

The background is a dark navy blue. It features several thin, gold-colored lines that form abstract, angular shapes. These lines radiate from the central text box, extending towards the corners and edges of the frame, creating a sense of dynamic movement and geometric complexity.

# ROUND 3

FINAL PRACTICE IMAGE


Hololive X Troy Cyber

# Mistakes

I'm only human, it's obvious that I would make some mistakes; even more so when I'm the one bug testing my own work. Here's some of the mistakes that may have affected your image experience:

WRONG

Our current policies require that we need to share information on this computer on our network. We would like to have the folder "Cover Corp" located on the C: Drive to be available and shared on this computer. As such, please do not delete any **unauthorized** content found within this folder. (For best results, name the share to "Cover Corp")



A screenshot of a user profile form for a user named 'yagoo'. The form includes fields for First name, Last name, Display name, Description, and Office. The Display name field contains the text 'Tanigo Motayasu', where 'Motayasu' is highlighted in yellow. The Description field contains the text 'CEO of Cover Corporation'.

RIGHT

Our current policies require that we need to share information on this computer on our network. We would like to have the folder "Cover Corp" located on the C: Drive to be available and shared on this computer. As such, please do not delete any **authorized** content found within this folder. (For best results, name the share to "Cover Corp")



A screenshot of a user profile form for a user named 'yagoo'. The form includes fields for First name, Last name, Display name, Description, and Office. The Display name field contains the text 'Tanigo Motoyasu', where 'Motoyasu' is highlighted in yellow. The Description field contains the text 'CEO of Cover Corporation'.

# Score Breakdown

Forensics Questions	20
Users & Groups Auditing	18
Local Policies	6
Defensive Security Measures	9
Unauthorized Software	18
Unauthorized Media	10
Service Auditing	6
Uncategorized Operating	13
System Vulnerabilities	
	<hr/>
	100 pts total



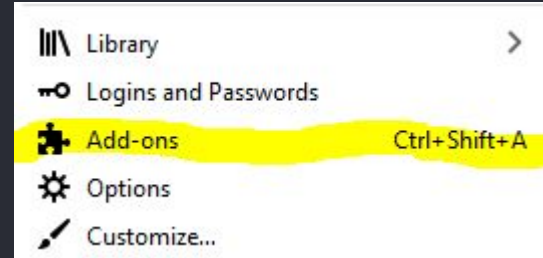
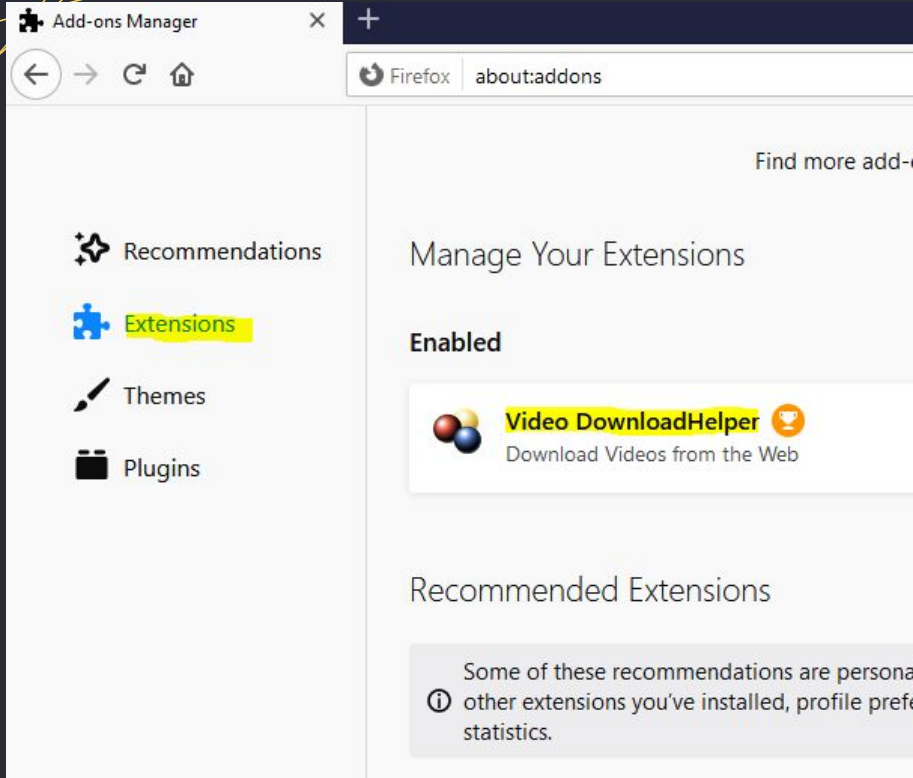
5



# Forensics Questions

20 Points Total

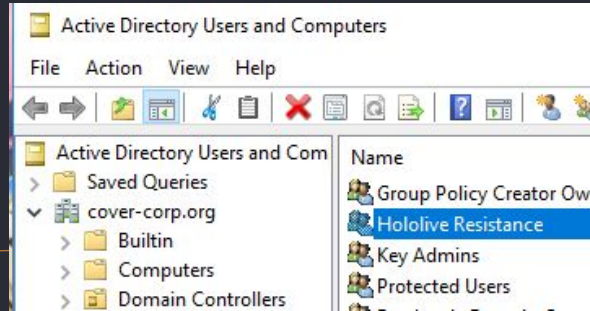
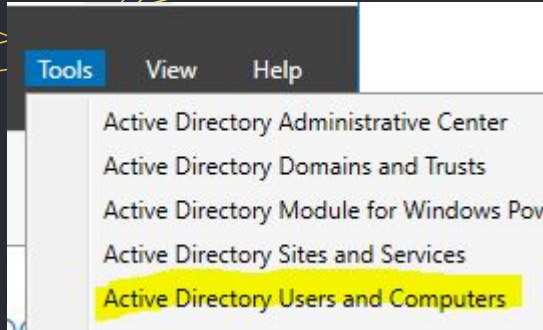
# Forensics Question 1 - 4 pts



What is the name of the Firefox Addon installed?

