PSP0201 Week 6 Writeup

Group Name: Undecided

Members

ID	Name	Role
1211101390	Aslamia Najwa Binti Ahmad Khadri	Leader
1211100431	Mohammad Omar Torofder	Member
1211103388	Vishnu Karmegam	Member
1211103092	Farryn Aisha Binti Muhd Firdaus	Member

Day 23 : Blue Teaming – The Grinch Strikes Again

Tools used: Attackbox, Remmina, Firefox

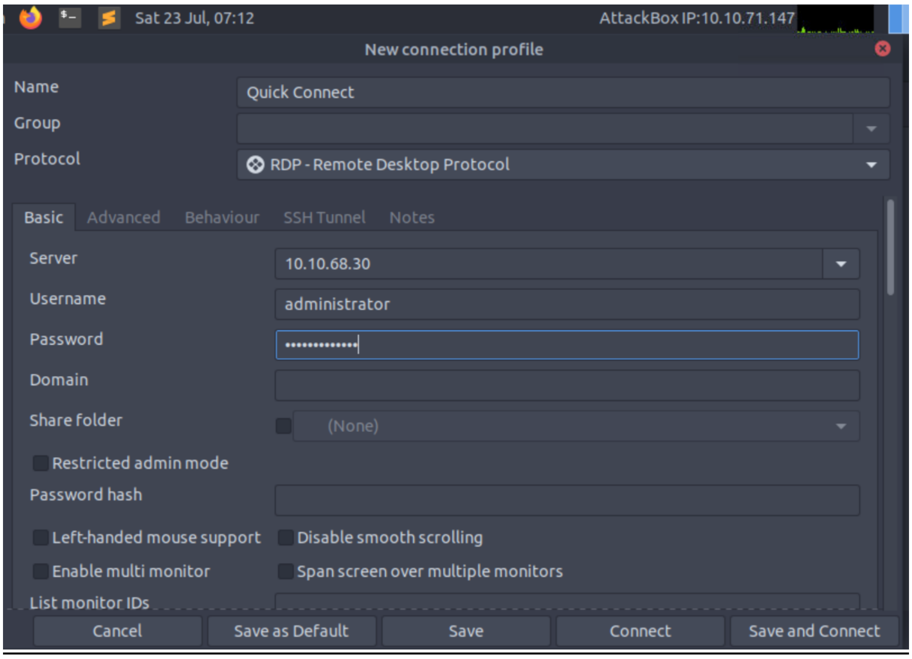
Solution/walkthrough:

Question 1

Upon starting the task, we first inserted the credentials as well as the IP address given for the profile. We then clicked on “Save and Connect” and managed to connect to the server.

User name: administrator

User password: sn0wF!akes!!!



Name: Quick Connect

Group:

Protocol: RDP - Remote Desktop Protocol

Server: 10.10.68.30

Username: administrator

Password: •••••••••••••

Domain:

Share folder: □ (None)

□ Restricted admin mode

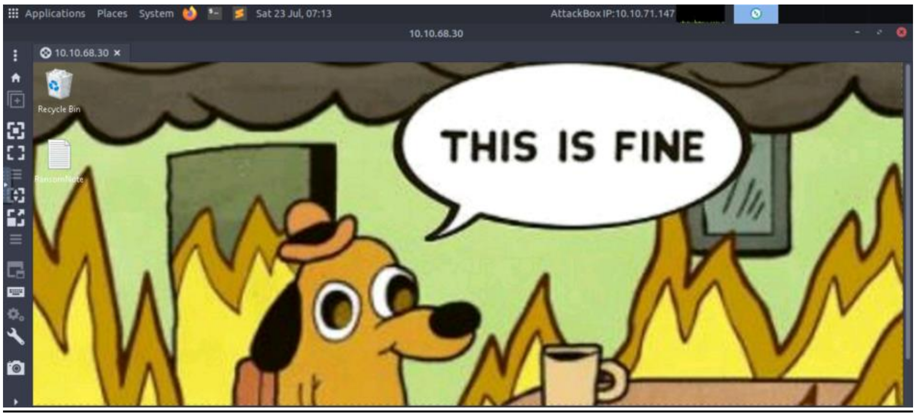
Password hash:

