Challenge: CrownJewel-2

Platform: HackTheBox

Category: Sherlock

Difficulty: Very Easy

Tools Used: EvtxECmd, Timeline Explorer

Summary: This sherlock involved investigating three Windows event logs from a compromised domain controller (DC). The tools primarily used were EvtxECmd and Timeline Explorer. I personally found this challenging, as I don't have experience with Kerberos authentication, so wrapping my head around correlating Kerberos events took a lot of time. Nonetheless, I still recommend giving this challenge a go.

Scenario: 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!!

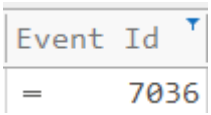
When utilizing ntdsutil.exe to dump NTDS on disk, it simultaneously employs the Microsoft Shadow Copy Service. What is the most recent timestamp at which this service entered the running state, signifying the possible initiation of the NTDS dumping process?

Ntdsutil.exe is a legitimate Windows command-line tool that is used to manage Active Directory Domain Services (AD DS). Threat actors can abuse ntdsutil to dump the NTDS.dit database, typically used for offline password cracking. For context, the NTDS.dit file is a crucial database for AD DS on domain controllers that stores all directory data, including user accounts, group memberships, and more. Crucially, this database also stores hashed passwords for all users in a domain.

Within this task, we are given three Windows event log files: SYSTEM.evtx, SECURITY.evtx, and APPLICATION.evtx. Let's start by parsing these logs using a tool called EvtxECmd:

- `.\EvtxECmd.exe -d . --csv . --csvf event_logs_out.csv`
    - -d points to a directory containing multiple .evtx files, in this case it's the current directory.
    - -- csv tells EvtxECmd to output the results in CSV format.
    - --csvf specifies the output filename.

To view the output, we can use a tool called Timeline Explorer. If you are coming from the CrownJewl-1 challenge, you will remember that event ID 7036 is logged whenever a Windows service changes state, such as starting, stopping, or restarting. If we filter for this event ID, we can find when the Volume Shadow Copy Service most recently entered the running state:



Payload Data1	Payload Data2
Name: Volume Shadow Copy | Volume Shadow Copy	Status: running
Name: Volume Shadow Copy | Volume Shadow Copy	Status: stopped
Name: Volume Shadow Copy | Volume Shadow Copy	Status: running
Name: Microsoft Software Shadow Copy Provider | Microsoft Software Shadow Copy Provider	Status: running

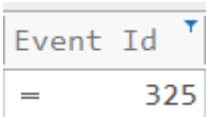
The question asks for the most recent timestamp, i.e. the last entry in the above image:

```
2024-05-15 05:39:55
```

Answer: 2024-05-15 05:39:55

Identify the full path of the dumped NTDS file.

As stated in the hint, we can filter for event ID 325, which logs every time a new NTDS.dit database is created:



Under the Payload Data1 column, on the 15th of May 2024 at 05:39:56, a new NTDS.dit database was created and saved to C:\Windows\Temp\dump_tmp\Active Directory\ntds.dit:

```
Database: C:\Windows\Temp\dump_tmp\Active Directory\ntds.dit
```

Answer: C:\Windows\Temp\dump_tmp\Active Directory\ntds.dit

When was the database dump created on the disk?

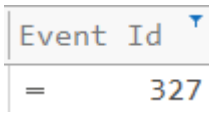
This is when the database dump was created, which we found in the previous question:

```
2024-05-15 05:39:56
```

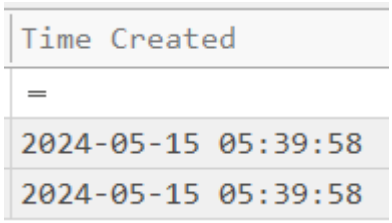
Answer: 2024-05-15 05:39:56

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

Whenever a newly created database is detached by the database engine and ready to use, it generates an event with event ID 327. We can filter for this event ID:



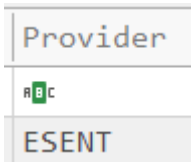
There are two events with this ID, both have the same timestamp:



Answer: 2024-05-15 05:39:58

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

If you take a look at the Provider column, you can see that the event source is ESENT:

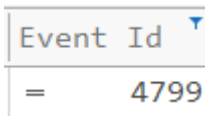


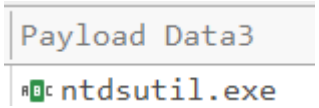
The ESENT event source indicates that the events are being logged by the Extensible Storage Engine (ESE), also known as the Microsoft Jet database engine.