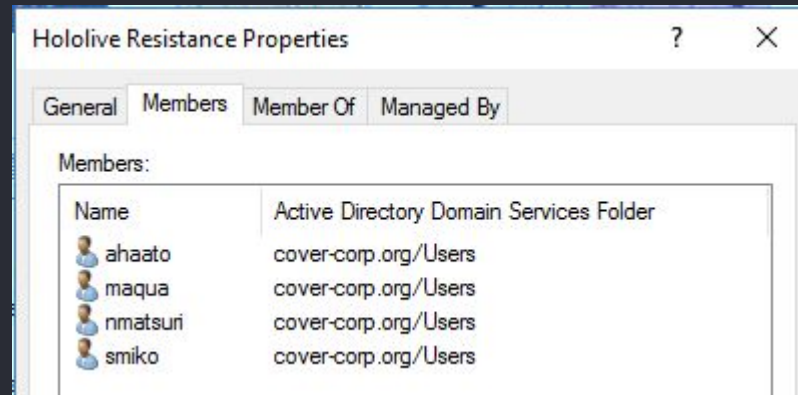
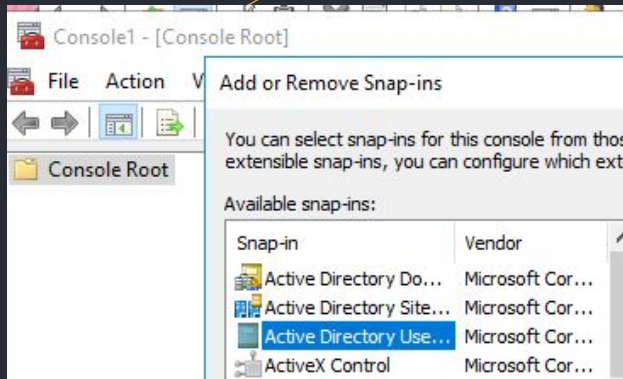
ANSWER: Video DownloadHelper

## Forensics Question 2 - 4 pts



What is the name of the group ahaato, maqua, nmatsuri, and smiko are in?

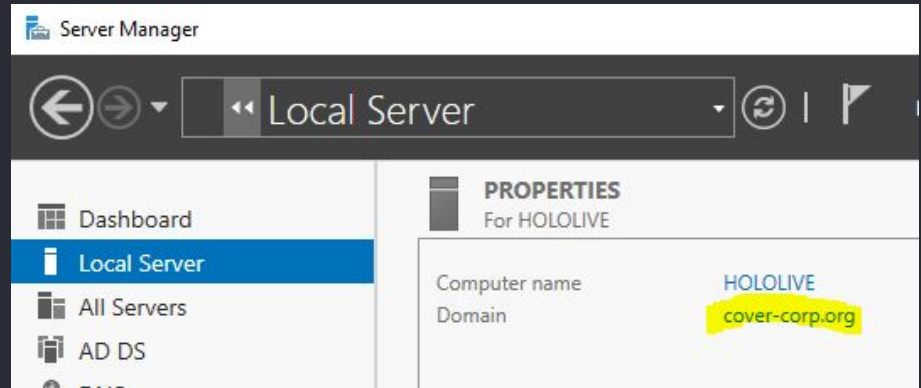
ANSWER: Hololive Resistance



# Forensics Question 3 - 4 pts

What is the domain name of this server?

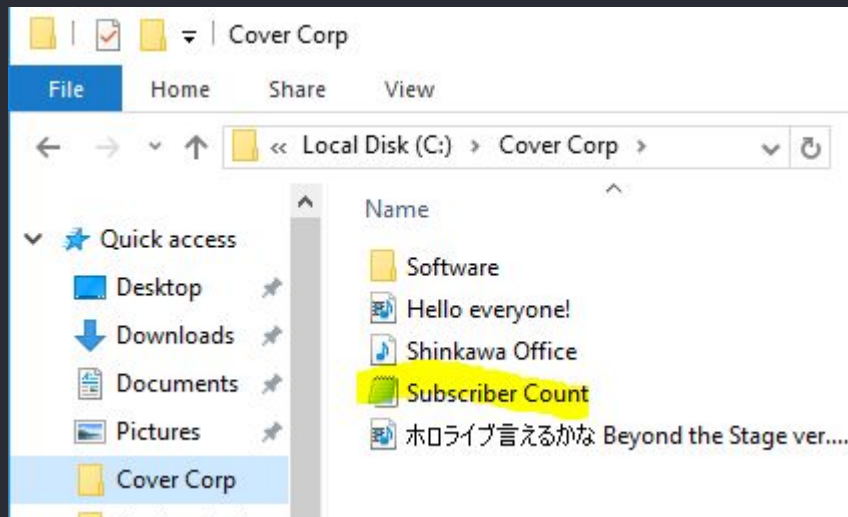
ANSWER: cover-corp.org



## Forensics Question 4 - 4 pts

Which talent has 902K subscribers during the latest data collection period?

