Blue Team Labs Online: Bruteforce

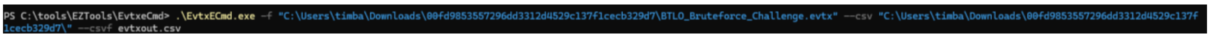
The following writeup is for Bruteforce on Blue Team Labs Online, it's a medium difficulty lab that involves analysing logs from an attempted RDP Bruteforce attack. The medium difficulty rating is farfetched, it's an easy challenge and that's coming from someone not experienced with RDP log analysis. Nonetheless, it was really enjoyable.

Scenario: One of our system administrators identified a large number of Audit Failure events in the Windows Security Event log.

There are a number of different ways to approach the analysis of these logs! Consider the suggested tools, but there are many others out there!

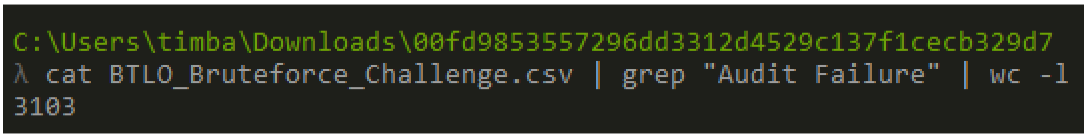
Question 1) How many Audit Failure events are there? (Format: Count of Events)

I'm going to start by parsing the provided EVTX file using EvtxECmd, which is a wonderful tool created by Eric Zimmerman that makes analysing EVTX files much easier than using Event Viewer.



```
PS C:\tools\EZTools\EvtxeCmd> .\EvtxECmd.exe -f "C:\Users\timba\Downloads\00fd9853557296dd3312d4529c137f1cecb329d7\BTLO_Bruteforce_Challenge.evtx" --csv "C:\Users\timba\Downloads\00fd9853557296dd3312d4529c137f
1cecb329d7\" --csvf evtxout.csv
```

Turns out, the evtx file only contains one event for failed logon, so let's take a look at the provided csv file instead. To answer this question, we can simply read the csv file, grep for Audit Failure and pipe that output to wc -l to count the number of lines:

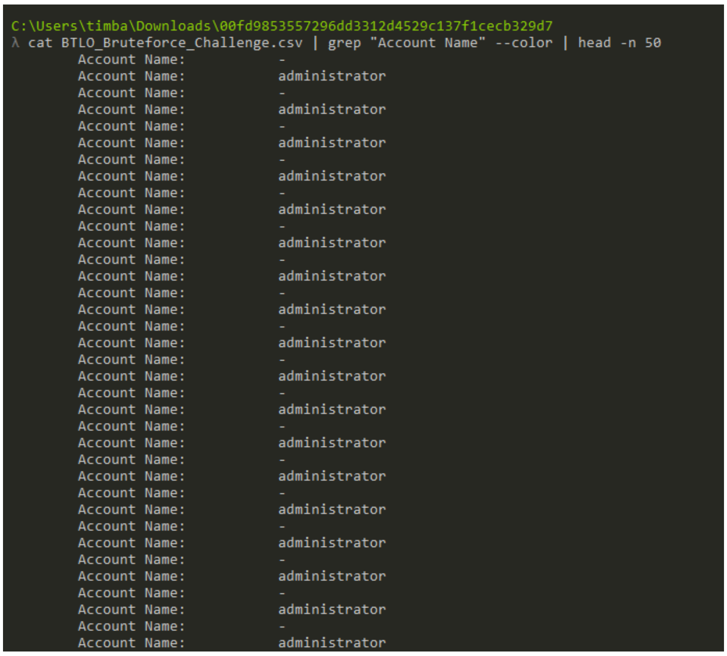


```
C:\Users\timba\Downloads\00fd9853557296dd3312d4529c137f1cecb329d7
λ cat BTLO_Bruteforce_Challenge.csv | grep "Audit Failure" | wc -l
3103
```

