LetsDefend

Official Incident Report

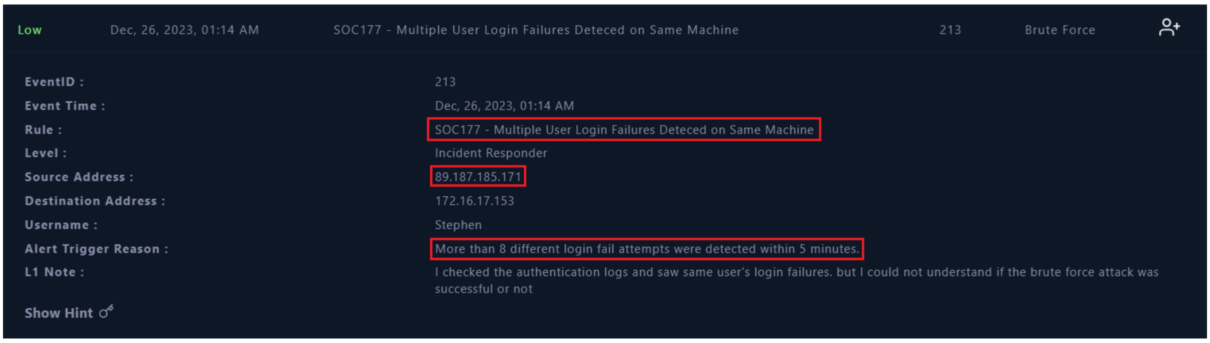
Event ID: 213

Rule Name: SOC177 - Multiple User Login Failures Detected on Same Machine

Table of contents

Alert

The alert was triggered due to more than eight different login fail attempts being detected within five minutes. It is observed in the alert details that the login attempts came from 89[.]187.185.171. It is seen in the alert that the attack was towards the same system. It is stated in the L1 analyst's notes that they saw the logs of the attack, but could not determine whether the attack was successful or not.



Low Dec, 26, 2023, 01:14 AM SOC177 - Multiple User Login Failures Deteced on Same Machine 213 Brute Force

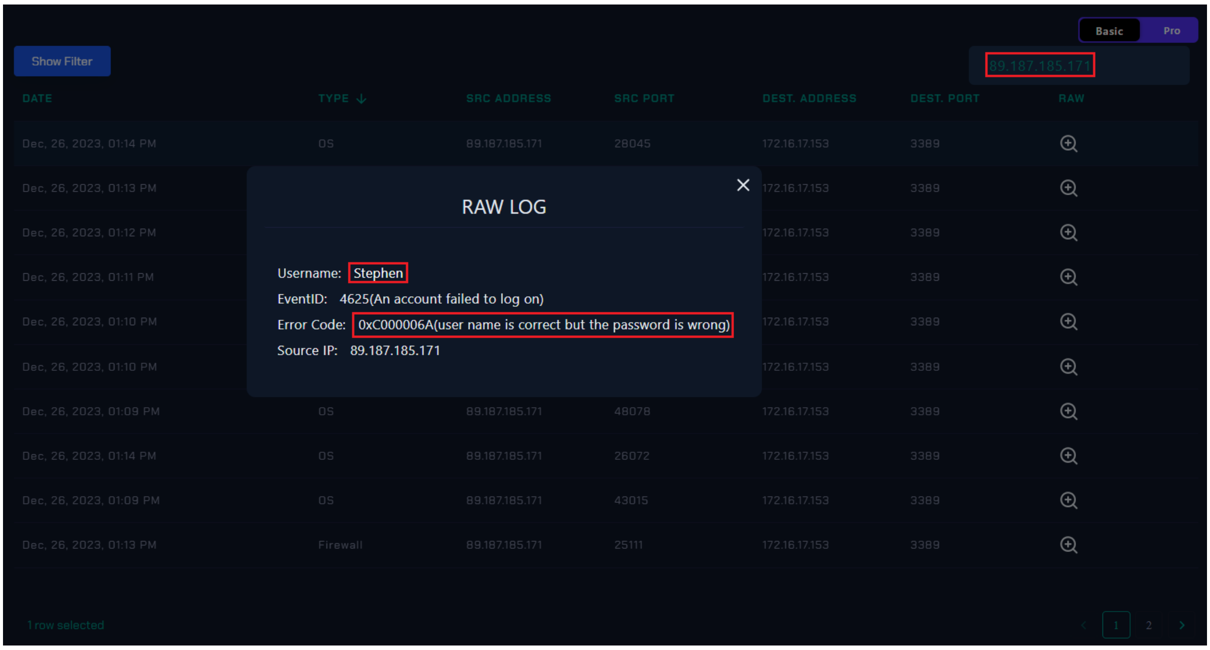
EventID :	213
Event Time :	Dec, 26, 2023, 01:14 AM
Rule :	SOC177 - Multiple User Login Failures Deteced on Same Machine
Level :	Incident Responder
Source Address :	89.187.185.171
Destination Address :	172.16.17.153
Username :	Stephen
Alert Trigger Reason :	More than 8 different login fail attempts were detected within 5 minutes.
L1 Note :	I checked the authentication logs and saw same user's login failures. but I could not understand if the brute force attack was successful or not

First, the alert should be verified by checking the available logs, and then it should be determined whether the attack was successful or not.

Detection

Verify

In Log Management, search for the source IP address (89[.]187.185.171) in the alert and examine the logs among the results. This way, all logs belonging to the attacker were checked.



89.187.185.171

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Dec, 26, 2023, 01:14 PM	OS	89.187.185.171	28045	172.16.17.153	3389	🔍
Dec, 26, 2023, 01:13 PM				172.16.17.153	3389	🔍
Dec, 26, 2023, 01:12 PM				172.16.17.153	3389	🔍
Dec, 26, 2023, 01:11 PM				172.16.17.153	3389	🔍
Dec, 26, 2023, 01:10 PM				172.16.17.153	3389	🔍
Dec, 26, 2023, 01:10 PM				172.16.17.153	3389	🔍
Dec, 26, 2023, 01:09 PM	OS	89.187.185.171	48078	172.16.17.153	3389	🔍
Dec, 26, 2023, 01:14 PM	OS	89.187.185.171	26072	172.16.17.153	3389	🔍
Dec, 26, 2023, 01:09 PM	OS	89.187.185.171	43015	172.16.17.153	3389	🔍
Dec, 26, 2023, 01:13 PM	Firewall	89.187.185.171	25111	172.16.17.153	3389	🔍

1 row selected

RAW LOG

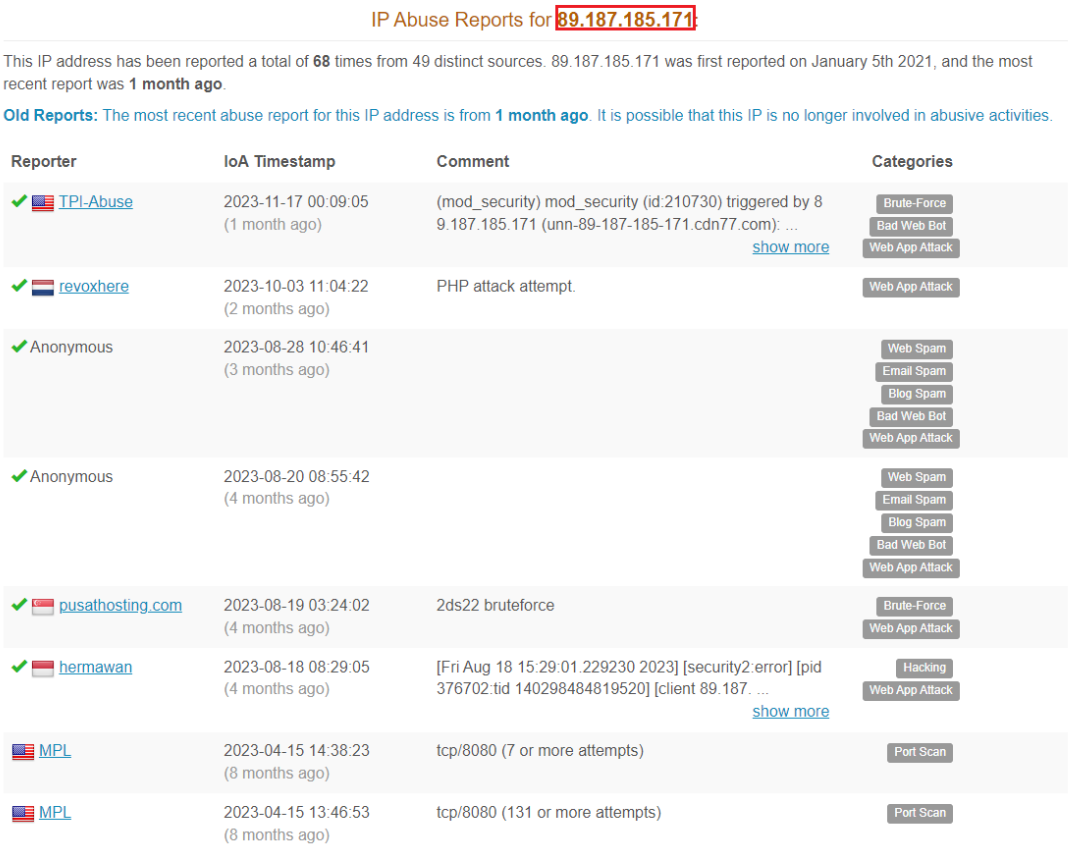
Username: Stephen
EventID: 4625(An account failed to log on)
Error Code: 0xC000006A(user name is correct but the password is wrong)
Source IP: 89.187.185.171

