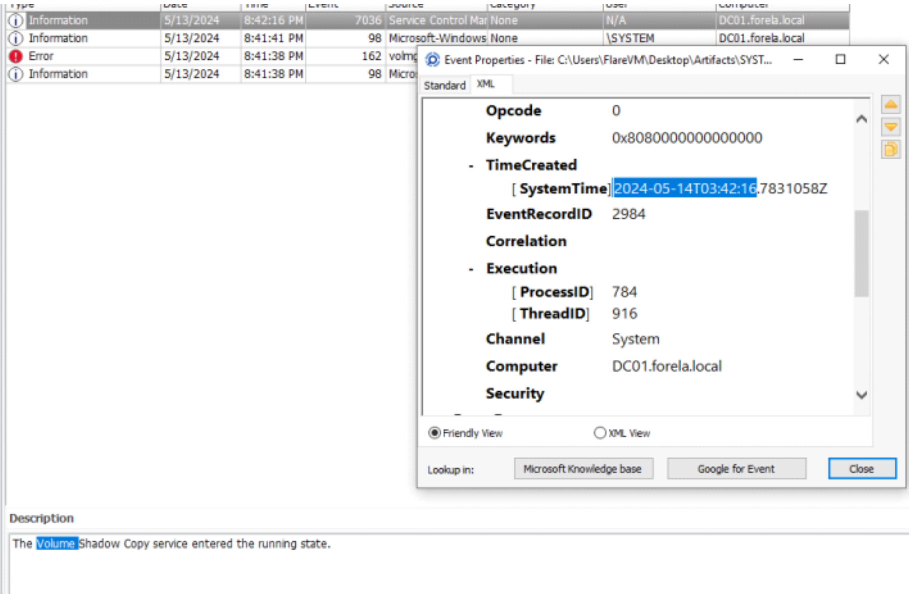
CrownJewel-1 - Walkthrough

Saturday, August 31, 2024 10:52 AM

Story:
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.

Task1: 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 filtered the 'System' logs by event ID 7036, then searched for 'Volume Shadow Copy'



Type	Date	Time	Event	Source	Category	User	Computer
Information	5/13/2024	8:42:16 PM	7036	Service Control Mar	None	N/A	DC01.forela.local
Information	5/13/2024	8:41:41 PM	98	Microsoft-Windows	None	\SYSTEM	DC01.forela.local
Error	5/13/2024	8:41:38 PM	162	volmg			
Information	5/13/2024	8:41:38 PM	98	Micro			

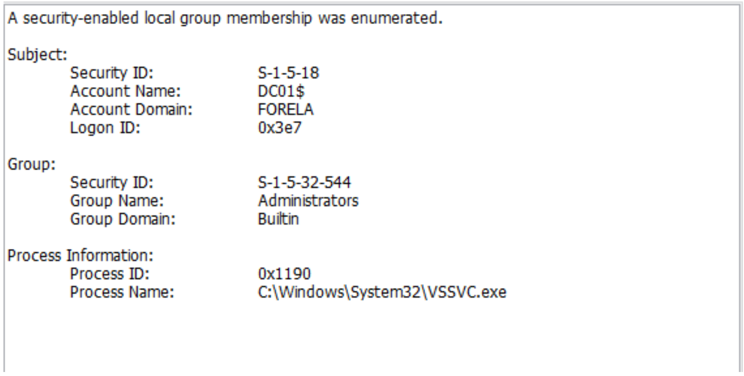
Event Properties - File: C:\Users\FlareVM\Desktop\Artifacts\SYST...

```
Opcode            0
Keywords          0x8080000000000000
- TimeCreated
    [ SystemTime] 2024-05-14T03:42:16.7831058Z
EventRecordID     2984
Correlation
- Execution
    [ ProcessID]  784
    [ ThreadID]   916
Channel           System
Computer          DC01.forela.local
Security
```

The Volume Shadow Copy service entered the running state.

Task2: 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

- To address this question, I filtered the 'Security' logs by Event ID 4799, which is related to "A security-enabled local group membership was enumerated." I identified that the operation was performed by the process named VSSVC.exe, which is associated with the Volume Shadow Copy Service. This indicates that we have identified the correct enumeration phase.



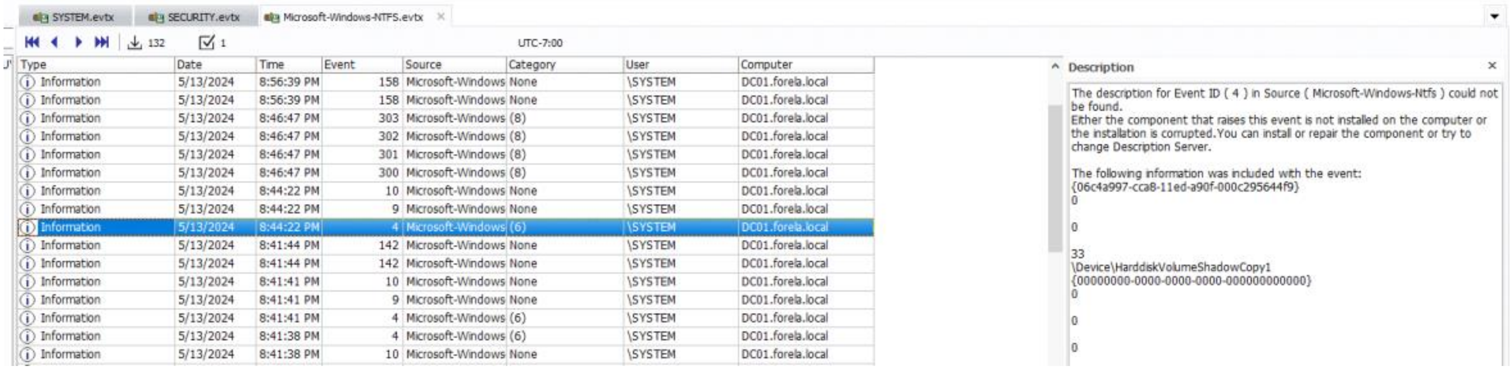
```
A security-enabled local group membership was enumerated.

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
```

