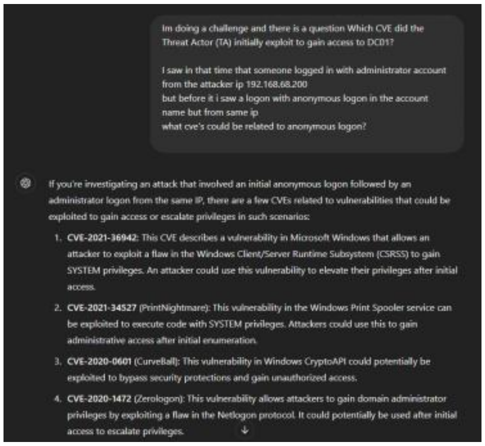
# OpTinselTrace-5 Challenge

Sherlock Scenario
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 doomed 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! Christmas 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!

Task 1:
Which CVE did the Threat Actor (TA) initially exploit to gain access to DC 01?

(I answered this question after I completed task 2-5-6-7)
When I saw that Administrator logged in, right before it there was another event ID 4624 with logon type 3 from the same attacker IP but with Anonymous logon.
So I asked the Chat what CVE's could be related to this activity

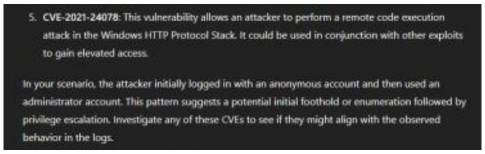


Im doing a challenge and there is a question Which CVE did the Threat Actor (TA) initially exploit to gain access to DC01?

I saw in that time that someone logged in with administrator account from the attacker ip 192.168.68.200
but before it i saw a logon with anonymous logon in the account name but from same ip
what cve's could be related to anonymous logon?

If you're investigating an attack that involved an initial anonymous logon followed by an administrator logon from the same IP, there are a few CVEs related to vulnerabilities that could be exploited to gain access or escalate privileges in such scenarios:

1. **CVE-2021-36942:** This CVE describes a vulnerability in Microsoft Windows that allows an attacker to exploit a flaw in the Windows Client/Server Runtime Subsystem (CSRSS) to gain SYSTEM privileges. An attacker could use this vulnerability to elevate their privileges after initial access.
2. **CVE-2021-34527** (PrintNightmare): This vulnerability in the Windows Print Spooler service can be exploited to execute code with SYSTEM privileges. Attackers could use this to gain administrative access after initial enumeration.
3. **CVE-2020-0601** (CurveBall): This vulnerability in Windows CryptoAPI could potentially be exploited to bypass security protections and gain unauthorized access.
4. **CVE-2020-1472** (Zerologon): This vulnerability allows attackers to gain domain administrator privileges by exploiting a flaw in the Netlogon protocol. It could potentially be used after initial access to escalate privileges.



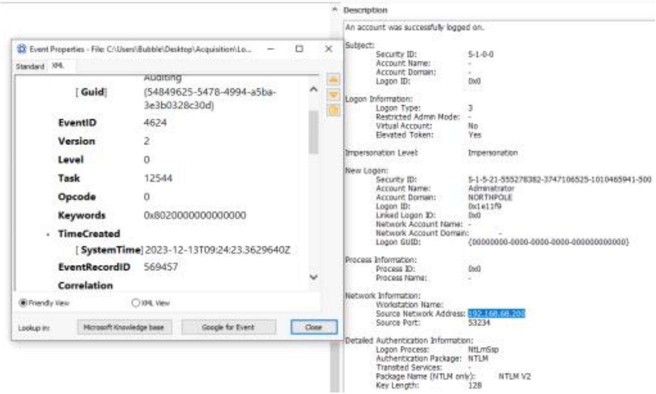
5. **CVE-2021-24078:** This vulnerability allows an attacker to perform a remote code execution attack in the Windows HTTP Protocol Stack. It could be used in conjunction with other exploits to gain elevated access.

