Bruteforce

Contents

Scenario

Can you analyse logs from an attempted RDP bruteforce attack?

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

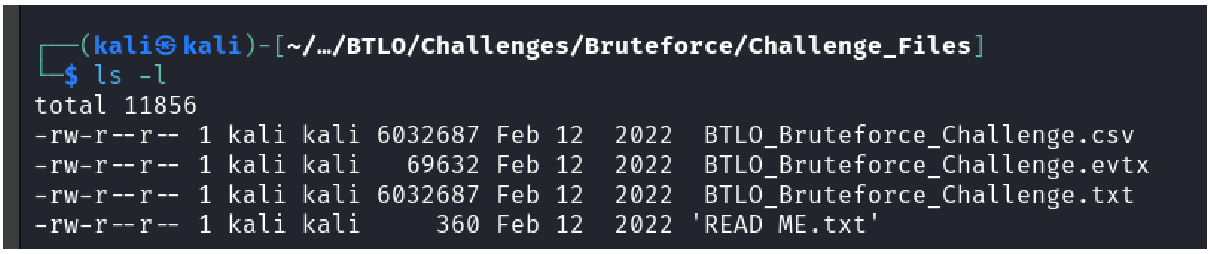
There are a number of different ways to approach the analysis of these logs! Consider the suggested tools, but there are many others out there!

Pre-requisites

- Load kali
- Run sudo apt update && sudo apt -y upgrade > reboot
- Change network to host only instead of NAT – to restrict network so malware inside the pcap is contained within the VM
- Load Wireshark and open the pcap file

Initial thoughts from scenario

- Listing the contents of the extracted download folder, a text file and a CSV file immediately stand out as they can be easily read and grep-ed

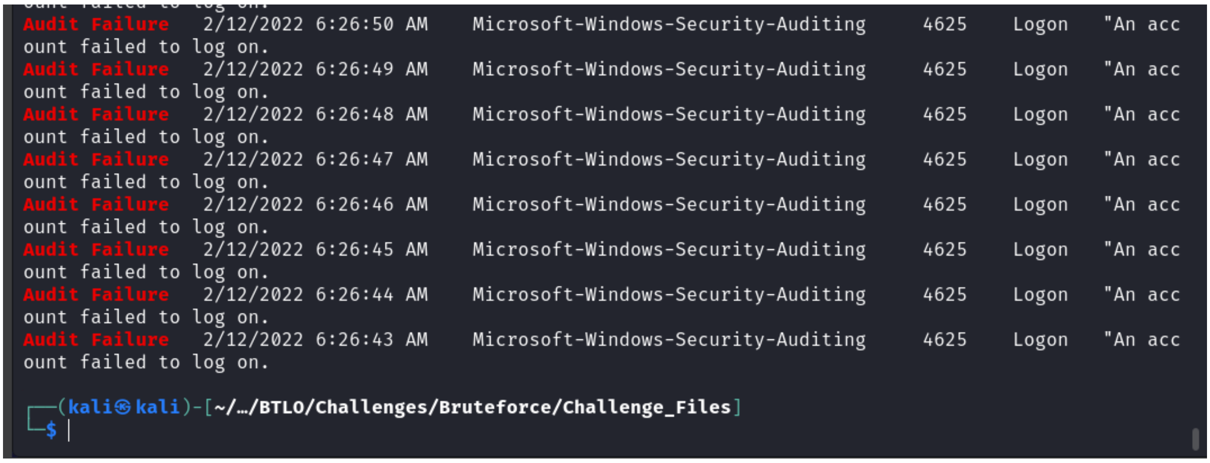


```
┌──(kali㉿kali)-[~/…/BTLO/Challenges/Bruteforce/Challenge_Files]
└─$ ls -l
total 11856
-rw-r--r-- 1 kali kali 6032687 Feb 12  2022  BTLO_Bruteforce_Challenge.csv
-rw-r--r-- 1 kali kali   69632 Feb 12  2022  BTLO_Bruteforce_Challenge.evtx
-rw-r--r-- 1 kali kali 6032687 Feb 12  2022  BTLO_Bruteforce_Challenge.txt
-rw-r--r-- 1 kali kali     360 Feb 12  2022 'READ ME.txt'
```

