BTLO –Bruteforce|writeup

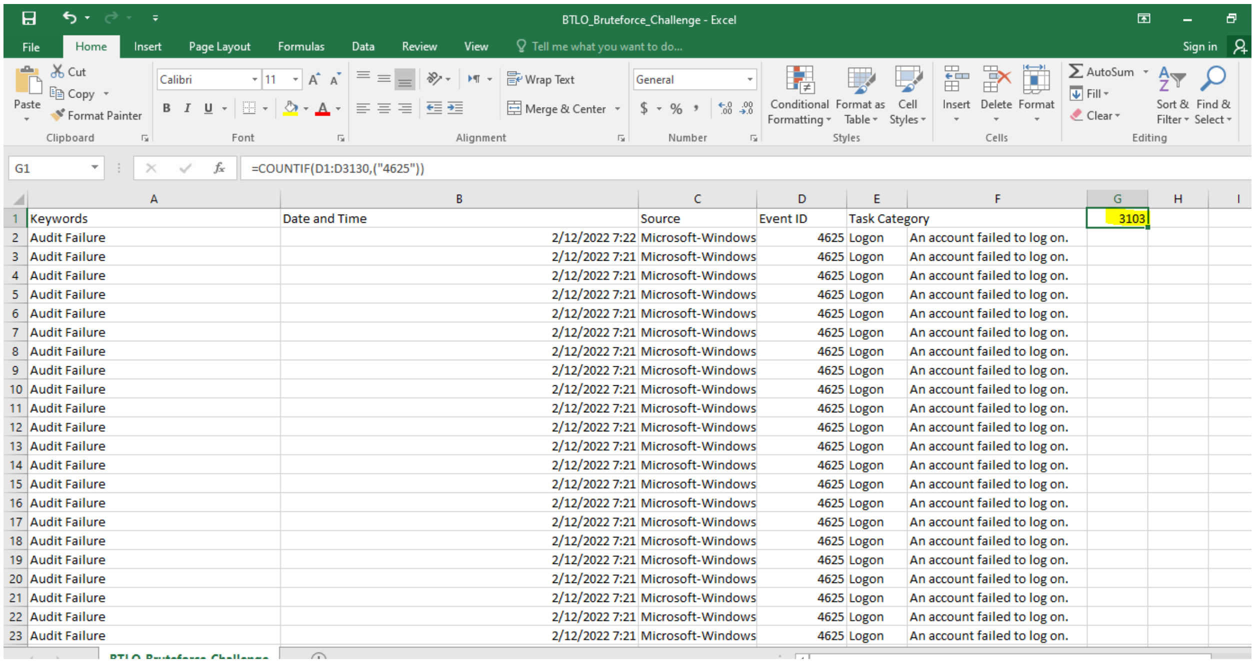
Scenario

Can you analyze 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!

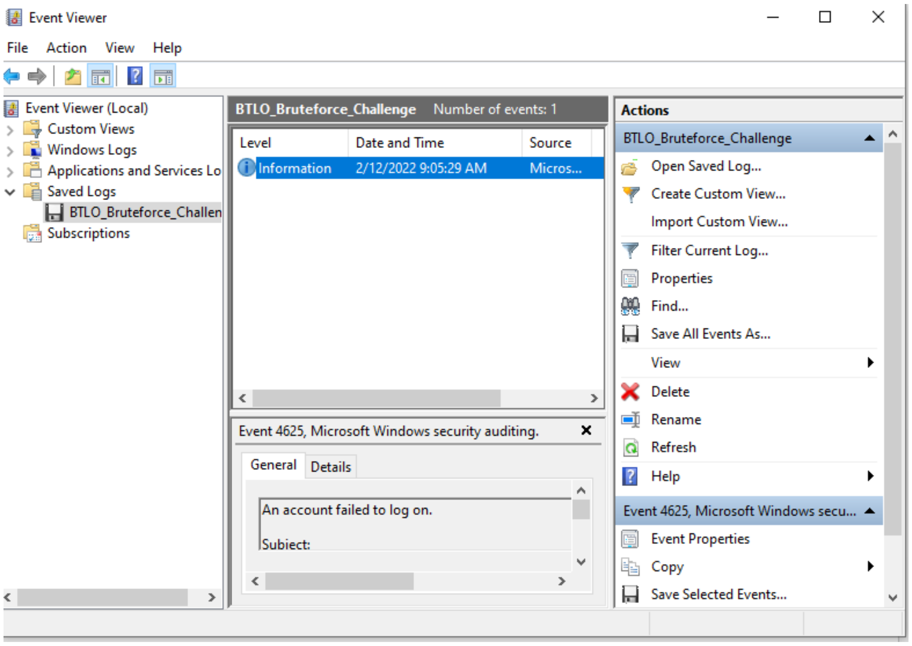
1) How many Audit Failure events are there? (Format: Count of Events)



