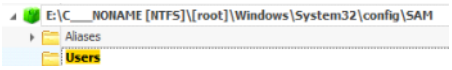
Latus Challenge

Sherlock Scenario
Our customer discovered illegal RDP sessions without Privileged Access Management (PAM) in their system on June 28. They collected evidence on a server they suspected was an intermediary server to move laterally to others. Even though the attacker deleted the event log, I believe the few remaining artifacts are enough to help confirm the attack flow and trace the attacker's behavior.

Task 1:
When was the last failed logon attempt using emman.t user? (UTC)

I checked the SAM Hive and searched for Users key
HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users



Last Incorrect Passw...	Expi...	User Name
==	==	n□c
		Guest
		DefaultAccount
		WDAGUtilityAccount
2024-06-26 07:24:35		emman.t

Answer: 2024-06-26 07:24:35

Task 2:
What are the first 3 IP addresses that emman.t connected to using Remote Desktop (RDP)?

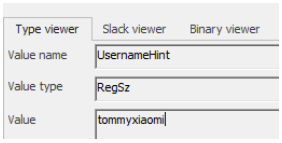
I answered task 3 first so I just did same like task 3
I checked the timestamps of the first IP's

Answer: 192.168.86.250,192.168.25.128,192.168.25.131

Task 3:
What is the destination username used to remote desktop to for the first time on 2024-06-20 16:01:05 UTC?

I checked the NTUSER.DAT and then the HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers
And saw the timestamp 2024-06-20 16:01:05

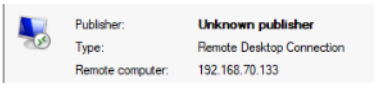
Terminal Server Client	1	2	2024-06-28 13:16:00
Servers	0	10	2024-06-28 13:28:34
192.168.86.250	2	0	2024-06-19 09:34:45
192.168.70.133	2	0	2024-06-26 08:34:08
192.168.25.131	2	0	2024-06-20 02:48:16
192.168.25.128	2	0	2024-06-19 09:43:34
192.168.25.129	2	0	2024-06-20 03:33:16
192.168.70.132	2	0	2024-06-21 03:58:14
192.168.25.132	2	0	2024-06-20 03:18:08
192.168.70.128	2	0	2024-06-28 13:28:43
192.168.70.130	2	0	2024-06-20 15:50:08
192.168.70.131	2	0	2024-06-20 16:01:05



Answer: tommyxiaomi

Task 4:
What is the destination IP address of the last Remote Desktop (RDP) session?

I answered this task after I did several tasks.
Same like task 10, I assumed the IP is the one inside the Default.rdp



Answer: 192.168.70.133

Task 5:
emman.t is very careless in always saving RDP credentials to connect to other hosts, so we believe that attacker somehow leaked them. Please confirm credentials of the server with ip 192.168.70.133 that was leaked?

This task was the most challenging part of the Sherlock investigation.

First, I dumped the SAM and SYSTEM hives, found the usernames and NTLM hashes, and cracked the passwords:

User: admin01
NTLM: a118f08c2940f0570cee0b015bba8492
Password: khongcomatkhau

User: emman | emman.t
NTLM: 444e4af1a1a81457cd9d46675db0a08d
Password: emman2024

User: Administrator
NTLM: 69943c5e63b4d2c104dbbcc15138b72b
Password: 1

This allowed me to extract the password for the 'Emman.t' account, which was 'emman2024'.

The investigation revealed that the attacker had enumerated RDP credentials and logged into the remote host using 'HQ-DOM-03\Administrator.'
I found several stored credentials and methodically tried them based on their timestamps, ultimately identifying the correct one: '063D7EF36287654137F1E552FF79E61E.'

Next, I used the command:

dpapi::cred /in:"E:\C___NONAME [NTFS]\[root]\Users\emman.t\AppData\Local\Microsoft\Credentials\063D7EF36287654137F1E552FF79E61E"
This command decrypted the Windows DPAPI (Data Protection API) credentials stored in the file. It led us to the guidMasterKey: '{ac986fb1-8431-4749-bc7b-92ecdf5d7d64}', a unique identifier for the master key used to encrypt and decrypt sensitive data.