OS logs show more than eight attempts within five minutes. In the detail of the OS logs, it was seen that all attempts belonging to the user “Stephen” failed. Thus, the alert is confirmed and can be called True Positive.

Analysis

IP Reputation

The attacker IP address belongs to 89[.]187.185.171 hosting company located in the USA. The reputation records of the IP according to AbuseIPDB and Virus Total are as follows. It is reported as web attack, brute force, and malicious in different sources.



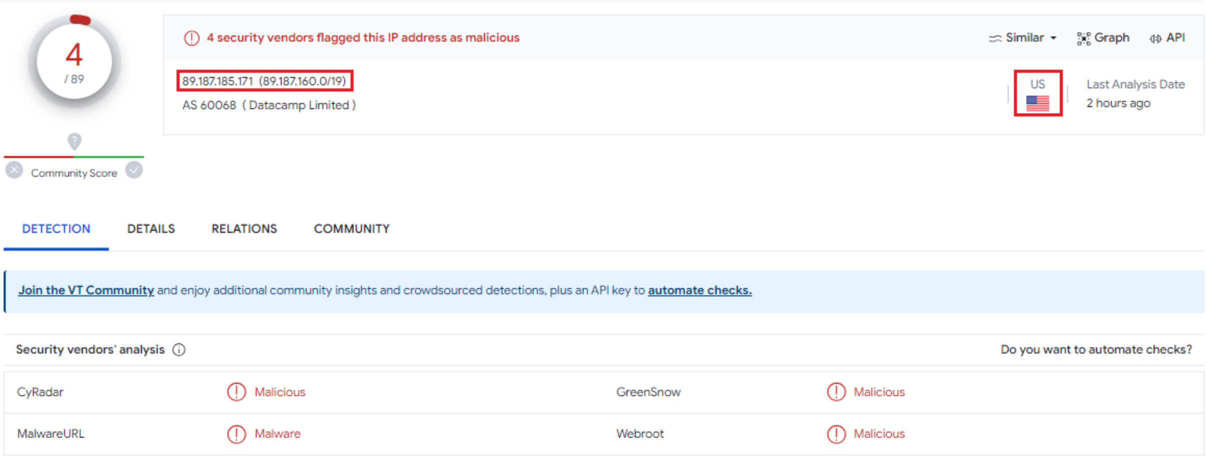
IP Abuse Reports for 89.187.185.171:

This IP address has been reported a total of **68** times from 49 distinct sources. 89.187.185.171 was first reported on January 5th 2021, and the most recent report was **1 month ago**.

Old Reports: The most recent abuse report for this IP address is from **1 month ago**. It is possible that this IP is no longer involved in abusive activities.

Reporter	IoA Timestamp	Comment	Categories
✓ TPI-Abuse	2023-11-17 00:09:05 (1 month ago)	(mod_security) mod_security (id:210730) triggered by 89.187.185.171 (unn-89-187-185-171.cdn77.com): ... show more	Brute-Force Bad Web Bot Web App Attack
✓ revoxhere	2023-10-03 11:04:22 (2 months ago)	PHP attack attempt.	Web App Attack
✓ Anonymous	2023-08-28 10:46:41 (3 months ago)		Web Spam Email Spam Blog Spam Bad Web Bot Web App Attack
✓ Anonymous	2023-08-20 08:55:42 (4 months ago)		Web Spam Email Spam Blog Spam Bad Web Bot Web App Attack
✓ pusathosting.com	2023-08-19 03:24:02 (4 months ago)	2ds22 bruteforce	Brute-Force Web App Attack
✓ hermawan	2023-08-18 08:29:05 (4 months ago)	[Fri Aug 18 15:29:01.229230 2023] [security2:error] [pid 376702:tid 140298484819520] [client 89.187. ... show more	Hacking Web App Attack
MPL	2023-04-15 14:38:23 (8 months ago)	tcp/8080 (7 or more attempts)	Port Scan
MPL	2023-04-15 13:46:53 (8 months ago)	tcp/8080 (131 or more attempts)	Port Scan

hxxps://www.abuseipdb.com/check/89.187.185.171



4 security vendors flagged this IP address as malicious

89.187.185.171 (89.187.160.0/19)

AS 60068 (Datacamp Limited)

US

Last Analysis Date
2 hours ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

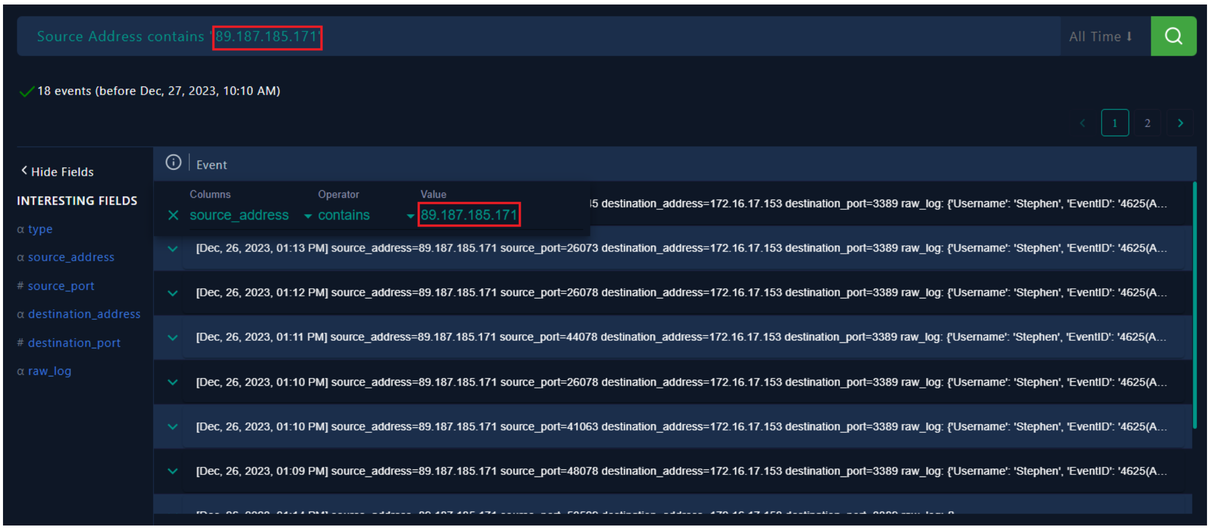
Do you want to automate checks?

