LAB REPORT

30th November 2024

TryHackMe: Ice

Name : Sarthak Das

Session : 9th November 2024 – 18th January 2025

For the class of Ethical Hacking, taught by

Oihik Mitra

Abstract

This report is a documentation of my walk-through of the TryHackMe room titled "Ice: Deploy & hack into a Windows machine, exploiting a very poorly secured media server." The link for the same can be found here: https://tryhackme.com/r/room/ice. The upcoming sections will cover each of the seven tasks one after another. For each section, the first subsection will repeat the task question for reference and the second will document my progress through the task.

Contents

1 Connect: Connect to the TryHackMe network!

1.1 Problem

Please note that this machine does not respond to ping (ICMP) and may take a few minutes to boot up. The virtual machine used in this room (Ice) can be downloaded for offline usage from this link. The sequel to this room, Blaster, can be found here. Connect to our network using OpenVPN. Here is a mini walkthrough of connecting:

- Go to your access page and download your configuration file.
- Use an OpenVPN client to connect. In my example I am on Linux, on the access page we have a windows tutorial (change "ben.ovp" to your config file). When you run this you see lots of text, at the end it will say Initialization Sequence Completed.
- You can verify you are connected by looking on your access page. Refresh the page. You should see a green tick next to Connected. It will also show you your internal IP address.

You are now ready to use our machines on our network! Now when you deploy material, you will see an internal IP address of your Virtual Machine.

1.2 My Solution

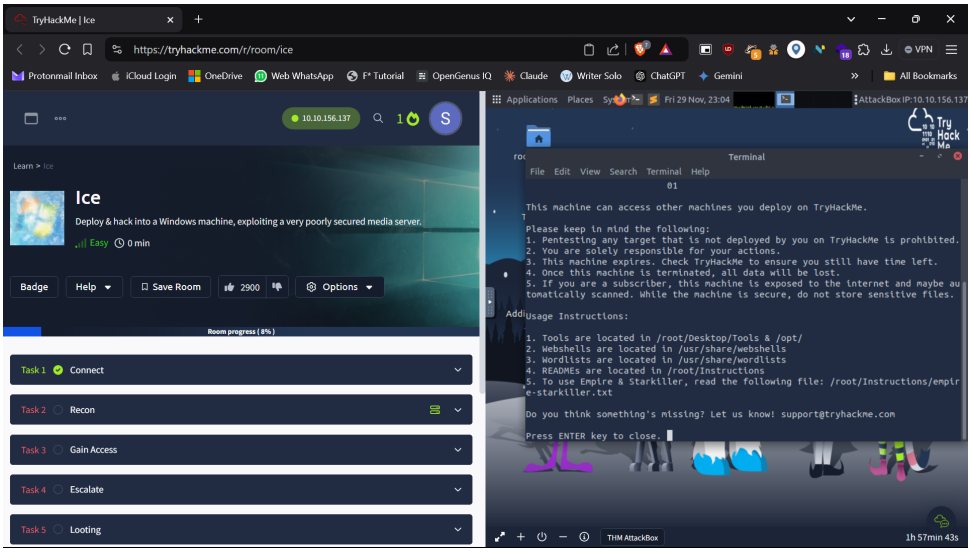

Figure 1: I downloaded an OpenVPN config file from the IN-Regular-1 server but due to the firewall configurations in my system the connection did not pass through despite the OpenVPN client showing 'Connected' status and assigning an IP. Thus, I connected via THM AttackBox.

2 Recon: Scan and enumerate our victim!

2.1 Problem

Deploy the machine! This may take up to three minutes to start. Launch a scan against our target machine, I recommend using a SYN scan set to scan all ports on the machine. The scan command will be provided as a hint, however, it's recommended to complete the room 'Nmap' prior to this room. Once the scan completes, we'll see a number of interesting ports open on this machine. As you might have guessed, the firewall has been disabled (with the service completely shutdown), leaving very little to protect this machine. One of the more interesting ports that is open is Microsoft Remote Desktop (MSRDP).