Challenge Questions

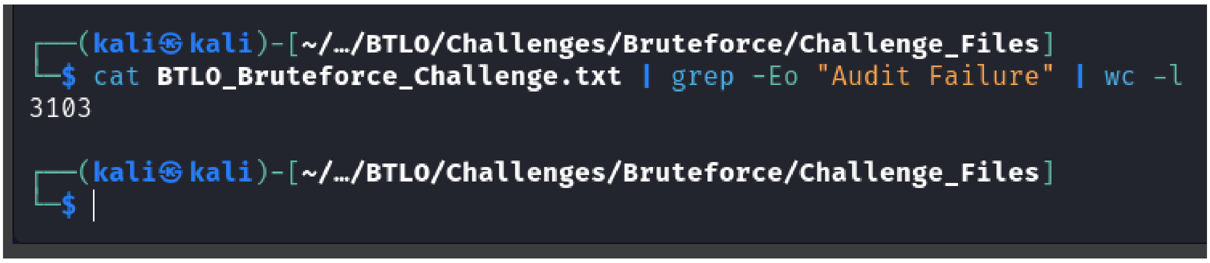
How many Audit Failure events are there?

- Answer: 3103



```
ount failed to log on.
Audit Failure   2/12/2022 6:26:50 AM    Microsoft-Windows-Security-Auditing     4625    Logon   "An acc
ount failed to log on.
Audit Failure   2/12/2022 6:26:49 AM    Microsoft-Windows-Security-Auditing     4625    Logon   "An acc
ount failed to log on.
Audit Failure   2/12/2022 6:26:48 AM    Microsoft-Windows-Security-Auditing     4625    Logon   "An acc
ount failed to log on.
Audit Failure   2/12/2022 6:26:47 AM    Microsoft-Windows-Security-Auditing     4625    Logon   "An acc
ount failed to log on.
Audit Failure   2/12/2022 6:26:46 AM    Microsoft-Windows-Security-Auditing     4625    Logon   "An acc
ount failed to log on.
Audit Failure   2/12/2022 6:26:45 AM    Microsoft-Windows-Security-Auditing     4625    Logon   "An acc
ount failed to log on.
Audit Failure   2/12/2022 6:26:44 AM    Microsoft-Windows-Security-Auditing     4625    Logon   "An acc
ount failed to log on.
Audit Failure   2/12/2022 6:26:43 AM    Microsoft-Windows-Security-Auditing     4625    Logon   "An acc
ount failed to log on.

┌──(kali㉿kali)-[~/…/BTLO/Challenges/Bruteforce/Challenge_Files]
└─$ |
```

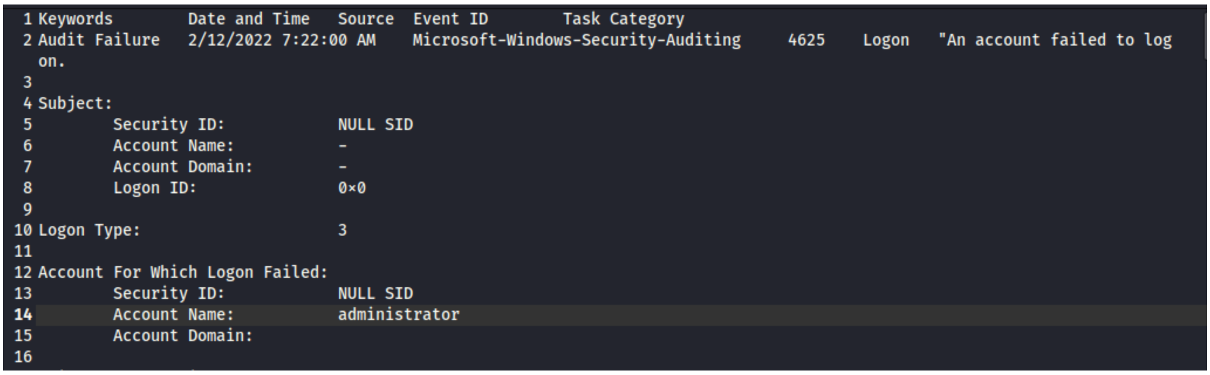
Grep-ing the file for "Audit Failure" provides far too many to either scroll through. So we can use the "-Eo" grep option and pipe it into "wc -l" to count all the occurrences:



```
┌──(kali㉿kali)-[~/…/BTLO/Challenges/Bruteforce/Challenge_Files]
└─$ cat BTLO_Bruteforce_Challenge.txt | grep -Eo "Audit Failure" | wc -l
3103

┌──(kali㉿kali)-[~/…/BTLO/Challenges/Bruteforce/Challenge_Files]
└─$ 
```

What is the username of the local account that is being targeted?

