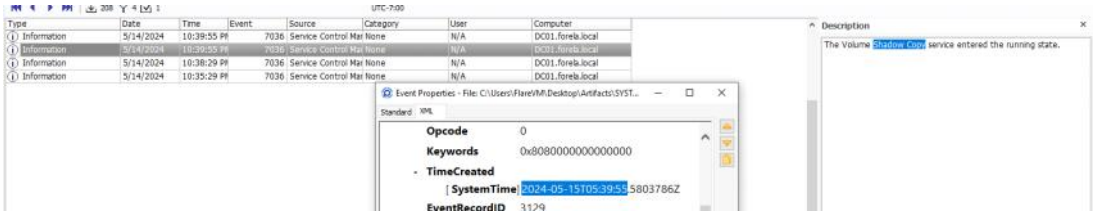
CrownJewel-2 - Walkthrough

Sunday, September 1, 2024 7:10 PM

Story:
Forela's Domain environment is pure chaos.
Just got another alert from the Domain controller of NTDS.dit database being exfiltrated.
Just one day prior you responded to an alert on the same domain controller where an attacker dumped NTDS.dit via vssadmin utility.
However, you managed to delete the dumped files kick the attacker out of the DC, and restore a clean snapshot.
Now they again managed to access DC with a domain admin account with their persistent access in the environment.
This time they are abusing ntdsutil to dump the database.
Help Forela in these chaotic times!!

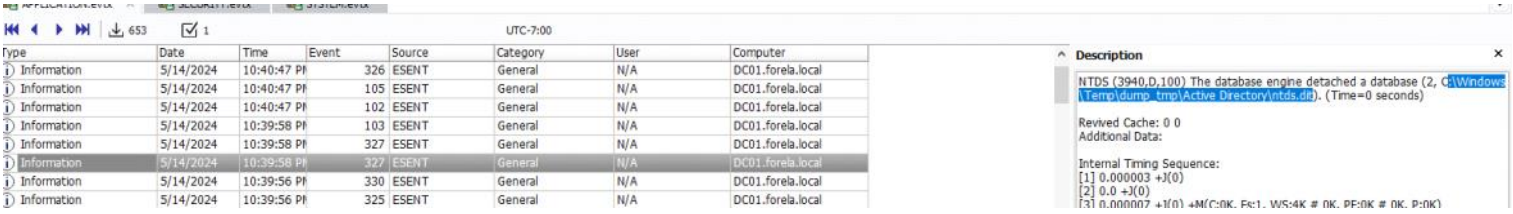
Task1: When utilizing ntdsutil.exe to dump NTDS on disk, it simultaneously employs the Microsoft Shadow Copy Service. What is the most recent timestamp at which this service entered the running state, signifying the possible initiation of the NTDS dumping process?

- In the Security logs, we can see the usage of 'ntdsutil.exe' at 10:39 local time. At the same time, the System logs show that a service entered the running state.



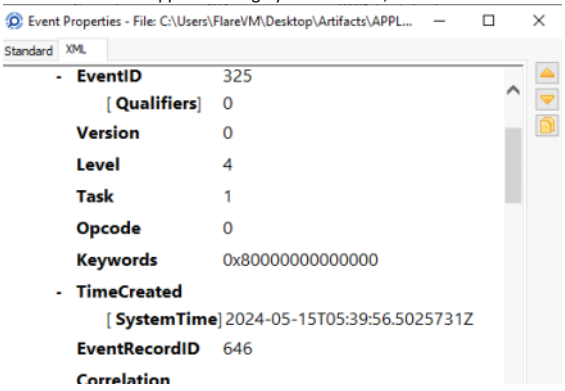
Task2: Identify the full path of the dumped NTDS file.

- To address this question, I searched in the timeframe of the execution of 'ntdustiil.exe' and found the dump of the Ntds.dit