- What port is this open on?
- What service did nmap identify as running on port 8000? (First word of this service)
- What does Nmap identify as the hostname of the machine? (All caps for the answer)

2.2 My Solution

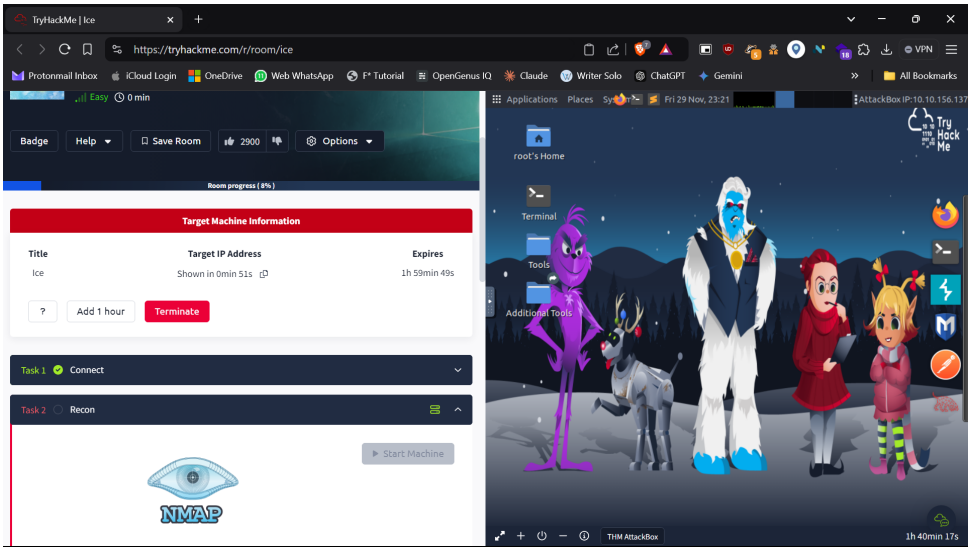

Figure 2: I deployed the target machine. The target IP was shown to be 10.10.54.185.

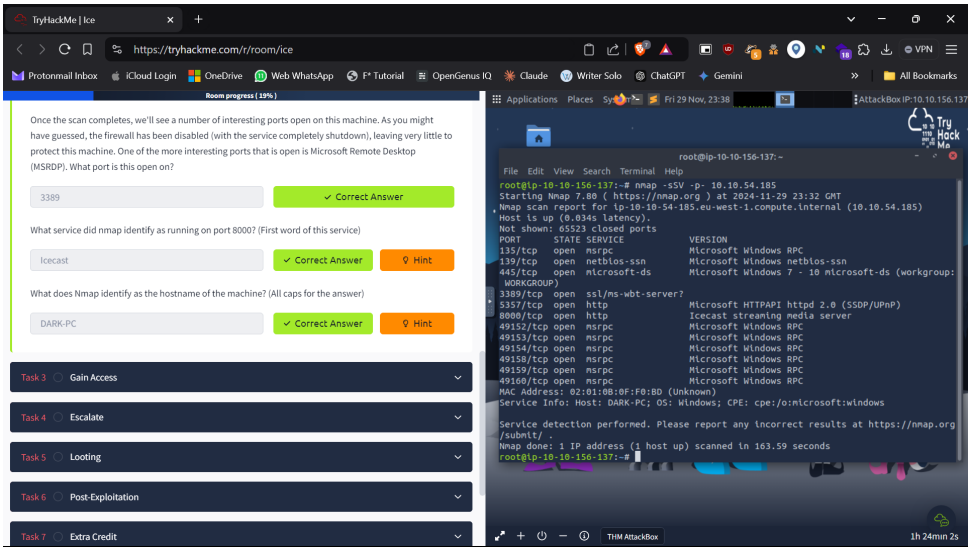

Figure 3: I performed an nmap scan using the command 'nmap -sSV -p- 10.10.54.185' (for TCP/SYN scan with service versions shown) and answered all the questions. MSRDP was open on port 3389, port 8000 was running Icecast, and the hostname of the target machine was detected to be DARK-PC.

3 Gain Access: Exploit the target vulnerable service to gain a foothold!

3.1 Problem

Now that we've identified some interesting services running on our target machine, let's do a little bit of research into one of the weirder services identified: Icecast. Icecast, or well at least this version running on our target, is heavily flawed and has a high level vulnerability with a score of 7.5 (7.4 depending on where you view it).

- What is the Impact Score for this vulnerability? Use this site for this question and the next.
- What is the CVE number for this vulnerability? This will be in the format: CVE-0000-0000

Now that we've found our vulnerability, let's find our exploit. For this section of the room, we'll use the Metasploit module associated with this exploit. Let's go ahead and start Metasploit using the command 'msfconsole'.

- After Metasploit has started, let's search for our target exploit using the command 'search icecast'. What is the full path (starting with exploit) for the exploitation module? If you are not familiar with metasploit, take a look at the Metasploit module.

Let's go ahead and select this module for use. Type either the command 'use icecast' or 'use 0' to select our search result.

- Following selecting our module, we now have to check what options we have to set. Run the command 'show options'. What is the only required setting which currently is blank?

First let's check that the LHOST option is set to our tun0 IP (which can be found on the access page). With that done, let's set that last option to our target IP. Now that we have everything ready to go, let's run our exploit using the command 'exploit'.

