OpTinselTrace-5 - Walkthrough

Saturday, August 31, 2024 7:52 AM

Story:
You'll notice a lot of our critical server infrastructure was recently transferred from the domain of our MSSP - Forela.local over to Northpole.local.
We actually managed to purchase some second-hand servers from the MSSP who have confirmed they are as secure as Christmas is! It seems not as we believe Christmas is doo med and the attackers seemed to have the stealth of a clattering sleigh bell, or they didn't want to hide at all!!!!!! We have found nasty notes from the Grinch on all of our TinkerTech workstations and servers! Christ mas seems doomed. Please help us recover from whoever committed this naughty attack! Please note - these Sherlocks are built to be completed sequentially and in order!

Task1: Which CVE did the Threat Actor (TA) initially exploit to gain access to DC01?

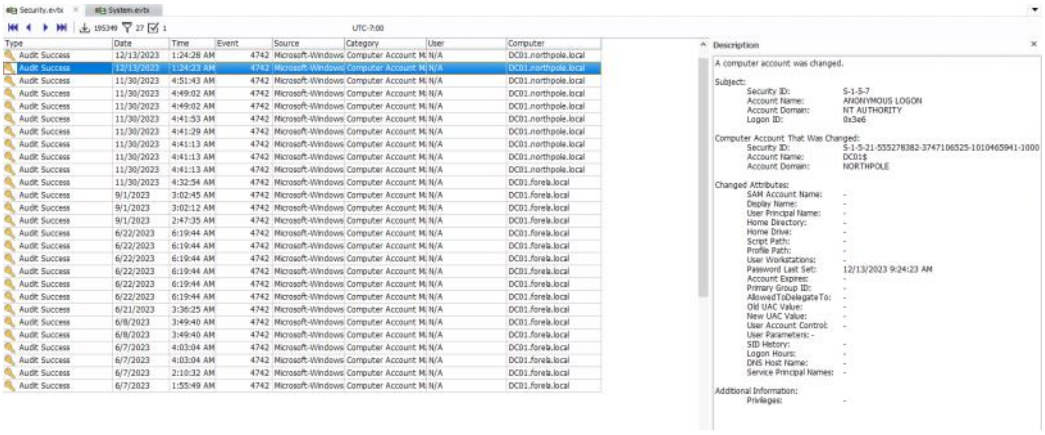
After struggling to move forward in my investigation, I decided to explore known vulnerabilities affecting DCs, such as PrintNightmare. Eventually, I focused on checking for activity related to the **ZeroLogon** vulnerability.

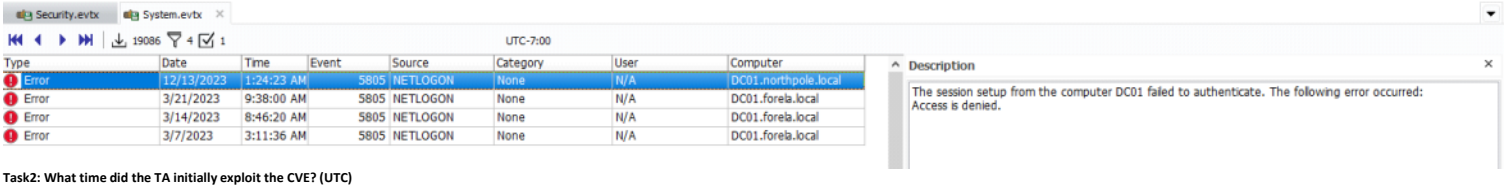
CVE-2020-1472, also known as "ZeroLogon," is a privilege escalation vulnerability in Microsoft's Netlogon Remote Protocol.
This vulnerability allows an attacker with a foothold on the internal network to gain Domain Admin privileges with a single dick, as long as they can establish a connection to the Domain Controller.

How to Detect ZeroLogon Exploitation

Successful exploitation of ZeroLogon results in the reset of the computer account password.
This can be detected in the Security logs with **Event ID 4742**, which indicates that a computer account was changed.
Specifically, look for instances where the password last set field has changed, and the action was performed by an **Anonymous Logon**.