We then navigated to the following directory:
C:\Users\emman.t\AppData\Roaming\Microsoft\Protect\S-1-5-21-1281496067-1440983016-2272511217-1000\
This Protect directory contains the DPAPI credentials for the specified user account, including files that store encryption keys and related data. With the guidMasterKey '{ac986fb1-8431-4749-bc7b-92ecdf5d7d64}' identified, I executed the command:

dpapi::masterkey /in:"E:\C___NONAME [NTFS]\[root]\Users\emman.t\AppData\Roaming\Microsoft\Protect\S-1-5-21-1281496067-1440983016-2272511217-1000\ac986fb1-8431-4749-bc7b-92ecdf5d7d64" /password:emman2024
This command retrieved the master key:
'5902689a5601048b83a7858a842c20d79abff55d82c6d1a35148cc97533760b212d2354057fe3bbdb4d8fdf0ea6fdd1aa79d8bef0101136ebad6ce0eb73e93e8.' The master key is essential for encrypting and decrypting sensitive data, such as passwords and credentials.
Now that we had the compromised user password, the guidMasterKey, and the master key, we connected all the pieces.

I executed the following command:

dpapi::cred /in:"E:\C___NONAME [NTFS]\[root]\Users\emman.t\AppData\Local\Microsoft\Credentials\063D7EF36287654137F1E552FF79E61E" /masterkey:5902689a5601048b83a7858a842c20d79abff55d82c6d1a35148cc97533760b212d2354057fe3bbdb4d8fdf0ea6fdd1aa79d8bef0101136e

This command ultimately retrieved the plaintext password for the domain user who logged into the remote server, which was 'C@mv@0s3rv3r'.

```
Decrypting Credential:
 * volatile cache: GUID:{ac986fb1-8431-4749-bc7b-92ecdf5d7d64};KeyHash:a528c10e17aceb7166928a0694b6fd1836224f55
**CREDENTIAL**
  credFlags      : 00000030 - 48
  credSize       : 000000da - 218
  credUnk0       : 00000000 - 0

  Type           : 00000002 - 2 - domain_password
  Flags          : 00000000 - 0
  LastWritten    : 6/26/2024 8:26:49 AM
  unkFlagsOrSize : 00000018 - 24
  Persist        : 00000002 - 2 - local_machine
  AttributeCount : 00000000 - 0
  unk0           : 00000000 - 0
  unk1           : 00000000 - 0
  TargetName     : Domain:target=TERMSRV/192.168.70.133
  UnkData        : (null)
  Comment        : (null)
  TargetAlias    : (null)
  UserName       : HQ-DOM-03\Administrator
  CredentialBlob : C@mv@0s3rv3r
  Attributes     : 0
```

Answer: Administrator:C@mv@0s3rv3r

Task 6:
When was the last time the Remote Desktop Connection application was executed? (UTC)

I checked the MSTSC inside the Prefetch and checked the "Last Run"

Last Run
=
2024-06-28 13:15:16
2024-06-20 03:36:09
2024-06-28 13:56:48

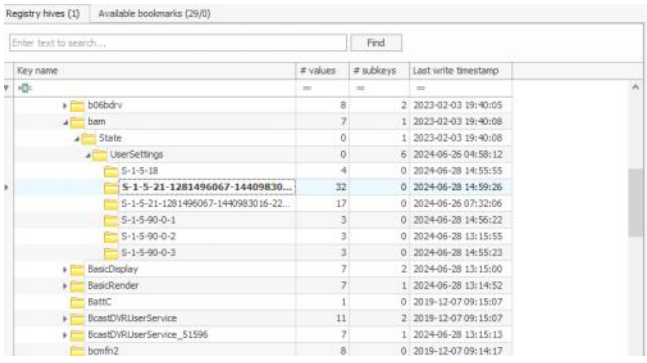
Answer: 2024-06-28 13:56:48

Task 7:
When was the last time the Remote Desktop Connection application was terminated? (UTC)

This one took me a lot of time to complete.
I found the answer at the BAM artifact

HKLM\SYSTEM\ControlSet00X\Services\bam\State\UserSettings\SID\

After talking with a HackTheBox member, with whom I completed some tasks, he told me it was in the BAM. The issue is that I checked several times in the BAM, but I was looking for it in the "Available bookmarks" rather than the Registry hives. This was a valuable lesson, as I didn't find it in the Available bookmarks.



Answer: 2024-06-28 14:01:26

Task 8:
How long did the penultimate RDP session last?

I learned about a new artifact called "ActivitiesCache.db" stored at E:\C___NONAME
[NTFS]\[root]\Users\emman.t\AppData\Local\ConnectedDevicesPlatform\L.emman.t

The ActivitiesCache artifact in Windows tracks user activity, such as app usage, file access, and browsing history.