In your scenario, the attacker initially logged in with an anonymous account and then used an administrator account. This pattern suggests a potential initial foothold or enumeration followed by privilege escalation. Investigate any of these CVEs to see if they might align with the observed behavior in the logs.

Answer: CVE-2020-1472

Task 2:
What time did the TA initially exploit the CVE? (UTC)

After I found task 5-6-7 I tought to myself maybe it was the time when he logged on with the Administrator account So I checked the event Id 4624 again and search for the attacker IP 192.168.68.200
Then I checked the SysemTime



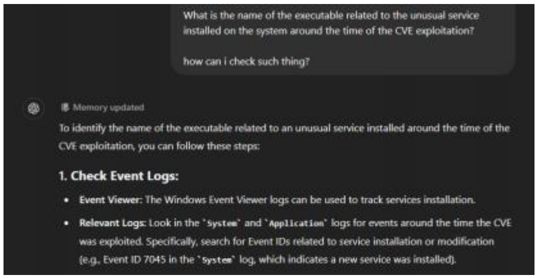
```
Auditing
  [ Guid]       {54849625-5478-4994-a5ba-3e3b0328c30d}
EventID         4624
Version         2
Level           0
Task            12544
Opcode          0
Keywords        0x8020000000000000
TimeCreated
  [ SystemTime] 2023-12-13T09:24:23.3629640Z
EventRecordID   569457
Correlation
```

```
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:         Yes

Impersonation Level:            Impersonation

New Logon:
        Security ID:            S-1-5-21-555278382-3747106525-1010465941-500
        Account Name:           Administrator
        Account Domain:         NORTHPOLE
        Logon ID:               0x1e11f9
        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:            53234

Detailed Authentication Information:
        Logon Process:          NtLmSsp
        Authentication Package: NTLM
        Transited Services:     -
        Package Name (NTLM only):       NTLM V2
        Key Length:             128
```

Answer: 2023-12-13 09:24:23

Task 3:
What is the name of the executable related to the unusual service installed on the system around the time of the CVE exploitation?

I copied the question and asked the Chat how can I find it



What is the name of the executable related to the unusual service installed on the system around the time of the CVE exploitation?

how can i check such thing?

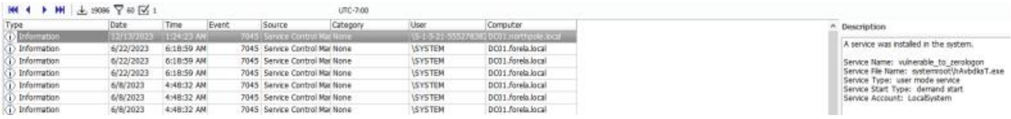
Memory updated

To identify the name of the executable related to an unusual service installed around the time of the CVE exploitation, you can follow these steps:

### 1. Check Event Logs:

- **Event Viewer:** The Windows Event Viewer logs can be used to track services installation.
- **Relevant Logs:** Look in the `System` and `Application` logs for events around the time the CVE was exploited. Specifically, search for Event IDs related to service installation or modification (e.g., Event ID 7045 in the `System` log, which indicates a new service was installed).

I checked the System logs and filtered for event ID 7045



```
19086  60  1                                   UTC-7:00
Type         Date        Time        Event  Source              Category  User                  Computer
Information  12/13/2023  1:24:23 AM  7045   Service Control Mar None      \S-1-5-21-555278382   DC01.northpole.local
Information  6/22/2023   6:18:59 AM  7045   Service Control Mar None      \SYSTEM               DC01.forela.local
Information  6/22/2023   6:18:59 AM  7045   Service Control Mar None      \SYSTEM               DC01.forela.local
Information  6/22/2023   6:18:59 AM  7045   Service Control Mar None      \SYSTEM               DC01.forela.local
Information  6/8/2023    4:48:32 AM  7045   Service Control Mar None      \SYSTEM               DC01.forela.local
Information  6/8/2023    4:48:32 AM  7045   Service Control Mar None      \SYSTEM               DC01.forela.local
Information  6/8/2023    4:48:32 AM  7045   Service Control Mar None      \SYSTEM               DC01.forela.local
```

