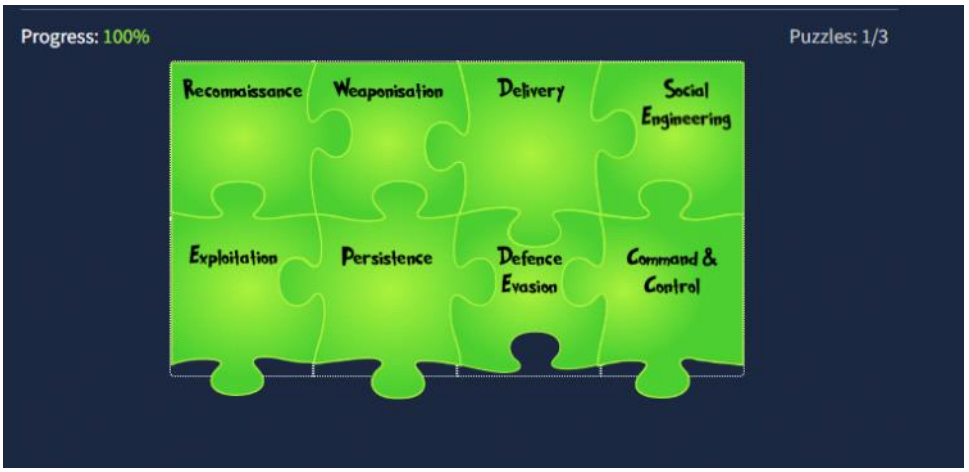
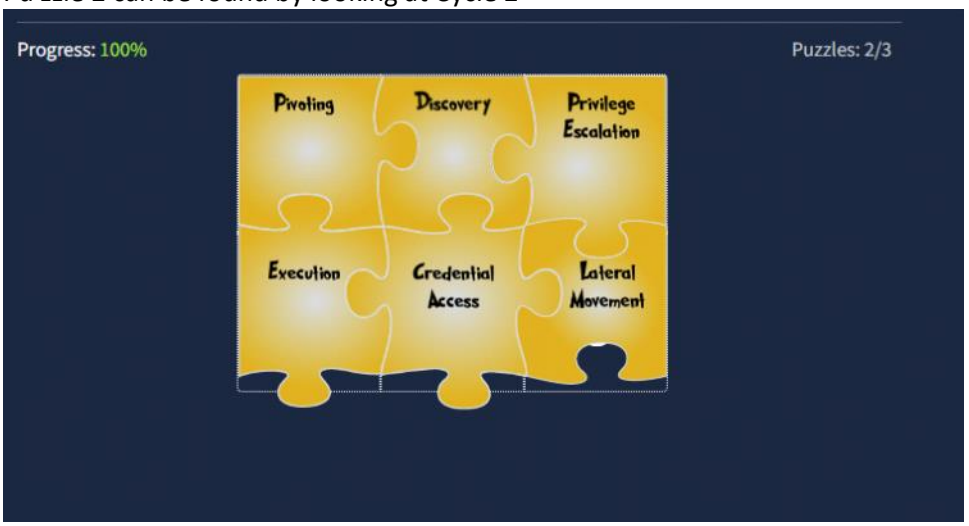
AOC 2022 writeup

Tuesday, August 2, 2022 12:17 PM

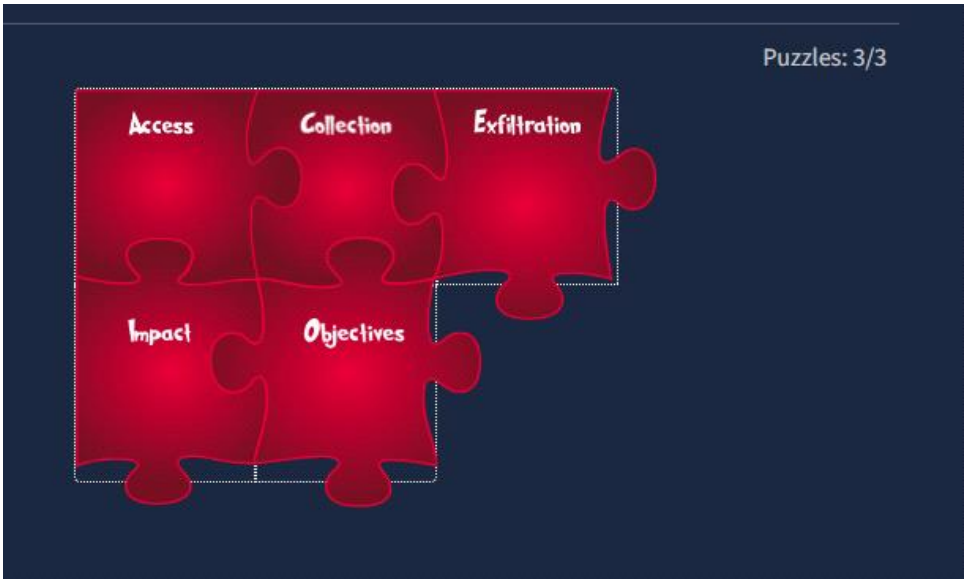
Day 1
You need to spin up the vm and solve 3 puzzles for
Puzzle 1 can be found by looking at Cycle 1: In of the unified cyber kill chain . These stage helps a hacker get **in.**