- Answer: administrator

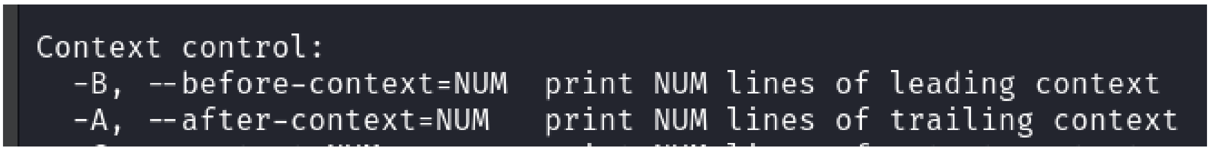


```
 1 Keywords        Date and Time    Source  Event ID        Task Category
 2 Audit Failure   2/12/2022 7:22:00 AM    Microsoft-Windows-Security-Auditing     4625     Logon    "An account failed to log
   on.
 3
 4 Subject:
 5         Security ID:            NULL SID
 6         Account Name:           -
 7         Account Domain:         -
 8         Logon ID:               0×0
 9
10 Logon Type:                     3
11
12 Account For Which Logon Failed:
13         Security ID:            NULL SID
14         Account Name:           administrator
15         Account Domain:
16
```

Viewing the .txt file in mousepad shows that the “Account name:” line is 3 lines below the line stating that the event is a logon failure

- Line 12 shows “Account for which logon failed:”
- Line 14 2 lines below shows the account name

So to confirm the account name we can grep with the “-A”:



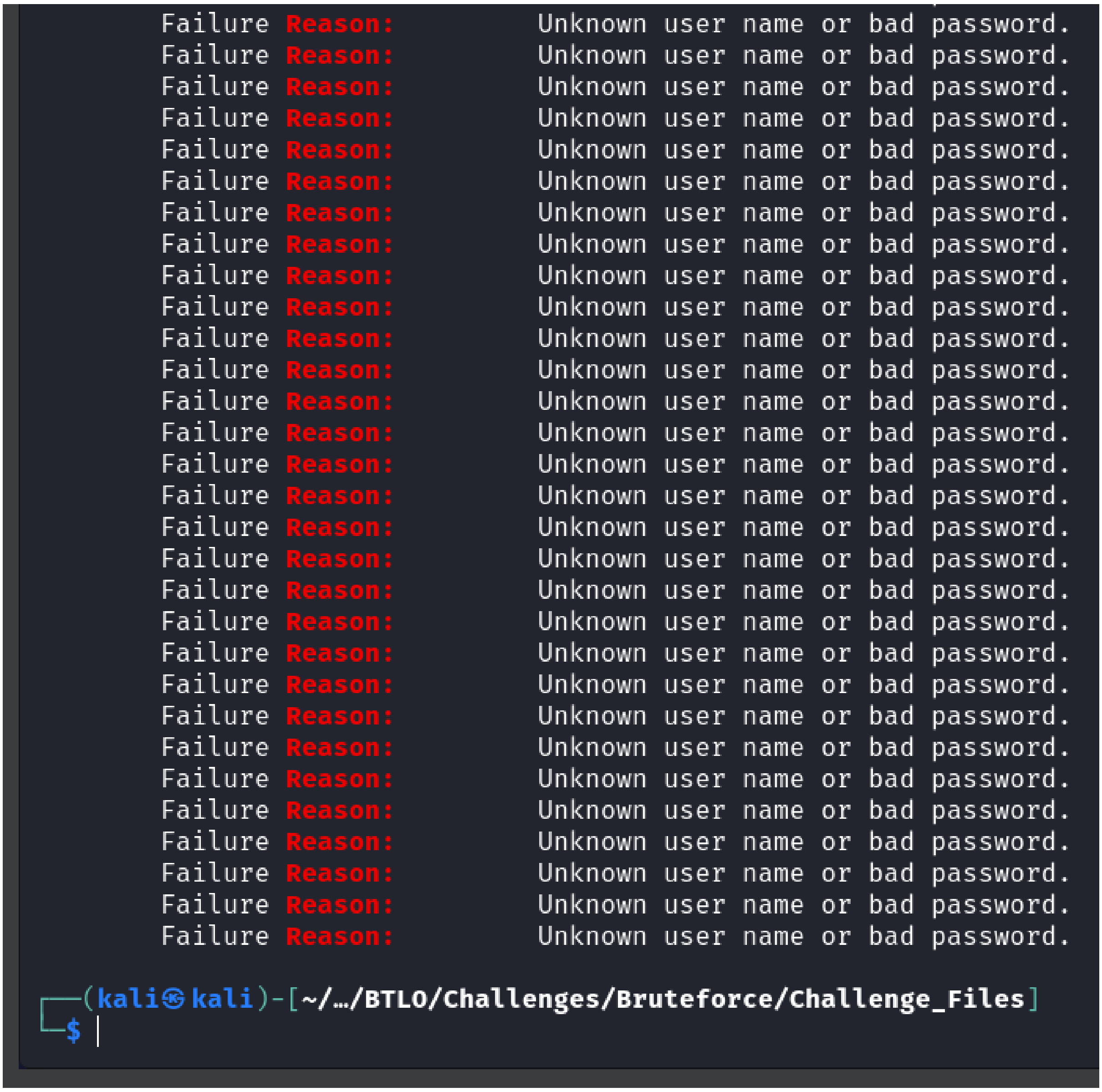
```
Context control:
  -B, --before-context=NUM  print NUM lines of leading context
  -A, --after-context=NUM   print NUM lines of trailing context
```

