

Bruteforce

Question 1) How many Audit Failure events are there?

```
cat BTLO_Bruteforce_Challenge.txt | grep -i "failure" | sort | uniq -c
```

```
3103 Failure Information:  
3103      Failure Reason: Unknown user name or bad password.
```

Question 2) What is the username of the local account that is being targeted?

```
cat BTLO_Bruteforce_Challenge.txt | less
```

```
Account For Which Logon Failed:  
    Security ID:          NULL SID  
    Account Name:         administrator  
    Account Domain:
```

Question 3) What is the failure reason related to the Audit Failure logs?

```
cat BTLO_Bruteforce_Challenge.txt | less
```

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

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

```
Audit Failure  2/12/2022 7:21:59 AM  Microsoft-Windows-Security-Auditing  
4625      Logon    "An account failed to log on.
```

Question 5) What is the source IP conducting this attack?

```
(kali㉿kali)-[~/Desktop/Bruteforce]  
└─$ cat BTLO_Bruteforce_Challenge.txt | grep "Source Network Address" | sort  
| uniq -c  
 4          Source Network Address: -  
3103       Source Network Address: 113.161.192.227
```

Question 6) What country is this IP address associated with?

Go sur ce site → <https://search.censys.io/>

Question 7) What is the range of source ports that were used by the attacker to make these login requests?

```
cat BTLO_Bruteforce_Challenge.txt | grep "Source Port" | sort | uniq -c
```