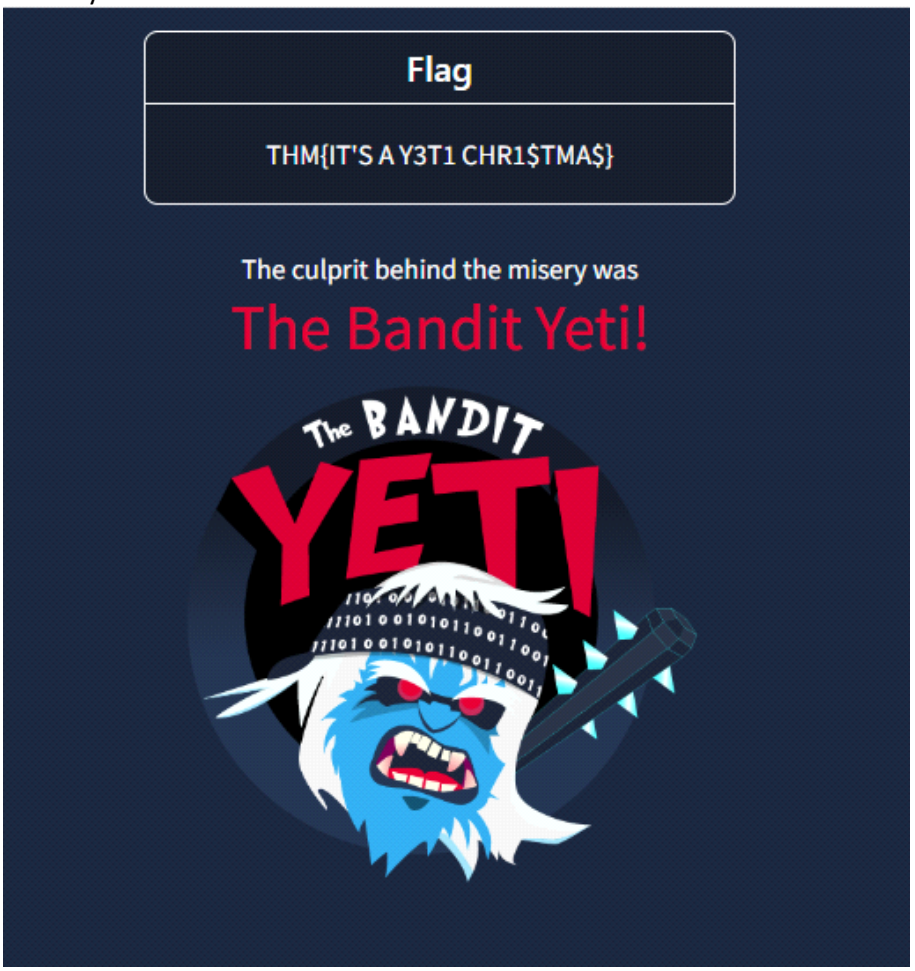
Pu zzle 2 can be found by looking at Cycle 2



Puzzle 3: Cycle 3 Out
NOTE: A key element that one may think is missing is Access. This is not formally covered as a phase of the UKC, as it overlaps with other phases across the different levels, leading to the adversary achieving their goals for an attack.