Note: Event ID 4742 occurs periodically because Active Directory automatically resets computer account passwords every 30 days. This can lead to false positives, so it's important to combine this with other artifacts, such as **System Event ID 5805** ("NETLOGON"), to confirm a potential exploitation attempt.



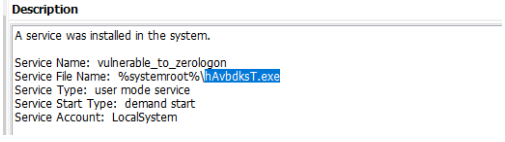


Task2: What time did the TA initially exploit the CVE? (UTC)

- We identified a match between the events previously mentioned.
  The CVE exploited at **2023-12-13 09:24:23 UTC**.

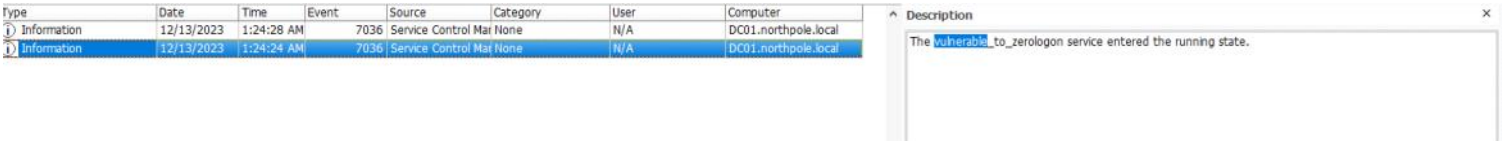
Task3: What is the name of the executable related to the unusual service installed on the system around the time of the CVE e xploitation?

- To address this question, I filtered event ID '7045' in the System logs to find 'Service installed' and found the suspiciousservice:



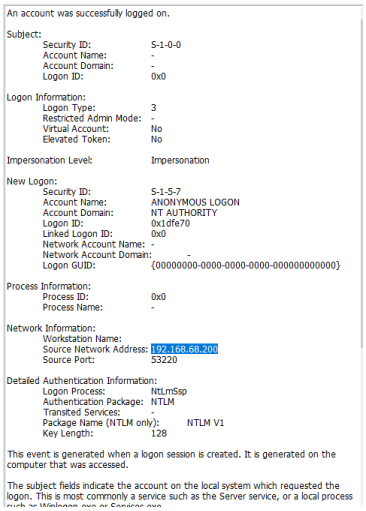
Task4: What date & time was the unusual service start?

- I filtered the event logs by Event ID **7036**, which relates to service start events, and then searched for the specific service name. It was pretty straightforward.



Task5: What was the TA's IP address within our internal network?

- I filtered the Security event logs by **Event ID 4624** and searched for **ANONYMOUS LOGON** within the timeframe we identified for the ZeroLogon activity.



An account was successfully logged on.

Subject:
- Security ID: S-1-0-0
- Account Name: -
- Account Domain: -
- Logon ID: 0x0

Logon Information:
- Logon Type: 3
- Restricted Admin Mode: -
- Virtual Account: No
- Elevated Token: No

Impersonation Level: Impersonation

New Logon:
- Security ID: S-1-5-7
- Account Name: ANONYMOUS LOGON
- Account Domain: NT AUTHORITY
- Logon ID: 0x1dfe70
- Linked Logon ID: 0x0
- Network Account Name: -
- Network Account Domain: -
- Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:
- Process ID: 0x0
- Process Name: -

Network Information:
- Workstation Name:
- Source Network Address: 192.168.68.200
- Source Port: 53220

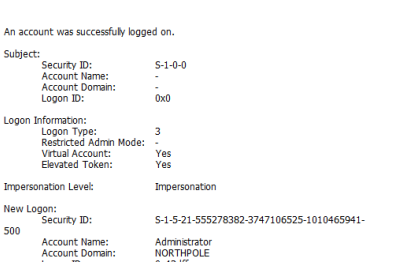
Detailed Authentication Information:
- Logon Process: NtLmSsp
- Authentication Package: NTLM
- Transited Services: -
- Package Name (NTLM only): NTLM V1
- Key Length: 128

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process

Task6: Please list all user accounts the TA utilised during their access. (Ascending order)

- I filtered the Security event logs by **Event ID 4624** and searched for the threat actor's IP address. I reviewed the logs within the timeframe indicating ZeroLogon activity and found the associated accounts.