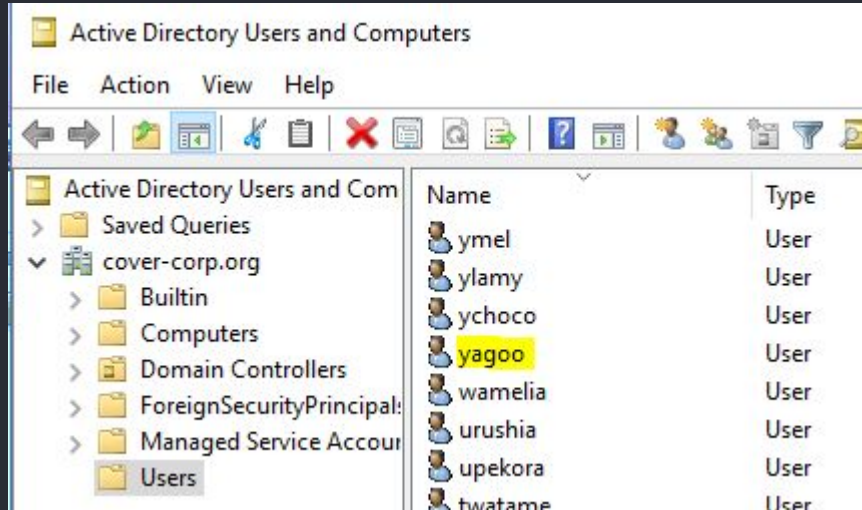
ANSWER: Kiryu Coco



Name	Belong	Subscribers	Round
Gawr Gura	English	"1,920,000"	2021-01-10 02:00 (1.9M)
Inugami Korone	Gamers	"1,240,000"	2020-12-28 03:50 (1.2M)
Shirakami Fubuki	1st	"1,170,000"	2020-12-12 14:20 (1.1M)
Usada Pekora	3rd	"1,150,000"	2020-12-28 21:10 (1.1M)
Minato Aqua	2nd	"984,000"	2020-12-10 22:40 (900K)
Houshou Marine	3rd	"962,000"	2020-12-28 08:00 (900K)
Mori Calliope	English	"921,000"	2021-01-07 20:50 (900K)
Kiryu Coco	4th	"902,000"	2021-01-11 08:40 (900K)
Akai Haato	1st	"894,000"	2020-11-27 20:40 (800K)
Watson Amelia	English	"886,000"	2020-12-23 03:50 (800K)



## Forensics Question 5 - 4 pts



What is the full name of yagoo?

ANSWER: Tanigo Motoyasu

yagoo

First name:  Initials:

Last name:

Display name:

Description:

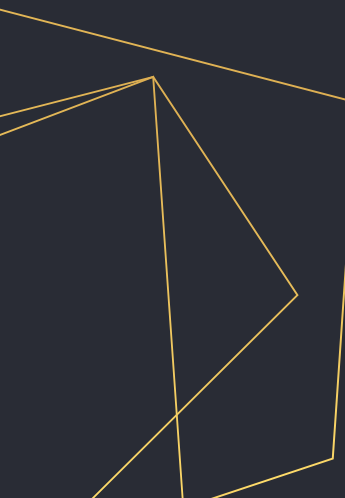
Office:



5

# Users & Groups Auditing

18 Points Total



# Unauthorized Users

"hchris" is not an  
authorized user

4 pts

"ahaato" is not an  
authorized user

4 pts

"maloe" is not an  
authorized user

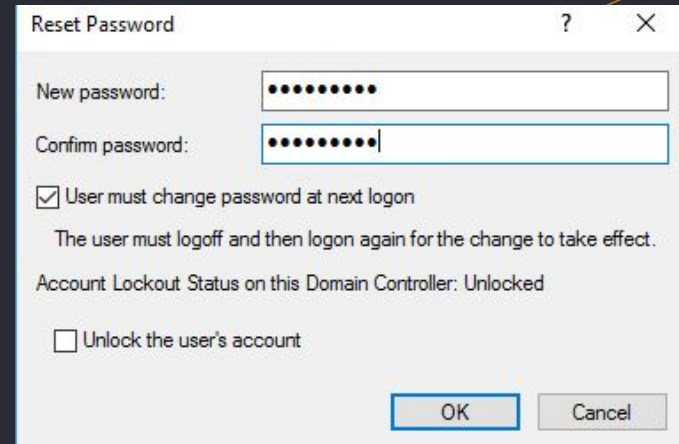
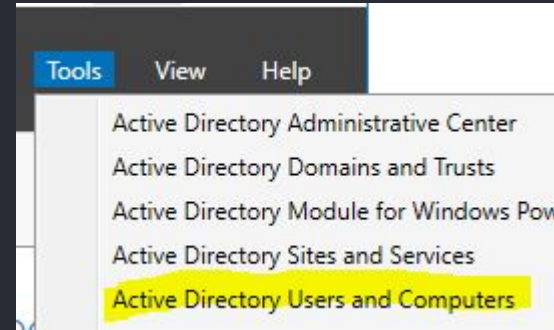
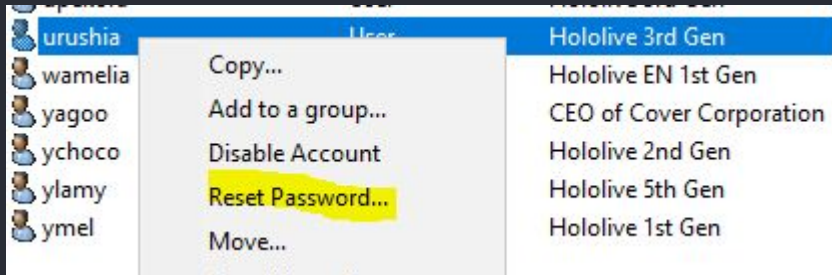
4 pts

**Note:** Either disabling or deleting users will count toward these points. However, disabling is preferable in case you deleted the wrong user.