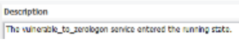
```
Description
A service was installed in the system.

Service Name:  vulnerable_to_zerologon
Service File Name:  systemroot\\hAvbdksT.exe
Service Type:  user mode service
Service Start Type:  demand start
Service Account:  LocalSystem
```

I also saw a service name "vulnerable_to_zerologon" and the filename

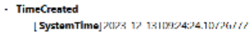
Answer: hAvbdksT.exe

Task 4:
What date & time was the unusual service start?

Same like task 3, I searched around the time of 1:24:23 and I saw the service name "vulnerable_to_zerlogon"



```
Description
The vulnerable_to_zerologon service entered the running state.
```



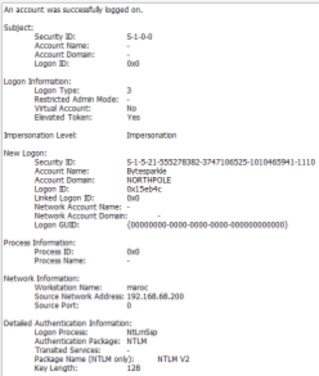
```
- TimeCreated
     [ SystemTime] 2023-12-13T09:24:24.107267[illegible]
```

Answer: 2023-12-13 09:24:23

Task 5:
What was the TA's IP address within our internal network?

(I started the challenge from this task)

I checked the Security logs and filtered for event ID 4624 and noticed a logon type 3 from the user Bytesparkle from workstation name "maroc"

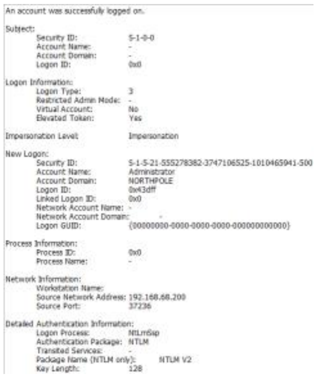


```
An account was successfully logged on.

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:         Yes

Impersonation Level:            Impersonation

New Logon:
        Security ID:            S-1-5-21-555278382-3747106525-1010465941-1110
        Account Name:           Bytesparkle
        Account Domain:         NORTHPOLE
        Logon ID:               0x15eb4c
        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:       maroc
        Source Network Address: 192.168.68.200
        Source Port:            0

Detailed Authentication Information:
        Logon Process:          NtLmSsp
        Authentication Package: NTLM
        Transited Services:     -
        Package Name (NTLM only):       NTLM V2
        Key Length:             128
```

Answer: 192.168.68.200

Task 6:
Please list all user accounts the TA utilised during their access. (Ascending order)

Same like task 5, I kept investigating the logs and saw another logon type 3 from the same IP with the user Administrator

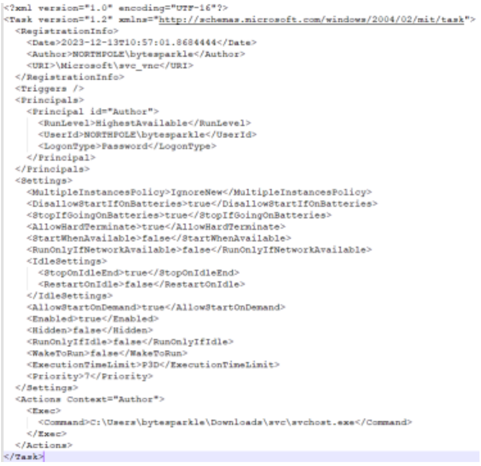


```
An account was successfully logged on.

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:         Yes

Impersonation Level:            Impersonation

New Logon:
        Security ID:            S-1-5-21-555278382-3747106525-1010465941-500
        Account Name:           Administrator
        Account Domain:         NORTHPOLE
        Logon ID:               0x43dff
        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:            37236

Detailed Authentication Information:
        Logon Process:          NtLmSsp
        Authentication Package: NTLM
        Transited Services:     -
        Package Name (NTLM only):       NTLM V2
        Key Length:             128
```

Answer: Administrator, Bytesparkle

Task 7:
What was the name of the scheduled task created by the TA?