G1 =COUNTIF(D1:D3130,("4625"))

	A	B	C	D	E	F	G
1	Keywords	Date and Time	Source	Event ID	Task Category		3103
2	Audit Failure	2/12/2022 7:22	Microsoft-Windows	4625	Logon	An account failed to log on.	
3	Audit Failure	2/12/2022 7:21	Microsoft-Windows	4625	Logon	An account failed to log on.	
4	Audit Failure	2/12/2022 7:21	Microsoft-Windows	4625	Logon	An account failed to log on.	
5	Audit Failure	2/12/2022 7:21	Microsoft-Windows	4625	Logon	An account failed to log on.	
6	Audit Failure	2/12/2022 7:21	Microsoft-Windows	4625	Logon	An account failed to log on.	
7	Audit Failure	2/12/2022 7:21	Microsoft-Windows	4625	Logon	An account failed to log on.	
8	Audit Failure	2/12/2022 7:21	Microsoft-Windows	4625	Logon	An account failed to log on.	
9	Audit Failure	2/12/2022 7:21	Microsoft-Windows	4625	Logon	An account failed to log on.	
10	Audit Failure	2/12/2022 7:21	Microsoft-Windows	4625	Logon	An account failed to log on.	
11	Audit Failure	2/12/2022 7:21	Microsoft-Windows	4625	Logon	An account failed to log on.	
12	Audit Failure	2/12/2022 7:21	Microsoft-Windows	4625	Logon	An account failed to log on.	
13	Audit Failure	2/12/2022 7:21	Microsoft-Windows	4625	Logon	An account failed to log on.	
14	Audit Failure	2/12/2022 7:21	Microsoft-Windows	4625	Logon	An account failed to log on.	
15	Audit Failure	2/12/2022 7:21	Microsoft-Windows	4625	Logon	An account failed to log on.	
16	Audit Failure	2/12/2022 7:21	Microsoft-Windows	4625	Logon	An account failed to log on.	
17	Audit Failure	2/12/2022 7:21	Microsoft-Windows	4625	Logon	An account failed to log on.	
18	Audit Failure	2/12/2022 7:21	Microsoft-Windows	4625	Logon	An account failed to log on.	
19	Audit Failure	2/12/2022 7:21	Microsoft-Windows	4625	Logon	An account failed to log on.	
20	Audit Failure	2/12/2022 7:21	Microsoft-Windows	4625	Logon	An account failed to log on.	
21	Audit Failure	2/12/2022 7:21	Microsoft-Windows	4625	Logon	An account failed to log on.	
22	Audit Failure	2/12/2022 7:21	Microsoft-Windows	4625	Logon	An account failed to log on.	
23	Audit Failure	2/12/2022 7:21	Microsoft-Windows	4625	Logon	An account failed to log on.	

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



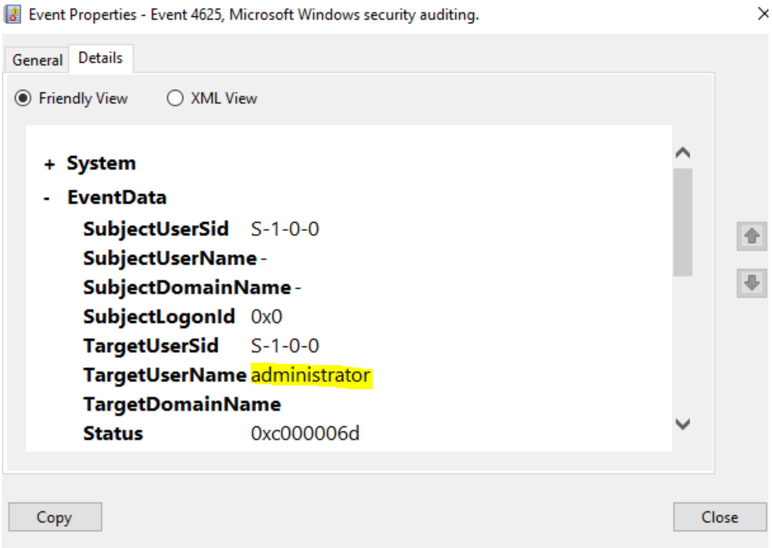
BTLO_Bruteforce_Challenge Number of events: 1

Level	Date and Time	Source
Information	2/12/2022 9:05:29 AM	Micros...

