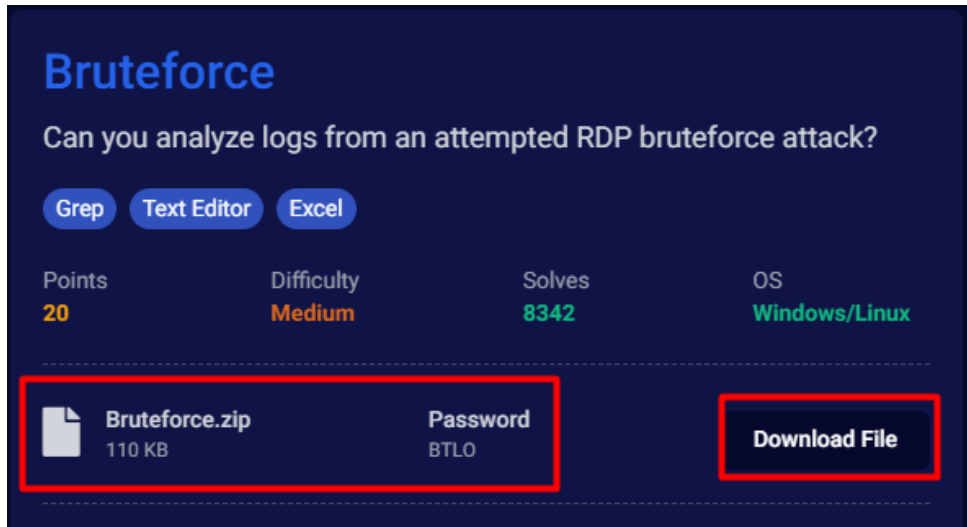


Challenge URL: <https://blueteamlabs.online/home/challenge/bruteforce-16629bf9a2>



The image shows the 'Bruteforce' challenge page. At the top, it asks 'Can you analyze logs from an attempted RDP bruteforce attack?'. Below this are three buttons: 'Grep', 'Text Editor', and 'Excel'. A summary section displays 'Points: 20', 'Difficulty: Medium', 'Solves: 8342', and 'OS: Windows/Linux'. A file named 'Bruteforce.zip' (110 KB) is listed with a 'Password: BTLO'. A 'Download File' button is also present. Red boxes highlight the file information and the download button.

**Bruteforce**

Can you analyze logs from an attempted RDP bruteforce attack?

