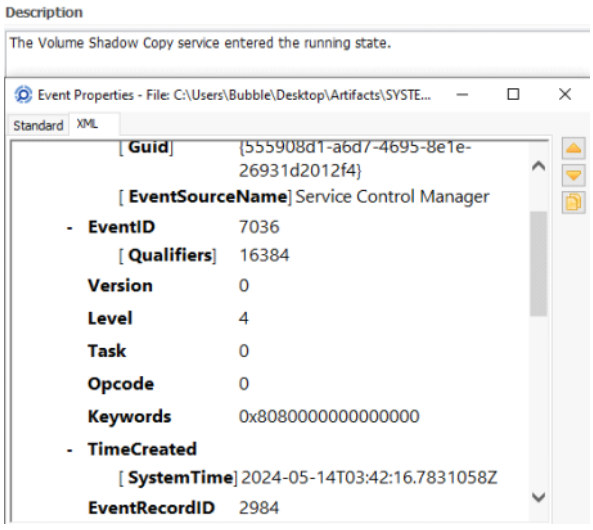
CrownJewel-1 Challenge

Sherlock Scenario
Forela's domain controller is under attack. The Domain Administrator account is believed to be compromised, and it is suspected that the threat actor dumped the NTDS.dit database on the DC. We just received an alert of vssadmin being used on the DC, since this is not part of the routine schedule we have good reason to believe that the attacker abused this LOLBIN utility to get the Domain environment's crown jewel. Perform some analysis on provided artifacts for a quick triage and if possible kick the attacker as early as possible.

Task 1:
Attackers can abuse the vssadmin utility to create volume shadow snapshots and then extract sensitive files like NTDS.dit to bypass security mechanisms. Identify the time when the Volume Shadow Copy service entered a running state.

I searched for Event ID 7036 and investigated the logs until I noticed
"The Volume Shadow Copy service entered the running state."



Answer: 2024-05-14 03:42:16

Task 2:
When a volume shadow snapshot is created, the Volume shadow copy service validates the privileges using the Machine account and enumerates User groups. Find the User groups it enumerates, the Subject Account name, and also identify the Process ID(in decimal) of the Volume shadow copy service process

I searched for "vss" in Security logs and found in the description that a security groups was enumerated.

A security-enabled local group membership was enumerated.

Subject:
Security ID: S-1-5-18
Account Name: DC01$
Account Domain: FORELA
Logon ID: 0x3e7

Group:
Security ID: S-1-5-32-551
Group Name: Backup Operators
Group Domain: Builtin

Process Information:
Process ID: 0x1190
Process Name: C:\Windows\System32\VSSVC.exe

A security-enabled local group membership was enumerated.

Subject:
Security ID: S-1-5-18
Account Name: DC01$
Account Domain: FORELA
Logon ID: 0x3e7

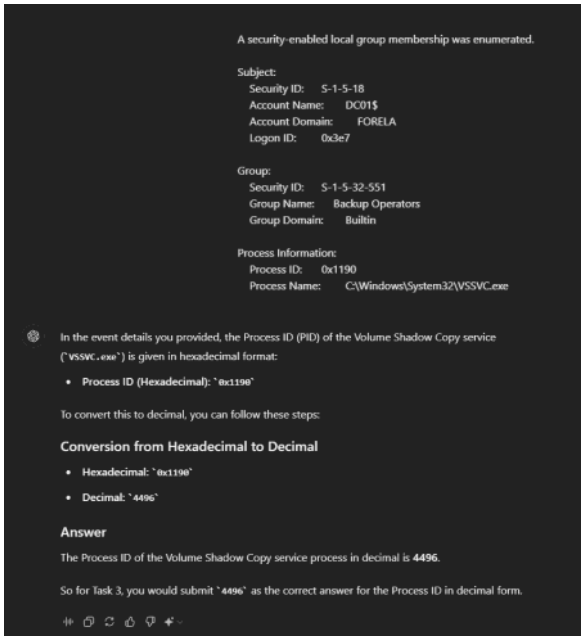
Group:
Security ID: S-1-5-32-544
Group Name: Administrators
Group Domain: Builtin

Process Information:
Process ID: 0x1190
Process Name: C:\Windows\System32\VSSVC.exe

Answer: Administrators, Backup Operators, DC01$

Task 3:
Identify the Process ID (in Decimal) of the volume shadow copy service process.

I copied the log from task 3 to ChatGPT and asked him what is the Decimal



Answer: 4496

Task 4:
Find the assigned Volume ID/GUID value to the Shadow copy snapshot when it was mounted.

I analyzed the NTFS logs until I saw something with "User request" so I assumed this is the GUID

The description for Event ID (303) in Source (Microsoft-Windows-Ntfs) could not be found.
Either the component that raises this event is not installed on the computer or the installation is corrupted.You can install or repair the component or try to change Description Server.

The following information was included with the event:
{06c4a997-cca8-11ed-a90f-000c295644f9}
0

0

33
\Device\HarddiskVolumeShadowCopy1
{00000000-0000-0000-0000-000000000000}
0

0

0

0

0
0

0xffff800f93fd41b0
1736
svchost.exe
User request

Answer: {06c4a997-cca8-11ed-a90f-000c295644f9}

Task 5:
Identify the full path of the dumped NTDS database on disk.

I searched for NTDS in the MFT with Timeline Explorer and checked the path's

Parent Path	File Name
= .\Users\Administrator\Documents\backup_sync_dc	dc
.\Users\Administrator\Documents\backup_sync_dc	ntds.dit

Answer: C:\Users\Administrator\Documents\backup_sync_Dc\Ntds.dit

Task 6:
When was newly dumped ntds.dit created on disk?

Answer can be found in the same way like task 5

Last Modified0x10
=
2023-03-27 14:02:43

Answer: 2024-05-14 03:44:22

Task 7:
A registry hive was also dumped alongside the NTDS database. Which registry hive was dumped and what is its file size in bytes?

I searched for the path "Users\Administrator\Documents\"

Parent Path	File Name	Extension	Is Directory	Has Ads	Is Ads	File Size	Created0x10
=			☐	☐	☐	=	=
.\Users\Administrator	My Documents		☑	☐	☐	0	2023-03-07 19:46:18
.\Users\Administrator\Documents	backup_sync_dc		☑	☐	☐	0	2024-05-14 03:38:46
.\Users\Administrator\Documents	My Music		☑	☐	☐	0	2023-03-07 19:46:18
.\Users\Administrator\Documents	My Pictures		☑	☐	☐	0	2023-03-07 19:46:18
.\Users\Administrator\Documents	My Videos		☑	☐	☐	0	2023-03-07 19:46:18
.\Users\Administrator\Documents	desktop.ini	.ini	☐	☐	☐	402	2023-03-07 19:46:20
.\Users\Administrator\Documents\backup_sync_dc	SYSTEM		☐	☐	☐	17563648	2024-05-14 03:44:42
.\Users\Administrator\Documents\backup_sync_dc	ntds.dit	.dit	☐	☐	☐	16777216	2024-05-14 03:44:22

Answer: SYSTEM, 17563648