The only account name that shows in the output of grep is administrator

What is the failures reason related to the Audit Failure logs?

- Answer:

Doing a quick grep for “[Rr]eason” within the .txt file shows the only reason is “Unknown user name or bad password”

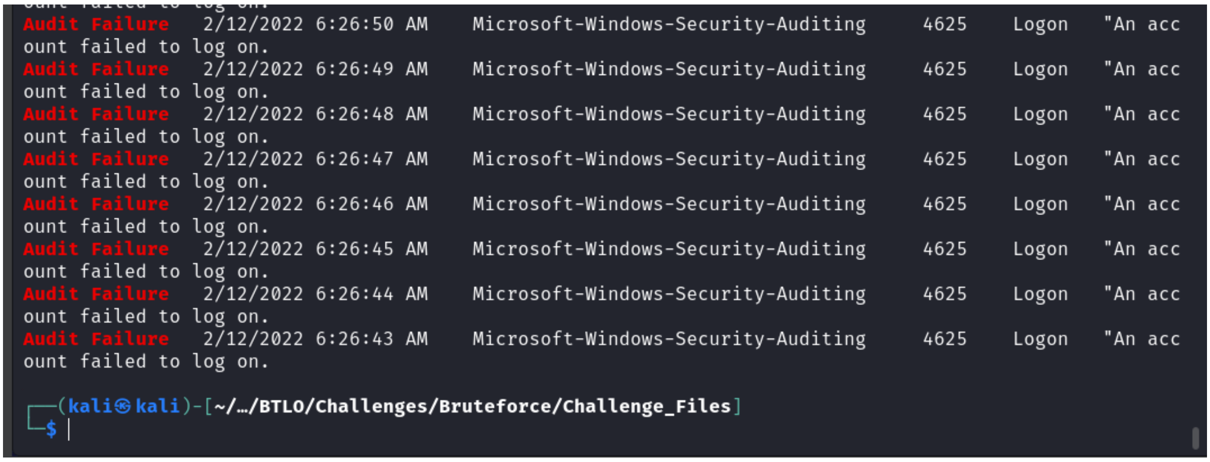


```
        Failure Reason:         Unknown user name or bad password.
        Failure Reason:         Unknown user name or bad password.
        Failure Reason:         Unknown user name or bad password.
        Failure Reason:         Unknown user name or bad password.
        Failure Reason:         Unknown user name or bad password.
        Failure Reason:         Unknown user name or bad password.
        Failure Reason:         Unknown user name or bad password.
        Failure Reason:         Unknown user name or bad password.
        Failure Reason:         Unknown user name or bad password.
        Failure Reason:         Unknown user name or bad password.
        Failure Reason:         Unknown user name or bad password.
        Failure Reason:         Unknown user name or bad password.
        Failure Reason:         Unknown user name or bad password.
        Failure Reason:         Unknown user name or bad password.
        Failure Reason:         Unknown user name or bad password.
        Failure Reason:         Unknown user name or bad password.
        Failure Reason:         Unknown user name or bad password.
        Failure Reason:         Unknown user name or bad password.
        Failure Reason:         Unknown user name or bad password.
        Failure Reason:         Unknown user name or bad password.
        Failure Reason:         Unknown user name or bad password.
        Failure Reason:         Unknown user name or bad password.
        Failure Reason:         Unknown user name or bad password.
        Failure Reason:         Unknown user name or bad password.
        Failure Reason:         Unknown user name or bad password.
        Failure Reason:         Unknown user name or bad password.
        Failure Reason:         Unknown user name or bad password.
        Failure Reason:         Unknown user name or bad password.
        Failure Reason:         Unknown user name or bad password.
        Failure Reason:         Unknown user name or bad password.

┌──(kali㉿kali)-[~/…/BTLO/Challenges/Bruteforce/Challenge_Files]
└─$ 
```

What is the Windows Event ID associated with these logon failures?

