



# 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 attack occurred on 02/22/2020 at 1130, where the download speed decreased exponentially from 109.16 Mbps to 7.87 bps and it lasted till 2330 on 02/23/2020, when the speed reverted back to normal over 122.91 Mbps.

Two screenshots of the Splunk interface showing search results for BeEF activity.

**Screenshot 1:**

```
source="server_speedtest.csv" host="Speed Test" sourcetype="csv"
```

Events (23) | Patterns | Statistics | Visualization

Format Timeline | Zoom Out | Zoom to Selection | Deselect

1 hour per column

Time	Event
2/24/20 8:30:00:00 PM	198.153.194.2, 2/24/2020 8:30 PM, GHT, 126.91.26.51, 14, "Atlanta, GA", 7, multi
2/24/20 6:30:00:00 PM	host = Speed Test   source = server_speedtest.csv   sourcetype = csv
2/24/20 4:30:00:00 PM	198.153.194.2, 2/24/2020 6:30 PM, GHT, 125.91.25.51, 13, "Atlanta, GA", 6, multi
2/24/20 11:30:00:00 PM	host = Speed Test   source = server_speedtest.csv   sourcetype = csv
2/23/20 11:30:00:00 PM	198.153.194.1, 2/23/2020 11:30 PM, GHT, 124.91.24.51, 12, "Atlanta, GA", 5, multi
2/23/20 11:30:00:00 PM	host = Speed Test   source = server_speedtest.csv   sourcetype = csv
2/23/20 11:30:00:00 PM	198.153.194.1, 2/23/2020 11:30 PM, GHT, 122.91.7.51, 10, "Atlanta, GA", 3, multi
2/23/20 10:30:00:00 PM	host = Speed Test   source = server_speedtest.csv   sourcetype = csv

1 hour per column

Events (23) | Patterns | Statistics | Visualization

Format Timeline | Zoom Out | Zoom to Selection | Deselect

1 hour per column

Time	Event
2/24/20 8:30:00:00 PM	198.153.194.2, 2/24/2020 8:30 PM, GHT, 126.91.26.51, 14, "Atlanta, GA", 7, multi
2/24/20 6:30:00:00 PM	host = Speed Test   source = server_speedtest.csv   sourcetype = csv
2/24/20 4:30:00:00 PM	198.153.194.2, 2/24/2020 4:30 PM, GHT, 124.91.24.51, 12, "Atlanta, GA", 5, multi
2/23/20 11:30:00:00 PM	198.153.194.2, 2/23/2020 11:30 PM, GHT, 123.91.8.51, 11, "Atlanta, GA", 4, multi
2/23/20 11:30:00:00 PM	198.153.194.1, 2/23/2020 11:30 PM, GHT, 122.91.7.51, 10, "Atlanta, GA", 3, multi
2/23/20 10:30:00:00 PM	198.153.194.1, 2/23/2020 10:30 PM, GHT, 78.34.6.51, 12, "Atlanta, GA", 2, multi

1 hour per column

**Screenshot 2:**

```
source="server_speedtest.csv" | eval new_field_name = 'fieldA' / 'fieldB'
```

Events (23) | Patterns | Statistics | Visualization

Format Timeline | Zoom Out | Zoom to Selection | Deselect

1 hour per column

Time	Event
2/24/20 8:30:00:00 PM	198.153.194.2, 2/24/2020 8:30 PM, GHT, 126.91.26.51, 14, "Atlanta, GA", 7, multi
2/24/20 6:30:00:00 PM	host = Speed Test   source = server_speedtest.csv   sourcetype = csv
2/24/20 4:30:00:00 PM	198.153.194.1, 2/24/2020 4:30 PM, GHT, 124.91.24.51, 12, "Atlanta, GA", 5, multi
2/23/20 11:30:00:00 PM	198.153.194.2, 2/23/2020 11:30 PM, GHT, 123.91.8.51, 11, "Atlanta, GA", 4, multi
2/23/20 11:30:00:00 PM	198.153.194.1, 2/23/2020 11:30 PM, GHT, 122.91.7.51, 10, "Atlanta, GA", 3, multi
2/23/20 10:30:00:00 PM	198.153.194.1, 2/23/2020 10:30 PM, GHT, 78.34.6.51, 12, "Atlanta, GA", 2, multi