Inside the System32\tasks\Microsoft there is a suspicious file "svc_vnc"
I opened it with Notepad and saw that the task Run Level is the HighetAvailable which means high privileged from the user bytesparkle and a path of "C: \Users\bytesparkle\Downloads\svc \svchost.exe"

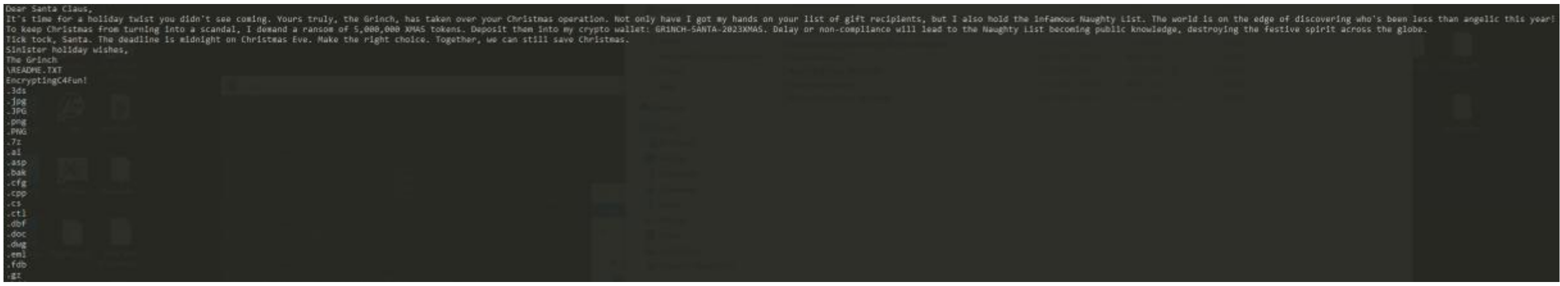


```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <Date>2023-12-13T10:57:01.8684444</Date>
    <Author>NORTHPOLE\bytesparkle</Author>
    <URI>\Microsoft\svc_vnc</URI>
  </RegistrationInfo>
  <Triggers />
  <Principals>
    <Principal id="Author">
      <RunLevel>HighestAvailable</RunLevel>
      <UserId>NORTHPOLE\bytesparkle</UserId>
      <LogonType>Password</LogonType>
    </Principal>
  </Principals>
  <Settings>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
    <DisallowStartIfOnBatteries>true</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
    <AllowHardTerminate>true</AllowHardTerminate>
    <StartWhenAvailable>false</StartWhenAvailable>
    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
    <IdleSettings>
      <StopOnIdleEnd>true</StopOnIdleEnd>
      <RestartOnIdle>false</RestartOnIdle>
    </IdleSettings>
    <AllowStartOnDemand>true</AllowStartOnDemand>
    <Enabled>true</Enabled>
    <Hidden>false</Hidden>
    <RunOnlyIfIdle>false</RunOnlyIfIdle>
    <WakeToRun>false</WakeToRun>
    <ExecutionTimeLimit>P3D</ExecutionTimeLimit>
    <Priority>7</Priority>
  </Settings>
  <Actions Context="Author">
    <Exec>
      <Command>C:\Users\bytesparkle\Downloads\svc\svchost.exe</Command>
    </Exec>
  </Actions>
</Task>
```

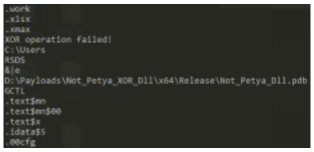
Answer: svc_vnc

Task 8:
Santa's memory is a little bad recently! He tends to write a lot of stuff down, but all our critical files have been encrypted! Which creature is Santa's new sleigh design planning to use?