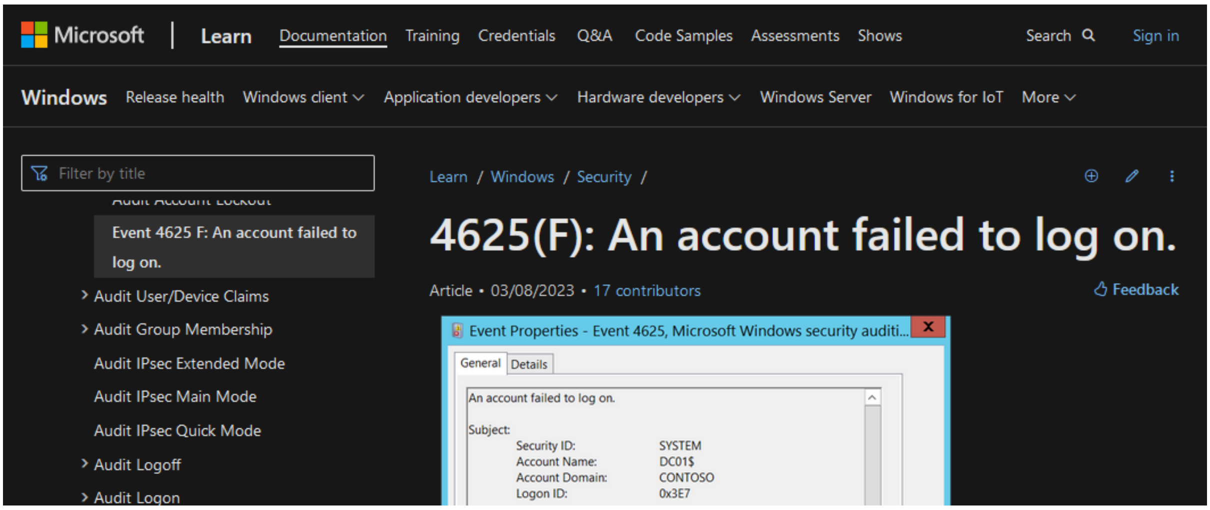
- Answer: 4625

We saw this in the first challenge:



```
ount failed to log on.
Audit Failure   2/12/2022 6:26:50 AM    Microsoft-Windows-Security-Auditing     4625    Logon   "An acc
ount failed to log on.
Audit Failure   2/12/2022 6:26:49 AM    Microsoft-Windows-Security-Auditing     4625    Logon   "An acc
ount failed to log on.
Audit Failure   2/12/2022 6:26:48 AM    Microsoft-Windows-Security-Auditing     4625    Logon   "An acc
ount failed to log on.
Audit Failure   2/12/2022 6:26:47 AM    Microsoft-Windows-Security-Auditing     4625    Logon   "An acc
ount failed to log on.
Audit Failure   2/12/2022 6:26:46 AM    Microsoft-Windows-Security-Auditing     4625    Logon   "An acc
ount failed to log on.
Audit Failure   2/12/2022 6:26:45 AM    Microsoft-Windows-Security-Auditing     4625    Logon   "An acc
ount failed to log on.
Audit Failure   2/12/2022 6:26:44 AM    Microsoft-Windows-Security-Auditing     4625    Logon   "An acc
ount failed to log on.
Audit Failure   2/12/2022 6:26:43 AM    Microsoft-Windows-Security-Auditing     4625    Logon   "An acc
ount failed to log on.

┌──(kali㉿kali)-[~/…/BTLO/Challenges/Bruteforce/Challenge_Files]
└─$ |
```

The fourth column in the grep-ed output is the Windows Event ID, which is 4625. A quick double check on google confirms this:



Microsoft | Learn Documentation Training Credentials Q&A Code Samples Assessments Shows Search Sign in
Windows Release health Windows client Application developers Hardware developers Windows Server Windows for IoT More
Filter by title
Audit Account Lockout
Event 4625 F: An account failed to log on.
Audit User/Device Claims
Audit Group Membership
Audit IPsec Extended Mode
Audit IPsec Main Mode
Audit IPsec Quick Mode
Audit Logoff
Audit Logon
Learn / Windows / Security /
Feedback
Event Properties - Event 4625, Microsoft Windows security auditi...
General Details

4625(F): An account failed to log on.