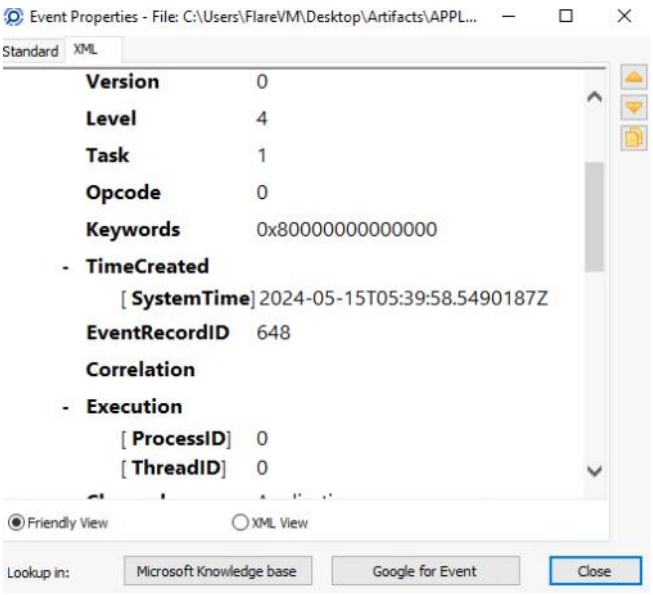
Task3: When was the database dump created on the disk?

- I filtered the Application log by event ID 325, which indicates creation of a new database



Task4: When was the newly dumped database considered complete and ready for use?

- I filtered the Application log by event ID 327, which indicates the database engine detached a database

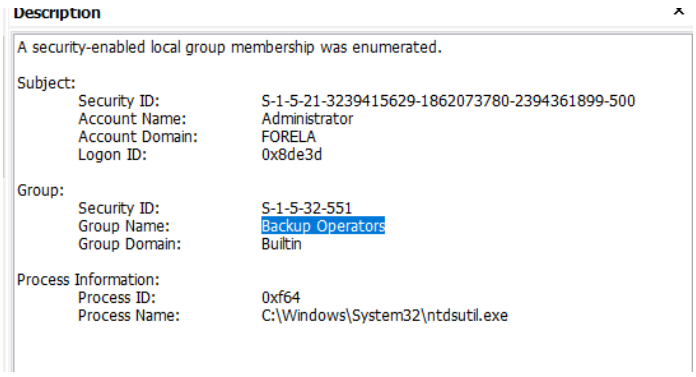


Task5: Event logs use event sources to track events coming from different sources. Which event source provides database status data like creation and detachment?

- **ESENT** is an embeddable, transactional database engine.

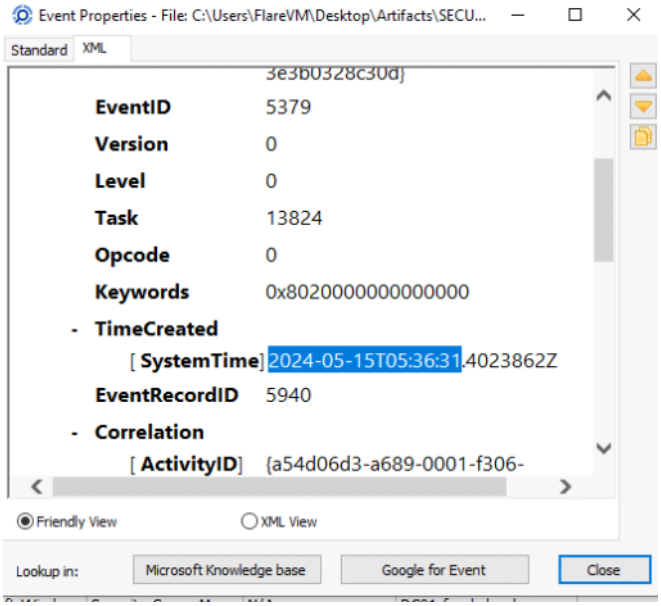
Task6: When ntdsutil.exe is used to dump the database, it enumerates certain user groups to validate the privileges of the account being used. Which two groups are enumerated by the ntdsutil.exe process? Also, find the Logon ID so we can easily track the malicious session in our hunt.

- I filtered in 'Security logs' by event ID 4799 which indicates a security-enabled local group membership was enumerated and found the 'ntdsutil.exe' process enumerated 'Administrators' and 'Backup Operators'.
  The can find the logon-id in the log itself.



Task7: Now you are tasked to find the Login Time for the malicious Session. Using the Logon ID, find the Time when the user logon session started.

- **To address this question, I searched the logon ID '0x8de3d' as keyword and found the first log with this logon ID.**


Event Properties - File: C:\Users\FlareVM\Desktop\Artifacts\SECU...
Standard
XML
3e3b0328c30d}
EventID 5379
Version 0
Level 0
Task 13824
Opcode 0
Keywords 0x8020000000000000
- TimeCreated
[SystemTime] 2024-05-15T05:36:31.4023862Z
EventRecordID 5940
- Correlation
[ActivityID] {a54d06d3-a689-0001-f306-
Friendly View
XML View
Lookup in:
Microsoft Knowledge base
Google for Event
Close