I did strings on the splunk_svc.dll file from the suspicious file directory

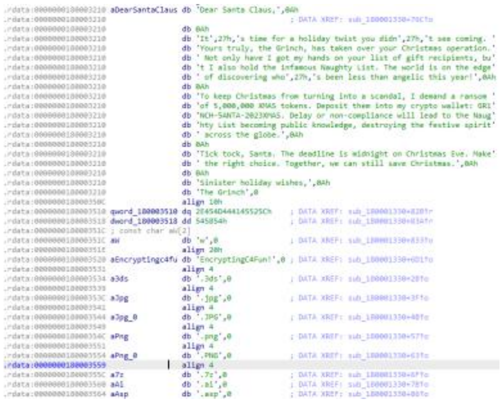


```
Dear Santa Claus,
It's time for a holiday twist you didn't see coming. Yours truly, the Grinch, has taken over your Christmas operation. Not only have I got my hands on your list of gift recipients, but I also hold the infamous Naughty List. The world is on the edge of discovering who's been less than angelic this year!
To keep Christmas from turning into a scandal, I demand a ransom of 5,000,000 XMAS tokens. Deposit them into my crypto wallet: GR1NCH-SANTA-2023XMAS. Delay or non-compliance will lead to the Naughty List becoming public knowledge, destroying the festive spirit across the globe.
Tick tock, Santa. The deadline is midnight on Christmas Eve. Make the right choice. Together, we can still save Christmas.
Sinister holiday wishes,
The Grinch
\README.TXT
EncryptingC4Fun!
.3ds
.jpg
.JPG
.png
.PNG
.7z
.ai
.asp
.bak
.cfg
.cpp
.cs
.ctl
.dbf
.doc
.dwg
.eml
.fdb
.gz
```



```
.work
.xlsx
.xmax
XOR operation failed!
C:\Users
RSDS
&|e
D:\Payloads\Not_Petya_XOR_Dll\x64\Release\Not_Petya_Dll.pdb
GCTL
.text$mn
.text$mn$00
.text$x
.idata$5
.00cfg
```

I saw the "XOR" operation failed so I assumed this encryption is with XOR
Then I opened it in IDA