CyRadar	Malicious	GreenSnow	Malicious
MalwareURL	Malware	Webroot	Malicious

hxxps://www.virustotal.com/gui/ip-address/89.187.185.171

Initial Access

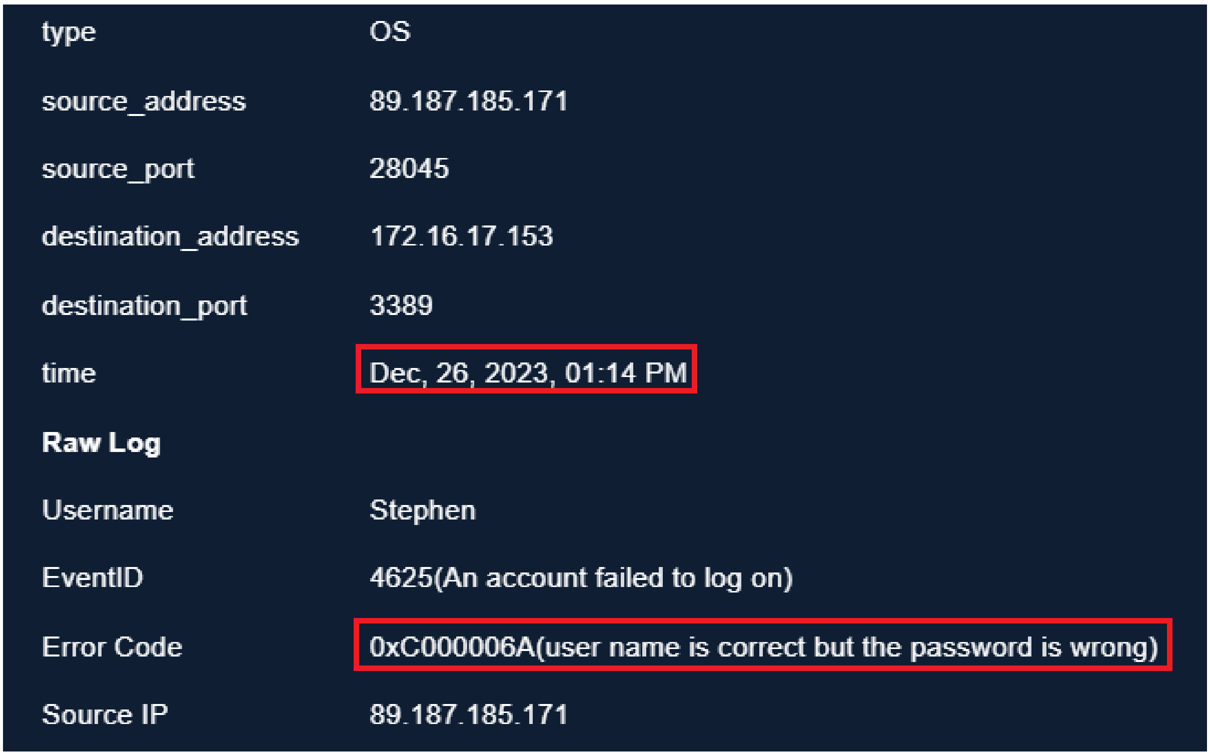
It was detected that nine requests were made towards the RDP port of 172[.]16.17.153 address as of March 26, 01:08 PM. It seems that the attacker targeted only one address, however, the scope of the analysis should be expanded if there are different destination addresses.



18 events (before Dec, 27, 2023, 10:10 AM)

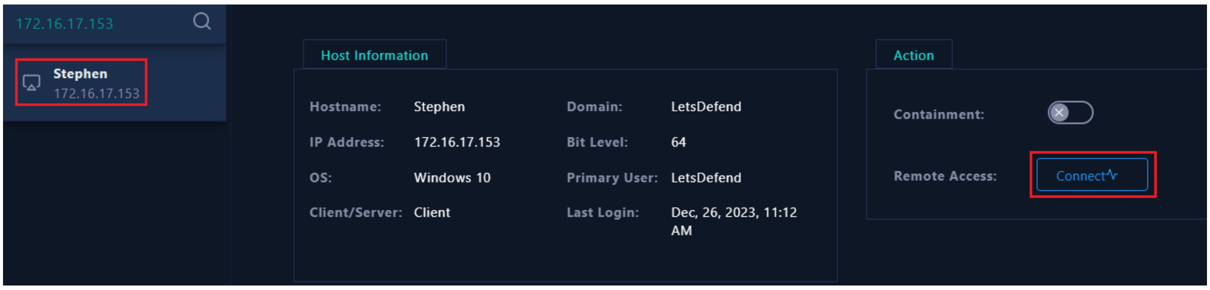
```
5 destination_address=172.16.17.153 destination_port=3389 raw_log: {'Username': 'Stephen', 'EventID': '4625(A...
[Dec, 26, 2023, 01:13 PM] source_address=89.187.185.171 source_port=26073 destination_address=172.16.17.153 destination_port=3389 raw_log: {'Username': 'Stephen', 'EventID': '4625(A...
[Dec, 26, 2023, 01:12 PM] source_address=89.187.185.171 source_port=26078 destination_address=172.16.17.153 destination_port=3389 raw_log: {'Username': 'Stephen', 'EventID': '4625(A...
[Dec, 26, 2023, 01:11 PM] source_address=89.187.185.171 source_port=44078 destination_address=172.16.17.153 destination_port=3389 raw_log: {'Username': 'Stephen', 'EventID': '4625(A...
[Dec, 26, 2023, 01:10 PM] source_address=89.187.185.171 source_port=26078 destination_address=172.16.17.153 destination_port=3389 raw_log: {'Username': 'Stephen', 'EventID': '4625(A...
[Dec, 26, 2023, 01:10 PM] source_address=89.187.185.171 source_port=41063 destination_address=172.16.17.153 destination_port=3389 raw_log: {'Username': 'Stephen', 'EventID': '4625(A...
[Dec, 26, 2023, 01:09 PM] source_address=89.187.185.171 source_port=48078 destination_address=172.16.17.153 destination_port=3389 raw_log: {'Username': 'Stephen', 'EventID': '4625(A...
```

Although all requests seem to have failed as shown in the log details, you should connect to the system and check whether there is a success log in order to confirm.



type	OS
source_address	89.187.185.171
source_port	28045
destination_address	172.16.17.153
destination_port	3389
time	Dec, 26, 2023, 01:14 PM
Raw Log	
Username	Stephen
EventID	4625(An account failed to log on)
Error Code	0xC000006A(user name is correct but the password is wrong)
Source IP	89.187.185.171

Click on the "connect" button on Endpoint Security to connect to the system as below.



172.16.17.153

Stephen
172.16.17.153

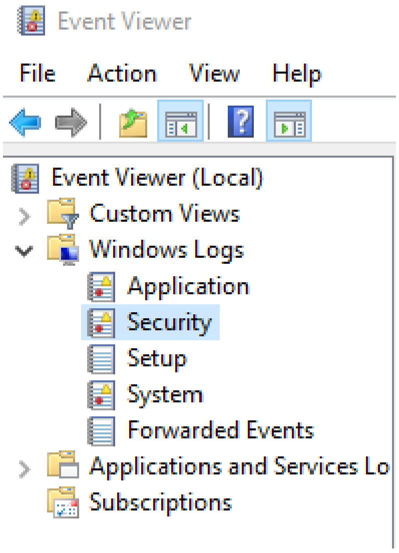
Host Information

Hostname: Stephen
IP Address: 172.16.17.153
OS: Windows 10
Client/Server: Client
Domain: LetsDefend
Bit Level: 64
Primary User: LetsDefend
Last Login: Dec, 26, 2023, 11:12 AM