1 hour per column

Search | Splunk 9.1.1 | ⚡ BeEF Control Panel | Sign In - Google Acco | 0.0.0.0:3000/demos/ | Vulnerability: Stored | +

localhost:800/en-US/app/search/search?q=search%20source%3Dserver\_speedtest.csv%20%7C%20eval%20new\_field\_name%20%3D%20%27fieldA%27%20%20%2F%20%27field... ➤ ⭐ 🌐 Update

Search Analytics Datasets Reports Alerts Dashboards

New Search

source="server\_speedtest.csv" | eval new\_field\_name = 'fieldA' / 'fieldB'

✓ 23 events (before 12/2/23 5:28:17.000 PM) No Event Sampling \*

Events (23) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection X Deselect

List Format 20 Per Page

< Hide Fields All Fields

SELECTED FIELDS  
# host 1  
# source 1  
# sourcetype 1

INTERESTING FIELDS  
# CONNECTION\_MODE 1  
# date\_hour 6  
# date\_mday 5  
# date\_minute 2  
# date\_month 1  
# date\_wday 5  
# date\_year 1  
# date\_zone 1

Your Report Has Been Created

You may now view your report, add it to a dashboard, change additional settings, or continue editing it.

Additional Settings:

- Permissions
- Schedule
- Acceleration
- Embed

Continue Editing Add to Dashboard View

Save As Create Table View Close

All time 1 hour per column

Job 🔍 Smart Mode 🔍

1 hour per column

Prev 1 2 Next >

Time	Event
2/24/20 8:30:00:000 PM	198.153.194.2, 2/24/2020 8:38 PM, GHT, 126.91.26.51,14,"Atlanta, GA",7,multi host = Speed Test   source = server_speedtest.csv   sourcetype = csv
2/24/20 6:30:00:000 PM	198.153.194.2, 2/24/2020 6:38 PM, GHT, 125.91.25.51,13,"Atlanta, GA",6,multi host = Speed Test   source = server_speedtest.csv   sourcetype = csv
2/24/20 4:30:00:000 PM	198.153.194.1, 2/24/2028 4:38 PM, GHT, 124.91.24.51,12,"Atlanta, GA",5,multi host = Speed Test   source = server_speedtest.csv   sourcetype = csv
2/23/20 11:30:00:000 PM	198.153.194.2 ,2/23/2028 11:38 PM, GHT, 123.91.8.51,11,"Atlanta, GA",4,multi host = Speed Test   source = server_speedtest.csv   sourcetype = csv
2/23/20 11:30:00:000 PM	198.153.194.1 ,2/23/2028 11:38 PM, GHT, 122.91.7.51,10,"Atlanta, GA",3,multi host = Speed Test   source = server_speedtest.csv   sourcetype = csv
2/23/20	198.153.194.1 ,2/23/2028 10:38 PM, GHT, 121.91.6.51,12,"Atlanta, GA",2,multi host = Speed Test   source = server_speedtest.csv   sourcetype = csv

**Speed Test report**

All time ▾

✓ 23 events (before 12/2/23 5:28:17.000 PM)

20 per page ▾

i	Time	Event
>	2/24/20 8:30:00.000 PM	198.153.194.2, 2/24/2020 8:30 PM,GHT,126.91,26.51,14,"Atlanta, GA",7,multi host = Speed Test   source = server_speedtest.csv sourcetype = csv
>	2/24/20 6:30:00.000 PM	198.153.194.2, 2/24/2020 6:30 PM,GHT,125.91,25.51,13,"Atlanta, GA",6,multi host = Speed Test   source = server_speedtest.csv sourcetype = csv
>	2/24/20 4:30:00.000 PM	198.153.194.1, 2/24/2020 4:30 PM,GHT,124.91,24.51,12,"Atlanta, GA",5,multi host = Speed Test   source = server_speedtest.csv sourcetype = csv
>	2/23/20 11:30:00.000 PM	198.153.194.2, 2/23/2020 11:30 PM,GHT,123.91,8.51,11,"Atlanta, GA",4,multi host = Speed Test   source = server_speedtest.csv sourcetype = csv
>	2/23/20 11:30:00.000 PM	198.153.194.1, 2/23/2020 11:30 PM,GHT,122.91,7.51,10,"Atlanta, GA",3,multi host = Speed Test   source = server_speedtest.csv sourcetype = csv
>	2/23/20 10:30:00.000 PM	198.153.194.1, 2/23/2020 10:30 PM,GHT,78.34,4.23,13,"Atlanta, GA",1,multi host = Speed Test   source = server_speedtest.csv sourcetype = csv
>	2/23/20 8:30:00.000 PM	198.153.194.2, 2/23/2020 8:30 PM,GHT,65.34,4.6,51,12,"Atlanta, GA",2,multi host = Speed Test   source = server_speedtest.csv sourcetype = csv
>	2/23/20 6:30:00.000 PM	198.153.194.2, 2/23/2020 6:30 PM,GHT,17.56,3.43,88,"Atlanta, GA",8,multi host = Speed Test   source = server_speedtest.csv sourcetype = csv