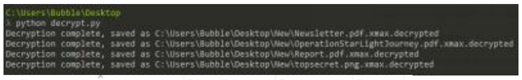


```
.rdata:0000000180003210 aDearSantaClaus db 'Dear Santa Claus,',0Ah
.rdata:0000000180003210                                         ; DATA XREF: sub_180001330+70C↑o
.rdata:0000000180003210                 db 0Ah
.rdata:0000000180003210                 db 'It',27h,'s time for a holiday twist you didn',27h,'t see coming. '
.rdata:0000000180003210                 db 'Yours truly, the Grinch, has taken over your Christmas operation.'
.rdata:0000000180003210                 db ' Not only have I got my hands on your list of gift recipients, bu'
.rdata:0000000180003210                 db 't I also hold the infamous Naughty List. The world is on the edge'
.rdata:0000000180003210                 db ' of discovering who',27h,'s been less than angelic this year!',0Ah
.rdata:0000000180003210                 db 0Ah
.rdata:0000000180003210                 db 'To keep Christmas from turning into a scandal, I demand a ransom '
.rdata:0000000180003210                 db 'of 5,000,000 XMAS tokens. Deposit them into my crypto wallet: GR1'
.rdata:0000000180003210                 db 'NCH-SANTA-2023XMAS. Delay or non-compliance will lead to the Naug'
.rdata:0000000180003210                 db 'hty List becoming public knowledge, destroying the festive spirit'
.rdata:0000000180003210                 db ' across the globe.',0Ah
.rdata:0000000180003210                 db 0Ah
.rdata:0000000180003210                 db 'Tick tock, Santa. The deadline is midnight on Christmas Eve. Make'
.rdata:0000000180003210                 db ' the right choice. Together, we can still save Christmas.',0Ah
.rdata:0000000180003210                 db 0Ah
.rdata:0000000180003210                 db 'Sinister holiday wishes,',0Ah
.rdata:0000000180003210                 db 'The Grinch',0
.rdata:000000018000350C                 align 10h
.rdata:0000000180003510 qword_180003510 dq 2E454D4441455252Ch   ; DATA XREF: sub_180001330+820↑r
.rdata:0000000180003518 dword_180003518 dd 545854h              ; DATA XREF: sub_180001330+83A↑r
.rdata:000000018000351C ; const char aW[2]
.rdata:000000018000351C aW              db 'w',0                ; DATA XREF: sub_180001330+833↑o
.rdata:000000018000351E                 align 20h
.rdata:0000000180003520 aEncryptingc4fu db 'EncryptingC4Fun!',0 ; DATA XREF: sub_180001330+6D1↑o
.rdata:0000000180003531                 align 4
.rdata:0000000180003534 a3ds            db '.3ds',0             ; DATA XREF: sub_180001330+28↑o
.rdata:0000000180003539                 align 4
.rdata:000000018000353C aJpg            db '.jpg',0             ; DATA XREF: sub_180001330+3F↑o
.rdata:0000000180003541                 align 4
.rdata:0000000180003544 aJpg_0          db '.JPG',0             ; DATA XREF: sub_180001330+4B↑o
.rdata:0000000180003549                 align 4
.rdata:000000018000354C aPng            db '.png',0             ; DATA XREF: sub_180001330+57↑o
.rdata:0000000180003551                 align 4
.rdata:0000000180003554 aPng_0          db '.PNG',0             ; DATA XREF: sub_180001330+63↑o
.rdata:0000000180003559                 align 4
.rdata:000000018000355C a7z             db '.7z',0              ; DATA XREF: sub_180001330+6F↑o
.rdata:0000000180003560 aAi             db '.ai',0              ; DATA XREF: sub_180001330+7B↑o
.rdata:0000000180003564 aAsp            db '.asp',0             ; DATA XREF: sub_180001330+87↑o
```

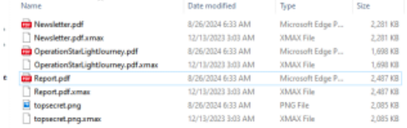
After I keep investigating I assumed  maybe the key is like in the string and on IDA which is "EncryptingC4Fun!"

So I told Chat to build me a python script

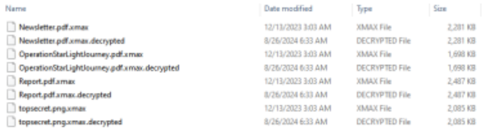
```
import os

def xor_decrypt(filename, key):
    try:
        # Open the encrypted file
        with open(filename, "rb") as f:
            encrypted_data = f.read()

        # Decrypt the data using the XOR key
        key_bytes = key.encode()
        key_len = len(key_bytes)
        decrypted_data = bytearray()

        for i, byte in enumerate(encrypted_data):
            decrypted_data.append(byte ^ key_bytes[i % key_len])

        # Write the decrypted data back to a new file
        decrypted_filename = filename + ".decrypted"
        with open(decrypted_filename, "wb") as f:
            f.write(decrypted_data)

        print(f"Decryption complete, saved as {decrypted_filename}")
    except FileNotFoundError:
        print(f"File not found: {filename}")
    except Exception as e:
        print(f"An error occurred with file {filename}: {e}")

def main():
    directory = r"C:\Users\Bubble\Desktop\New"  # Specify the directory containing the encrypted
files
    key = "EncryptingC4Fun!"  # Use the discovered key
    # Loop through all files in the specified directory
    for filename in os.listdir(directory):
        filepath = os.path.join(directory, filename)
        if os.path.isfile(filepath):
            xor_decrypt(filepath, key)

if __name__ == "__main__":
    main()
```