Action

Containment:
Remote Access: Connect

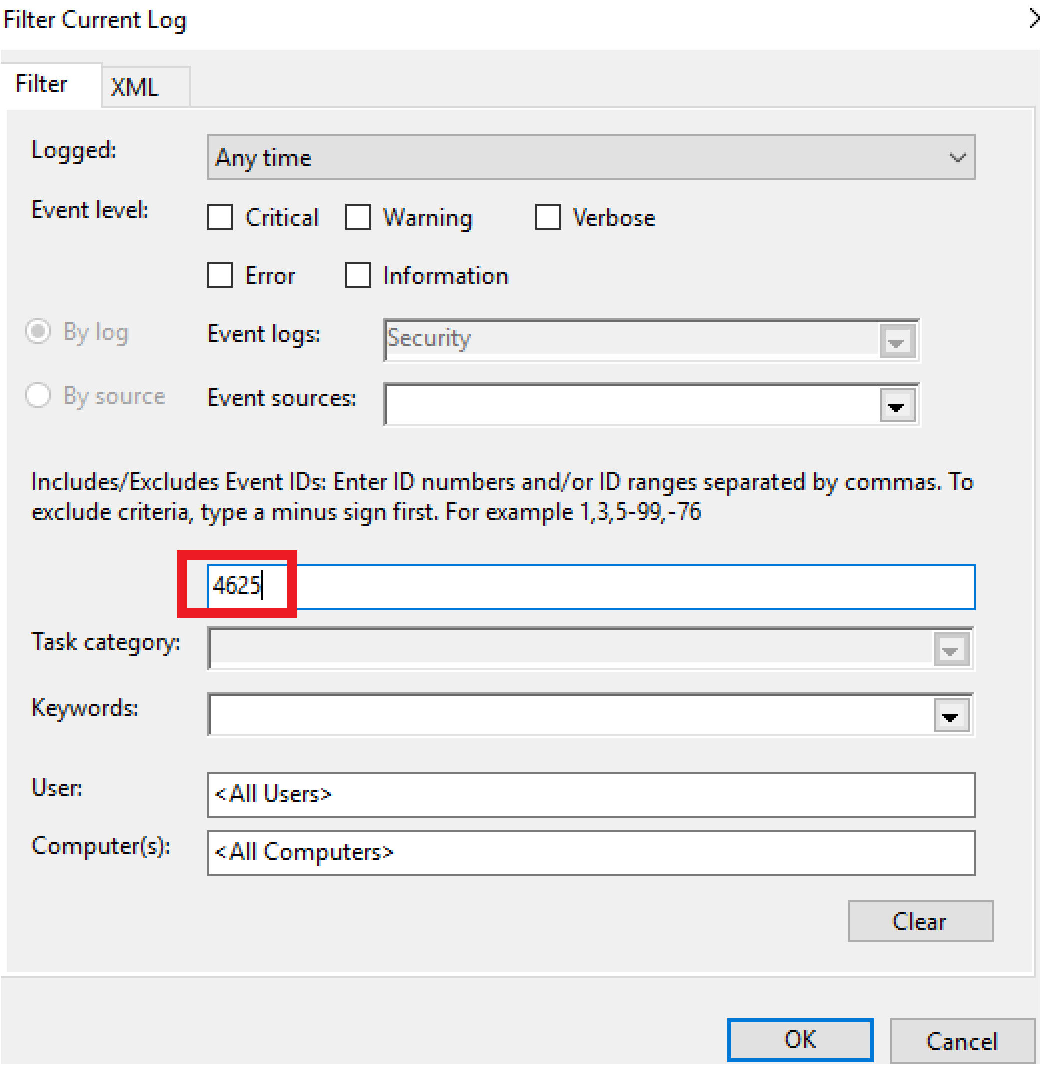
After connecting to the device, select “Security” logs on Event Viewer.



You should pay attention mainly to Event ID 4624 and 4625.

- Event ID 4624: An account was successfully logged on
- Event ID 4625: An account failed to log on

You should check if there is a successful authentication log (Event ID 4624) after the failed logs (Event ID 4625) from the same source address to see if the brute force attack was successful.



Filter Current Log

Logged: Any time

Event level: □ Critical □ Warning □ Verbose □ Error □ Information

● By log Event logs: Security

○ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

4625

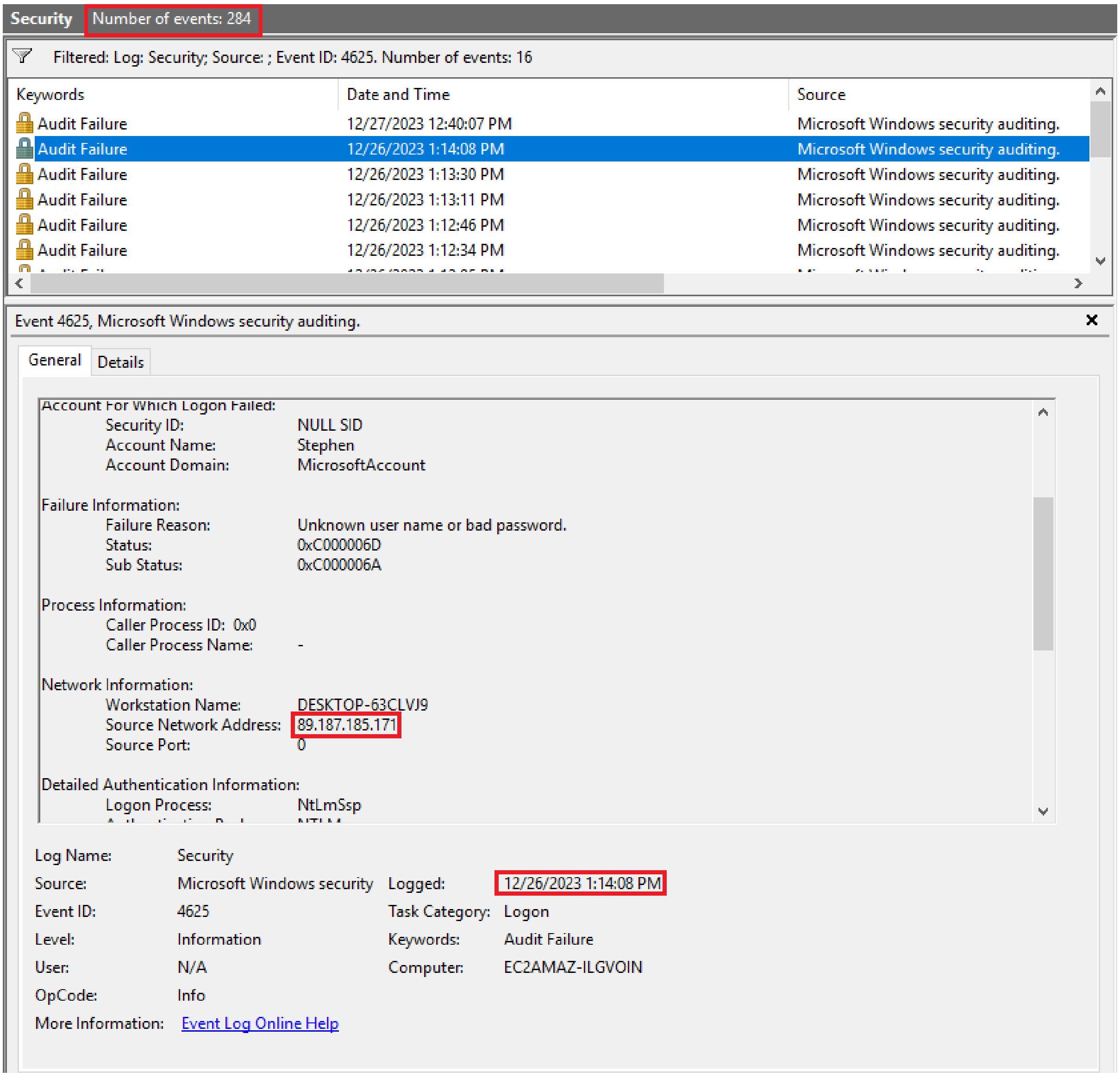
Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

All login failure logs on the system are as follows.