□ Left-handed mouse support □ Disable smooth scrolling

□ Enable multi monitor □ Span screen over multiple monitors

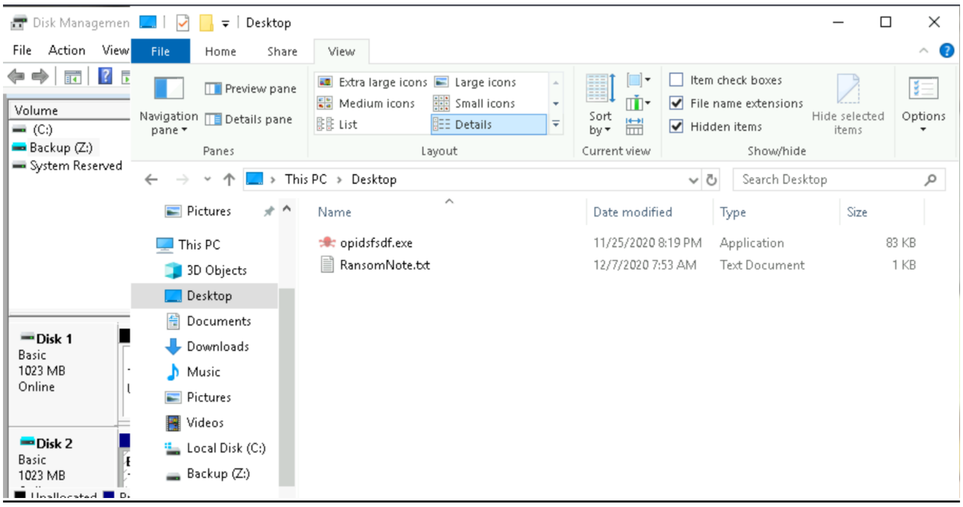
List monitor IDs:

Once connected to the server, we were shown with a wallpaper that says, “THIS IS FINE”.



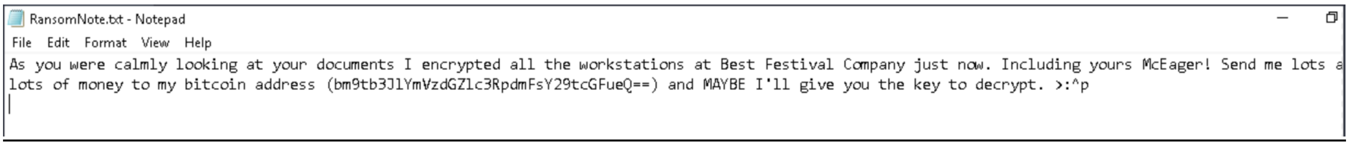
Question 2

We proceeded on clicking the file explorer and opening the ransom note that was placed in the desktop.



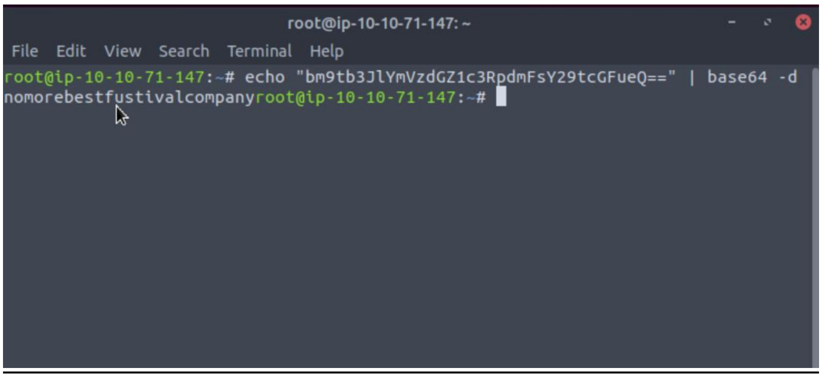
Name	Date modified	Type	Size
opidsfsdf.exe	11/25/2020 8:19 PM	Application	83 KB
RansomNote.txt	12/7/2020 7:53 AM	Text Document	1 KB