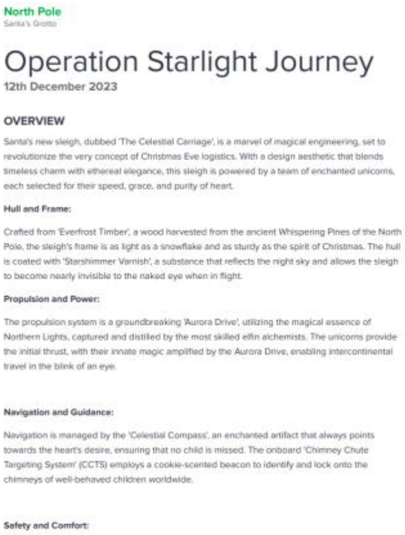
```
C:\Users\Bubble\Desktop
λ python decrypt.py
Decryption complete, saved as C:\Users\Bubble\Desktop\New\Newsletter.pdf.xmax.decrypted
Decryption complete, saved as C:\Users\Bubble\Desktop\New\OperationStarLightJourney.pdf.xmax.decrypted
Decryption complete, saved as C:\Users\Bubble\Desktop\New\Report.pdf.xmax.decrypted
Decryption complete, saved as C:\Users\Bubble\Desktop\New\topsecret.png.xmax.decrypted
```



| Name | Date modified | Type | Size |
|---|---|---|---|
| Newsletter.pdf | 8/26/2024 6:33 AM | Microsoft Edge P... | 2,281 KB |
| Newsletter.pdf.xmax | 12/13/2023 3:03 AM | XMAX File | 2,281 KB |
| OperationStarLightJourney.pdf | 8/26/2024 6:33 AM | Microsoft Edge P... | 1,698 KB |
| OperationStarLightJourney.pdf.xmax | 12/13/2023 3:03 AM | XMAX File | 1,698 KB |
| Report.pdf | 8/26/2024 6:33 AM | Microsoft Edge P... | 2,487 KB |
| Report.pdf.xmax | 12/13/2023 3:03 AM | XMAX File | 2,487 KB |
| topsecret.png | 8/26/2024 6:33 AM | PNG File | 2,085 KB |
| topsecret.png.xmax | 12/13/2023 3:03 AM | XMAX File | 2,085 KB |



| Name | Date modified | Type | Size |
|---|---|---|---|
| Newsletter.pdf.xmax | 12/13/2023 3:03 AM | XMAX File | 2,281 KB |
| Newsletter.pdf.xmax.decrypted | 8/26/2024 6:33 AM | DECRYPTED File | 2,281 KB |
| OperationStarLightJourney.pdf.xmax | 12/13/2023 3:03 AM | XMAX File | 1,698 KB |
| OperationStarLightJourney.pdf.xmax.decrypted | 8/26/2024 6:33 AM | DECRYPTED File | 1,698 KB |
| Report.pdf.xmax | 12/13/2023 3:03 AM | XMAX File | 2,487 KB |
| Report.pdf.xmax.decrypted | 8/26/2024 6:33 AM | DECRYPTED File | 2,487 KB |
| topsecret.png.xmax | 12/13/2023 3:03 AM | XMAX File | 2,085 KB |
| topsecret.png.xmax.decrypted | 8/26/2024 6:33 AM | DECRYPTED File | 2,085 KB |



**North Pole**
Santa's Grotto

# Operation Starlight Journey

12th December 2023

## OVERVIEW

Santa's new sleigh, dubbed 'The Celestial Carriage', is a marvel of magical engineering, set to revolutionize the very concept of Christmas Eve logistics. With a design aesthetic that blends timeless charm with ethereal elegance, this sleigh is powered by a team of enchanted unicorns, each selected for their speed, grace, and purity of heart.

**Hull and Frame:**

Crafted from 'Everfrost Timber', a wood harvested from the ancient Whispering Pines of the North Pole, the sleigh's frame is as light as a snowflake and as sturdy as the spirit of Christmas. The hull is coated with 'Starshimmer Varnish', a substance that reflects the night sky and allows the sleigh to become nearly invisible to the naked eye when in flight.