Security Number of events: 284

Filtered: Log: Security; Source: ; Event ID: 4625. Number of events: 16

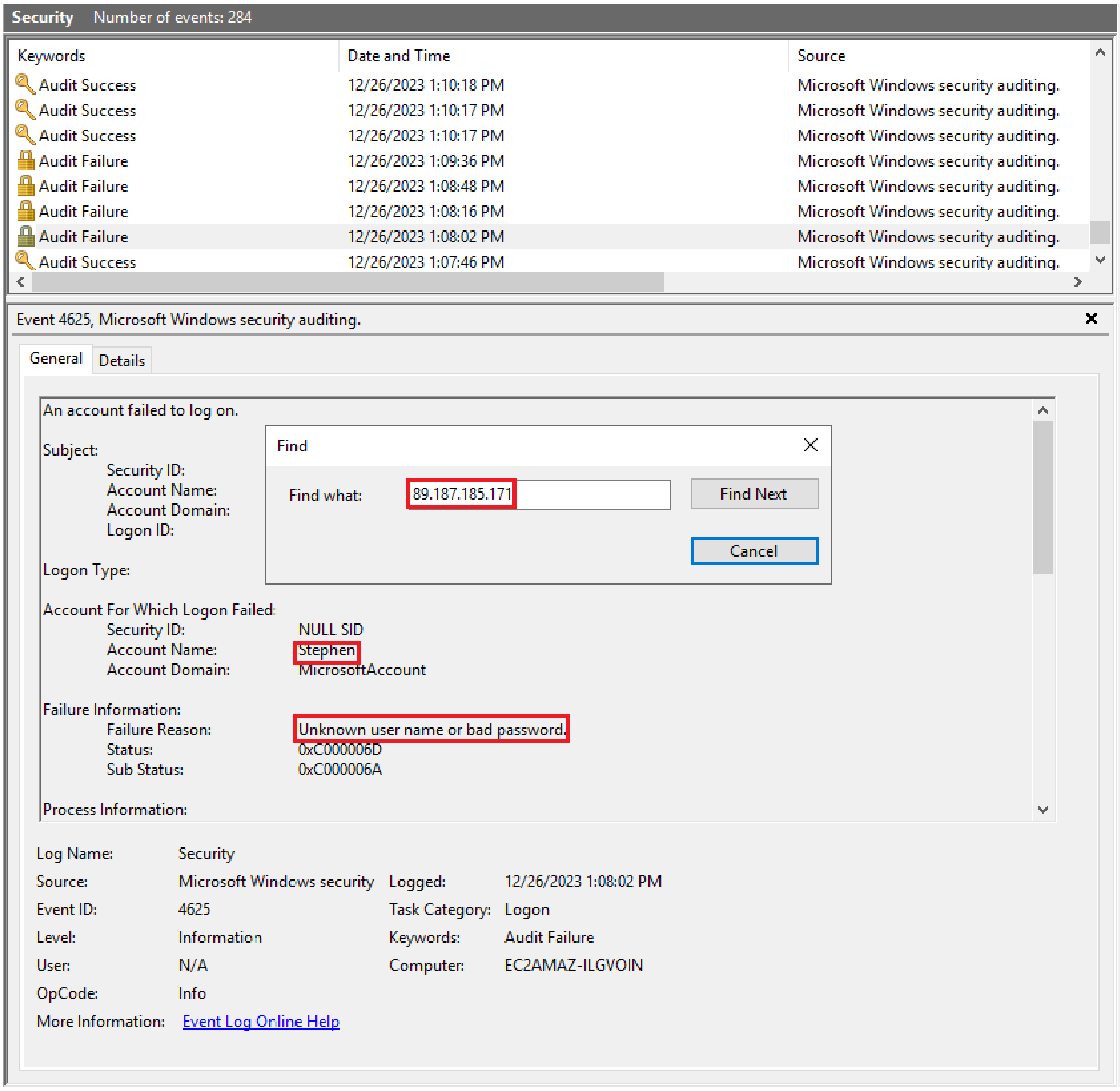
Keywords	Date and Time	Source
Audit Failure	12/27/2023 12:40:07 PM	Microsoft Windows security auditing.
Audit Failure	12/26/2023 1:14:08 PM	Microsoft Windows security auditing.
Audit Failure	12/26/2023 1:13:30 PM	Microsoft Windows security auditing.
Audit Failure	12/26/2023 1:13:11 PM	Microsoft Windows security auditing.
Audit Failure	12/26/2023 1:12:46 PM	Microsoft Windows security auditing.
Audit Failure	12/26/2023 1:12:34 PM	Microsoft Windows security auditing.

Event 4625, Microsoft Windows security auditing.

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

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:         DESKTOP-63CLVJ9
          Source Network Address:   89.187.185.171
          Source Port:              0

Detailed Authentication Information:
          Logon Process:            NtLmSsp
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	12/26/2023 1:14:08 PM
Event ID:	4625	Task Category:	Logon
Level:	Information	Keywords:	Audit Failure
User:	N/A	Computer:	EC2AMAZ-ILGVOIN
OpCode:	Info		
More Information:	Event Log Online Help		

Regardless of the EventID, when all logs belonging to the attacker IP are checked, it is seen that all attempts failed. There is no successful login for the IP 89[.]187.185.171 on the system. It is understood from this that the Brute Force attempt failed. In addition, it can be said that the "External Remote Services" technique was used for initial access since access attempts to the system were made via remote access such as RDP. This method is frequently used by attackers.



Security Number of events: 284

Keywords	Date and Time	Source
Audit Success	12/26/2023 1:10:18 PM	Microsoft Windows security auditing.
Audit Success	12/26/2023 1:10:17 PM	Microsoft Windows security auditing.
Audit Success	12/26/2023 1:10:17 PM	Microsoft Windows security auditing.
Audit Failure	12/26/2023 1:09:36 PM	Microsoft Windows security auditing.
Audit Failure	12/26/2023 1:08:48 PM	Microsoft Windows security auditing.
Audit Failure	12/26/2023 1:08:16 PM	Microsoft Windows security auditing.
Audit Failure	12/26/2023 1:08:02 PM	Microsoft Windows security auditing.
Audit Success	12/26/2023 1:07:46 PM	Microsoft Windows security auditing.

Event 4625, Microsoft Windows security auditing.

```
An account failed to log on.

Subject:
        Security ID:
        Account Name:
        Account Domain:
        Logon ID:

Logon Type:

Account For Which Logon Failed:
        Security ID:            NULL SID
        Account Name:           Stephen
        Account Domain:         MicrosoftAccount

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

Process Information:
```

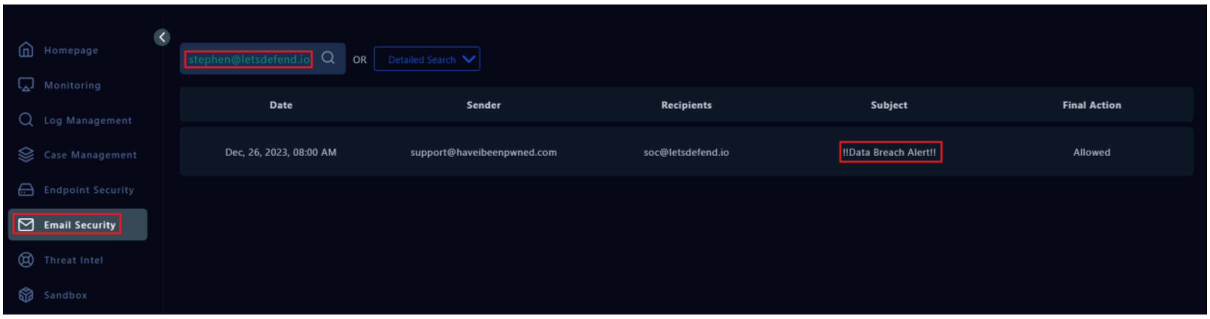
Find

Find what: 89.187.185.171

```
Log Name:         Security
Source:           Microsoft Windows security   Logged:         12/26/2023 1:08:02 PM
Event ID:         4625                         Task Category:  Logon
Level:            Information                  Keywords:       Audit Failure
User:             N/A                          Computer:       EC2AMAZ-ILGVOIN
OpCode:           Info
More Information: Event Log Online Help
```

Another thing to note here is how the attacker only tried the user "Stephen" on the target system. If they tried different users on the system and then discovered Stephen, this could be called a dictionary attack. However, this situation looks like a targeted attack. The reason for this may be that the user's credentials were leaked. Therefore, you should also examine the user's mail traffic. It should be checked for both internal phishing and external phishing. If there is such a situation, the attacker may have accessed the credential information.

As a result of a search on Email Security, it was seen that the e-mail address “stephen[@]letsdefend[.]io” was included in the e-mail with the subject “!!! Data Breach Alert!!!”.