3.2 My Solution

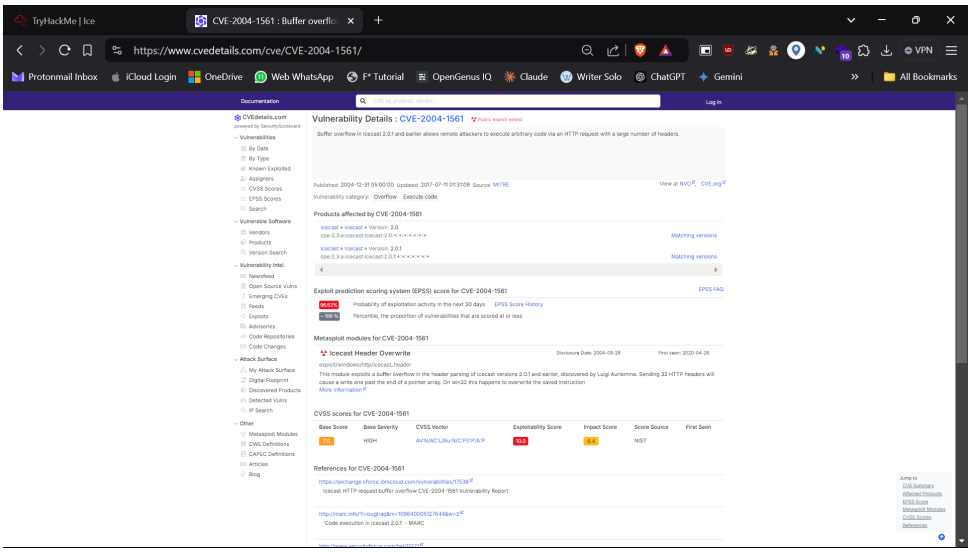

Figure 4: I searched the CVE database for Icecast>>Icecast and found that only one public exploit exists: CVE-2004-1561, with an impact score of 6.4.

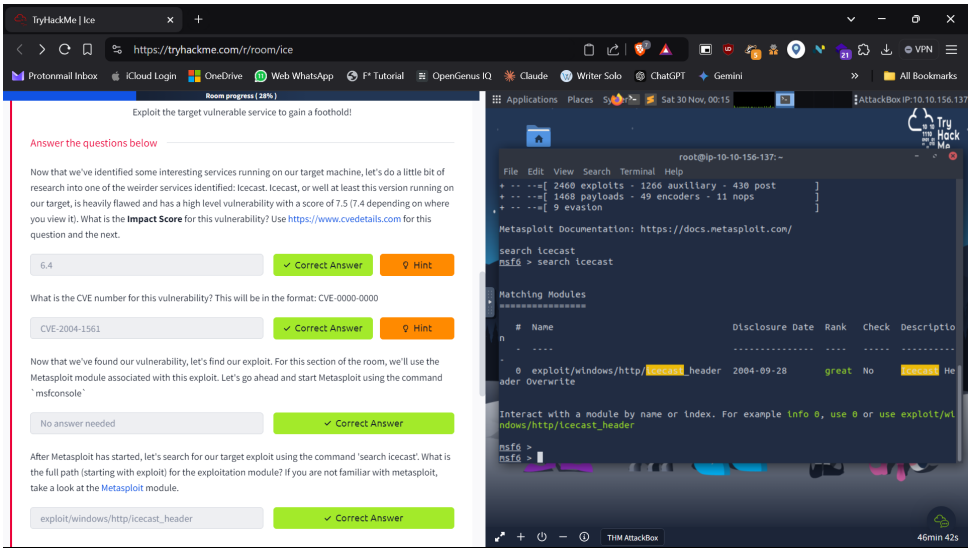

Figure 5: I started the msfconsole and performed 'search icecast'. The module returned was 'exploit/windows/http/icecast_header'.