You need to finish all 3 puzzles and click finish. This then allows you to see a new screen with the flag and the name of the adversary. This is a classic defacement . When a hacker hacks into a site they will sometimes leave some sort of signature to say they hacked it. The hacker left behind a flag , their name and a symbol



1. Who is the adversary that attacked Santa's network this year? The Bandit Yeti
2. What's the flag that they left behind?THM{IT'S A Y3T1 CHR1TMA}
3. Looking to learn more? Check out the rooms on Unified Kill Chain, Cyber Kill Chain, MITRE, or the whole Cyber Defence Frameworks module! No answer needed

Day 2

1.Ensure you are connected to the deployable machine in this task. No answer needed

2.Use the `ls` command to list the files present in the current directory. How many log files are present?

answer is 2

we see SSHD.log and webserver.log

```
elfmcblue@day-2-log-analysis:~$ ls -lah
total 19M
drwxr-xr-x 3 elfmcblue elfmcblue 4.0K Dec  2 19:13 .
drwxr-xr-x 5 root      root      4.0K Nov 21 14:56 ..
-rw------- 1 elfmcblue elfmcblue    3 Dec  2 19:13 .bash_history
-rw-r--r-- 1 elfmcblue elfmcblue  220 Nov 21 14:56 .bash_logout
-rw-r--r-- 1 elfmcblue elfmcblue 3.7K Nov 21 14:56 .bashrc
drwx------ 2 elfmcblue elfmcblue 4.0K Dec  2 19:13 .cache
-rw-r--r-- 1 elfmcblue elfmcblue  807 Nov 21 14:56 .profile
-rw-r--r-- 1 elfmcblue elfmcblue 219K Nov 30 13:27 SSHD.log
-rw-r--r-- 1 elfmcblue elfmcblue  19M Nov 21 14:56 webserver.log
```

3.Elf McSkidy managed to capture the logs generated by the web server. What is the name of this log file? Webserver.log we see a log named webserver.log which is the log file elfmcblue made as seen from the owner of the file . We assume the elfmcblue is the account associated with Elf McSkidy due to the similarities between the username and Elf's actual name.

Webserver.log

4.Begin investigating the log file from question #3 to answer the following questions. No answer needed

```
elfmcblue@day-2-log-analysis:~$ cat webserver.log | grep santa
10.10.249.191 - - [18/Nov/2022:12:28:16 +0000] "GET /santa HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:28:17 +0000] "GET /santa claus HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:28:17 +0000] "GET /evilsanta HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:28:18 +0000] "GET /santana HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:28:18 +0000] "GET /santabarbara HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:34:39 +0000] "GET /santaslist.txt HTTP/1.1" 200 133872 "-" "Wget/1.19.4 (linux-gnu)"
10.10.249.191 - - [18/Nov/2022:12:35:18 +0000] "GET /santafe HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:35:18 +0000] "GET /jasonsantamar-20 HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:35:18 +0000] "GET /santa maria maggiore HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:35:18 +0000] "GET /santa-clara-county HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:35:20 +0000] "GET /texas-santa-barbara HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:35:21 +0000] "GET /topicsantafe HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:35:22 +0000] "GET /jasonsantamaria HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
10.10.249.191 - - [18/Nov/2022:12:35:27 +0000] "GET /carlossantana 75 HTTP/1.1" 404 437 "-" "gobuster/3.0.1"
```

Cat webserver.log | grep santa

We used cat to show the contents of the log file on the terminal but since showing every line in the log is undesirable since its very long we used | and grep santa to filter out irrelevant content and only show log entries with the word santa in it .

5.On what day was Santa's naughty and nice list stolen? Friday we can see from the log file output that all entries in the log with the word santa in it were made on november 18 which a goolge search shows us was a friday

6.What is the IP address of the attacker?

