failed to log on.
                      Subject:
                              Security ID:            NT AUTHORITY\SYSTEM
                      Show all 136 lines
                      source = Administrator_logs.csv  |  sourcetype = csv
>  2/21/20            02/21/2020 14:15:15,,WINDOWS,ADMINISTRATOR,,UNKNOWN,,,,,,,,,,,,,,,,SE-001,,,,,-,5058,Key file operation,Information,,,win\directory\directory2\57DAFB8BDAA355015C
   2:15:15.000 PM     B5B1_EF3D1C55-1962-1962-1962-AE5B876B294B,,,,,,,,,EF3D1C55-1962-1962-1962-AE5B876B294B,User key.,Audit Success,Security,,,,0x937,,,,,,"Key file operation.
                      Subject:
                              Security ID:            WINDOWS\SERVER2012$
                              Account Name:           ADMINISTRATOR
                              Account Domain:         WINDOWS
                      Show all 60 lines
                      source = Administrator_logs.csv  |  sourcetype = csv
>  2/21/20            02/21/2020 14:14:46,,"WINDOWS
   2:14:46.000 PM     WINDOWS","ADMINISTRATOR
                      ADMINISTRATOR",,,NTLM,,,,,,,,,,,,,,,,BUSDEV-001,,,,No,-,4624,An account was successfully logged on,Information,,,,,,,,Abcde,,,20,,,Audit Success,Security,,,{C38A7
                      860-9860-CE20C8B2D07E},"0x865
                      0x865   Linked Logon ID:                0x5",C38A7999,20,,,,"An account was successfully logged on.
                      Subject:
                      Show all 152 lines
```

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

Based on the logs, the baseline is 6 to 23 logs per hour (the 34 records included brute force attempts). The threshold will be set at 35 logs per hour, which will help reduce false positives.