As seen, the note was written with a suspicious 'bitcoin address' which was known to be fake.



```
As you were calmly looking at your documents I encrypted all the workstations at Best Festival Company just now. Including yours McEager! Send me lots a
lots of money to my bitcoin address (bm9tb3J1YmVzdGZ1c3RpdmFsY29tcGFueQ==) and MAYBE I'll give you the key to decrypt. >:^p
```

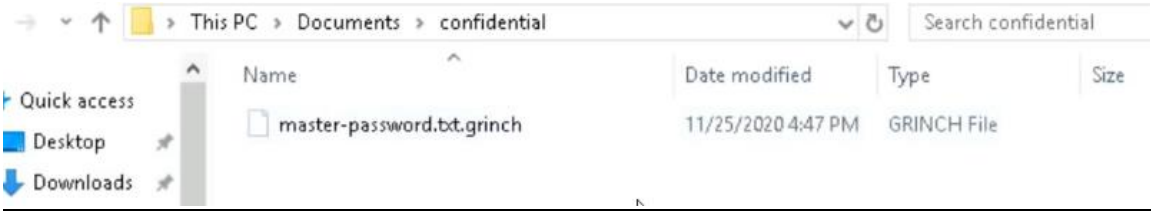
Thus, we opened the terminal in order to decrypt it by using the method base64 and received the plain text value.



```
root@ip-10-10-71-147:~# echo "bm9tb3JlYmVzdGZ1c3RpdmFsY29tcGFueQ==" | base64 -d
nomorebestfustivalcompanyroot@ip-10-10-71-147:~#
```

Question 3

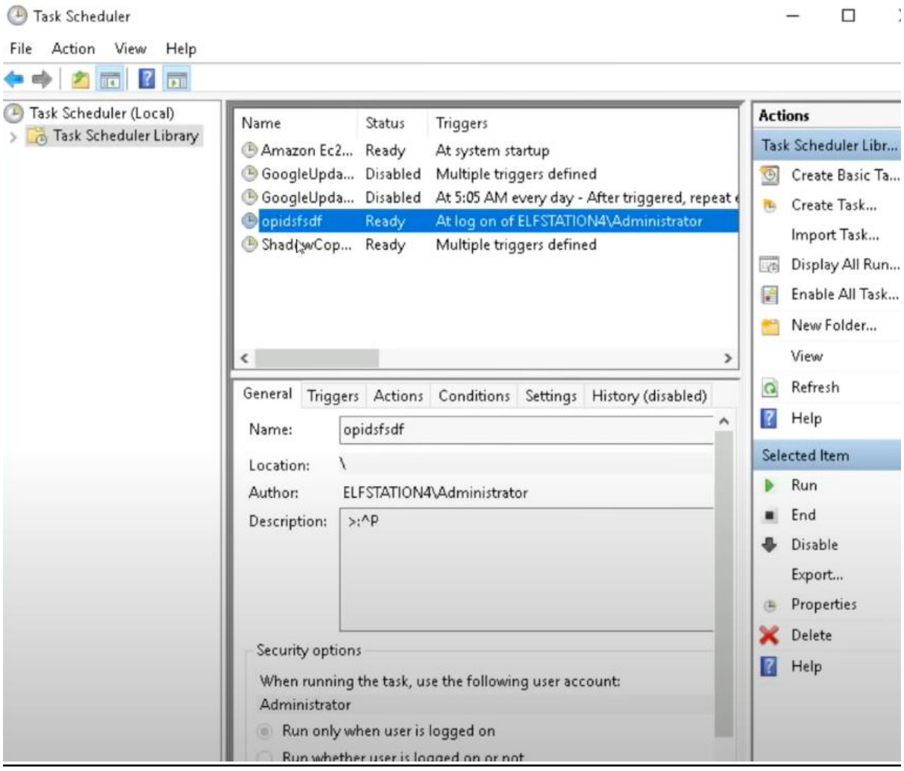
We clicked on the confidential file and got the file extension(.grinch).



Name	Date modified	Type	Size
master-password.txt.grinch	11/25/2020 4:47 PM	GRINCH File	

Question 4

The suspicious scheduled task file was in the Task Scheduler. Thus, we opened it to find the name of the file which was opidsfsdf.