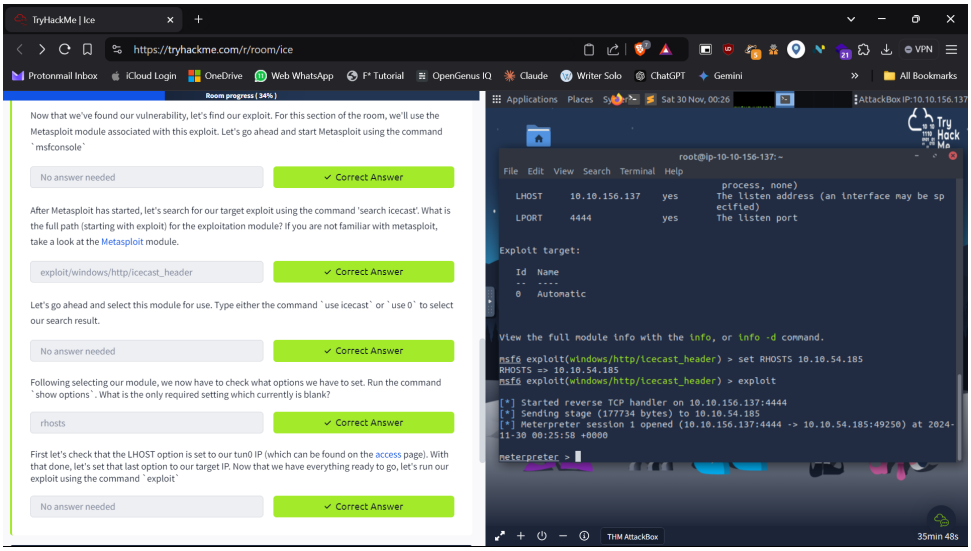

Figure 6: I set up the module for use and performed 'show options'. The only blank required option was 'RHOSTS' which I set to the IP address of the target machine using the command 'set RHOSTS 10.10.54.185'. After checking that the LHOST was correctly configured, I performed the exploit and got access to the meterpreter shell.

4 Escalate: Enumerate the machine and find potential privilege escalation paths to gain Admin powers!

4.1 Problem

Woohoo! We've gained a foothold into our victim machine!

- What's the name of the shell we have now?
- What user was running that Icecast process? The commands used in this question and the next few are taken directly from the 'Metasploit' module.
- What build of Windows is the system?
- Now that we know some of the finer details of the system we are working with, let's start escalating our privileges. First, what is the architecture of the process we're running?

Now that we know the architecture of the process, let's perform some further recon. While this doesn't work the best on x64 machines, let's now run the following command 'run post/multi/recon/local_exploit_suggester'. This can appear to hang as it tests exploits and might take several minutes to complete.

- Running the local exploit suggester will return quite a few results for potential escalation exploits. What is the full path (starting with exploit/) for the first returned exploit?

Now that we have an exploit in mind for elevating our privileges, let's background our current session using the command 'background' or 'CTRL + z'. Take note of what session number we have, this will likely be 1 in this case. We can list all of our active sessions using the command 'sessions' when outside of the meterpreter shell.

Go ahead and select our previously found local exploit for use using the command 'use FULL_PATH _FOR_EXPLOIT'.

Local exploits require a session to be selected (something we can verify with the command 'show options'), set this now using the command 'set session SESSION_NUMBER'.

- Now that we've set our session number, further options will be revealed in the options menu. We'll have to set one more as our listener IP isn't correct. What is the name of this option?

Set this option now. You might have to check your IP on the TryHackMe network using the command 'ip addr'.

After we've set this last option, we can now run our privilege escalation exploit. Run this now using the command 'run'. Note, this might take a few attempts and you may need to relaunch the box and exploit the service in the case that this fails.

Following completion of the privilege escalation a new session will be opened. Interact with it now using the command 'sessions SESSION_NUMBER'.

- We can now verify that we have expanded permissions using the command 'getprivs'. What permission listed allows us to take ownership of files?

4.2 My Solution

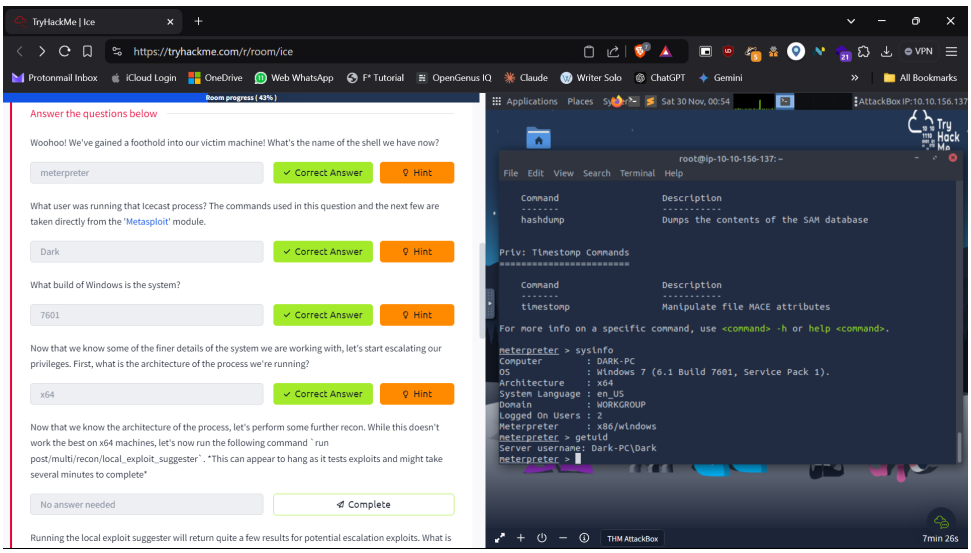

Figure 7: In the meterpreter shell I used the command 'getuid' to get the server username Dark, and the command 'sysinfo' to get the OS and architecture information – Windows 7 (6.1 Build 7601 SP1) x64. Then, I ran the command 'run post/multi/recon/local_exploit_suggester' as recommended.