Please note: 36 hours of logs between February 20, 6 AM and February 21, 6 PM is not enough information to make a decision about the threshold of logs per hour. The threshold should probably be revised over time.

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



Save As Alert

Settings

Title: Possible Brute Force Attack on Vandaly server

Description: Optional

Permissions: Private | Shared in App

Alert type: Scheduled | Real-time

Run every hour

At 0 minutes past the hour

Expires: 24 hour(s)

Trigger Conditions

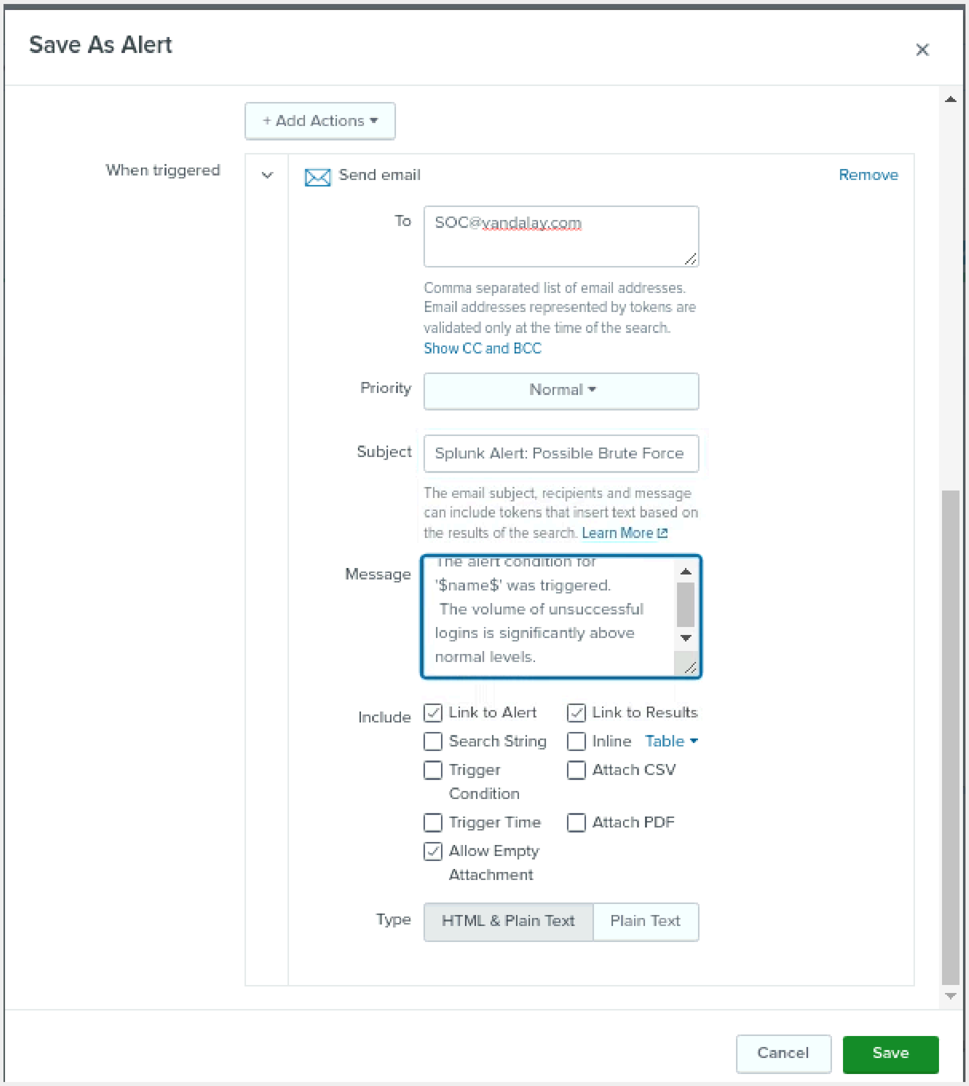
Trigger alert when: Number of Results

is greater than 35

Trigger: Once | For each result

Throttle ? □

Trigger Actions



Save As Alert

When triggered — Send email

To: SOC@vandalay.com

Comma separated list of email addresses. Email addresses represented by tokens are validated only at the time of the search.
Show CC and BCC

Priority: Normal ▾

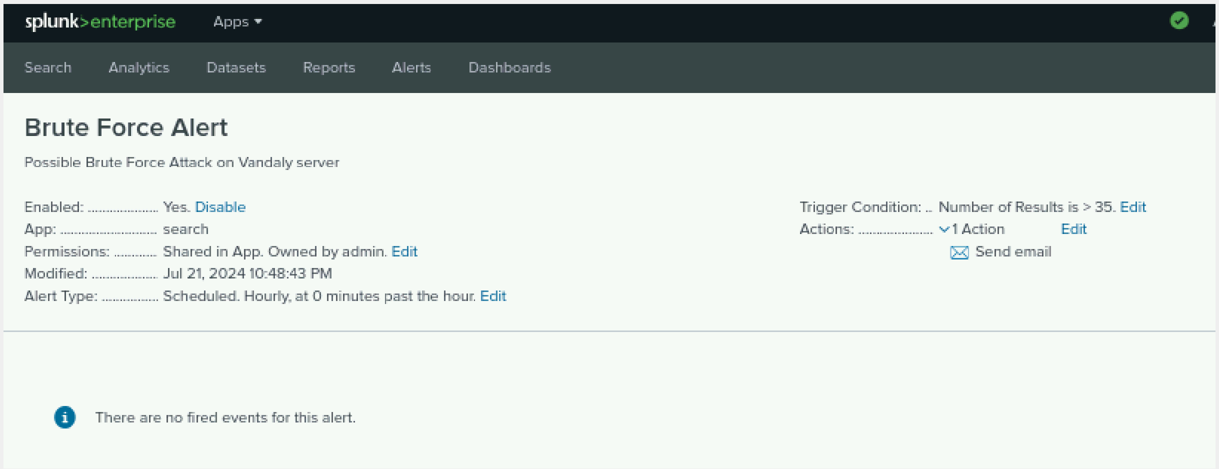
Subject: Splunk Alert: Possible Brute Force

The email subject, recipients and message can include tokens that insert text based on the results of the search. Learn More

Message: The alert condition for '$name$' was triggered.
The volume of unsuccessful logins is significantly above normal levels.

Include:
☑ Link to Alert ☑ Link to Results
□ Search String □ Inline Table ▾
□ Trigger Condition □ Attach CSV
□ Trigger Time □ Attach PDF
☑ Allow Empty Attachment

Type: HTML & Plain Text | Plain Text



Brute Force Alert

Possible Brute Force Attack on Vandaly server

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Shared in App. Owned by admin. Edit
Modified: .... Jul 21, 2024 10:48:43 PM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

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

There are no fired events for this alert.