7.What is the name of the important list that the attacker stole from Santa? We see a file mentioned in the above screenshot called santaslist.txt so the answer is santalist.txt

8.Look through the log files for the flag. The format of the flag is: THM{}

elfmcblue@day-2-log-analysis:~$ cat webserver.log | grep THM

10.10.249.191 - - [18/Nov/2022:12:35:20 +0000] "GET /AU7VTHM1YVYV8 HTTP/1.1" 404 437 "-" "gobuster/3.0.1"

elfmcblue@day-2-log-analysis:~$ cat SSHD.log | grep THM

THM{STOLENSANTASLIST}

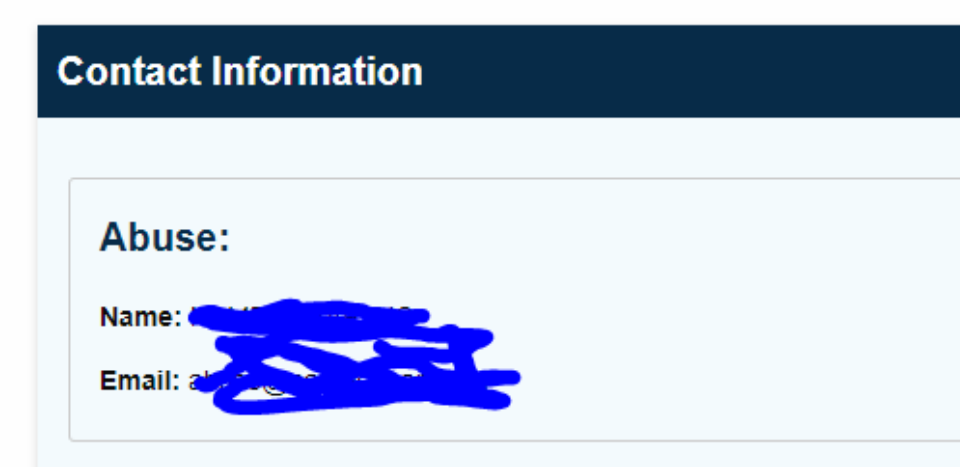
9.Interested in log analysis? We recommend the Windows Event Logs room or the Endpoint

Security Monitoring Module no answer needed

Day 3

1.What is the name of the Registrar for the domain santagift.shop?

Go to https://lookup.icann.org/en/lookup and lookup santagift.shop look for the abuse section of the contact information box



ANSWER:namecheap inc

2.Find the website's source code (repository) on github.com and open the file containing sensitive credentials. Can you find the flag?

search for santasgiftshop in github and look for config.php look at line 2
ANSWER:{THM_OSINT_WORKS}

3.What is the name of the file containing passwords? Look at the previous question for your answer

Answer: config.php
4.What is the name of the QA server associated with the website? Look through the readme file of the github repo
Answer:qa.santagift.shop

5.What is the DB_PASSWORD that is being reused between the QA and PROD environments? Scroll through the config.php file

Answer:S@nta2022
6.Check out this room if you'd like to learn more about Google Dorking!

No answer needed
Day 4

We did a nmap scan with the –sC and –sV flags because it gives us more information than nmap –ss.

```
Sc is equivalent to --script=default and scans using the default
discovery nse script which ouputs a lot of potentially useful info on
```

the host .

SV gives us a list of running services on a live host

See https://linux.die.net/man/1/nmap or https://nmap.org/book/nse-usage.html for more info on nmap switches and nse scripts.

nmap -sC -sV 10.10.214.44

Starting Nmap 7.60 (https://nmap.org) at 2022-12-05 21:52 GMT

Nmap scan report for ip-10-10-214-44.eu-west-1.compute.internal (10.10.214.44)

Host is up (0.00077s latency).

Not shown: 996 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 b1:f7:44:4a:ff:ae:3f:38:a4:b8:e2:f2:d1:59:16:86 (RSA)

| 256 03:bf:3d:33:1f:93:05:05:e8:7f:32:15:12:20:22:34 (ECDSA)

|_ 256 49:7b:e8:49:1f:77:a5:26:08:50:79:a1:70:6e:6a:92 (EdDSA)

80/tcp open http Apache httpd 2.4.29 ((Ubuntu))

|_http-server-header: Apache/2.4.29 (Ubuntu)

|_http-title: Apache2 Ubuntu Default Page: It works

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)

MAC Address: 02:5B:2E:66:DF:25 (Unknown)

Service Info: Host: IP-10-10-214-44; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:

|_nbstat: NetBIOS name: IP-10-10-214-44, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

| smb-os-discovery:

| OS: Windows 6.1 (Samba 4.7.6-Ubuntu)

| Computer name: ip-10-10-214-44

| NetBIOS computer name: IP-10-10-214-44\x00

| Domain name: eu-west-1.compute.internal

| FQDN: ip-10-10-214-44.eu-west-1.compute.internal

|_ System time: 2022-12-05T21:52:24+00:00

| smb-security-mode:

| account_used: guest

| authentication_level: user

| challenge_response: supported

|_ message_signing: disabled (dangerous, but default)

| smb2-security-mode:

| 2.02:

|_ Message signing enabled but not required

| smb2-time:

| date: 2022-12-05 21:52:24

|_ start_date: 1600-12-31 23:58:45

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 13.64 seconds

1.What is the name of the HTTP server running on the remote host?