Answer: 3103

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

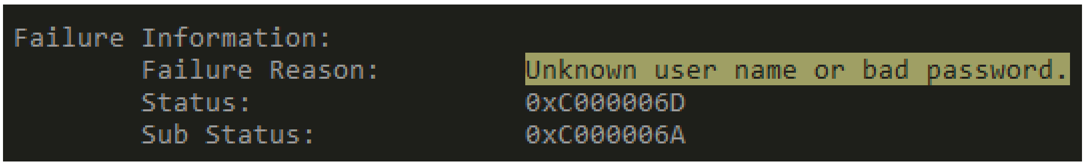
If you grep for Account Name, you will see that there are thousands of failed logon attempts for the administrator account:



```
C:\Users\timba\Downloads\00fd9853557296dd3312d4529c137f1cecb329d7
λ cat BTLO_Bruteforce_Challenge.csv | grep "Account Name" --color | head -n 50
        Account Name:           -
        Account Name:           administrator
        Account Name:           -
        Account Name:           administrator
        Account Name:           -
        Account Name:           administrator
        Account Name:           -
        Account Name:           administrator
        Account Name:           -
        Account Name:           administrator
        Account Name:           -
        Account Name:           administrator
        Account Name:           -
        Account Name:           administrator
        Account Name:           -
        Account Name:           administrator
        Account Name:           -
        Account Name:           administrator
        Account Name:           -
        Account Name:           administrator
        Account Name:           -
        Account Name:           administrator
        Account Name:           -
        Account Name:           administrator
        Account Name:           -
        Account Name:           administrator
        Account Name:           -
        Account Name:           administrator
        Account Name:           -
        Account Name:           administrator
        Account Name:           -
        Account Name:           administrator
        Account Name:           -
        Account Name:           administrator
        Account Name:           -
        Account Name:           administrator
```

Answer: administrator

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

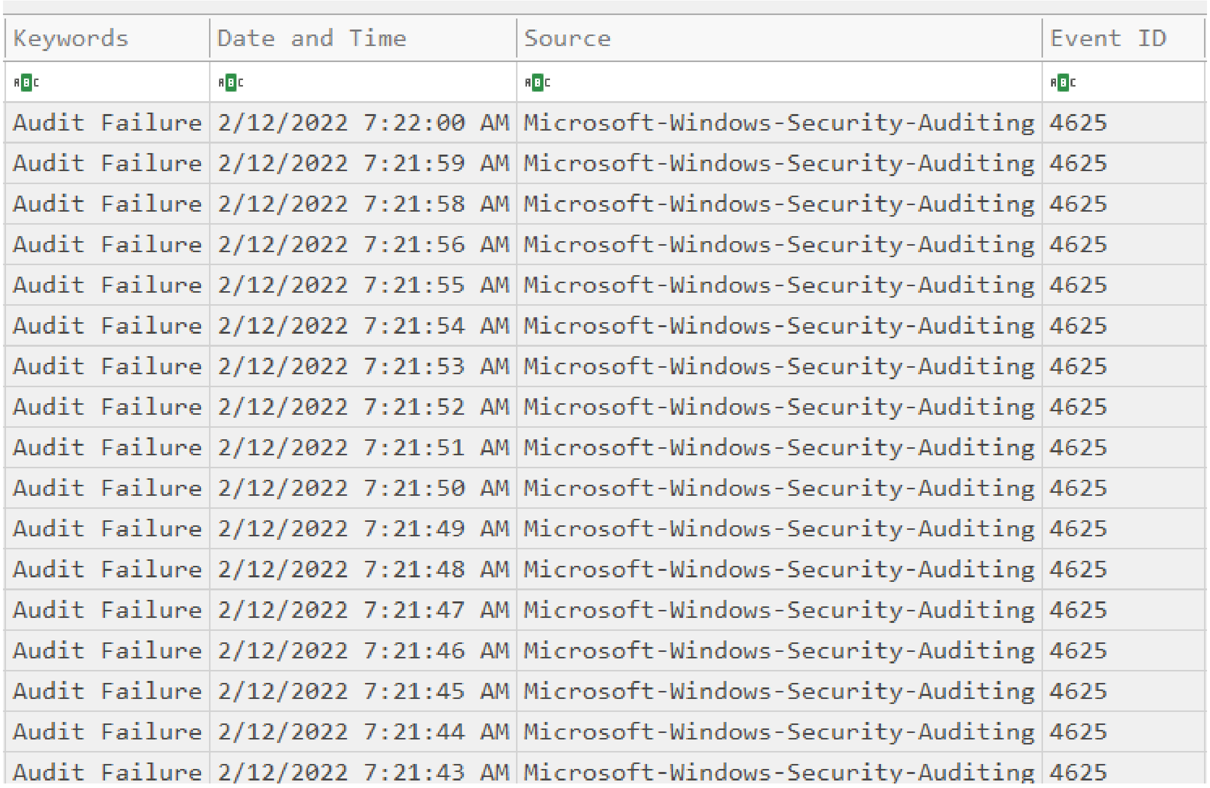


```
Failure Information:
        Failure Reason:         Unknown user name or bad password.
        Status:                 0xC000006D
        Sub Status:             0xC000006A
```