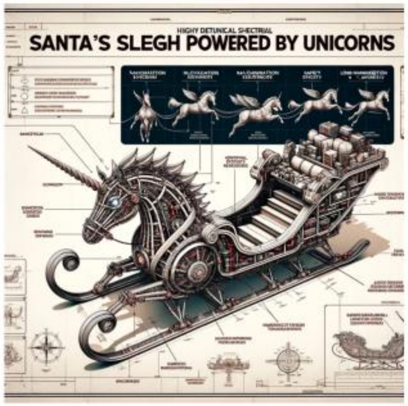
**Propulsion and Power:**

The propulsion system is a groundbreaking 'Aurora Drive', utilizing the magical essence of Northern Lights, captured and distilled by the most skilled elfin alchemists. The unicorns provide the initial thrust, with their innate magic amplified by the Aurora Drive, enabling intercontinental travel in the blink of an eye.

**Navigation and Guidance:**

Navigation is managed by the 'Celestial Compass', an enchanted artifact that always points towards the heart's desire, ensuring that no child is missed. The onboard 'Chimney Chute Targeting System' (CCTS) employs a cookie-scented beacon to identify and lock onto the chimneys of well-behaved children worldwide.

**Safety and Comfort:**



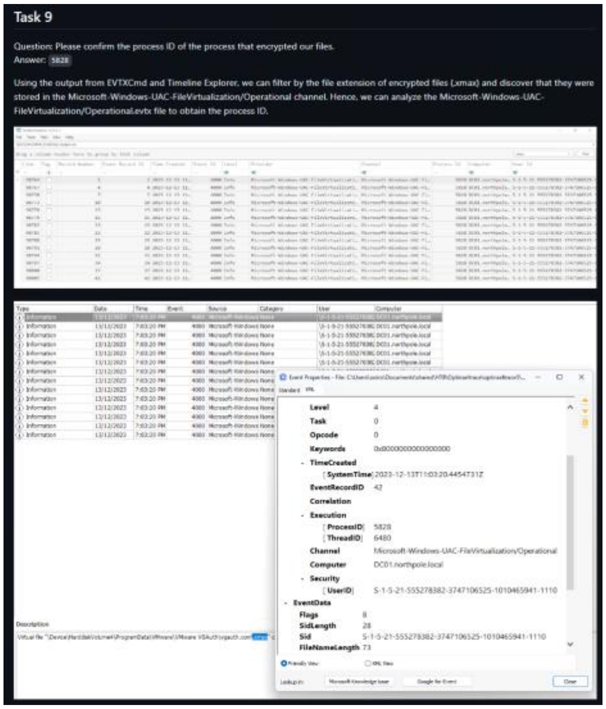
I copied all the PDF text to Chat and asked him who is the creature

Answer: Unicorn

Task 9:
Please confirm the process ID of the process that encrypted our files.

After I tried everything, and I also was pretty closed because I parsed all the evtx files to one CSV and also checked for some xmax files with Timeline Explorer. I didn 't found the answer and checked the write-up.

This task is useless



## Task 9

Question: Please confirm the process ID of the process that encrypted our files.
Answer: `5828`

Using the output from EVTXCmd and Timeline Explorer, we can filter by the file extension of encrypted files (.xmax) and discover that they were stored in the Microsoft-Windows-UAC-FileVirtualization/Operational channel. Hence, we can analyze the Microsoft-Windows-UAC-FileVirtualization/Operational.evtx file to obtain the process ID.

```
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-FileVirtualization/Operational
Computer         DC01.northpole.local
- Security
    [ UserID]     S-1-5-21-555278382-3747106525-1010465941-1110
- EventData
  Flags          8
  SidLength      28
  Sid            S-1-5-21-555278382-3747106525-1010465941-1110
  FileNameLength 73
```

Answer: 5828