Snipped from the nmap scan

80/tcp open http Apache httpd 2.4.29 ((Ubuntu))

|_http-server-header: Apache/2.4.29 (Ubuntu)

|_http-title: Apache2 Ubuntu Default Page: It works

Well http's port is port 80 for this server and we see from our nmap result that the http-title page is called Apache2 Ubuntu Default Page, so we assume the name of server is apache.

Answer:Apache

2.What is the name of the service running on port 22 on the QA server? Well we can see from our nmap scan that the service on port 22 is named ssh

Snipped from nmap scan

22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 b1:f7:44:4a:ff:ae:3f:38:a4:b8:e2:f2:d1:59:16:86 (RSA)

| 256 03:bf:3d:33:1f:93:05:05:e8:7f:32:15:12:20:22:34 (ECDSA)

|_ 256 49:7b:e8:49:1f:77:a5:26:08:50:79:a1:70:6e:6a:92 (EdDSA)

Answer: ssh

3.What flag can you find after successfully accessing the Samba service?

Remember how this is the qa server from the previous days osint task. In the last task we did some osint on the github and we found a username and password

- Username: ubuntu
- Password: S@nta2022

Lets see if we can make these credentials useful.
We see from the following snippet of our nmap scan that we can log in using smb

smb-security-mode:

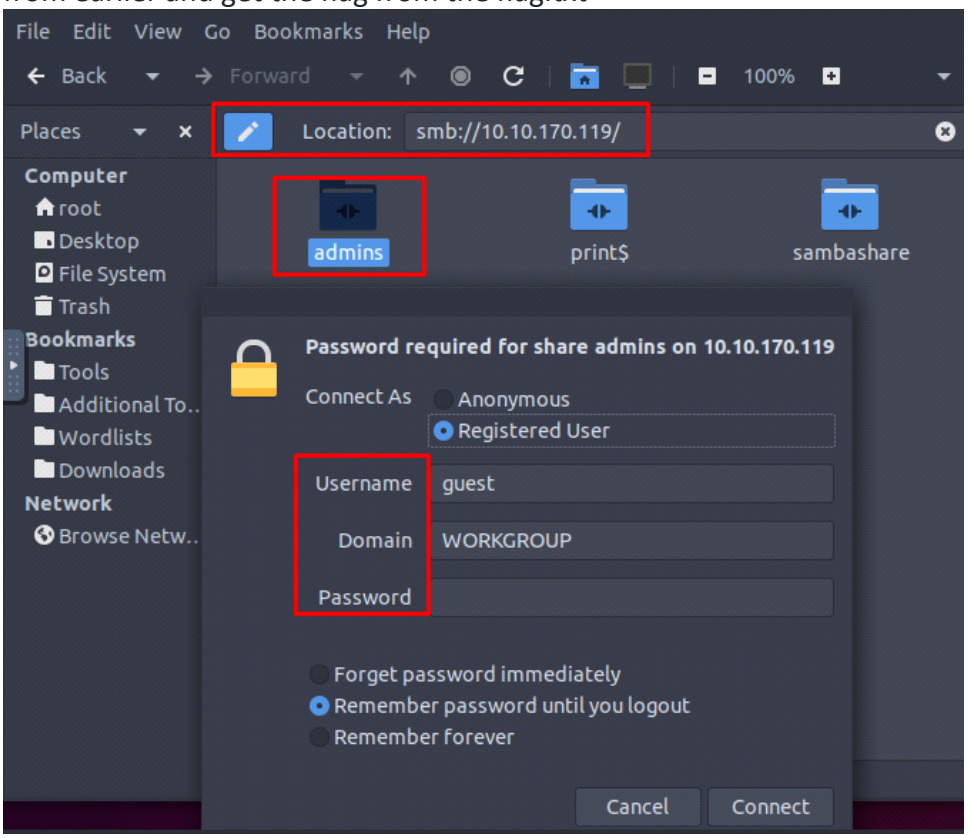
| account_used: guest

| authentication_level: user

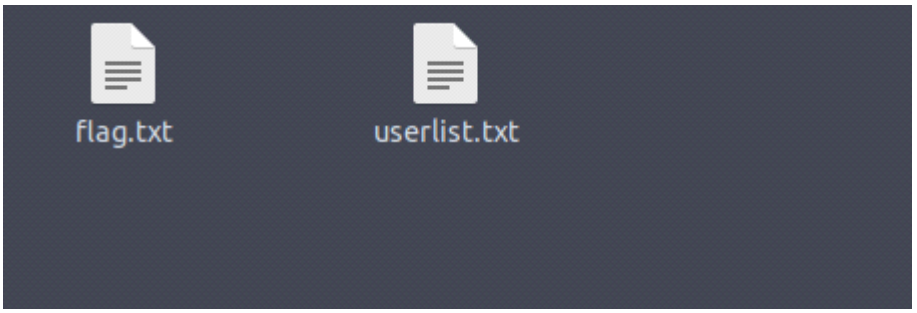
| challenge_response: supported

|_ message_signing: disabled (dangerous, but default)

So lets try the above credentials to login to the smb part of the server.
Navigate to your file explorer on kali linux like pictured below and type in smb:victimip
Select the admins section and it will prompt you to login . Put the username and password from earlier and get the flag from the flag.txt



Answer: {THM_SANTA_SMB_SERVER}



4.What is the password for the username santahr?

Check the userlist.txt file from the previous question. There will be a list of usernames and passwords there including the password for santahr. Note save the contents of this file for later rooms. There is chance they will prove useful in future rooms.

Answer: santa25

5.If you want to learn more scanning techniques, we have a module dedicated to Nmap!