# Passwords

"urushia" now has a secure password

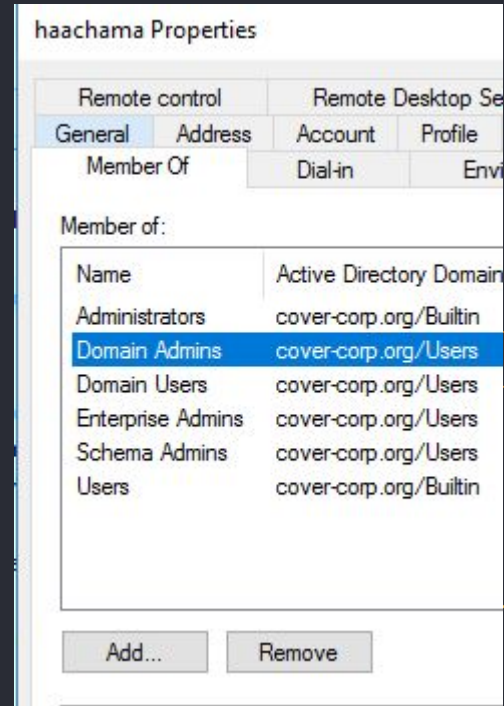
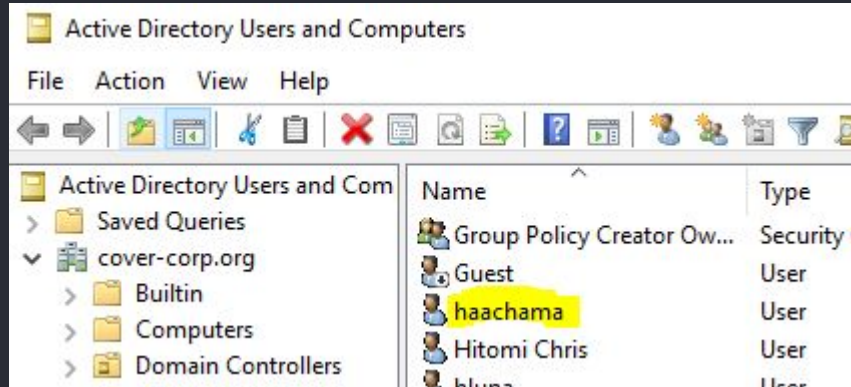
4 pts



# Groups

"haachama" removed from  
Domain Admins group

2 pts



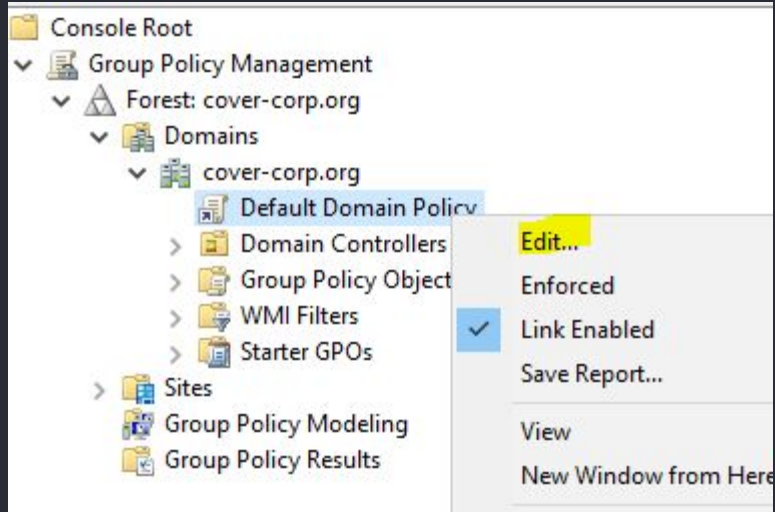


2

# Local Policies

6 Points Total

# Changing Policies on a Domain Controller



Find the Group Policy Management Tool and Edit the Default Domain Policy. When finished, run the command “gpupdate /force” in the command prompt

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\achan>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