✓ 23 events (before 12/2/23 5:31:18.000 PM) No Event Sampling ▾

Events (23) Patterns Statistics Visualization

Format Timeline ▾    Zoom Out    Zoom to Selection    Deselect

source="server\_speedtest.csv" | eval ratio="DOWNLOAD\_MEGABITS/UPLOAD\_MEGABITS"

1 hour per column

i	Time	Event
>	2/24/20 8:30:00.000 PM	198.153.194.2, 2/24/2020 8:30 PM,GHT,126.91,26.51,14,"Atlanta, GA",7,multi host = Speed Test   source = server_speedtest.csv sourcetype = csv
>	2/24/20 6:30:00.000 PM	198.153.194.2, 2/24/2020 6:30 PM,GHT,125.91,25.51,13,"Atlanta, GA",6,multi host = Speed Test   source = server_speedtest.csv sourcetype = csv
>	2/24/20 4:30:00.000 PM	198.153.194.1, 2/24/2020 4:30 PM,GHT,124.91,24.51,12,"Atlanta, GA",5,multi host = Speed Test   source = server_speedtest.csv sourcetype = csv
>	2/23/20 11:30:00.000 PM	198.153.194.2, 2/23/2020 11:30 PM,GHT,123.91,8.51,11,"Atlanta, GA",4,multi host = Speed Test   source = server_speedtest.csv sourcetype = csv
>	2/23/20 11:30:00.000 PM	198.153.194.1, 2/23/2020 11:30 PM,GHT,122.91,7.51,10,"Atlanta, GA",3,multi host = Speed Test   source = server_speedtest.csv sourcetype = csv
>	2/23/20 10:30:00.000 PM	198.153.194.1, 2/23/2020 10:30 PM,GHT,78.34,4.23,13,"Atlanta, GA",1,multi host = Speed Test   source = server_speedtest.csv sourcetype = csv
>	2/23/20 8:30:00.000 PM	198.153.194.2, 2/23/2020 8:30 PM,GHT,65.34,4.6,51,12,"Atlanta, GA",2,multi host = Speed Test   source = server_speedtest.csv sourcetype = csv

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

It took 24 hours to recover.

Provide a screenshot of your report:



## Step 2: Are We Vulnerable?

Provide a screenshot of your report:

Search | Splunk 9.1.1 x BeEF Control Panel x Sign in - Google Acco x 0.0.0:0.3000/demos/ x Vulnerability: Stored x +

localhost:8000/en-US/app/search/search?q=search%20source%3Dnessus\_logs.csv%20host%3D%20Logs%20source\_type%3D%20csv&earliest=0&latest=&sid=1701539043.2... Save As Create Table View Close Update

### New Search

source="nessus\_logs.csv" host="Nessus Logs" sourcetype="csv"

258 events (before 12/2/23 5:44:03.000 PM) No Event Sampling

Events (258) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection Deselect 1 hour per column

List Format 20 Per Page

< Hide Fields All Fields Time Event

SELECTED FIELDS  
a host 1  
a source 1  
a sourcetype 1

INTERESTING FIELDS  
# bid 20  
a cve 83  
# cvss 3  
# cvss\_base\_score 3  
cvss\_vector 3  
# date\_hour 5  
# date\_minute 60  
# date\_month 1  
# date\_second 60  
# date\_wday 1  
# date\_year 1  
a date\_zone 1