Event 4625, Microsoft Windows security auditing.

An account failed to log on.

Subject:


Event Properties - Event 4625, Microsoft Windows security auditing.
General
Details
Copy
Close

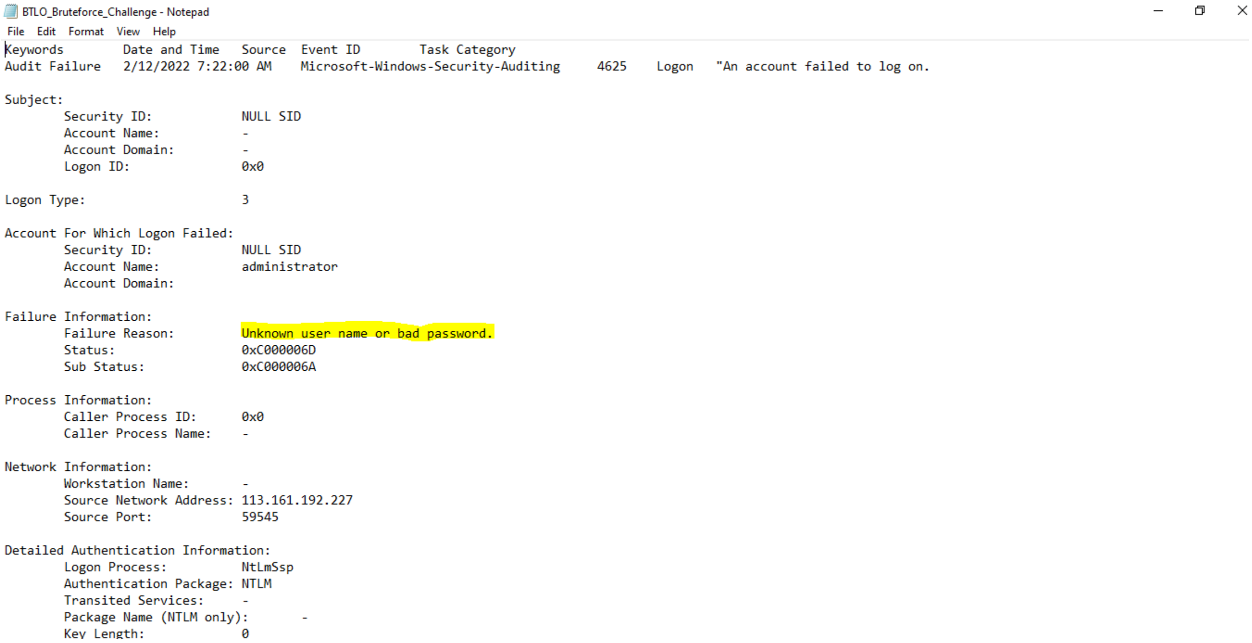
● Friendly View ○ XML View

+ System

- EventData

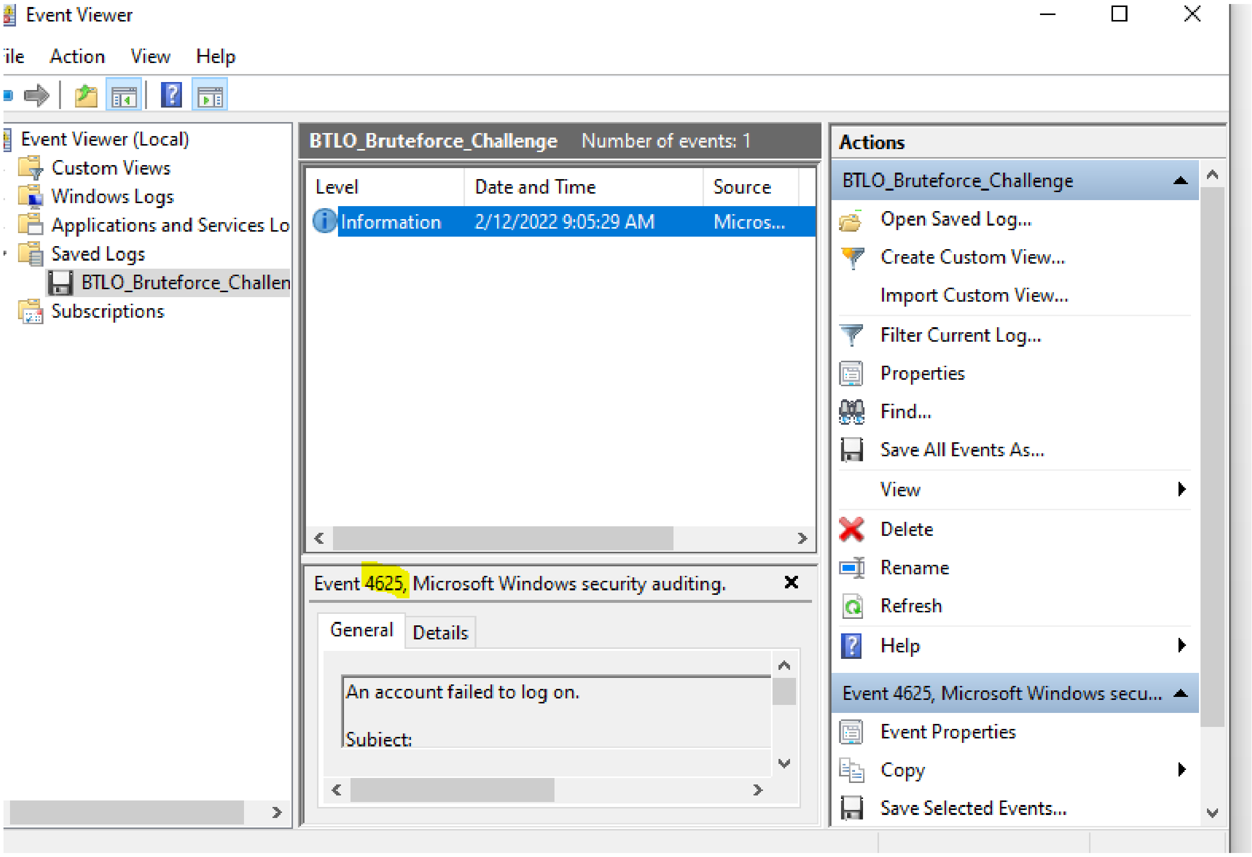
SubjectUserSid	S-1-0-0
SubjectUserName	-
SubjectDomainName	-
SubjectLogonId	0x0
TargetUserSid	S-1-0-0
TargetUserName	administrator
TargetDomainName	
Status	0xc000006d

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


BTLO_Bruteforce_Challenge - Notepad
File Edit Format View Help

```
Keywords        Date and Time   Source  Event ID        Task Category
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
        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
        Source Port:            59545

Detailed Authentication Information:
        Logon Process:          NtLmSsp
        Authentication Package: NTLM
        Transited Services:     -
        Package Name (NTLM only):       -
        Key Length:             0
```