I first opened it with DB SQLite and tried to calculate all the timestamps but nothing works

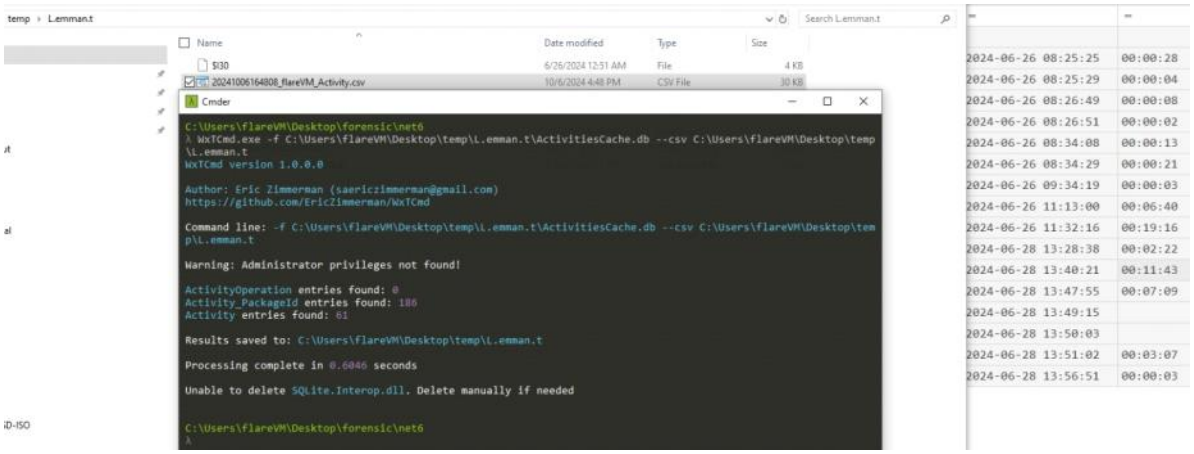
```
SELECT StartTime, EndTime,
    (EndTime - StartTime) AS Duration
FROM Activity
WHERE AppId LIKE '%Microsoft.Windows.RemoteDesktop%'
ORDER BY StartTime DESC
```

This is after calculating the StartTime and EndTime

00:06:40
00:00:03
00:00:21

00:00:13
00:00:02
00:00:08
00:00:04

Then I used Eric Zimerman tool
WxTCmd.exe -f "C:\Users\Bubble\Desktop\ActivitiesCache.db" --csv "C:\Users\Bubble\Desktop
\Artifacts"



=	=
2024-06-26 08:25:25	00:00:28
2024-06-26 08:25:29	00:00:04
2024-06-26 08:26:49	00:00:08
2024-06-26 08:26:51	00:00:02
2024-06-26 08:34:08	00:00:13
2024-06-26 08:34:29	00:00:21
2024-06-26 09:34:19	00:00:03
2024-06-26 11:13:00	00:06:40
2024-06-26 11:32:16	00:19:16
2024-06-28 13:28:38	00:02:22
2024-06-28 13:40:21	00:11:43
2024-06-28 13:47:55	00:07:09
2024-06-28 13:49:15	
2024-06-28 13:50:03	
2024-06-28 13:51:02	00:03:07
2024-06-28 13:56:51	00:00:03

The timestamp is 00:11:43 I reduced 1 second of it after I received some hints from other HackTheBox users.

Answer: 00:11:42

Task 9:
When did the attacker disconnect the last Remote Desktop (RDP) session? (UTC)

Took me ages to find this

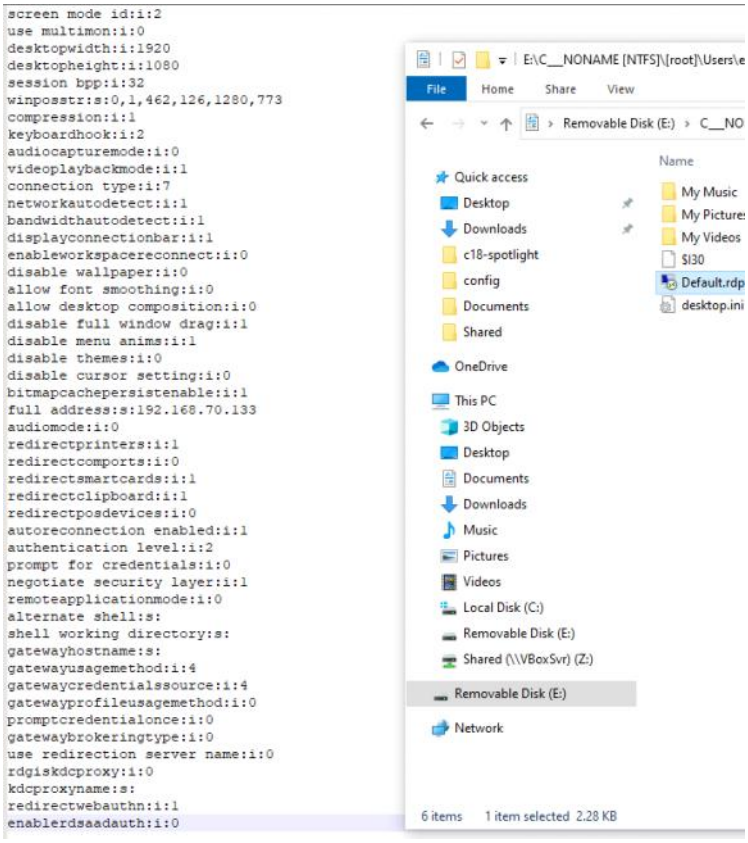
I checked the MFT and searched for mstsc and then I checked for every timestamp with 2024-06-28 at the
"Last Access0x10" until I found it