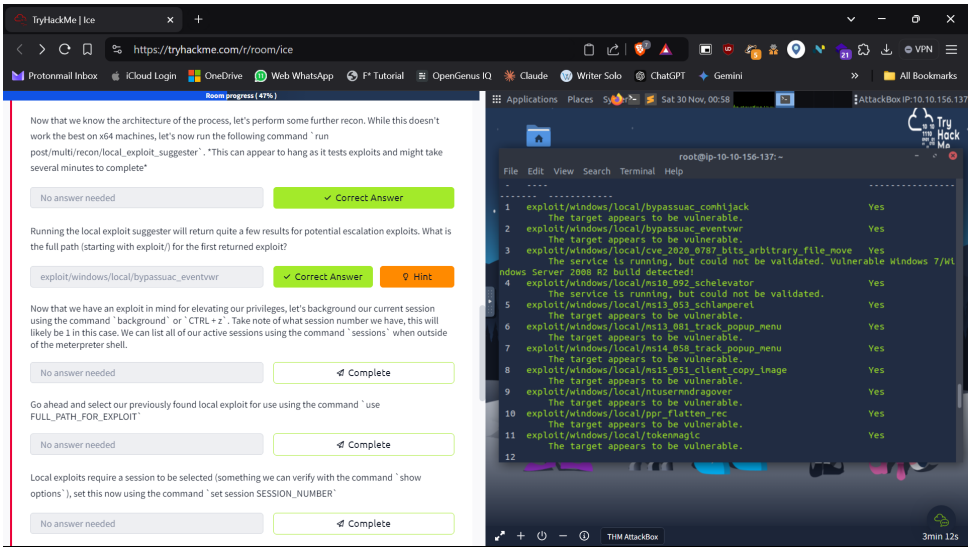

Figure 8: The top exploit suggested was 'exploit/windows/local/bypassuac_comhijack', but the answer was flagged as wrong. The second exploit 'exploit/windows/local/bypassuac_eventvwr' was accepted as the correct answer. After backgrounding the shell to session 2, I used the eventvwr exploit and set the session as 2.

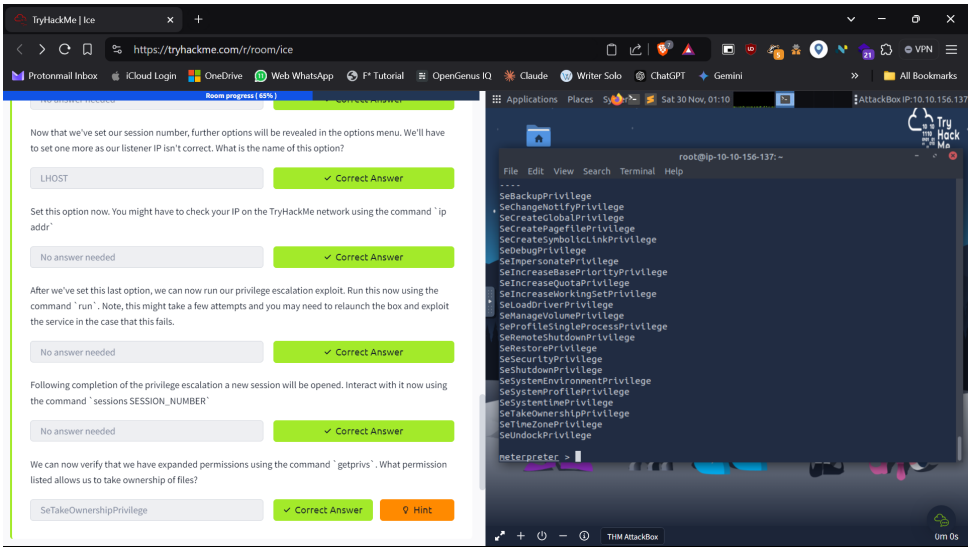

Figure 9: My LHOST ID was already set correctly, so I ran the exploit directly and escalated the privilege. The 'getprivs' command suggested the SeTakeOwnershipPrivilege privilege allows me to take ownership of files. At this point, my AttackBox timed out so I re-did the entire thing again.