2/20/20 6:09:23:000 PM ,start\_time="Thu Feb 20 18:09:23 2020" end\_time="Thu Feb 20 18:09:23 2020" dest\_dns="HOST-003" dest\_mac="52:70:fa:52:7c:e4" dest\_ip="10.11.36.11" os="Microsoft Windows XP Service Pack 2" osv="Microsoft Windows XP Service Pack 3" cvss\_base\_score="4.3" cvss\_vector="CVSS2AV:N/AC:H/Au:N/C:P/I:A/N" dest\_port\_proto="microsoft-ds(139/tcp)" severity\_id="0" signature\_family="Service detection" signature\_id="12122" signature="Terminal Services Encryption Level is not FIPS-140 Compliant" bid="1493" cve="CVE-2017-1000385" cve="CVE-2017-17428" cwe="208" osvdb="8230" osvdb="299" xref="OSVDB:8230" xref="OSVDB:299" xref="CVE-2017-1000385",Thu Feb 20 18:09:23 2020,nessus\_nessus\_end\_of\_event--  
,2020-02-20T18:15:48.000+0000,,1493,...,CVE-2017-1000385  
CVE-2017-17428  
CVSS2AV:N/AC:H/Au:N/C:P/I:A/N,200,HOST-003,...,HOST-003,10.11.36.11,false,,,52:70:fa:52:7c:e4,,untrust,139,microsoft-ds(139/tcp),false,,false,,  
,Thu Feb 20 18:09:23 2020,nessus\_nessus\_misconfigured\_device nessus\_plugin\_avail nessus\_system\_version,127.0.0.1,,main,,,4,,,Microsoft Windows XP Service Pack 2  
Show all 20 lines  
host = Nessus Logs | source = nessus\_logs.csv | sourcetype = csv

2/20/20 6:03:16:000 PM ,start\_time="Thu Feb 20 18:03:16 2020" end\_time="Thu Feb 20 18:03:16 2020" dest\_ip="10.11.36.6" os="Microsoft Windows XP Professional SP3" dest\_port\_proto="microft-ds(445/tcp)" severity\_id="3" signature\_id="1089" signature="Common Platform Enumeration (CPE)" dest\_dns="HOST-003" dest\_nt\_host="AOME-003" ---splunk-ta-nessus-end-of-event--  
,2020-02-20T18:07:16.000+0000,,...,HOST-003,...,HOST-003,10.11.36.23,false,,,AOME-003,,untrust,445,microsoft-ds(445/tcp),false,,false,,Thu Feb 20 18:03:16 2020,nessus\_nessus\_misconfigured\_device nessus\_plugin\_avail nessus\_system\_version,127.0.0.1,,main,,,4,,,Microsoft Windows XP Professional SP3,,Err:509,,high,3,,Common Platform Enumeration (CPE),,1089,eventgen,nessus,prd-p-vj7zglpcb88,...,Thu Feb 20 18:03:16 2020,nessus\_nessus\_end\_of\_event--

Search | Splunk 9.1.1 x BeEF Control Panel x Sign in - Google Acco x 0.0.0:0.3000/demos/ x Vulnerability: Stored x +

localhost:8000/en-US/app/search/search?q=search%20source%3Dnessus\_logs.csv%20dest\_ip%3D10.11.36.23%20severity%3D%20CRITICAL%3D%20count%20by%20severity&earliest=0&latest=&sid=1701539043.2... Save As Create Table View Close Update

spunk>enterprise Apps

Administrator Messages Settings Activity Help

Search & Reporting

### New Search

source="nessus\_logs.csv" dest\_ip="10.11.36.23" | eval CRITICAL=if(severity="critical", "Critical", "Non-Critical") | stats count by CRITICAL