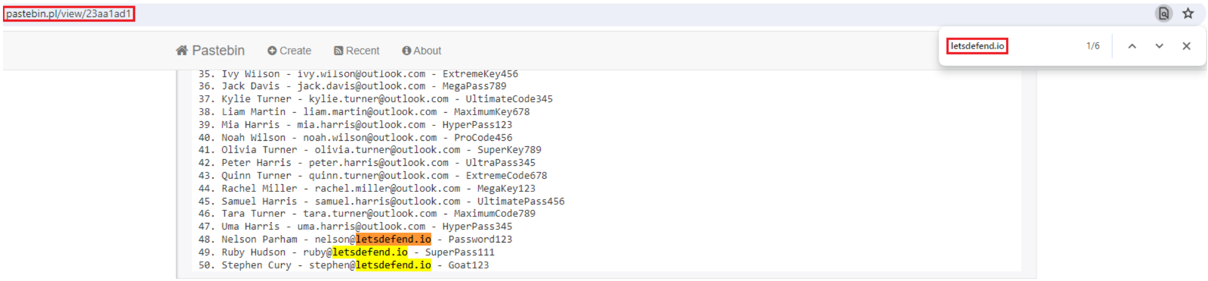


stephen@letsdefend.io

Date	Sender	Recipients	Subject	Final Action
Dec, 26, 2023, 08:00 AM	support@haveibeenpwned.com	soc@letsdefend.io	!!Data Breach Alert!!	Allowed

In the details of the mail, there is information that the credential information of users named Stephen, Nelson, and Ruby are part of the leaked data. The link with the details of the leak was shared in the relevant mail. In addition, the sender is “support[@]haveibeenpwned[.]com” and belongs to haveibeenpwned. The main purpose of HIBP is to help users check the security of their personal information. If an email address or password was exposed in a previous data leak, HIBP provides users with this information and tells them which leak it belongs to.

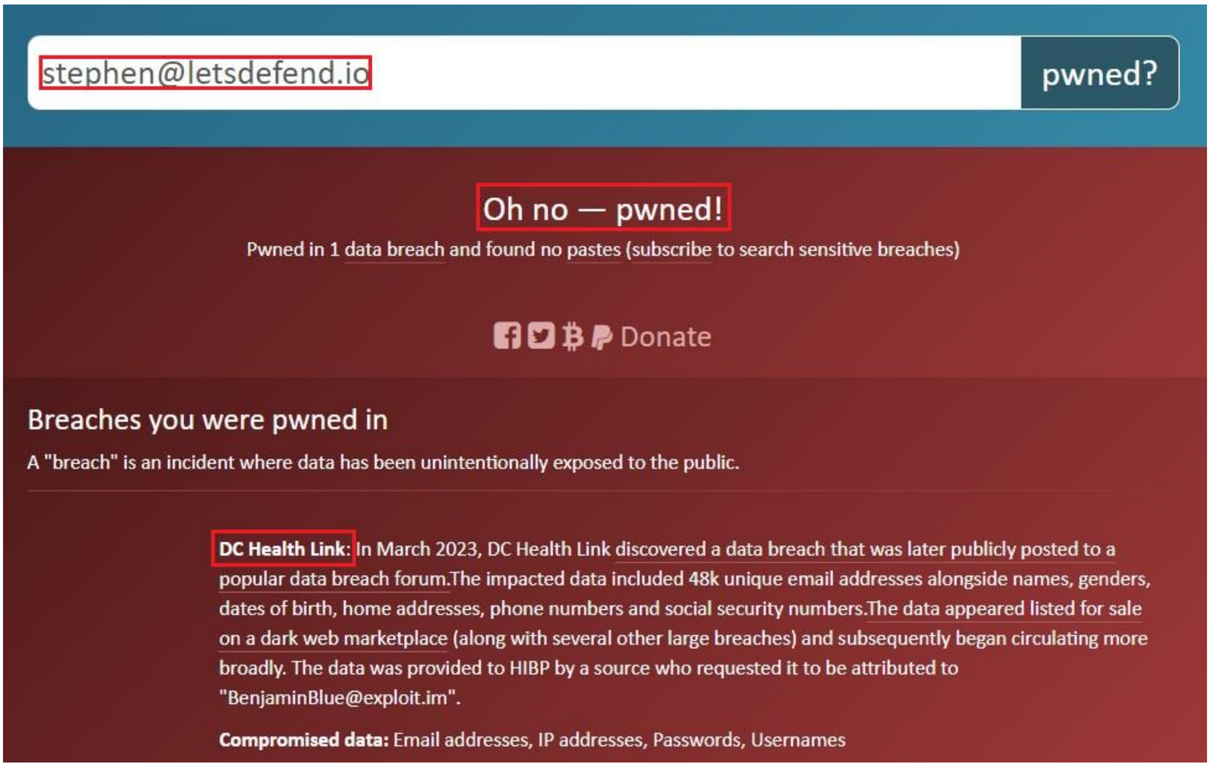
You can check the users who have been leaked with the link in the email. As can be seen below, the information of three users belonging to the domain “Letsdefend.io” is included as cleartext. This information can also be checked via havebeenpwned.



pastebin.pl/view/23aa1ad1

letsdefend.io

```
35. Ivy Wilson - ivy.wilson@outlook.com - ExtremeKey456
36. Jack Davis - jack.davis@outlook.com - MegaPass789
37. Kylie Turner - kylie.turner@outlook.com - UltimateCode345
38. Liam Martin - liam.martin@outlook.com - MaximumKey678
39. Mia Harris - mia.harris@outlook.com - HyperPass123
40. Noah Wilson - noah.wilson@outlook.com - ProCode456
41. Olivia Turner - olivia.turner@outlook.com - SuperKey789
42. Peter Harris - peter.harris@outlook.com - UltraPass345
43. Quinn Turner - quinn.turner@outlook.com - ExtremeCode678
44. Rachel Miller - rachel.miller@outlook.com - MegaKey123
45. Samuel Harris - samuel.harris@outlook.com - UltimatePass456
46. Tara Turner - tara.turner@outlook.com - MaximumCode789
47. Uma Harris - uma.harris@outlook.com - HyperPass345
48. Nelson Parham - nelson@letsdefend.io - Password123
49. Ruby Hudson - ruby@letsdefend.io - SuperPass111
50. Stephen Cury - stephen@letsdefend.io - Goat123
```



stephen@letsdefend.io

Oh no — pwned!

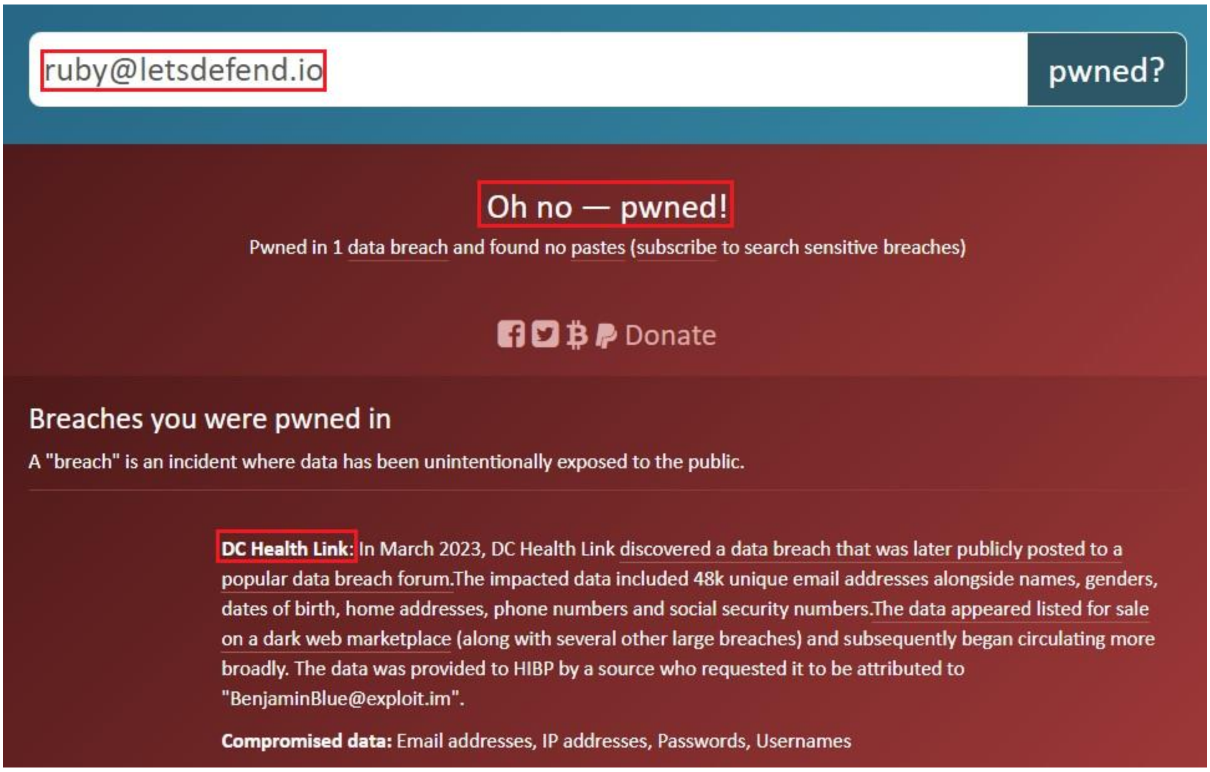
Pwned in 1 data breach and found no pastes (subscribe to search sensitive breaches)

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public.