# Account Policies

Password Complexity  
Required Enabled  
3 pts

Minimum Password Length  
Larger than 14  
3 pts





2

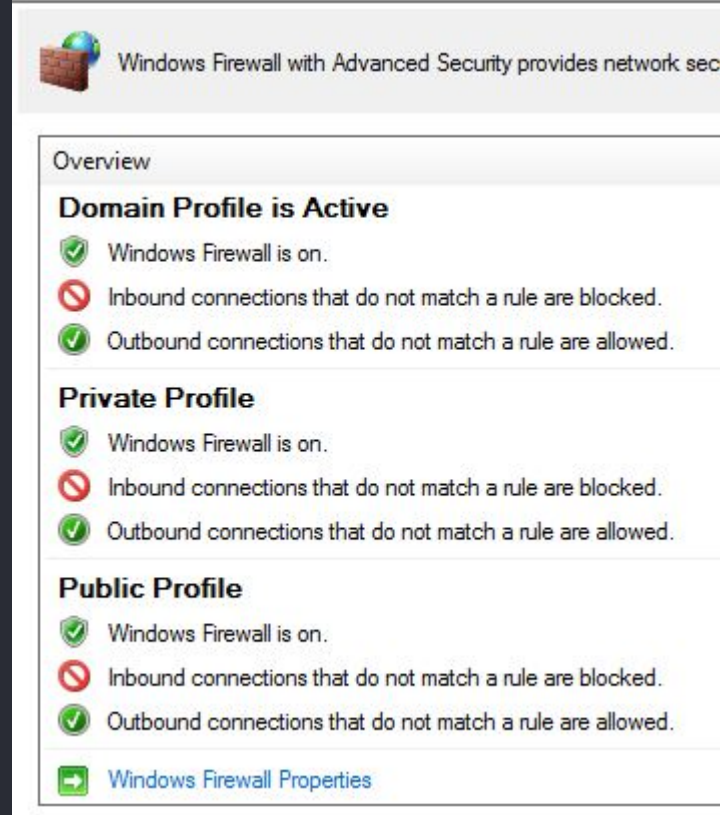
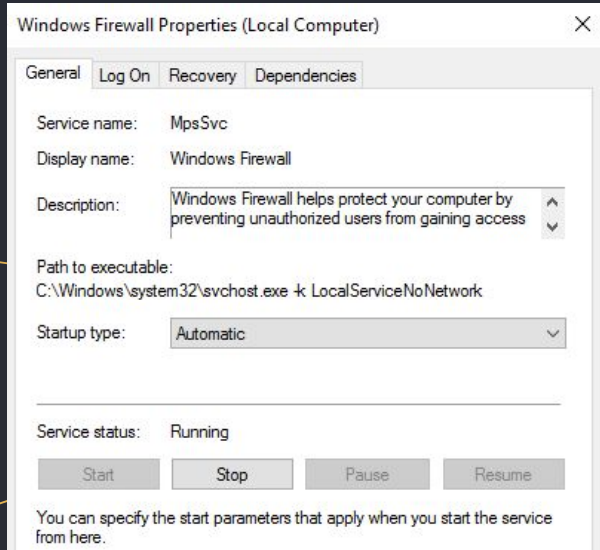