Answer: Unknown user name or bad password.

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

You can see per the csv file that the Event ID associated with logon failures is 4625:

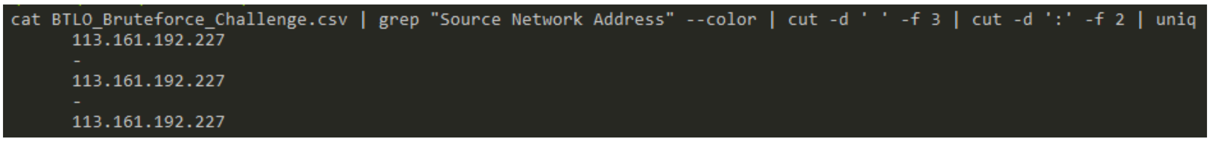


Keywords	Date and Time	Source	Event ID
ABC	ABC	ABC	ABC
Audit Failure	2/12/2022 7:22:00 AM	Microsoft-Windows-Security-Auditing	4625
Audit Failure	2/12/2022 7:21:59 AM	Microsoft-Windows-Security-Auditing	4625
Audit Failure	2/12/2022 7:21:58 AM	Microsoft-Windows-Security-Auditing	4625
Audit Failure	2/12/2022 7:21:56 AM	Microsoft-Windows-Security-Auditing	4625
Audit Failure	2/12/2022 7:21:55 AM	Microsoft-Windows-Security-Auditing	4625
Audit Failure	2/12/2022 7:21:54 AM	Microsoft-Windows-Security-Auditing	4625
Audit Failure	2/12/2022 7:21:53 AM	Microsoft-Windows-Security-Auditing	4625
Audit Failure	2/12/2022 7:21:52 AM	Microsoft-Windows-Security-Auditing	4625
Audit Failure	2/12/2022 7:21:51 AM	Microsoft-Windows-Security-Auditing	4625
Audit Failure	2/12/2022 7:21:50 AM	Microsoft-Windows-Security-Auditing	4625
Audit Failure	2/12/2022 7:21:49 AM	Microsoft-Windows-Security-Auditing	4625
Audit Failure	2/12/2022 7:21:48 AM	Microsoft-Windows-Security-Auditing	4625
Audit Failure	2/12/2022 7:21:47 AM	Microsoft-Windows-Security-Auditing	4625
Audit Failure	2/12/2022 7:21:46 AM	Microsoft-Windows-Security-Auditing	4625
Audit Failure	2/12/2022 7:21:45 AM	Microsoft-Windows-Security-Auditing	4625
Audit Failure	2/12/2022 7:21:44 AM	Microsoft-Windows-Security-Auditing	4625
Audit Failure	2/12/2022 7:21:43 AM	Microsoft-Windows-Security-Auditing	4625