5 Looting: Learn how to gather additional credentials and crack the saved hashes on the machine.

5.1 Problem

Prior to further action, we need to move to a process that actually has the permissions that we need to interact with the lsass service, the service responsible for authentication within Windows. First, let's list the processes using the command 'ps'. Note, we can see processes being run by NT AUTHORITY\SYSTEM as we have escalated permissions (even though our process doesn't).

In order to interact with lsass we need to be 'living in' a process that is the same architecture as the lsass service (x64 in the case of this machine) and a process that has the same permissions as lsass. The printer spool service happens to meet our needs perfectly for this and it'll restart if we crash it!

- What's the name of the printer service? Mentioned within this question is the term 'living in' a process. Often when we take over a running program we ultimately load another shared library into the program (a dll) which includes our malicious code. From this, we can spawn a new thread that hosts our shell.

Migrate to this process now with the command 'migrate -N PROCESS_NAME'.

- Let's check what user we are now with the command 'getuid'. What user is listed?

Now that we've made our way to full administrator permissions we'll set our sights on looting. Mimikatz is a rather infamous password dumping tool that is incredibly useful. Load it now using the command 'load kiwi' (Kiwi is the updated version of Mimikatz).

Loading kiwi into our meterpreter session will expand our help menu, take a look at the newly added section of the help menu now via the command 'help'.

- Which command allows up to retrieve all credentials?

- Run this command now. What is Dark's password? Mimikatz allows us to steal this password out of memory even without the user 'Dark' logged in as there is a scheduled task that runs the Icecast as the user 'Dark'. It also helps that Windows Defender isn't running on the box ;) (Take a look again at the ps list, this box isn't in the best shape with both the firewall and defender disabled)

5.2 My Solution

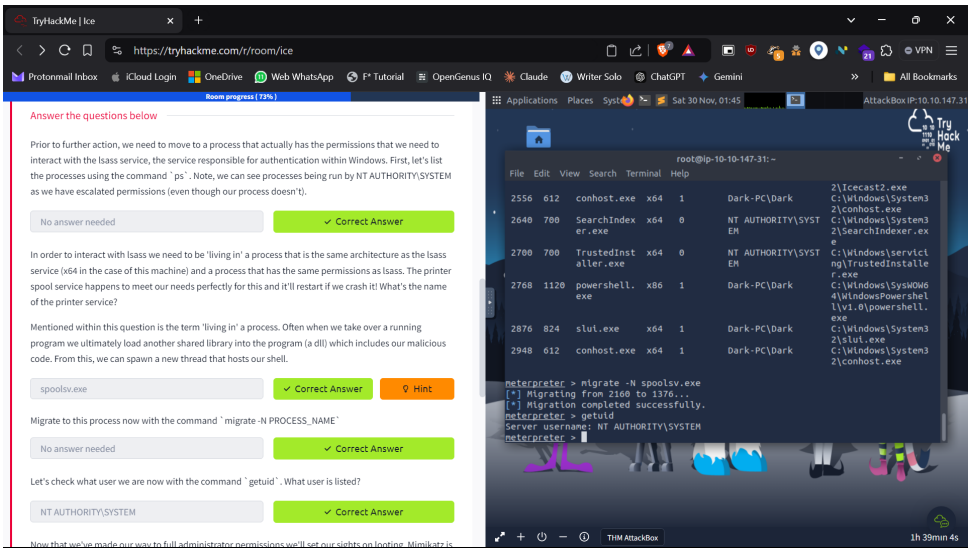

Figure 10: After escalating privilege, I identified spoolsv.exe as a vulnerable x64 process owned by NT AUTHORITY\SYSTEM and migrated to it.