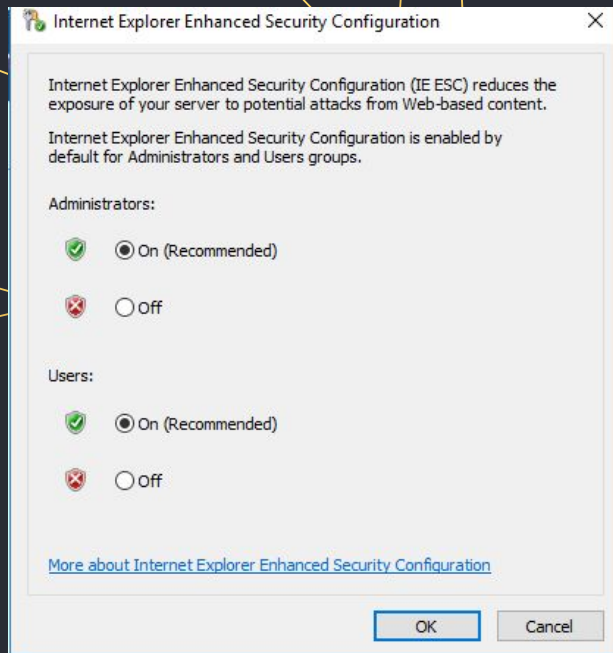
# Defensive Security Measures

9 Points Total

# Firewall Enabled

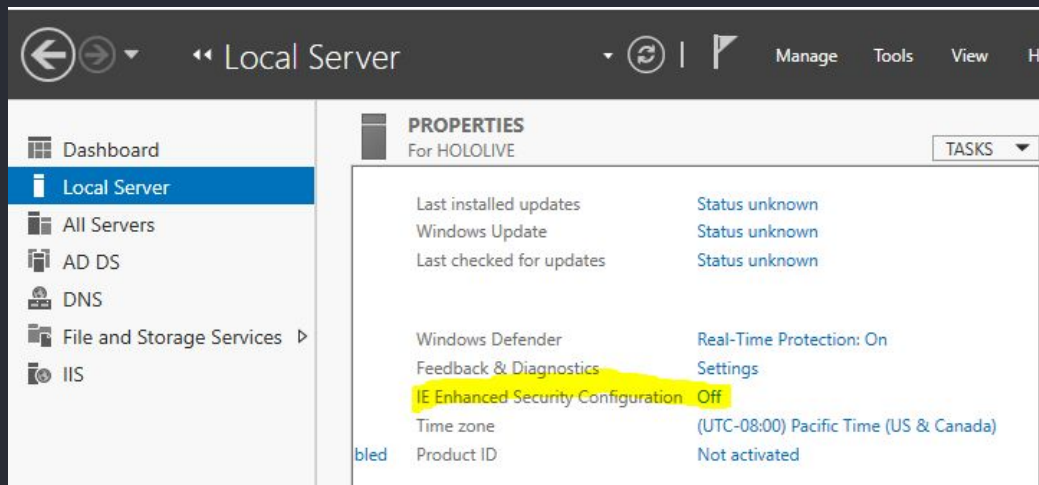
5 pts





# IE ESC Enabled

4 pts





3



# Unauthorized Software

18 Points Total

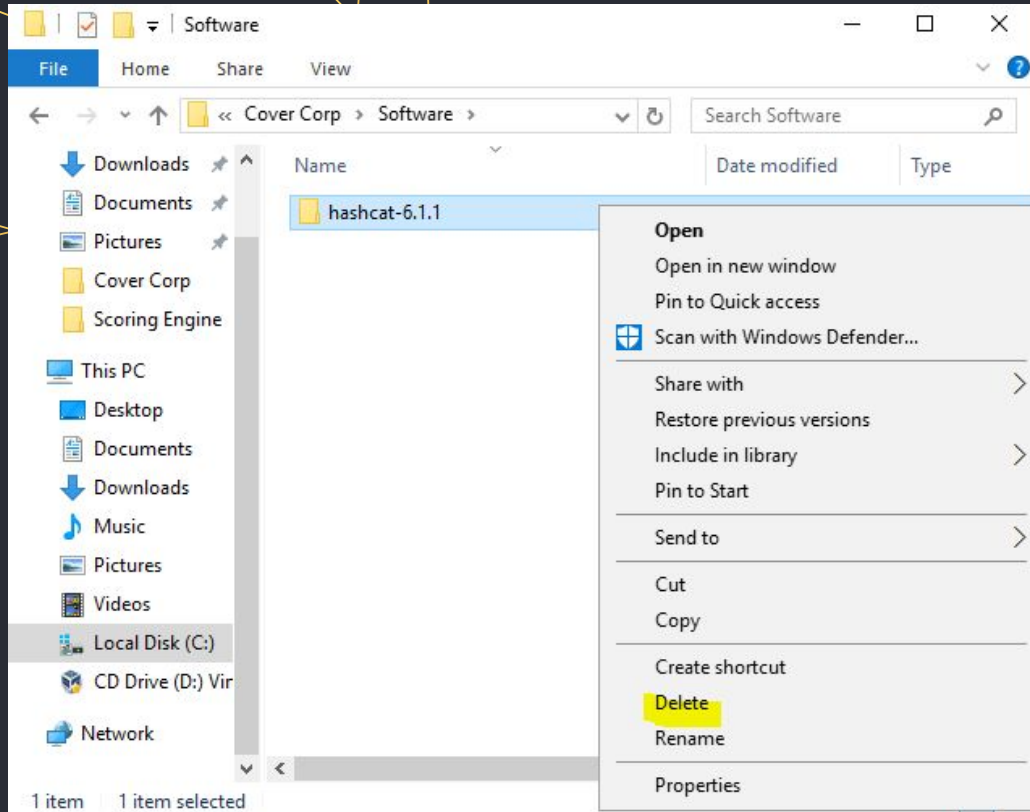
# Installed Programs

Steam has been uninstalled

5 pts

Nmap has been uninstalled

5 pts



Hashcat has been  
uninstalled

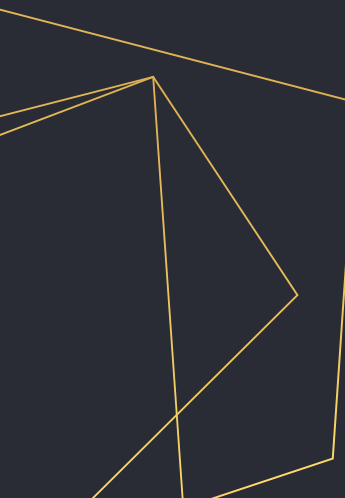
8 pts



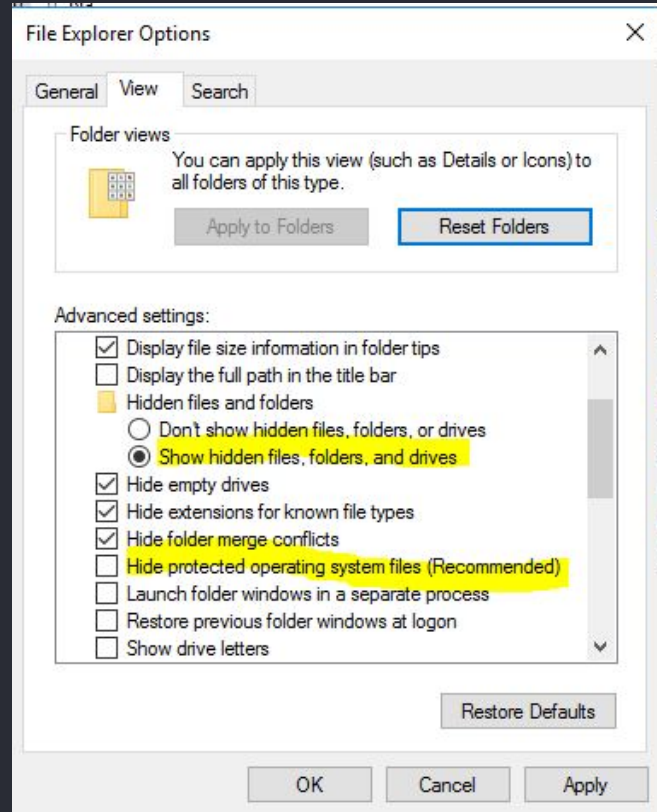
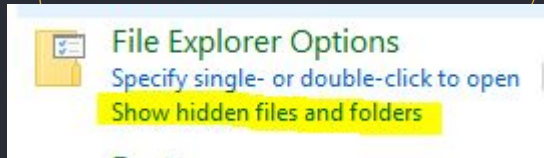
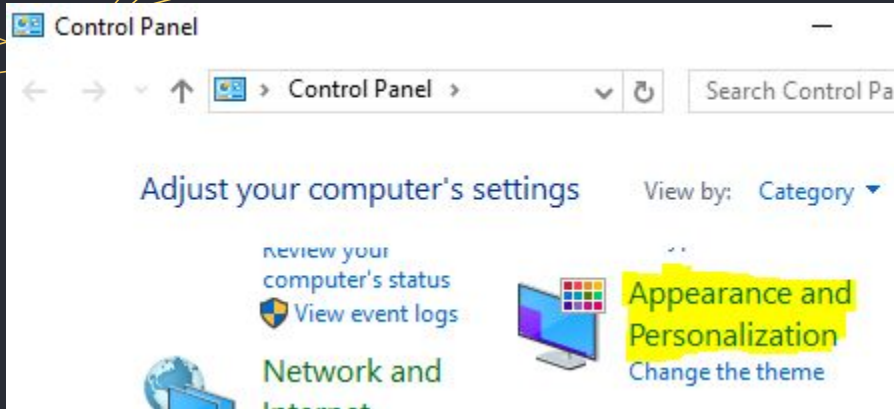
3