Answer: 4625

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

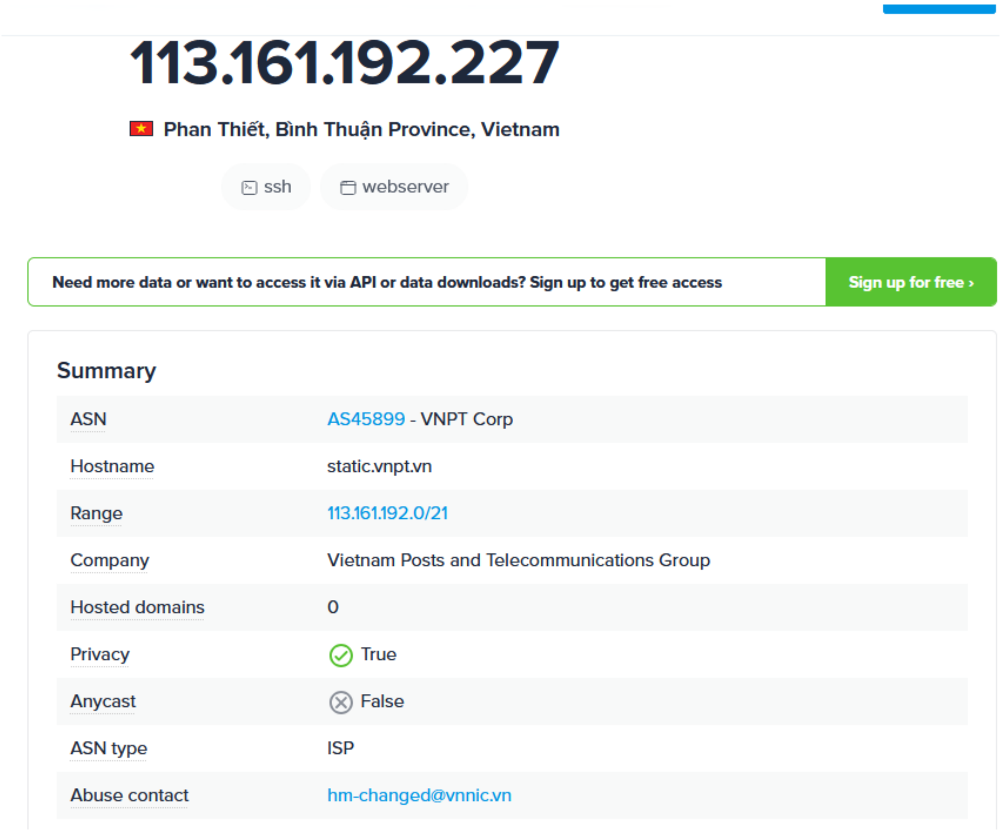
If you grep the input for Source Network Address, you can see that there is only one:



```
cat BTLO_Bruteforce_Challenge.csv | grep "Source Network Address" --color | cut -d ' ' -f 3 | cut -d ':' -f 2 | uniq
        113.161.192.227
        -
        113.161.192.227
        -
        113.161.192.227
```

Answer: 113.161.192.227

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



113.161.192.227

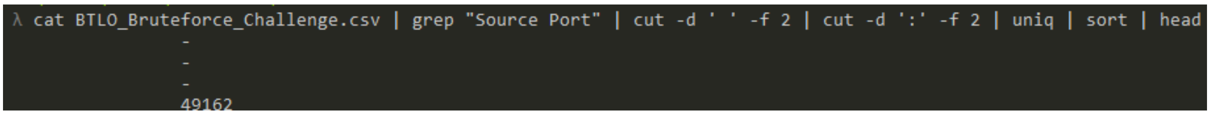
Phan Thiết, Bình Thuận Province, Vietnam

Summary

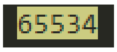
ASN	AS45899 - VNPT Corp
Hostname	static.vnpt.vn
Range	113.161.192.0/21
Company	Vietnam Posts and Telecommunications Group
Hosted domains	0
Privacy	✓ True
Anycast	⊗ False
ASN type	ISP
Abuse contact	hm-changed@vnnic.vn

Answer: Vietnam

Question 7) What is the range of source ports that were used by the attacker to make these login requests? (LowestPort-HighestPort - Ex: 100-541)



```
λ cat BTLO_Bruteforce_Challenge.csv | grep "Source Port" | cut -d ' ' -f 2 | cut -d ':' -f 2 | uniq | sort | head
              -
              -
              -
              49162
```



```
65534
```

Answer: 49162-65534