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



BTLO_Bruteforce_Challenge Number of events: 1

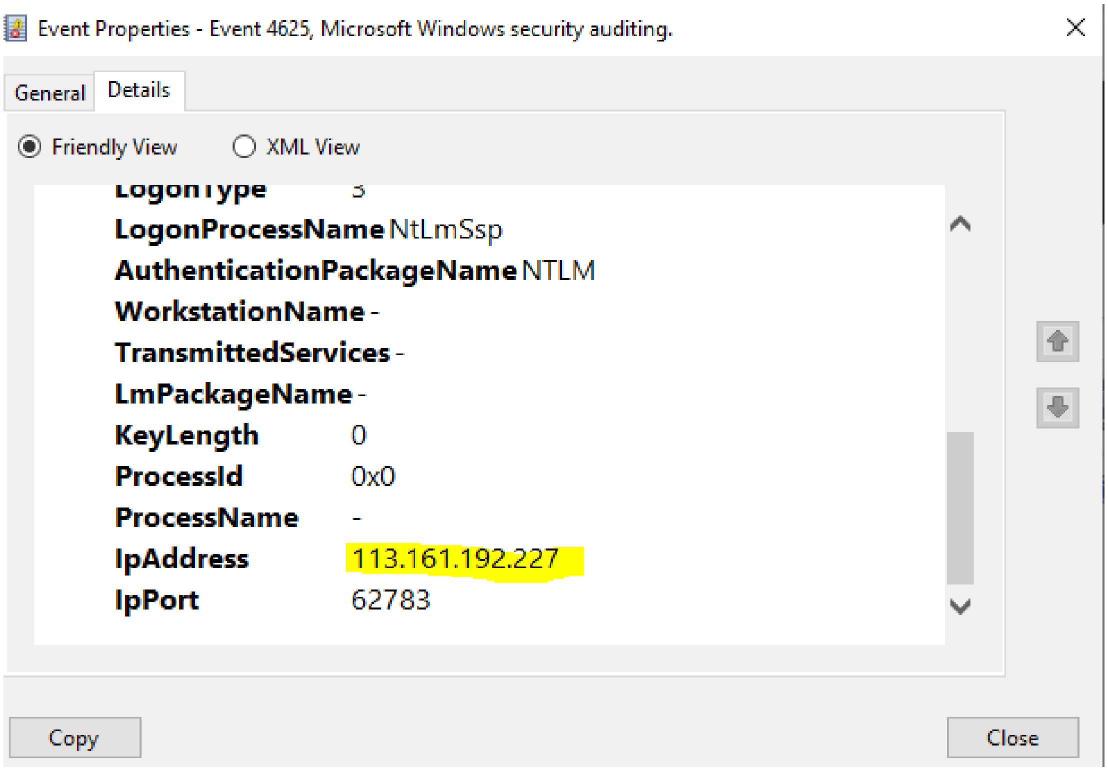
Level	Date and Time	Source
Information	2/12/2022 9:05:29 AM	Micros...

Event 4625, Microsoft Windows security auditing.

An account failed to log on.

Subject:

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

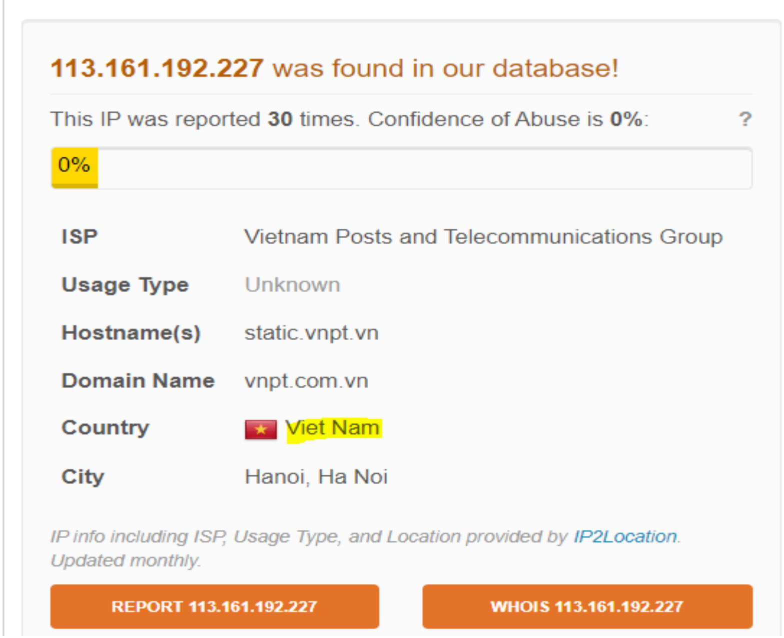


Event Properties - Event 4625, Microsoft Windows security auditing.

● Friendly View ○ XML View

LogonType	3
LogonProcessName	NtLmSsp
AuthenticationPackageName	NTLM
WorkstationName	-
TransmittedServices	-
LmPackageName	-
KeyLength	0
ProcessId	0x0
ProcessName	-
IpAddress	113.161.192.227
IpPort	62783

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



113.161.192.227 was found in our database!

This IP was reported **30** times. Confidence of Abuse is **0%**: ?

0%

ISP	Vietnam Posts and Telecommunications Group
Usage Type	Unknown
Hostname(s)	static.vnpt.vn
Domain Name	vnpt.com.vn
Country	Viet Nam
City	Hanoi, Ha Noi

IP info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly.

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

49162–65534