https://tryhackme.com/module/nmap

no answer needed
USERNAME PASSWORD

santa santa101

santahr santa25

santaciso santa30

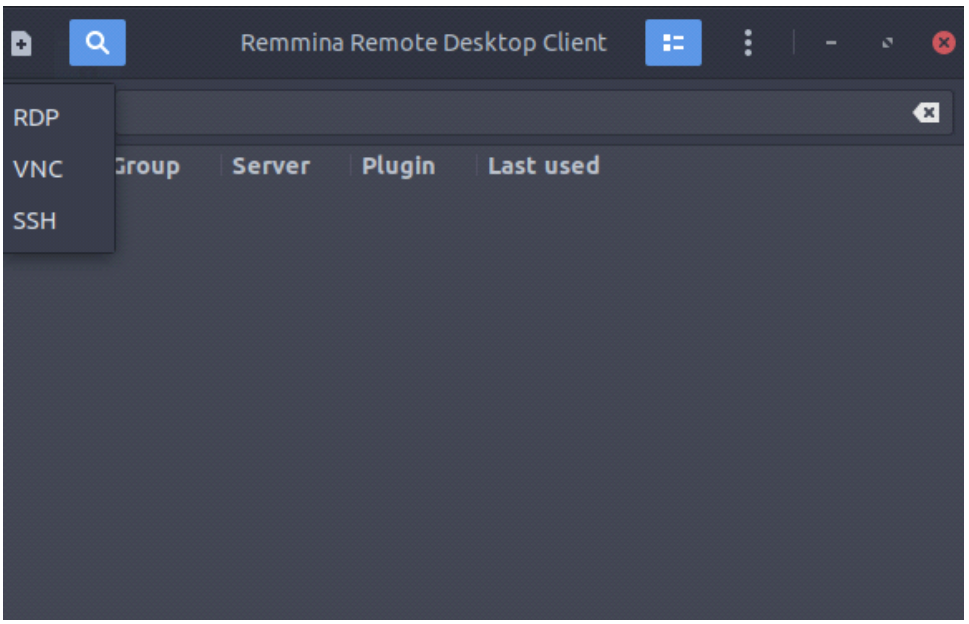
santatech santa200

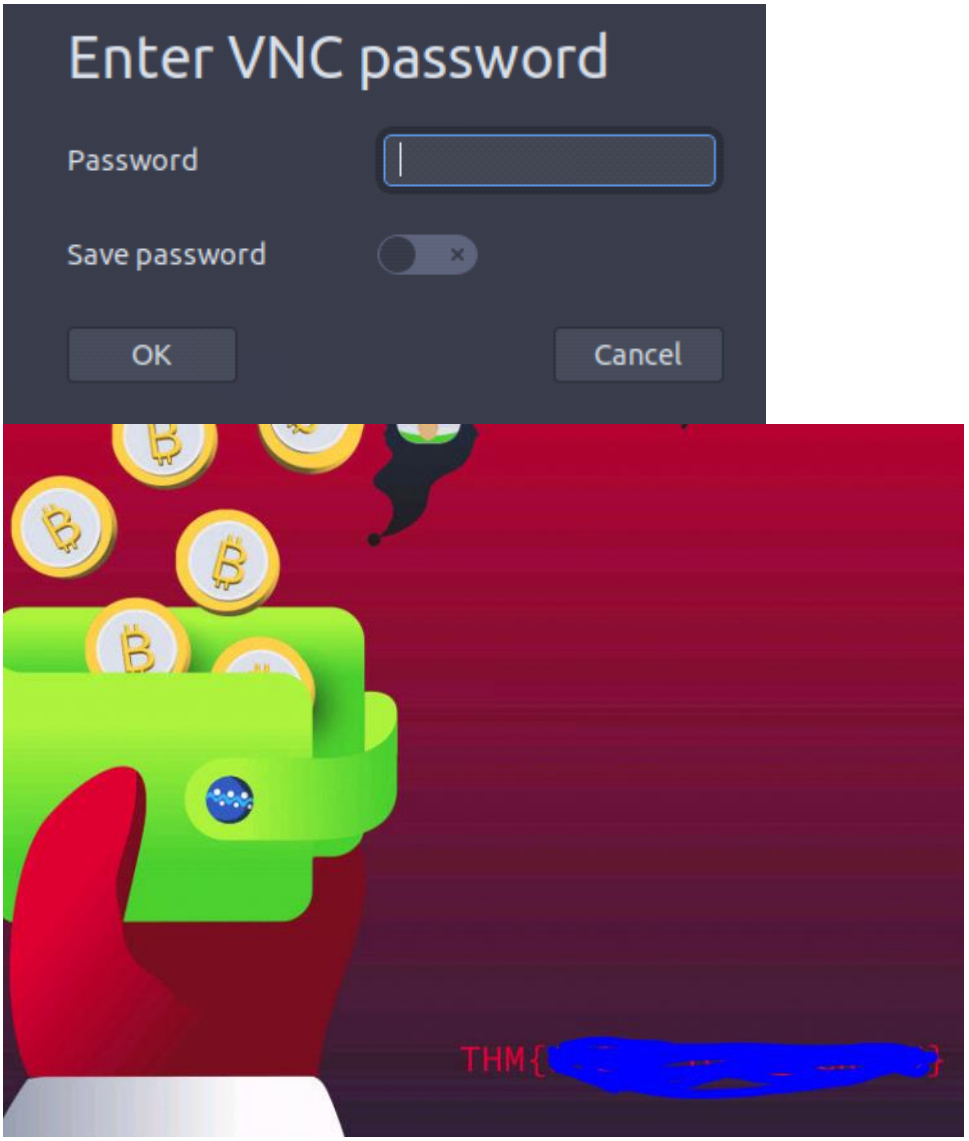
santaaccounts santa400
Day 5

1.Use Hydra to find the VNC password of the target with IP address `10.10.140.61`. What is the password? Run hydra using the following command
hydra -P /usr/share/wordlists/rockyou.txt 10.10.140.61 vnc
-P passes a wordlist with the file path 10.10.140.61 is the ip address of the server and vnc is the name of the serrvice we are attacking
Answer:1q2w3e4r

2.Using a VNC client on the AttackBox, connect to the target of IP address `10.10.140.61`. What is the flag written on the target's screen?

Use remmina to connect ,select the vnc option and put in the target ip address. A prompt will show up asking you for the password which you got from hydra





You will see the flag on the bottom right corner of the screen

THM{I_SEE_YOUR_SCREEN}

3.If you liked the topics presented in this task, check out these rooms next: Protocols and Servers 2, Hydra, Password Attacks, John the Ripper. No answer needed