Name	Status	Triggers
Amazon Ec2...	Ready	At system startup
GoogleUpda...	Disabled	Multiple triggers defined
GoogleUpda...	Disabled	At 5:05 AM every day - After triggered, repeat e
opidsfsdf	Ready	At log on of ELFSTATION4\Administrator
ShadowCop...	Ready	Multiple triggers defined

General Triggers Actions Conditions Settings History (disabled)

Name: opidsfsdf

Location: \

Author: ELFSTATION4\Administrator

Description: >:^P

Security options

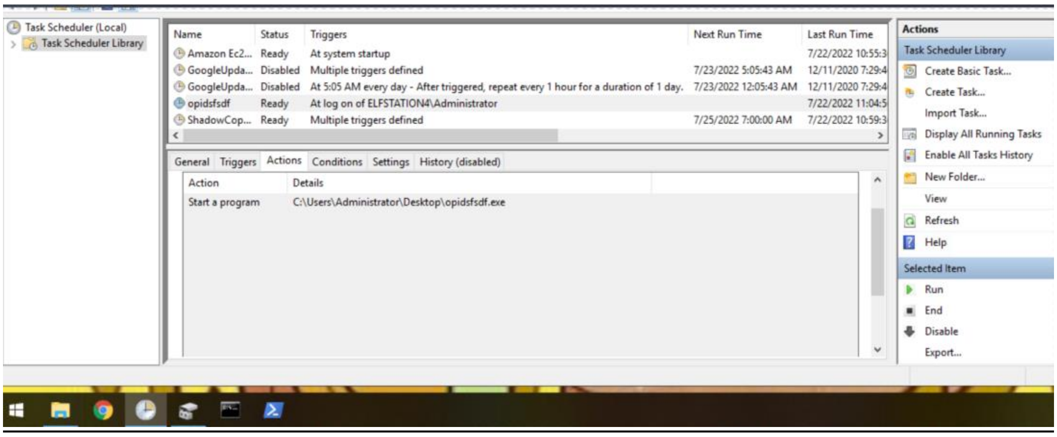
When running the task, use the following user account:
Administrator

● Run only when user is logged on

○ Run whether user is logged on or not

Question 5

In the Task Scheduler, we found the location of the executable that is run at login for the scheduled task by clicking on Actions which is C:\Users\Administrator\Desktop\opidsfsdf.exe.



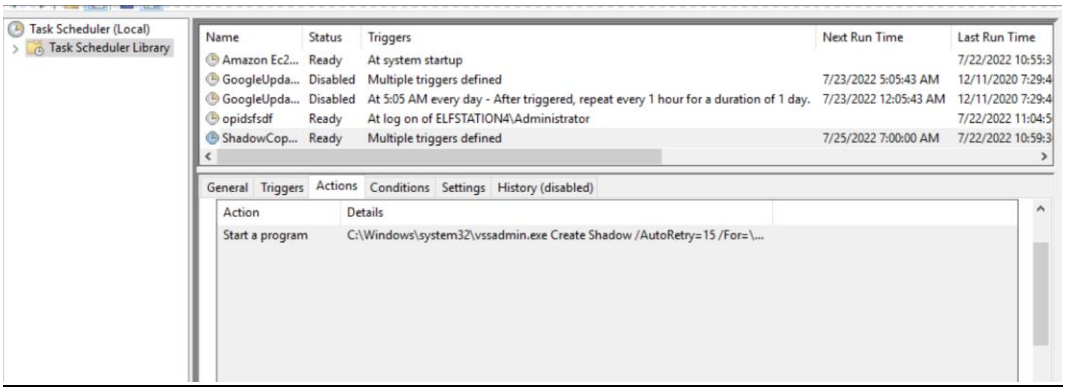
Name	Status	Triggers	Next Run Time	Last Run Time
Amazon Ec2...	Ready	At system startup		7/22/2022 10:55:3
GoogleUpda...	Disabled	Multiple triggers defined	7/23/2022 5:05:43 AM	12/11/2020 7:29:4
GoogleUpda...	Disabled	At 5:05 AM every day - After triggered, repeat every 1 hour for a duration of 1 day.	7/23/2022 12:05:43 AM	12/11/2020 7:29:4
opidsfsdf	Ready	At log on of ELFSTATION4\Administrator		7/22/2022 11:04:5
ShadowCop...	Ready	Multiple triggers defined	7/25/2022 7:00:00 AM	7/22/2022 10:59:3