DC Health Link: In March 2023, DC Health Link discovered a data breach that was later publicly posted to a popular data breach forum.The impacted data included 48k unique email addresses alongside names, genders, dates of birth, home addresses, phone numbers and social security numbers.The data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it to be attributed to "BenjaminBlue@exploit.im".

Compromised data: Email addresses, IP addresses, Passwords, Usernames



ruby@letsdefend.io

Oh no — pwned!

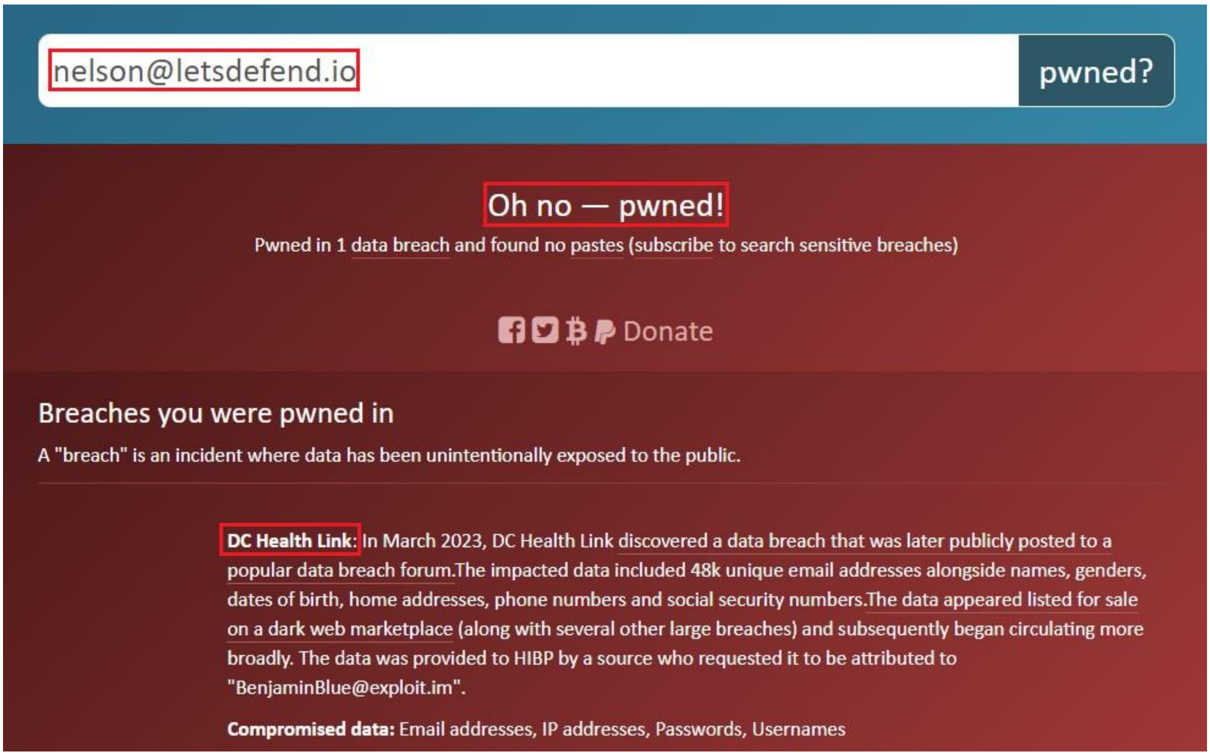
Pwned in 1 data breach and found no pastes (subscribe to search sensitive breaches)

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public.

DC Health Link: In March 2023, DC Health Link discovered a data breach that was later publicly posted to a popular data breach forum.The impacted data included 48k unique email addresses alongside names, genders, dates of birth, home addresses, phone numbers and social security numbers.The data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it to be attributed to "BenjaminBlue@exploit.im".

Compromised data: Email addresses, IP addresses, Passwords, Usernames



nelson@letsdefend.io

Oh no — pwned!

Pwned in 1 data breach and found no pastes (subscribe to search sensitive breaches)

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public.

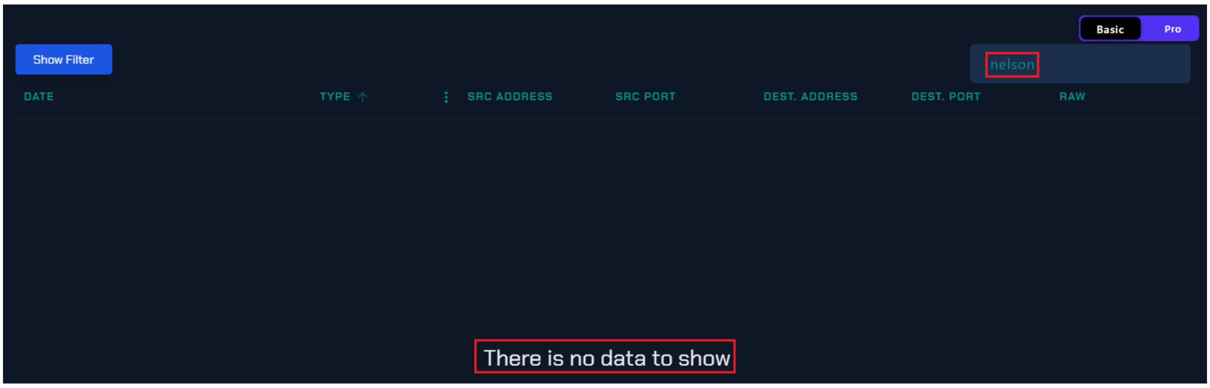
DC Health Link: In March 2023, DC Health Link discovered a data breach that was later publicly posted to a popular data breach forum.The impacted data included 48k unique email addresses alongside names, genders, dates of birth, home addresses, phone numbers and social security numbers.The data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it to be attributed to "BenjaminBlue@exploit.im".

Compromised data: Email addresses, IP addresses, Passwords, Usernames

It is shown above that all three users are among the data of the "DC Health Link". The logs of these three users should be checked in line with the information received from the CTI team. The reason for this is that this leaked information can also be obtained by attackers. The most common attack that can be faced in these situations is brute force.

Logs of the relevant users should be checked on Log Management. Therefore, they should be searched on Log Management respectively.