# Unauthorized Media

10 Points Total



# Showing Hidden Folders and Files





# Unauthorized Media

Unauthorized media has  
been removed

C:\Users\yagoo\Desktop  
\yagoos\_dream.jpg

2 pts

Hidden media has been  
removed

C:\Users\sfubuki\Videos\  
scatman.mp4

3 pts

Super hidden media has  
been removed

C:\Users\achan\Desktop  
\tsundere\_voice.mp3

5 pts

**Note:** To find hidden folders and files a lot easier, use file browsing software such as Everything or UltraSearch



2

# Service Auditing

6 Points Total

# Services

IP Helper service disabled

3 pts

Windows Update service enabled

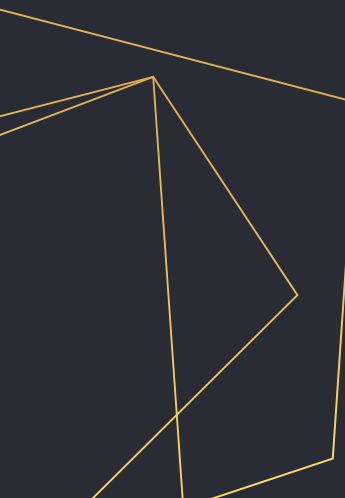
3 pts



3

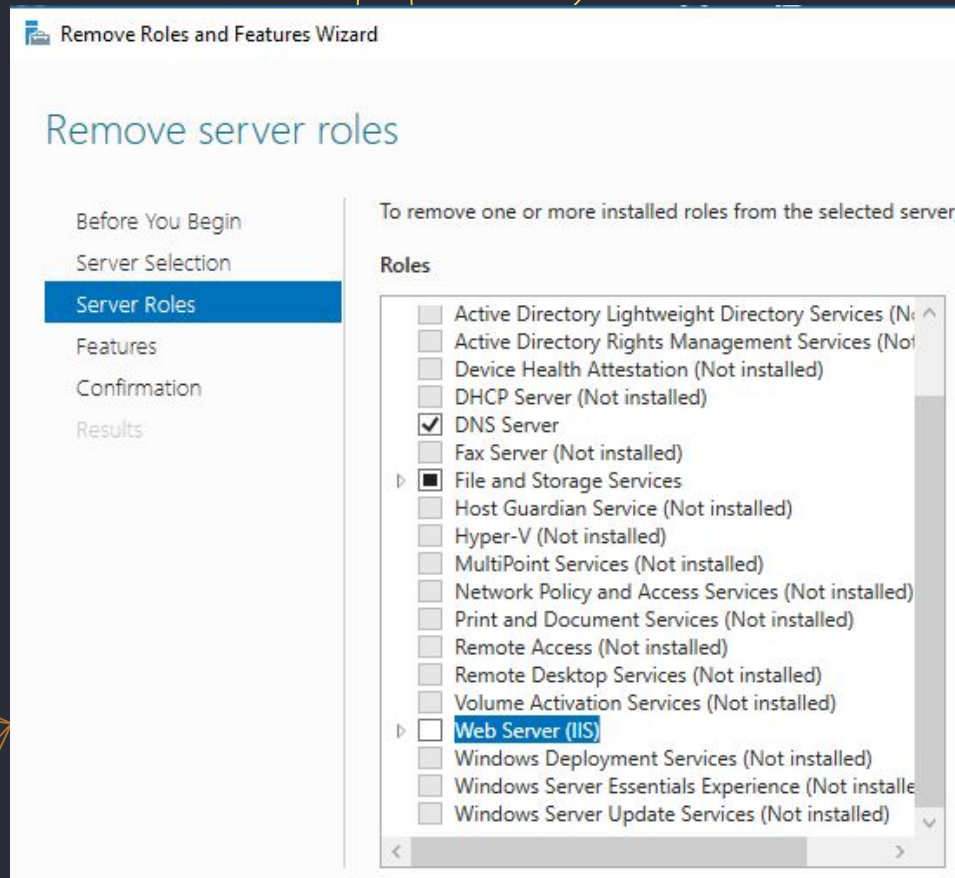
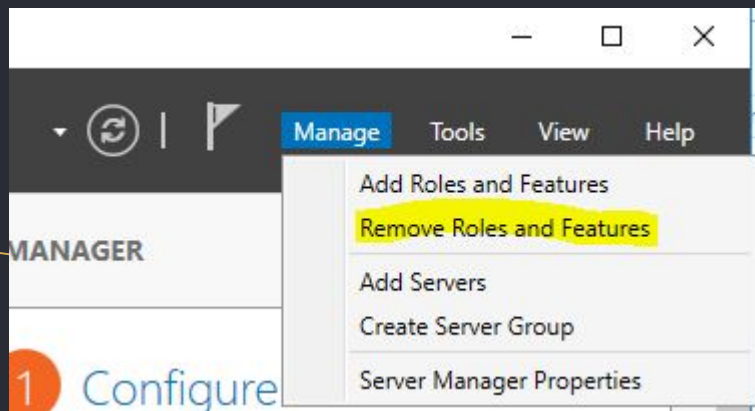
# Uncategorized Operating System Vulnerabilities