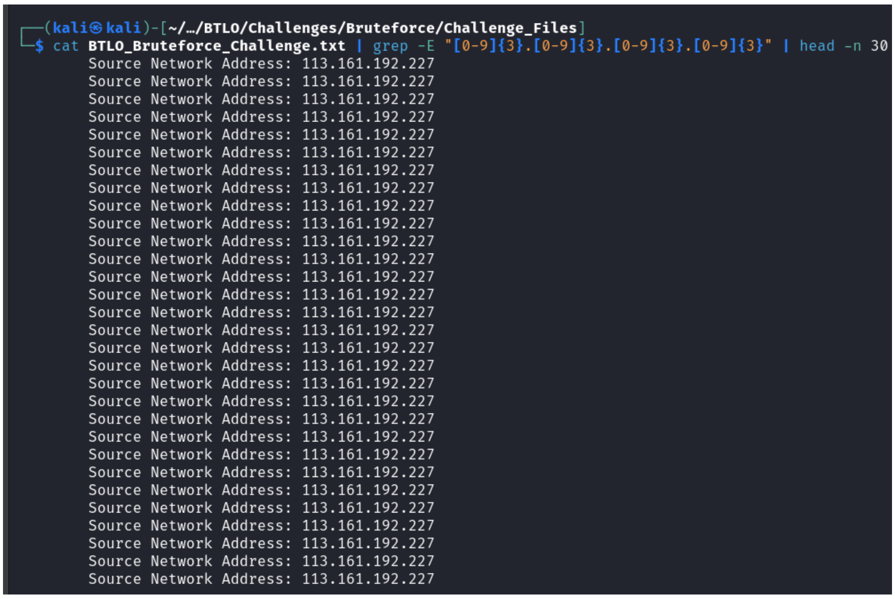
Article • 03/08/2023 • 17 contributors

An account failed to log on.

Subject:
Security ID: SYSTEM
Account Name: DC01$
Account Domain: CONTOSO
Logon ID: 0x3E7

What is the source IP conducting this attack?

- Answer: 113.161.192.227

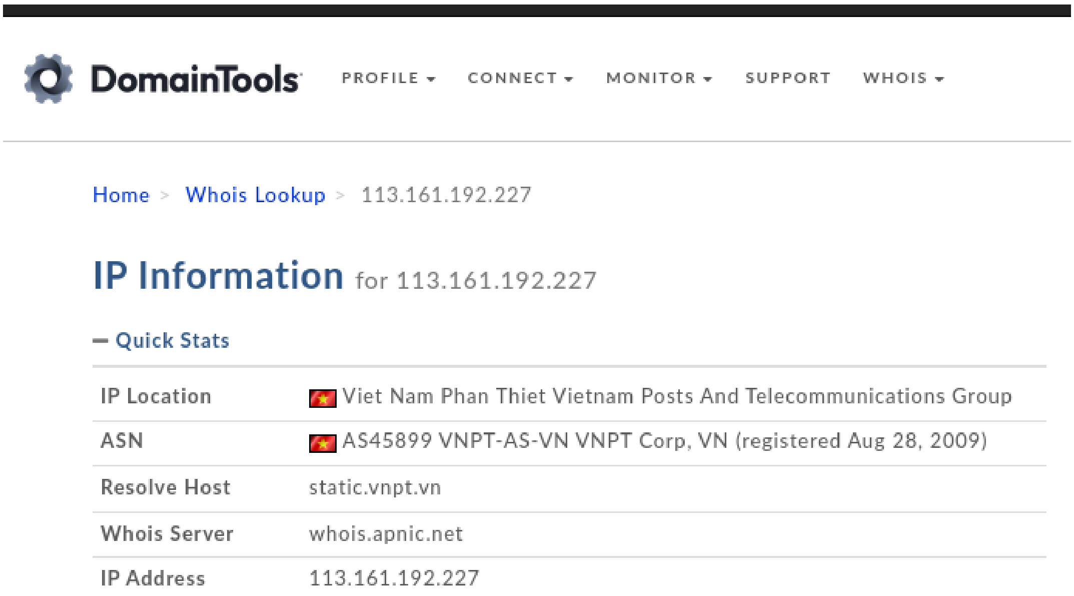


```
┌──(kali㉿kali)-[~/…/BTLO/Challenges/Bruteforce/Challenge_Files]
└─$ cat BTLO_Bruteforce_Challenge.txt | grep -E "[0-9]{3}.[0-9]{3}.[0-9]{3}.[0-9]{3}" | head -n 30
        Source Network Address: 113.161.192.227
        Source Network Address: 113.161.192.227
        Source Network Address: 113.161.192.227
        Source Network Address: 113.161.192.227
        Source Network Address: 113.161.192.227
        Source Network Address: 113.161.192.227
        Source Network Address: 113.161.192.227
        Source Network Address: 113.161.192.227
        Source Network Address: 113.161.192.227
        Source Network Address: 113.161.192.227
        Source Network Address: 113.161.192.227
        Source Network Address: 113.161.192.227
        Source Network Address: 113.161.192.227
        Source Network Address: 113.161.192.227
        Source Network Address: 113.161.192.227
        Source Network Address: 113.161.192.227
        Source Network Address: 113.161.192.227
        Source Network Address: 113.161.192.227
        Source Network Address: 113.161.192.227
        Source Network Address: 113.161.192.227
        Source Network Address: 113.161.192.227
        Source Network Address: 113.161.192.227
        Source Network Address: 113.161.192.227
        Source Network Address: 113.161.192.227
        Source Network Address: 113.161.192.227
        Source Network Address: 113.161.192.227
        Source Network Address: 113.161.192.227
        Source Network Address: 113.161.192.227
        Source Network Address: 113.161.192.227
        Source Network Address: 113.161.192.227
```