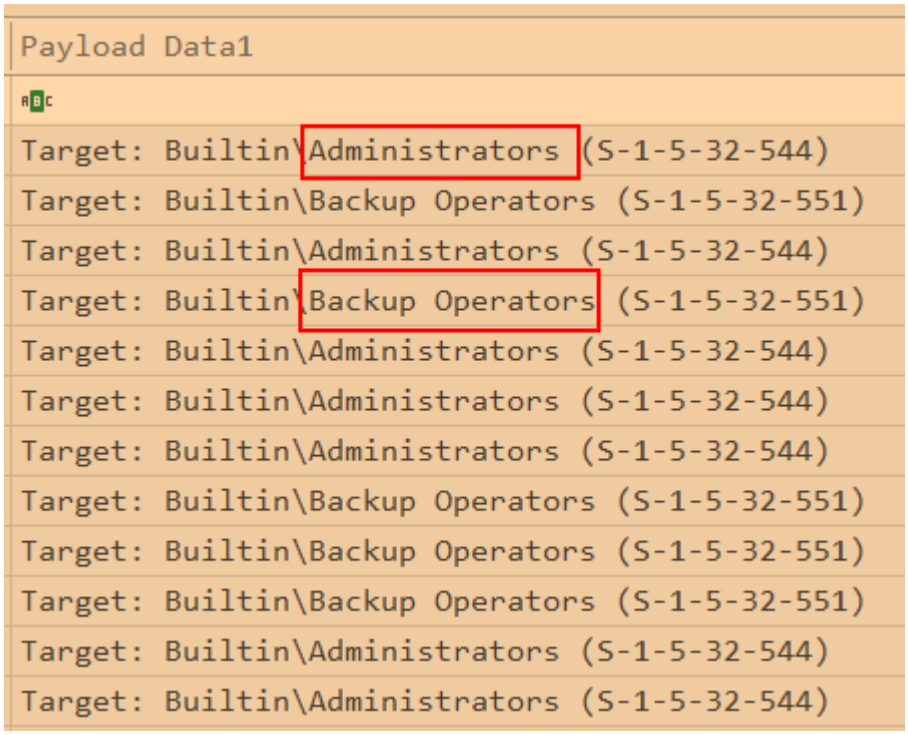
Answer: ESENT

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? Give the groups in alphabetical order joined by comma space.

When a security-enabled local group membership is enumerated, event ID 4799 is logged. We can filter for this event ID and the ntdsutil.exe caller process to determine what two groups were enumerated by the ntdsutil.exe process:







Payload Data1
Target: Builtin\Administrators (S-1-5-32-544)
Target: Builtin\Backup Operators (S-1-5-32-551)
Target: Builtin\Administrators (S-1-5-32-544)
Target: Builtin\Backup Operators (S-1-5-32-551)
Target: Builtin\Administrators (S-1-5-32-544)
Target: Builtin\Administrators (S-1-5-32-544)
Target: Builtin\Administrators (S-1-5-32-544)
Target: Builtin\Backup Operators (S-1-5-32-551)
Target: Builtin\Backup Operators (S-1-5-32-551)
Target: Builtin\Backup Operators (S-1-5-32-551)
Target: Builtin\Administrators (S-1-5-32-544)
Target: Builtin\Administrators (S-1-5-32-544)

As you can see, it enumerated two groups, Administrators and Backup Operators.

Answer: Administrators, Backup Operators

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.

Seeing as this is a domain controller, we need to investigate Kerberos related events.

- Event ID 4768: TGT (Ticket Granting Ticket) request, start of authentication.
- Event ID 4769: TGS (Service Ticket) request, accessing services.
- Event ID 5379: Credential manager credentials were read.

These events are logged on domain controllers, like the one we are investigating. Let's filter for these event IDs:

Time Created	Event Id	Payload Data1
=	= 4768	
2024-05-15 05:35:57	4768	Target: FORELA.LOCAL\DC01$
2024-05-15 05:35:57	4768	Target: FORELA.LOCAL\DC01$
2024-05-15 05:36:31	4768	Target: FORELA\Administrator

In the above image, we can see a TGT was requested for both the DC01$ and Administrator account.

Time Created	Event Id	Payload Data1
=	= 4769	
2024-05-15 05:35:57	4769	Target: FORELA.LOCAL\DC01$@FORELA.LOCAL
2024-05-15 05:35:57	4769	Target: FORELA.LOCAL\DC01$@FORELA.LOCAL
2024-05-15 05:36:18	4769	Target: FORELA.LOCAL\DC01$@FORELA.LOCAL
2024-05-15 05:36:18	4769	Target: FORELA.LOCAL\DC01$@FORELA.LOCAL
2024-05-15 05:36:18	4769	Target: FORELA.LOCAL\DC01$@FORELA.LOCAL
2024-05-15 05:36:18	4769	Target: FORELA.LOCAL\DC01$@FORELA.LOCAL
2024-05-15 05:36:31	4769	Target: FORELA.LOCAL\Administrator@FORELA.LOCAL

In the above image, we can see that FORELA.LOCAL\DC01$@FORELA.LOCAL has been requested several times, with FORELA.LOCAL\Administrator@FORELA.LOCAL being the final entry. This means that Kerberos tickets were being requested for both the DC machine account (DC01$) and the Administrator account. The timestamps show that these requests were made in quick succession, which is suspicious. If we filter for event ID 5379, we can find the Login ID we are tracking and when credentials were accessed:

Time Created	Event Id
=	= 5379
2024-05-15 05:35:29	5379
2024-05-15 05:35:29	5379
2024-05-15 05:35:29	5379
2024-05-15 05:35:31	5379
2024-05-15 05:35:31	5379
2024-05-15 05:35:31	5379
2024-05-15 05:35:31	5379
2024-05-15 05:35:31	5379
2024-05-15 05:35:31	5379
2024-05-15 05:36:31	5379
2024-05-15 05:36:31	5379
2024-05-15 05:36:31	5379
2024-05-15 05:36:35	5379

Administrator	LogonID: 0x8DE3D	CountOfCredentialsReturned: 0	WindowsLive:(token):name=02bhxmfidadsefde;serviceuri=*
Administrator	LogonID: 0x8DE3D	CountOfCredentialsReturned: 0	WindowsLive:(cert):name=02bhxmfidadsefde;serviceuri=*
Administrator	LogonID: 0x8DE3D	CountOfCredentialsReturned: 1	WindowsLive:target=virtualapp/didlogical
Administrator	LogonID: 0x8DE3D	CountOfCredentialsReturned: 0	ServerManager*

In the above image, we can see that the Administrator account was observed accessing different credentials. In summary, the threat actor initially requested a TGT and TGS for the Administrator account. Shortly after these events, a logon session tied to the Administrator account was established and Event ID 5379 was generated, showing access to stored credentials in the Windows Credential Manager.

Answer: 2024-05-15 05:36:31