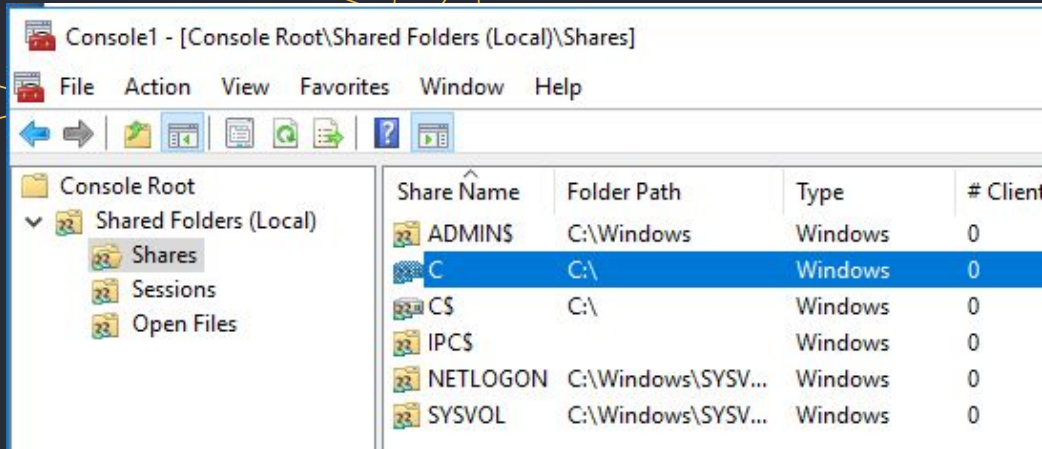
13 Points Total



# IIS uninstalled

5 pts





"C:" is unshared

4 pts

“Cover Corp” is  
shared with everyone

4 pts

Create A Shared Folder Wizard

**Name, Description, and Settings**  
Specify how people see and use this share over the network.

Type information about the share for users. To modify how people use the content while offline, click Change.

Share name:

Share path:

Description:

Offline setting:

< Back **Next >** Cancel



# 5

## Unscored Vulnerabilities

Not scored due to limitations  
in the Scorpio Program





# Firefox Settings

HTTPS-Only Mode  
Enabled

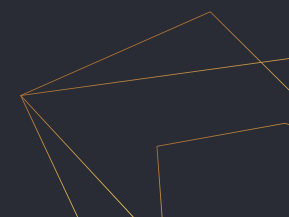
Ask for Certificates &  
Query for Validity

Block Dangerous and  
Deceptive Content

Block Pop-up Windows

Warn When Websites Try  
to Install Add-ons

Remove Video  
DownloadHelper



# Other Settings

Group "Hololive  
Resistance" removed

OBS is updated

UAC and Smart Screen  
Turned ON

Remote Desktop  
Turned OFF

## 100 out of 100 points received

**Connection Status:** Scoring Data Uploaded Successfully: No Errors Detected

Internet Connectivity Check: OK

Scorpio Connection Status: OK

Scorpio Score Upload Status: FAILED - Reason: Could not connect to server

**0 penalties assessed, for a loss of 0 points:**

**25 out of 25 scored security issues fixed, for a gain of 100 points:**

Forensics Question 1 Solved - 4 pts

Forensics Question 2 Solved - 4 pts

Forensics Question 3 Solved - 4 pts

Forensics Question 4 Solved - 4 pts

Forensics Question 5 Solved - 4 pts

"hchris" is not an authorized user - 4 pts

"ahaato" is not an authorized user - 4 pts

"maloe" is not an authorized user - 4 pts

"urushia" now has a secure password - 4 pts

"haachama" removed from "Domain Admins" group - 2 pts

Password Complexity Required - 3 pts

Minimum Password Length longer than 14 - 3 pts

Firewall Enabled - 5 pts

IIS uninstalled - 5 pts

Windows Update service is running - 3 pts

IP Helper service is disabled - 3 pts

"C:\Cover Corp" is shared with everyone - 4 pts

"C:" is unshared - 4 pts

Unauthorized media has been removed - 2 pts

Hidden media has been removed - 3 pts

Super hidden media has been removed - 5 pts

Steam has been uninstalled - 5 pts

Nmap has been uninstalled - 5 pts

Hashcat has been uninstalled - 8 pts

IE ESC enabled - 4 pts