We can pattern match for an IP address using grep (as above). The above screenshot only shows the top 30 matches to save space, but the IP address is the only IP address returned, confirming it is the answer.

What country is this IP address associated with?

- Answer: Vietnam



Home > Whois Lookup > 113.161.192.227

IP Information for 113.161.192.227

− Quick Stats

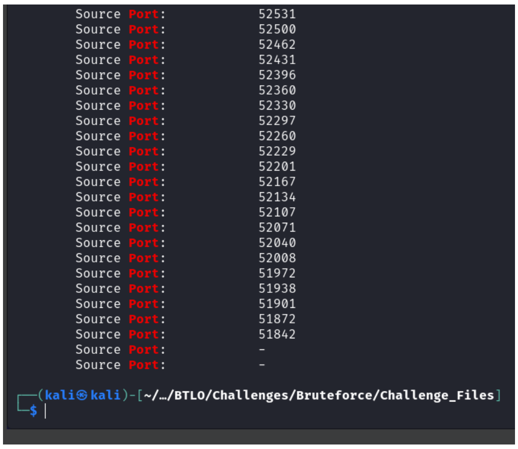
IP Location	Viet Nam Phan Thiet Vietnam Posts And Telecommunications Group
ASN	AS45899 VNPT-AS-VN VNPT Corp, VN (registered Aug 28, 2009)
Resolve Host	static.vnpt.vn
Whois Server	whois.apnic.net
IP Address	113.161.192.227

Reverse lookup of the discovered IP address on WhoIs Domain Tools shows it is associated with Vietnam.

What is the range of source ports that were used by the attacker to make these login requests?

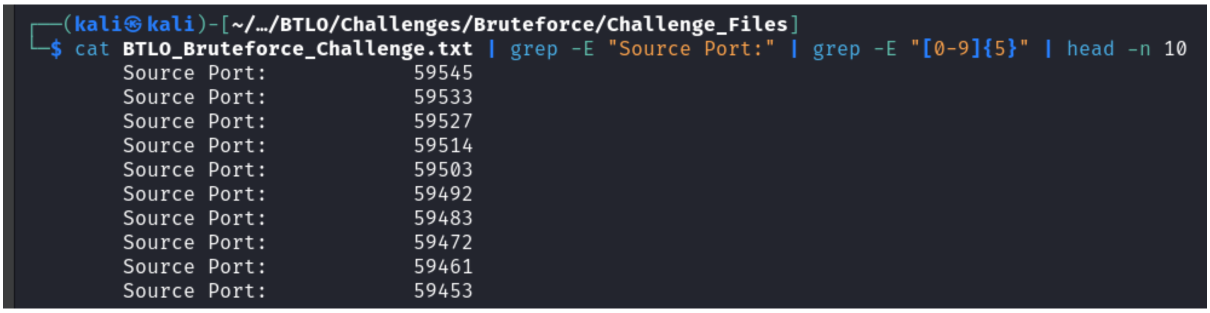
- Answer: 49162 – 65534

Trying a grep for “[Pp]ort” shows a wide range of numbers, none of which can be attributed to either the IP address or Vietnam.