Last Access0x10
=
2024-06-20 05:56:28
2024-06-20 05:56:28
2024-06-20 05:56:28
2024-06-20 05:56:28
2024-06-20 05:56:28
2024-06-20 05:56:28
2024-06-20 05:56:28
2024-06-20 05:56:28
2024-06-20 05:56:28
2024-06-20 05:56:28
2024-06-20 05:56:28
2024-06-20 05:56:28
2024-06-20 05:56:28
2024-06-20 06:05:42
2024-06-20 06:05:42
2024-06-20 05:57:34
2024-06-28 13:56:48
2024-06-28 13:56:48
2024-06-20 06:05:41
2024-06-28 13:51:03
2024-06-28 13:51:03
2024-06-20 06:05:41
2024-06-28 14:55:42
2024-06-28 14:55:42
2024-06-20 06:05:42
2024-06-28 14:01:26
2024-06-28 14:01:26
2024-06-20 06:05:42
2024-06-20 07:33:22
2024-06-20 07:33:22
2024-06-20 06:06:15
2024-06-20 07:33:10
2024-06-20 07:33:10
2024-06-20 06:06:16
2024-06-28 14:01:26
2024-06-28 14:01:26
2024-06-20 06:07:07
2024-06-28 14:55:42
2024-06-28 14:55:42
2024-06-20 06:07:07

Answer: 2024-06-28 13:51:03

Task 10:
What is the size of the remote desktop configured?

Inside the E:\C___NONAME [NTFS]\[root]\Users\emman.t\Documents there is a RDP file "Default.rdp"
I opened the file with Notepad++ and found the resolution



Answer: 1920:1080

Task 11:
What tool did attacker use to discover the network after moving laterally to 192.168.70.133?

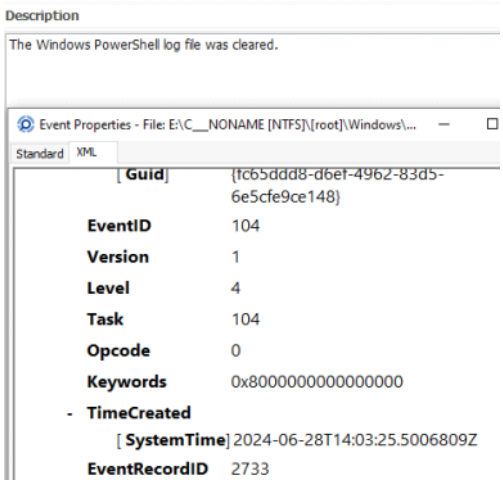
I used the bmc-tool to parse the RDP cache inside E:\C___NONAME [NTFS]\[root]\Users\emman.t
\AppData\Local\Microsoft\Terminal Server Client\Cache
And Then I used RdpCacheStitcher and found the tool

Answer: NetBScanner

Task 12:
When was the event log deleted by the attacker? (UTC)

I found this answer first

I checked the logs and found in the System logs an event with "The Windows PowerShell log file was cleared"

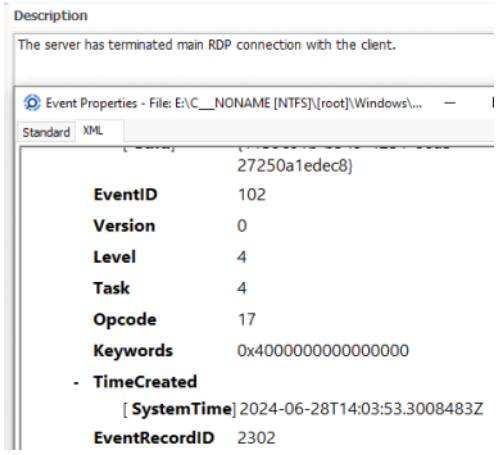


Answer: 2024-06-28 14:03:25

Task 13:
What time did attacker disconnect session to 192.168.70.129? (UTC)

I found this answer 2nd

I checked the logs just like I did in task 12 and I found something inside the "Windows-RemoteDesktopServices-RdpCoreTS" a log with "The server has terminated main RDP connection with the client" so I assumed this timestamp will be the answer



Answer: 2024-06-28 14:03:53