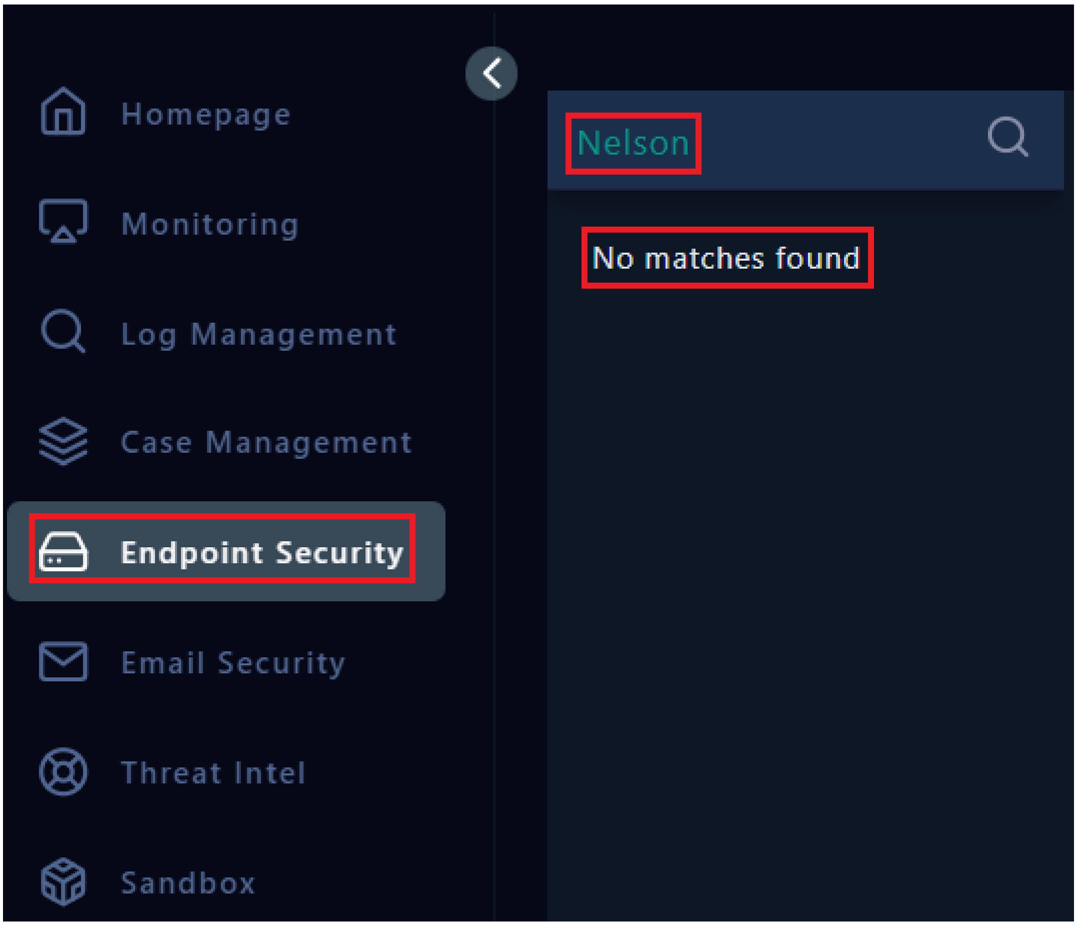
There is no log shown on Log Management when searching for the user named "Nelson". You should also check the user on Endpoint Security.



nelson

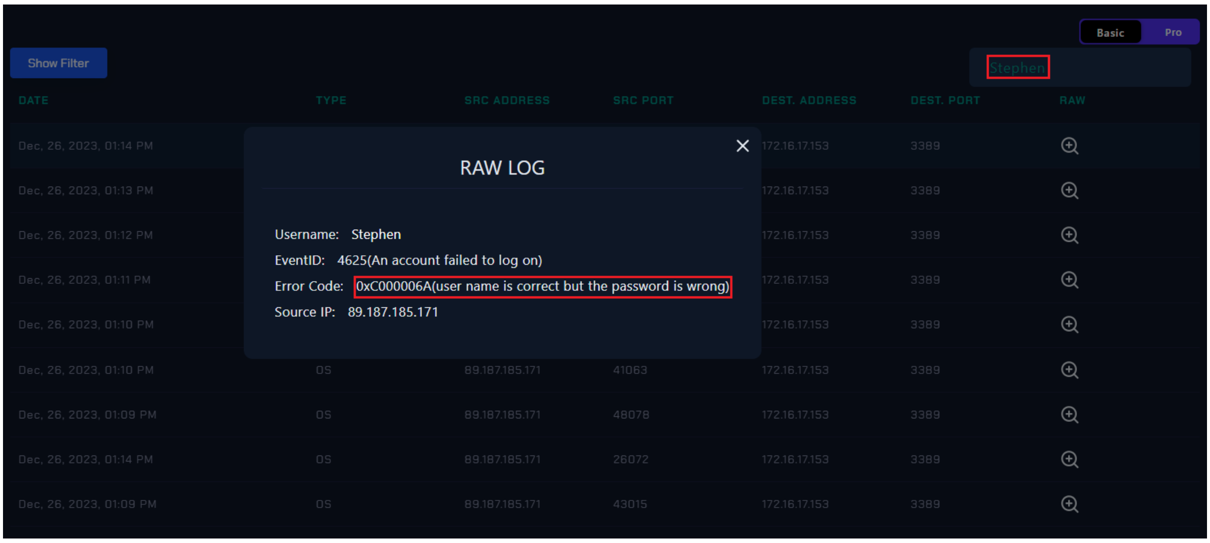
DATE	TYPE ↑	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW

There is no data to show



Why are there no records for this user? There may be two reasons for this. Firstly, the data shared may be fake. Secondly, users may have quit their jobs. The recency of the data is unknown. Sometimes the attacker can share old dated data as if it is up to date. However, search for other users on the domain just in case.

There is no record on the domain for the user named Ruby. However, there are records both on Endpoint and Log Management for the user named Stephen. When looking at the details of the relevant logs, it is found that these are the logs that caused this alert to occur. It is understood where the attacker IP (89[.]187.185.171) accessed the information of the user named Stephen. However, the previous analysis above does not show a successful login by the attacker. Therefore, it is thought that the password information in the data shared on Pastebin is old.



DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Dec, 26, 2023, 01:14 PM				172.16.17.153	3389	⊕
Dec, 26, 2023, 01:13 PM				172.16.17.153	3389	⊕
Dec, 26, 2023, 01:12 PM				172.16.17.153	3389	⊕
Dec, 26, 2023, 01:11 PM				172.16.17.153	3389	⊕
Dec, 26, 2023, 01:10 PM				172.16.17.153	3389	⊕
Dec, 26, 2023, 01:10 PM	OS	89.187.185.171	41063	172.16.17.153	3389	⊕
Dec, 26, 2023, 01:09 PM	OS	89.187.185.171	48078	172.16.17.153	3389	⊕
Dec, 26, 2023, 01:14 PM	OS	89.187.185.171	26072	172.16.17.153	3389	⊕
Dec, 26, 2023, 01:09 PM	OS	89.187.185.171	43015	172.16.17.153	3389	⊕

RAW LOG

```
Username:   Stephen
EventID:   4625(An account failed to log on)
Error Code:   0xC000006A(user name is correct but the password is wrong)
Source IP:   89.187.185.171
```

Containment

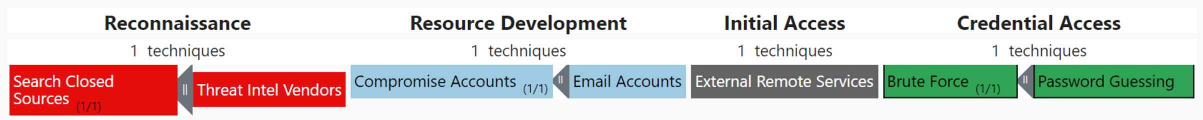
It is determined that the attacker performed a brute force attack on the system. The investigations revealed that there is no log showing that the attacker successfully logged in to the system. Therefore, there is no need to isolate the system from the network. However, the relevant hosts should be closed to remote access if it is not necessary within the scope of work or the MFA structure must be active in the systems for remote access.

Lesson Learned

- Services that provide remote access should not be activated unless it is mandatory.
- SSH/RDP services should be opened to certain people with the whitelist method if they are required to be opened.
- It is recommended to set a strong password policy on clients and servers.
- Employees should be trained periodically to increase awareness of information security.
- Company e-mails should not be used for private business in case of such data leakage.
- The passwords of employees should be updated at least every three months.

Appendix

MITRE



Reconnaissance	Resource Development	Initial Access	Credential Access
1 techniques	1 techniques	1 techniques	1 techniques
Search Closed Sources (1/1) | Threat Intel Vendors	Compromise Accounts (1/1) | Email Accounts	External Remote Services	Brute Force (1/1) | Password Guessing

MITRE Tactics	MITRE Techniques
Reconnaissance	Search Closed Sources: Threat Intel Vendors(T1597.001)
Resource Development	Compromise Accounts: Email Accounts(T1586.002)
Initial Access	External Remote Services(T1133)
Credential Access	Brute Force: Password Guessing(T1110.001)

Artifacts

Field	**Value**
Attacker IP Address	89[.]187.185.171
Users/IP	Stephen/172[.]16.17.153