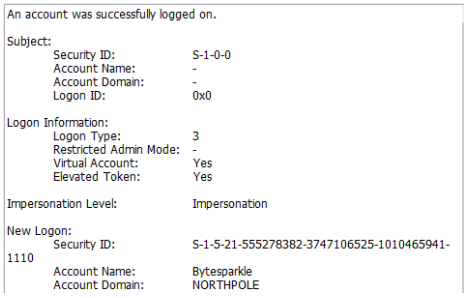
An account was successfully logged on.

Subject:
- Security ID: S-1-0-0
- Account Name: -
- Account Domain: -
- Logon ID: 0x0

Logon Information:
- Logon Type: 3
- Restricted Admin Mode: -
- Virtual Account: Yes
- Elevated Token: Yes

Impersonation Level: Impersonation

New Logon:
- Security ID: S-1-5-21-555278382-3747106525-1010465941-500
- Account Name: Administrator
- Account Domain: NORTHPOLE



An account was successfully logged on.

Subject:
- Security ID: S-1-0-0
- Account Name: -
- Account Domain: -
- Logon ID: 0x0

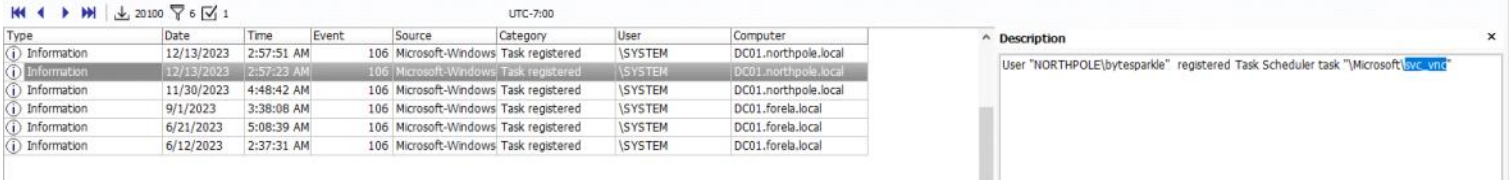
Logon Information:
- Logon Type: 3
- Restricted Admin Mode: -
- Virtual Account: Yes
- Elevated Token: Yes

Impersonation Level: Impersonation

New Logon:
- Security ID: S-1-5-21-555278382-3747106525-1010465941-1110
- Account Name: Bytesparkle
- Account Domain: NORTHPOLE

Task7: What was the name of the scheduled task created by the TA?

- To address this question, I filtered the 'TaskScheduler Operational' logs by Event ID**106** and found an operation performed by the compromised account within the detection timeframe.



20100 6 1 UTC-7:00

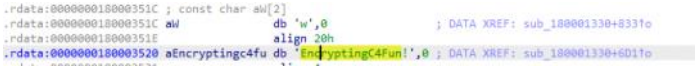
Type	Date	Time	Event	Source	Category	User	Computer
Information	12/13/2023	2:57:51 AM	106	Microsoft-Windows	Task registered	\SYSTEM	DC01.northpole.local
Information	12/13/2023	2:57:23 AM	106	Microsoft-Windows	Task registered	\SYSTEM	DC01.northpole.local
Information	11/30/2023	4:48:42 AM	106	Microsoft-Windows	Task registered	\SYSTEM	DC01.northpole.local
Information	9/1/2023	3:38:08 AM	106	Microsoft-Windows	Task registered	\SYSTEM	DC01.forela.local
Information	6/21/2023	5:08:39 AM	106	Microsoft-Windows	Task registered	\SYSTEM	DC01.forela.local
Information	6/12/2023	2:37:31 AM	106	Microsoft-Windows	Task registered	\SYSTEM	DC01.forela.local

Description

User "NORTHPOLE\bytesparkle" registered Task Scheduler task "\Microsoft\Svc_vnc"