General Triggers Actions Conditions Settings History (disabled)

Action	Details
Start a program	C:\Users\Administrator\Desktop\opidsfsdf.exe

Question 6

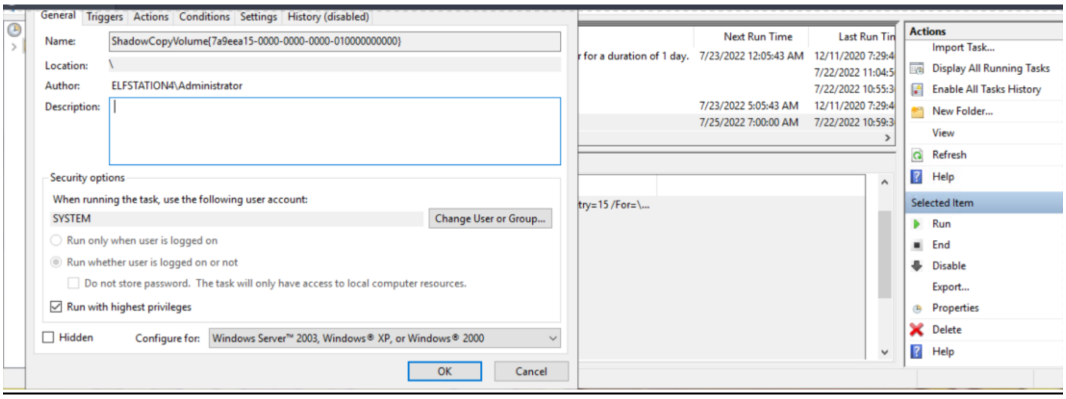
The other scheduled task that is related to VSS was ShadowCopyVolume under the Task Scheduler Library.



Name	Status	Triggers	Next Run Time	Last Run Time
Amazon Ec2...	Ready	At system startup		7/22/2022 10:55:3
GoogleUpda...	Disabled	Multiple triggers defined	7/23/2022 5:05:43 AM	12/11/2020 7:29:4
GoogleUpda...	Disabled	At 5:05 AM every day - After triggered, repeat every 1 hour for a duration of 1 day.	7/23/2022 12:05:43 AM	12/11/2020 7:29:4
opidsfsdf	Ready	At log on of ELFSTATION4\Administrator		7/22/2022 11:04:5
ShadowCop...	Ready	Multiple triggers defined	7/25/2022 7:00:00 AM	7/22/2022 10:59:3

Action	Details
Start a program	C:\Windows\system32\vssadmin.exe Create Shadow /AutoRetry=15 /For=\...

We then clicked on the properties at the bottom right in order to find the ID of the task under the name category.



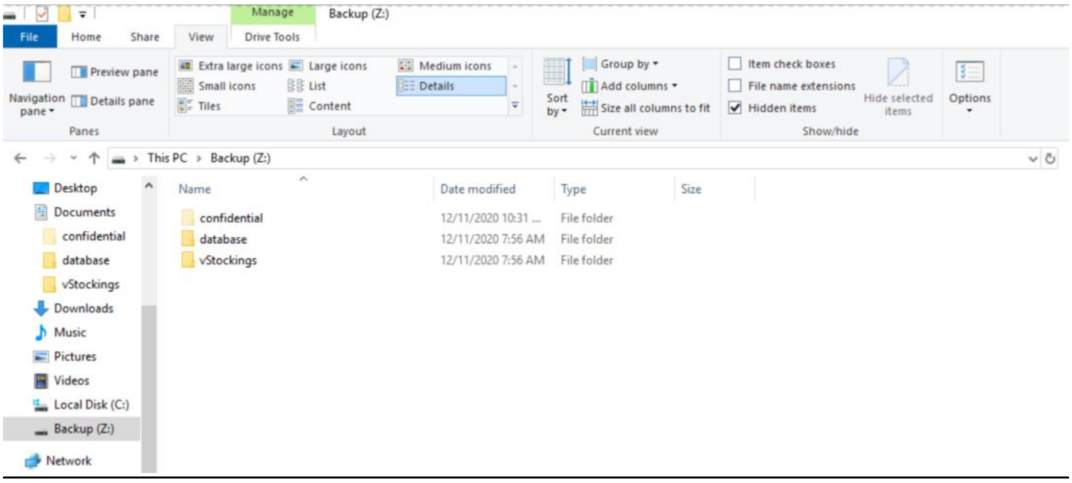
Name: ShadowCopyVolume{7a9eea15-0000-0000-0000-010000000000}
Location: \
Author: ELFSTATION4\Administrator
Description:

Security options
When running the task, use the following user account:
SYSTEM

○ Run only when user is logged on
● Run whether user is logged on or not
□ Do not store password. The task will only have access to local computer resources.
☑ Run with highest privileges
□ Hidden Configure for: Windows Server™ 2003, Windows® XP, or Windows® 2000

Question 7

In our backup drive, we clicked “View” to select for hidden items. This enabled us to view the hidden folder which is “confidential”.

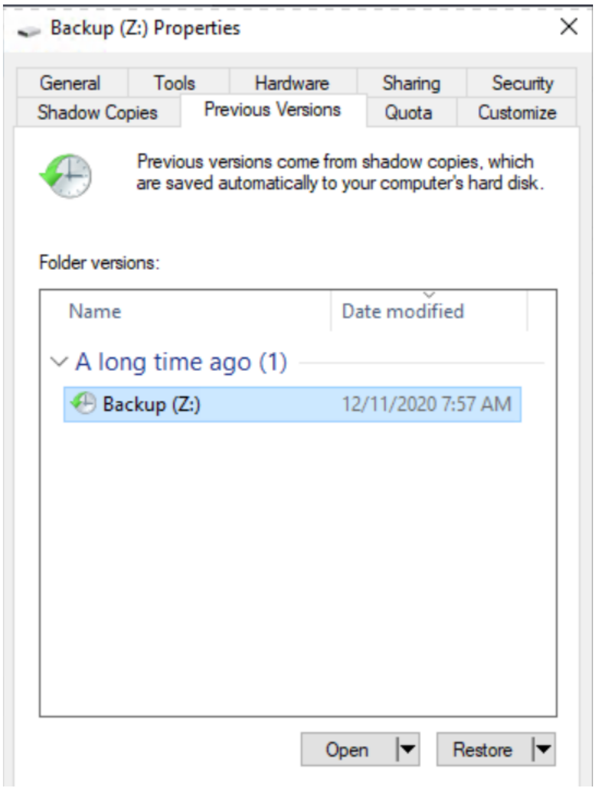


□ Item check boxes
□ File name extensions
☑ Hidden items

Name	Date modified	Type	Size
confidential	12/11/2020 10:31 ...	File folder	
database	12/11/2020 7:56 AM	File folder	
vStockings	12/11/2020 7:56 AM	File folder	

Question 8

We then right clicked on the confidential folder and inspected the properties. Then, we selected Previous Versions.



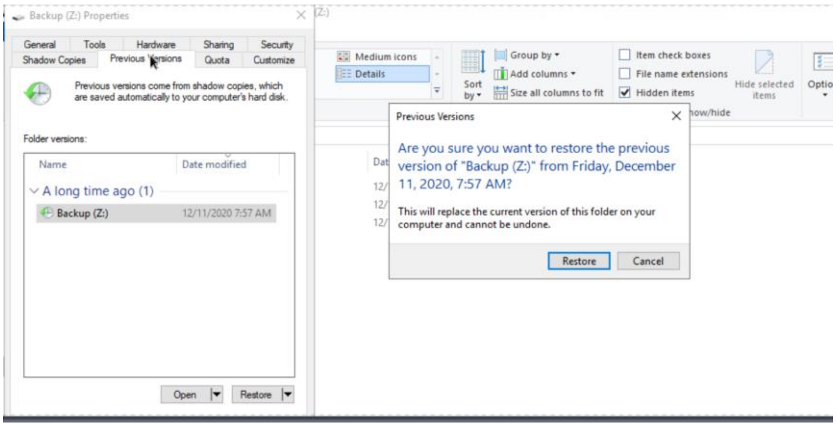
Backup (Z:) Properties

Previous versions come from shadow copies, which are saved automatically to your computer's hard disk.