Task3: Identify the Process ID (in Decimal) of the volume shadow copy service process.

- In previous question, we identified the PID of the VSS service.
  I asked from ChatGPT to convert '0x1190' to decimal - **'4496'**

Task4: Find the assigned Volume ID/GUID value to the Shadow copy snapshot when it was mounted.

- To address this question, I filtered the NTFS logs by Event ID 4, which records significant changes to the NTFS file system, such as file creations, deletions, or modifications. Since the service ran at 8:42 local time, the operation of the mount appears within that timeframe, and the answer was found.



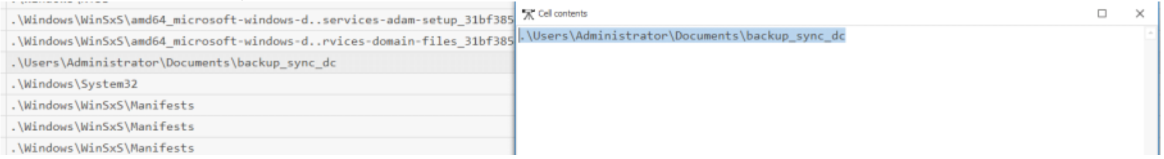
Type	Date	Time	Event	Source	Category	User	Computer
Information	5/13/2024	8:56:39 PM	158	Microsoft-Windows	None	\SYSTEM	DC01.forela.local
Information	5/13/2024	8:56:39 PM	158	Microsoft-Windows	None	\SYSTEM	DC01.forela.local
Information	5/13/2024	8:46:47 PM	303	Microsoft-Windows	(8)	\SYSTEM	DC01.forela.local
Information	5/13/2024	8:46:47 PM	302	Microsoft-Windows	(8)	\SYSTEM	DC01.forela.local
Information	5/13/2024	8:46:47 PM	301	Microsoft-Windows	(8)	\SYSTEM	DC01.forela.local
Information	5/13/2024	8:46:47 PM	300	Microsoft-Windows	(8)	\SYSTEM	DC01.forela.local
Information	5/13/2024	8:44:22 PM	10	Microsoft-Windows	None	\SYSTEM	DC01.forela.local
Information	5/13/2024	8:44:22 PM	9	Microsoft-Windows	None	\SYSTEM	DC01.forela.local
Information	5/13/2024	8:44:22 PM	4	Microsoft-Windows	(6)	\SYSTEM	DC01.forela.local
Information	5/13/2024	8:41:44 PM	142	Microsoft-Windows	None	\SYSTEM	DC01.forela.local
Information	5/13/2024	8:41:44 PM	142	Microsoft-Windows	None	\SYSTEM	DC01.forela.local
Information	5/13/2024	8:41:41 PM	10	Microsoft-Windows	None	\SYSTEM	DC01.forela.local
Information	5/13/2024	8:41:41 PM	9	Microsoft-Windows	None	\SYSTEM	DC01.forela.local
Information	5/13/2024	8:41:41 PM	4	Microsoft-Windows	(6)	\SYSTEM	DC01.forela.local
Information	5/13/2024	8:41:38 PM	4	Microsoft-Windows	(6)	\SYSTEM	DC01.forela.local
Information	5/13/2024	8:41:38 PM	10	Microsoft-Windows	None	\SYSTEM	DC01.forela.local

Description

```
The description for Event ID ( 4 ) 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
```

Task5: Identify the full path of the dumped NTDS database on disk.

- **To address this question, I parsed the MFT file and serached for 'NTDS.DIT'.
  I found unusual directory that the AD DB file was saved to:**

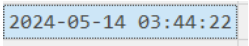


```
.\Windows\WinSxS\amd64_microsoft-windows-d..services-adam-setup_31bf385
.\Windows\WinSxS\amd64_microsoft-windows-d..rvices-domain-files_31bf385
.\Users\Administrator\Documents\backup_sync_dc
.\Windows\System32
.\Windows\WinSxS\Manifests
.\Windows\WinSxS\Manifests
.\Windows\WinSxS\Manifests
```

```
.\Users\Administrator\Documents\backup_sync_dc
```

Task6: When was newly dumped ntds.dit created on disk?

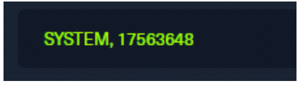
- **Already found it in the previous question, you able to see the creation time**



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

Task7: A registry hive was also dumped alongside the NTDS database. Which registry hive was dumped and what is its file size in bytes?

- The 'System' hive was found in the same path where the attacker dumped the AD database. You can find its size in the parsed MFT file.



```
SYSTEM, 17563648
```