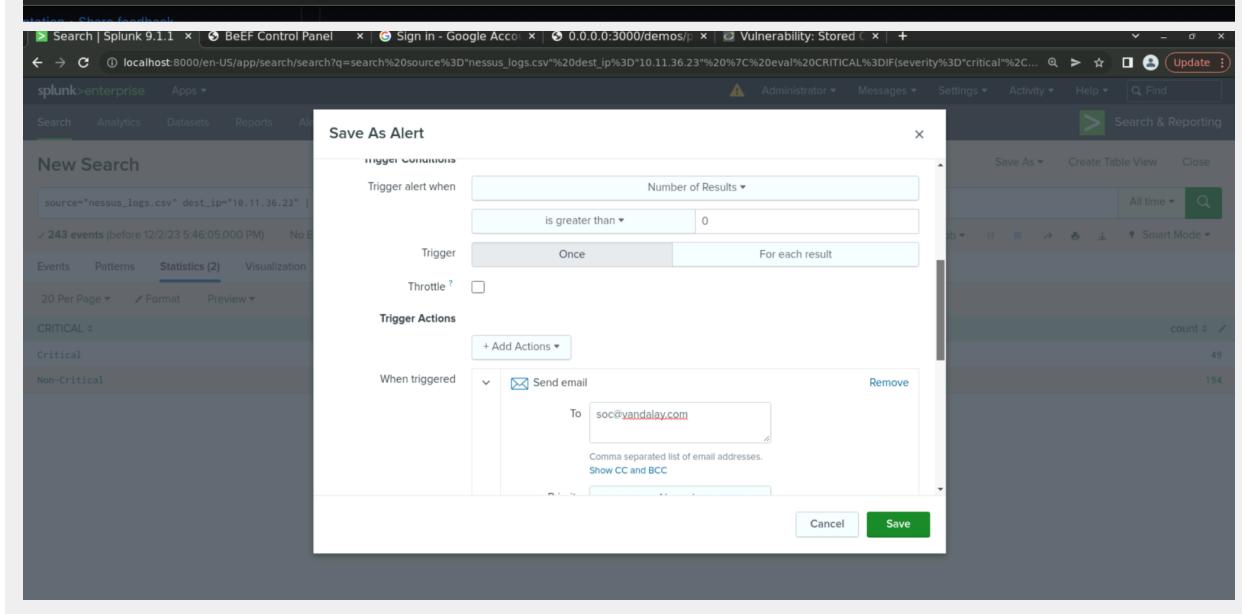
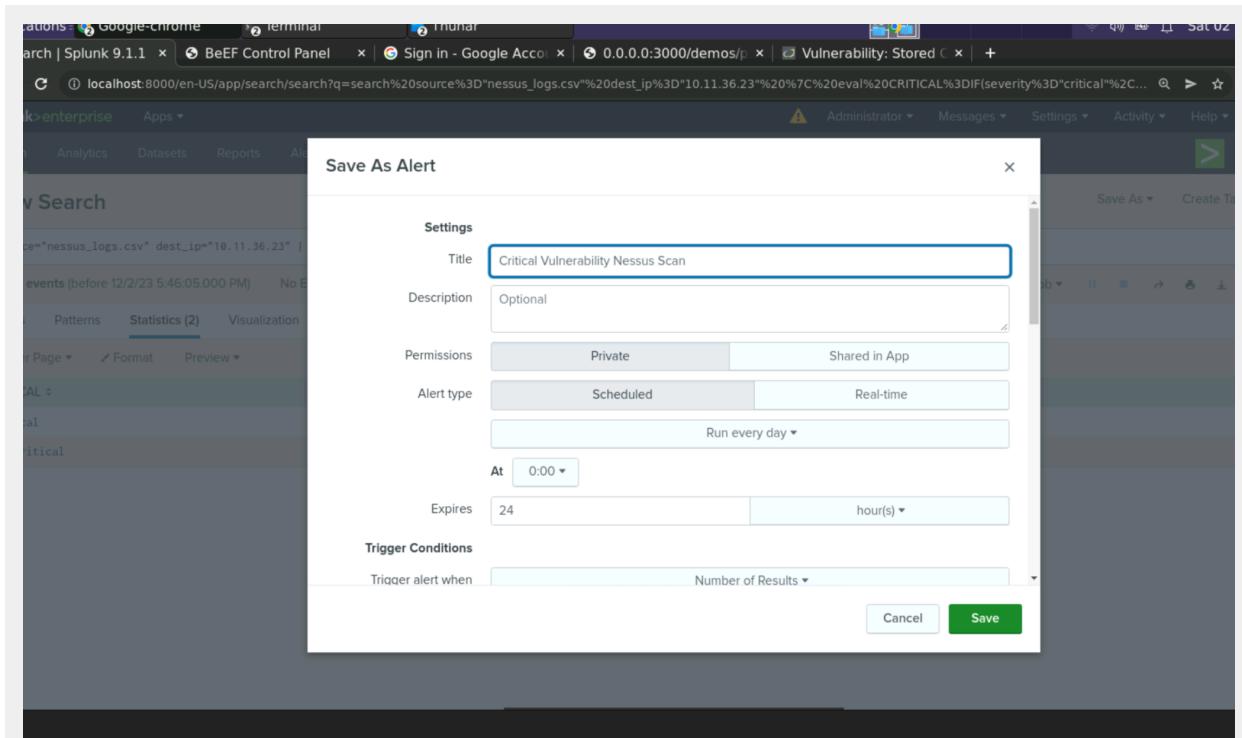
243 events (before 12/2/23 5:46:05.000 PM) No Event Sampling

Events Statistics (2) Visualization

20 Per Page Format Preview

CRITICAL : count :  
Critical 49  
Non-Critical 194

Provide a screenshot showing that the alert has been created:



The screenshot shows two related pages from the Splunk interface.