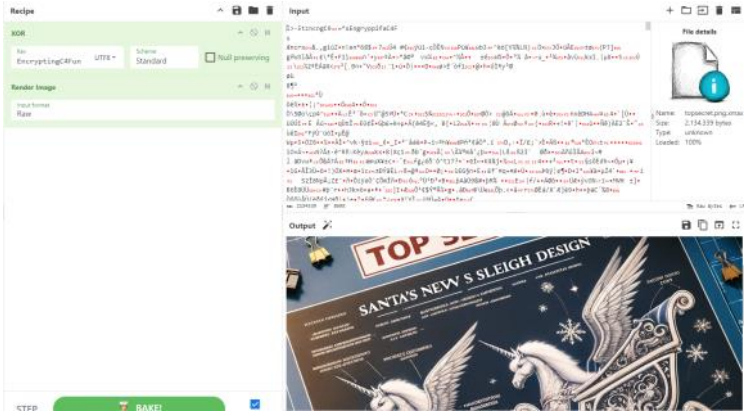
Task8: Santa's memory is a little bad recently! He tends to write a lot of stuff down, but all our critical files have been e ncrypted! Which creature is Santa's new sleigh design planning to use?

- I uploaded the suspicious DLL to IDA, I searched keywords like 'AES', 'RSA', 'Encrypt' and finally found some functions whichrelated to XOR.
  I found the function that encrypting the files and the simple decryption key:



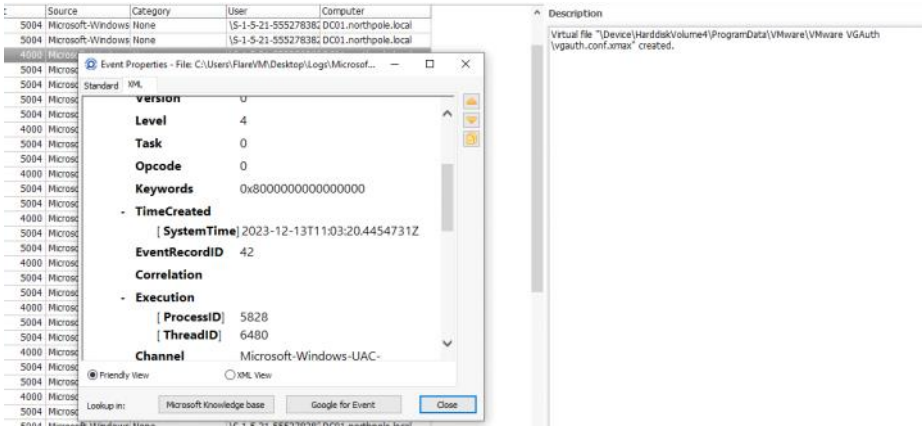
```
.rdata:0000000180003510 ; const char aW[2]
.rdata:0000000180003510 aW              db 'w',0                ; DATA XREF: sub_180001330+833↑o
.rdata:0000000180003512                 align 20h
.rdata:0000000180003520 aEncryptingc4fu db 'EncryptingC4Fun!',0 ; DATA XREF: sub_180001330+6D1↑o
```

- I uploaded the 'topsecret.png' file to CyberChef with the XOR decryption key to decrypt the PNG:
  (Unicorn)



Task9: Please confirm the process ID of the process that encrypted our files.

- I used walkthrough **(**https://github.com/warlocksmurf/HTBSherlock-writeups/blob/main/optinseltrace2023-sherlock/OpTinselTrace-5.md**)** to address this question.
  On 'UAC-FileVirtualization' logs we able to see PIDs.
  I filtered 'XMAX' files and found the answer:


Source
Category
User
Computer
Description
5004 Microsoft-Windows None \S-1-5-21-555278382 DC01.northpole.local
5004 Microsoft-Windows None \S-1-5-21-555278382 DC01.northpole.local
Virtual file "\Device\HarddiskVolume4\ProgramData\VMware\VMware VGAuth \vgauth.conf.xmax" created.
Event Properties - File: C:\Users\FlareVM\Desktop\Logs\Microsof...
Standard
XML
Level 4
Task 0
Opcode 0
Keywords 0x8000000000000000
TimeCreated
[SystemTime] 2023-12-13T11:03:20.4454731Z
EventRecordID 42
Correlation
Execution
[ProcessID] 5828
[ThreadID] 6480
Channel Microsoft-Windows-UAC-
Friendly View
XML View
Lookup in:
Microsoft Knowledge base
Google for Event
Close