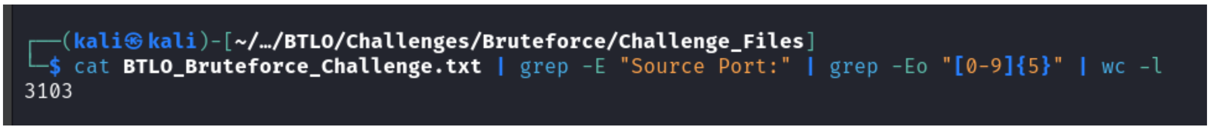
```
        Source Port:             52531
        Source Port:             52500
        Source Port:             52462
        Source Port:             52431
        Source Port:             52396
        Source Port:             52360
        Source Port:             52330
        Source Port:             52297
        Source Port:             52260
        Source Port:             52229
        Source Port:             52201
        Source Port:             52167
        Source Port:             52134
        Source Port:             52107
        Source Port:             52071
        Source Port:             52040
        Source Port:             52008
        Source Port:             51972
        Source Port:             51938
        Source Port:             51901
        Source Port:             51872
        Source Port:             51842
        Source Port:             -
        Source Port:             -

┌──(kali㉿kali)-[~/…/BTLO/Challenges/Bruteforce/Challenge_Files]
└─$ 
```

Doing a more restrictive grep for “Source Port:” and then piping the output into a grep to match port number shows the following (Again truncated so piped into head command to save space in this doc).



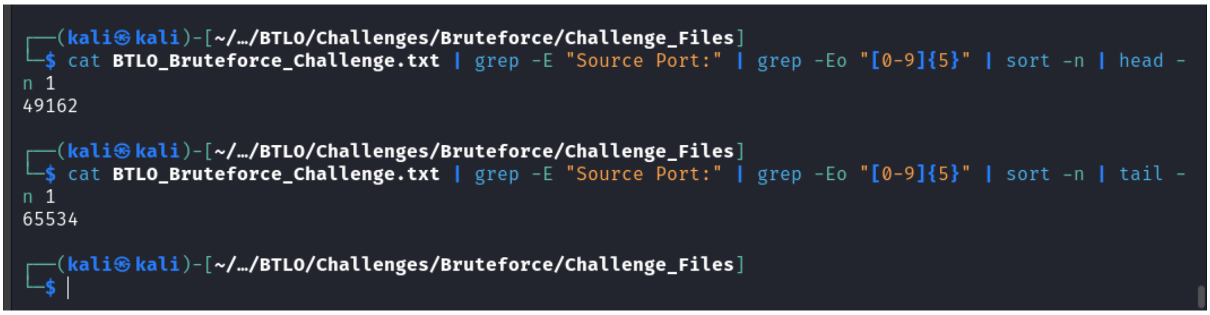
```
┌──(kali㉿kali)-[~/…/BTLO/Challenges/Bruteforce/Challenge_Files]
└─$ cat BTLO_Bruteforce_Challenge.txt | grep -E "Source Port:" | grep -E "[0-9]{5}" | head -n 10
        Source Port:            59545
        Source Port:            59533
        Source Port:            59527
        Source Port:            59514
        Source Port:            59503
        Source Port:            59492
        Source Port:            59483
        Source Port:            59472
        Source Port:            59461
        Source Port:            59453
```

Amending the grep to extract only port numbers, and performing a count shows that there are 3013 port numbers total.



```
┌──(kali㉿kali)-[~/…/BTLO/Challenges/Bruteforce/Challenge_Files]
└─$ cat BTLO_Bruteforce_Challenge.txt | grep -E "Source Port:" | grep -Eo "[0-9]{5}" | wc -l
3103
```

From here, doing some research/OSINT reveals the sort command which has a bunch of different option to sort data however you want. In this case we need the “-n” flag/option as we’re sorting numeric data.



```
┌──(kali㉿kali)-[~/…/BTLO/Challenges/Bruteforce/Challenge_Files]
└─$ cat BTLO_Bruteforce_Challenge.txt | grep -E "Source Port:" | grep -Eo "[0-9]{5}" | sort -n | head -
n 1
49162

┌──(kali㉿kali)-[~/…/BTLO/Challenges/Bruteforce/Challenge_Files]
└─$ cat BTLO_Bruteforce_Challenge.txt | grep -E "Source Port:" | grep -Eo "[0-9]{5}" | sort -n | tail -
n 1
65534

┌──(kali㉿kali)-[~/…/BTLO/Challenges/Bruteforce/Challenge_Files]
└─$ 
```

This will sort the output lowest to highest, which can then be finally piped into the head/tail commands to find the first & last values of the range: 49162 - 65534