**Top Window: Save As Alert**

- When triggered:** A dropdown menu is open.
- To:** soc@vandalay.com
- Priority:** Normal
- Subject:** Critical Vulnerabilities
- Message:** This alert condition is for critical vulnerabilities was more than zero.
- Buttons:** Cancel and Save

**Bottom Window: Critical Vulnerability Nessus Scan**

- Enabled:** Yes. Disable
- App:** search
- Permissions:** Private. Owned by admin. Edit
- Modified:** Dec 2, 2023 5:58:53 PM
- Alert Type:** Scheduled. Daily, at 0:00. Edit
- Trigger Condition:** Number of Results is > 0. Edit
- Actions:** 1 Action Edit
- Send email:** A link to edit the email settings.

**Information:** 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 occurred 0900 until 1400 on 2/21/2020 for 5 hours.

This screenshot shows a Splunk search interface with the following details:

- Title:** New Search
- Search Query:** source="Administrator\_logs.csv" sourcetype="csv" name="An account failed to log on" name="\*"
- Results:** 564 events (2/21/20 9:00:00.000 AM to 2/21/20 2:00:00.000 PM) No Event Sampling
- Event Count:** 564 events
- Time Range:** Feb 21, 2020 9:00 AM to Feb 21, 2020 2:00 PM (5 hours)
- Event Examples:**
  - 2/21/20 13:59:49, "WINDOWS", "ADMINISTRATOR", "ADMINISTRATOR", "HOST-001...", "4798, Information, Audit Success, Security, 0x488, "A User's local group membership was enumerated."
  - 2/21/20 13:59:41, "WINDOWS", "ADMINISTRATOR", "ADMINISTRATOR", "ACME-002...", "4798, Information, Audit Success, Security, 0x398, "A User's local group membership was enumerated."
- Fields:** host, source, sourcetype
- Interesting Fields:** Account\_Domain, Account\_Name, action, app, Authentication\_Package, body, category, ComputerName, date\_hour

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

According to the logs, the baseline is 5-35 logs per hour. Therefore the threshold should be set at 40 or higher login attempts each hour and the alert will be emailed to SOC@vandalay.com when it's triggered.

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

This screenshot shows the 'Save As Alert' dialog box in Splunk:

- Title:** Brute Force alert
- Description:** Optional
- Permissions:** Private
- Alert type:** Scheduled
- Run every hour:** At 0 minutes past the hour
- Expires:** 24 hour(s)
- Trigger Conditions:** Trigger alert when Number of Results is greater than 40

Splunk 9.1.1 | BeEF Control Panel | Sign In - Google Acco | 0.0.0:3000/demos/ | Vulnerability: Stored C | +

localhost:8000/en-US/app/search/search?q=search%20source%3DAdministrator\_logs.csv%20sourcetype%3D"csv"%20name%3D"An%20account%20failed%20to%20log%20on%"%20

### Save As Alert

When triggered

Send email

To: SOC@vandalay.com

Priority: Normal

Subject: Brute force admin

Message: The alert condition will trigger if it goes greater than 40.

Link to Alert  Link to Details

Cancel Save

Splunk 9.1.1 | BeEF Control Panel | Sign In - Google Acco | 0.0.0:3000/demos/ | Vulnerability: Stored C | +

localhost:8000/en-US/app/search/alert?s=%2FservicesNS%2Fadmin%2Fsearch%2Fsaved%2Fsearches%2FBrute%2520Force%2520alert

Brute Force alert

Enabled: Yes. Disable

App: search

Permissions: Private. Owned by admin. [Edit](#)

Modified: Dec 2, 2023 6:22:07 PM

Alert Type: Scheduled. Hourly, at 0 minutes past the hour. [Edit](#)

Trigger Condition: Number of Results is > 40. [Edit](#)

Actions: [1 Action](#) [Edit](#)

Send email

There are no fired events for this alert.