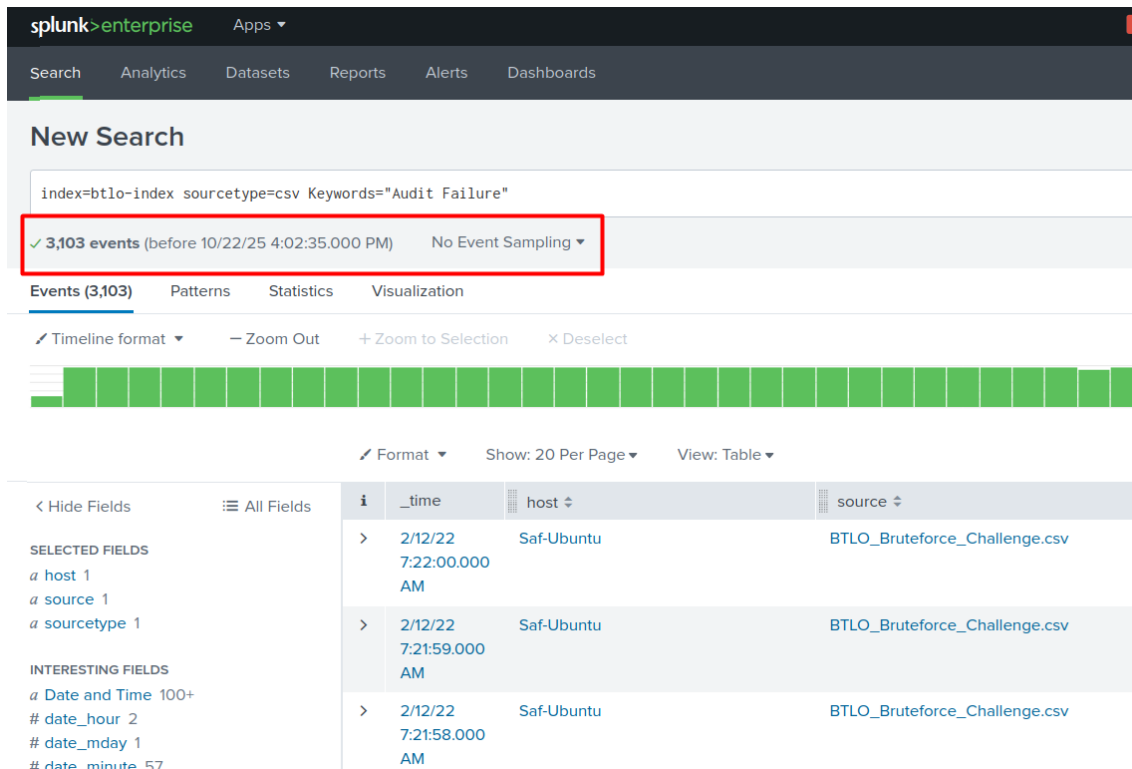
Grep Text Editor Excel

Points **20** Difficulty **Medium** Solves **8342** OS **Windows/Linux**

**Bruteforce.zip** 110 KB Password **BTLO** **Download File**

Download the zip file to analyze the log file.

Question 1) How many Audit Failure events are there? (Format: Count of Events)



The image shows the Splunk search interface. The search bar contains the query 'index=btlo-index sourcetype=csv Keywords="Audit Failure"'. The results show 3,103 events. Below the search bar, there are tabs for 'Events (3,103)', 'Patterns', 'Statistics', and 'Visualization'. The 'Events' tab is selected, showing a timeline view. The table below displays the search results in a table format.

splunk>enterprise Apps

Search Analytics Datasets Reports Alerts Dashboards

New Search

index=btlo-index sourcetype=csv Keywords="Audit Failure"

✓ 3,103 events (before 10/22/25 4:02:35.000 PM) No Event Sampling

Events (3,103) Patterns Statistics Visualization

Timeline format Zoom Out Zoom to Selection Deselect

Format Show: 20 Per Page View: Table

	_time	host	source
>	2/12/22 7:22:00.000 AM	Saf-Ubuntu	BTLO_Bruteforce_Challenge.csv
>	2/12/22 7:21:59.000 AM	Saf-Ubuntu	BTLO_Bruteforce_Challenge.csv
>	2/12/22 7:21:58.000 AM	Saf-Ubuntu	BTLO_Bruteforce_Challenge.csv

Hide Fields All Fields

SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- a Date and Time 100+
- # date\_hour 2
- # date\_mday 1
- # date\_minute 57

## Question 2) What is the username of the local account that is being targeted? (Format: Username)

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

- Search Query:** `search index%3Dbtlo-index sourcetype%3Dcsv Keywords%3D"Audit Failure"&display.page`
- Fields:** `_time`, `host`, `source`
- Log Entry:** `Audit Failure,2/12/2022 7:22:00 AM,Microsoft-Windows-Security-Auditing,4625,Logon,"An account failed to log on."`
- Subject:**
  - Security ID: NULL SID
  - Account Name: -
  - Account Domain: -
  - Logon ID: 0x0
- Logon Type:** 3
- Account For Which Logon Failed:**
  - Security ID: NULL SID
  - Account Name: administrator** (highlighted in red)
  - Account Domain: -
- Failure Information:**
  - Failure Reason: Unknown user name or bad password.
  - Status: 0xC000006D
  - Sub Status: 0xC000006A
- Process Information:**
  - Caller Process ID: 0x0
  - Caller Process Name: -
- Network Information:**
  - Workstation Name: -
  - Source Network Address: 113.161.192.227

## Question 3) What is the failure reason related to the Audit Failure logs? (Format: String)

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

- Search Query:** `search index%3Dbtlo-index sourcetype%3Dcsv Keywords%3D"Audit Failure"&displa`
- Fields:** `_time`, `host`, `source`
- Log Entry:** `Logon ID: 0x0`
- Logon Type:** 3
- Account For Which Logon Failed:**
  - Security ID: NULL SID
  - Account Name: administrator
  - Account Domain: -
- Failure Information:**
  - Failure Reason: Unknown user name or bad password.** (highlighted in red)
  - Status: 0xC000006D
  - Sub Status: 0xC000006A
- Process Information:**
  - Caller Process ID: 0x0
  - Caller Process Name: -
- Network Information:**
  - Workstation Name: -
  - Source Network Address: 113.161.192.227
  - Source Port: 59545
- Detailed Authentication Information:**
  - Logon Process: NtLmSsp