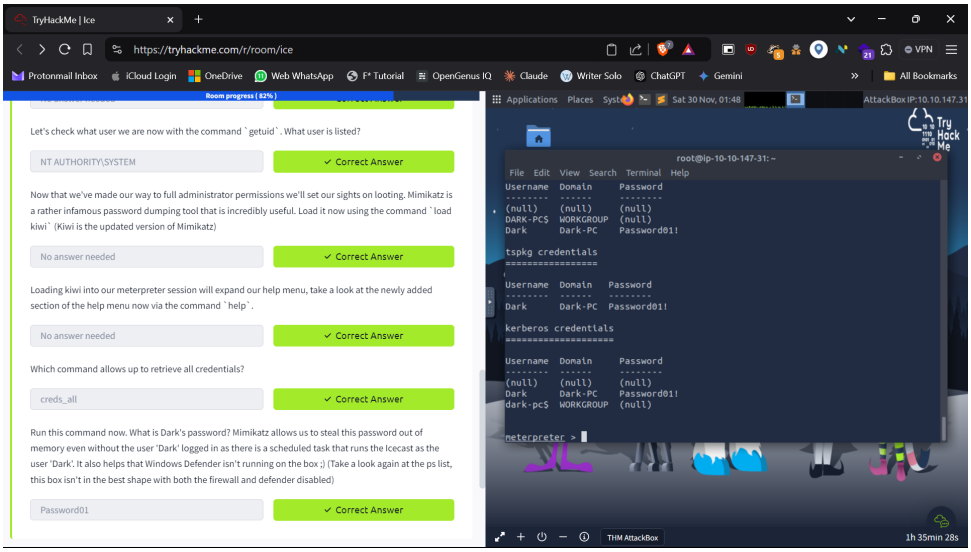

Figure 11: Following this, I loaded the Kiwi tool and ran the command 'creds_all' to get the credentials of Dark. Kiwi returned the password as 'Password01!'.

6 Post-Exploitation: Explore post-exploitation actions we can take on Windows.

6.1 Problem

Before we start our post-exploitation, let's revisit the help menu one last time in the meterpreter shell. We'll answer the following questions using that menu.

- What command allows us to dump all of the password hashes stored on the system? We won't crack the Administrative password in this case as it's pretty strong (this is intentional to avoid password spraying attempts)
- While more useful when interacting with a machine being used, what command allows us to watch the remote user's desktop in real time?
- How about if we wanted to record from a microphone attached to the system?
- To complicate forensics efforts we can modify timestamps of files on the system. What command allows us to do this? Don't ever do this on a pentest unless you're explicitly allowed to do so! This is not beneficial to the defending team as they try to breakdown the events of the pentest after the fact.
- Mimikatz allows us to create what's called a 'golden ticket', allowing us to authenticate anywhere with ease. What command allows us to do this?

Golden ticket attacks are a function within Mimikatz which abuses a component to Kerberos (the authentication system in Windows domains), the ticket-granting ticket. In short, golden ticket attacks allow us to maintain persistence and authenticate as any user on the domain.

One last thing to note. As we have the password for the user 'Dark' we can now authenticate to the machine and access it via remote desktop (MSRDP). As this is a workstation, we'd likely kick whatever user is signed onto it off if we connect to it, however, it's always interesting to remote into machines and view them as their users do. If this hasn't already been enabled, we can enable it via the following Metasploit module: 'run post/windows/manage/enable_rdp'.

6.2 My Solution

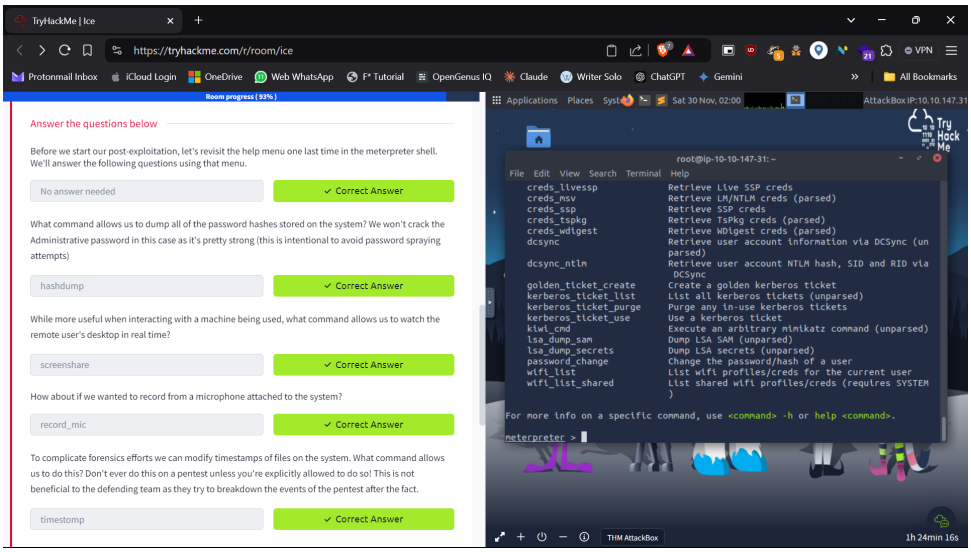

Figure 12: Finally, I revisited meterpreter help section and answered all the questions.