Folder versions:

Name	Date modified
A long time ago (1)	
Backup (Z:)	12/11/2020 7:57 AM

Next, we clicked on the restore option in order to restore the previous versions of the backup file.



Previous versions come from shadow copies, which are saved automatically to your computer's hard disk.

Folder versions:

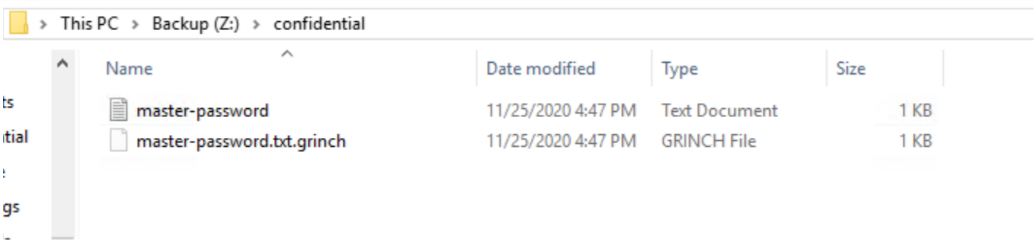
Name	Date modified
A long time ago (1)	
Backup (Z:)	12/11/2020 7:57 AM

Previous Versions

Are you sure you want to restore the previous version of "Backup (Z:)" from Friday, December 11, 2020, 7:57 AM?

This will replace the current version of this folder on your computer and cannot be undone.

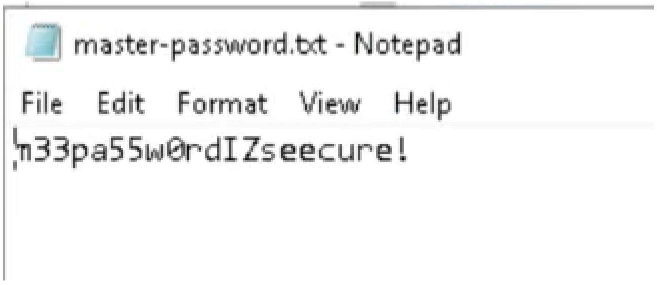
Once restored, we managed to obtain the master password text document.



This PC › Backup (Z:) › confidential

Name	Date modified	Type	Size
master-password	11/25/2020 4:47 PM	Text Document	1 KB
master-password.txt.grinch	11/25/2020 4:47 PM	GRINCH File	1 KB

When we clicked on it, we were shown the master password on the Notepad.



```
m33pa55w0rdIZseecure!
```

Thought Process/Methodology:

Firstly, we started the AttackBox as well as our machine. Then, we opened the terminal and used AttackBox and Remmina to connect to the remote machine via RDP(Remote Desktop Protocol). We proceeded on changing some settings in the application based on the given instructions. Then, at the new connection profile, we inserted the credentials given as well as the IP address and clicked on "Save and Connect" option in order to connect to the server. Once we managed to connect to the server, we noticed that the screen had a wallpaper that said, "THIS IS FINE". Next, we clicked on the file explorer and opened the ransom note that was placed on the desktop. When read, the note was written with a suspicious 'bitcoin address' which was known to be fake. Thus, we opened a new terminal to decrypt the fake address by using the method base64 and we received the plain text value. After that, we clicked on the confidential file and got the file extension which is ".grinch". We were then asked to find out the name of the suspicious scheduled task which was located in the Task Scheduler. Therefore, we opened Task Scheduler and managed to find the name which is "opidsfsdf". Later, we moved on to finding the location of the executable that is run at login regarding the scheduled task. So, from the same task, "opidsfsdf", we clicked on Actions in order to find the answer to our question. After that, we clicked on the task right below "opidsfsdf" which was "ShadowCopyVolume" as it was related to VSS. Then, we clicked on the properties at the bottom right corner to receive the ID of that task under the name category. We proceeded on opening the file explorer and clicked on the backup drive that we've saved. Once done, we clicked view to enable the "Hidden items" option. This enabled us to view the hidden folder which was "confidential". Finally, we inspected the properties of the confidential file. We selected Previous Versions and restored the previous version as it would restore the file within this hidden folder to the previous version. Once restored, we retrieved the password within the master password text document.