**Question 4) What is the Windows Event ID associated with these logon failures?  
(Format: ID)**

The screenshot shows a Splunk search interface. On the left, a list of fields is displayed, with **# Event ID 1** highlighted in a red box. On the right, the **Event ID** configuration panel is open. It shows a summary of the event ID field, including a report of values over time. The **Values** table at the bottom is highlighted with a red box, showing the following data:

Values	Count	%
4625	3,103	100%

**Question 5) What is the source IP conducting this attack? (Format: X.X.X.X)**

The screenshot shows a Splunk event view for a logon failure event. The **Network Information** section is expanded, and the **Source Network Address** field is highlighted with a red box, showing the IP address **113.161.192.227**. Other fields in the network section include Workstation Name (empty), Source Port (59545), and Detailed Authentication Information (Logon Process: NtLmSsp, Authentication Package: NTLM, Transited Services: empty, Package Name (NTLM only): empty, Key Length: 0).

**Question 6) What country is this IP address associated with? (Format: Country)**

# Whois IP 113.161.192.227

Updated 5 days ago

```
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '113.160.0.0 - 113.191.255.255'

% Abuse contact for '113.160.0.0 - 113.191.255.255' is 'hn-changed@vnnic.vn'

inetnum:        113.160.0.0 - 113.191.255.255
netname:        VNPT-VN
descr:          Vietnam Posts and Telecommunications Group
descr:          No 57, Huynh Thuc Khang Street, Lang Ha ward, Dong Da district, Ha Noi City
country:        VN
admin-c:        PTH13-AP
tech-c:         PTH13-AP
remarks:        for admin contact mail to Nguyen Xuan Cuong NXC1-AP
remarks:        for Tech contact mail to Nguyen Hien Khanh KNH1-AP
status:         ALLOCATED PORTABLE
mnt-by:         MAINT-VN-VNNIC
mnt-lower:      MAINT-VN-VNPT
mnt-routes:     MAINT-VN-VNPT
last-modified:  2018-01-25T03:55:17Z
mnt-irt:        IRT-VNNIC-AP
source:         APNIC

irt:            IRT-VNNIC-AP
address:        Ha Noi, VietNam
phone:          +84-24-35564944
fax-no:         +84-24-37821462
e-mail:         hn-changed@vnnic.vn
abuse-mailbox:  hn-changed@vnnic.vn
admin-c:        NTTTT1-AP
tech-c:         NTTTT1-AP
auth:          # Filtered
mnt-by:         MAINT-VN-VNNIC
last-modified:  2025-10-08T04:42:43Z
```

What is the range of source ports that were used by the attacker to make these login requests? (LowestPort-HighestPort - Ex: 100-541)

The screenshot shows the Splunk Enterprise interface. At the top, there's a navigation bar with 'splunk>enterprise' and various menu items like 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. Below this is a 'Search & Reporting' section with a 'New Search' button. The search query is entered in a text box: `index=btlo-index sourcetype=csv | rex field=EXTRA_FIELD_6 "Source Port:\s+(?<src_port>\d+)" | stats min(src_port) as Lowest_Port, max(src_port) as Highest_Port`. Below the query, it shows '3,129 events (before 10/22/25 4:10:50.000 PM)' and 'No Event Sampling'. At the bottom, there's a table with two columns: 'Lowest\_Port' and 'Highest\_Port'. The values '49162' and '65534' are shown in the respective columns, both highlighted with red boxes.

### To see the lowest and highest port

```
index=btlo-index sourcetype=csv
| rex field=EXTRA_FIELD_6 "Source Port:\s+(?<src_port>\d+)"
| stats min(src_port) as Lowest_Port, max(src_port) as Highest_Port
```

### To see all the ports with event

```
index=btlo-index sourcetype=csv
| rex field=EXTRA_FIELD_6 "Source Port:\s+(?<src_port>\d+)"
| table _time src_port host source
```

### Country Extraction and visualization

```
index=btlo-index sourcetype=csv
| rex field=EXTRA_FIELD_6 "Source Network
Address:\s+(?<src_ip>\d{1,3}(\.?\d{1,3}){3})"
| iplocation src_ip
| stats count by Country
| sort -count
```

### With Username and success failure

```
index=btlo-index sourcetype=csv
| eval Status=if(match(EXTRA_FIELD_6, "An account failed to log on"),
"Failure", "Success")
| rex field=EXTRA_FIELD_6 "Account Name:\s+(?<username>\S+)"
| stats count by Status, username
| sort - count
```