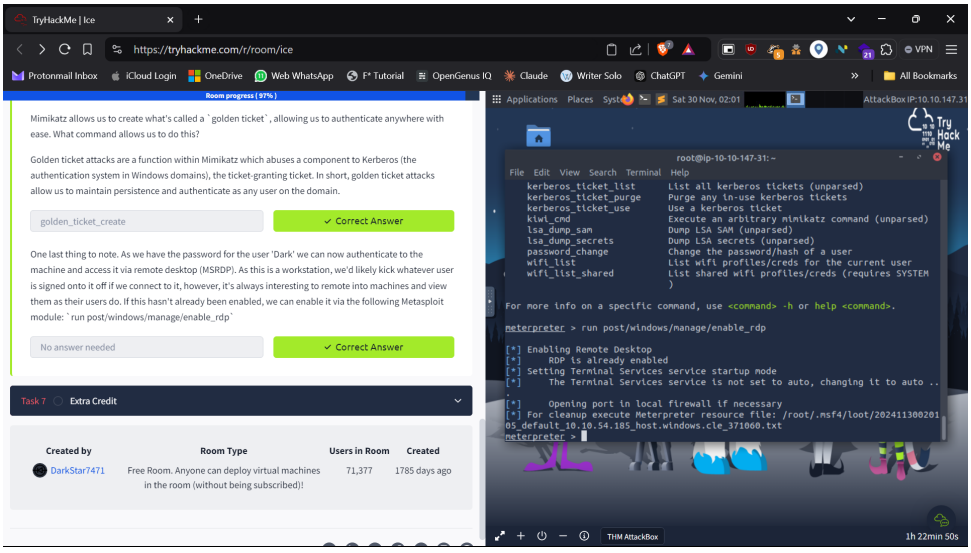

Figure 13: Running the 'run post/windows/manage/enable_rdp' command, I confirmed that the MSRDP service is already enabled. Now that we have the password of Dark, we can log into Dark's system as a remote user anytime.

7 Extra Credit

7.1 Problem

Explore manual exploitation via exploit code found on exploit-db. To learn more about alternative exploitation methods, check out the sequel to this room Blaster! As you advance in your pentesting skills, you will be faced eventually with exploitation without the usage of Metasploit. Provided above is the link to one of the exploits found on Exploit DB for hijacking Icecast for remote code execution. While not required by the room, it's recommended to attempt exploitation via the provided code or via another similar exploit to further hone your skills.

7.2 My Solution

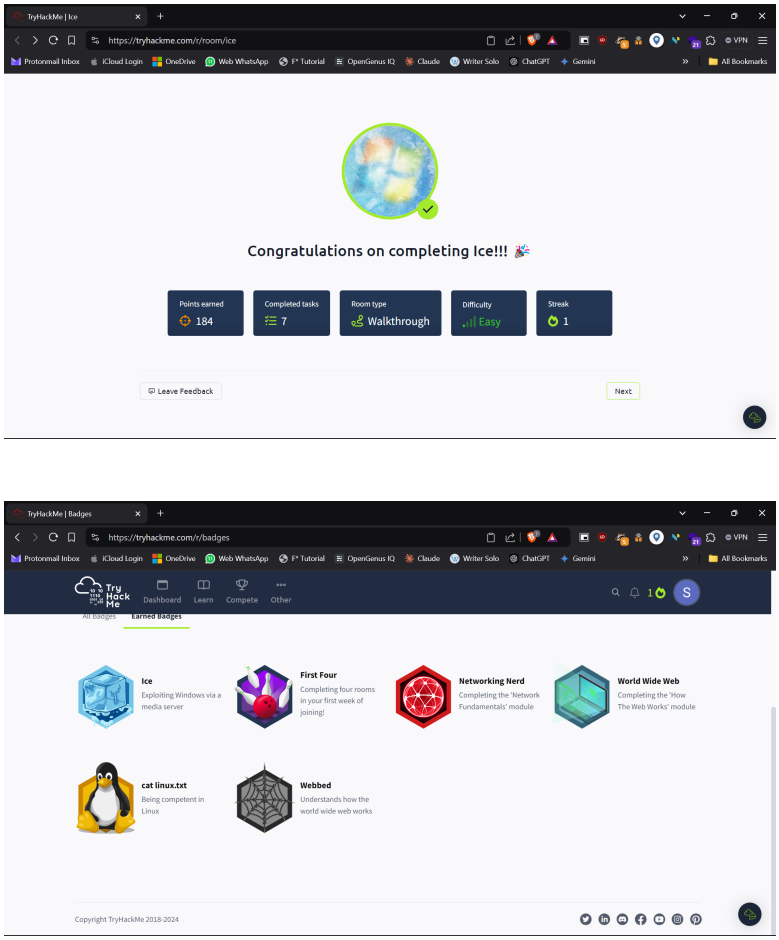

Figure 14: Finally I terminated the AttackBox as well as the target machine, and completed the room. I was awarded the Ice badge which can be seen on my TryHackMe profile.