SYNACKTIV

Faire vivre Responder avec son temps

Le potentiel caché de l'empoisonnement de résolution de noms

Barbhack 2025

Whoami.exe

SYNACKTIV

Quentin Roland

Pentester & Red Teamer @ Synacktiv

Active Directory & Windows

Introduction

Introduction

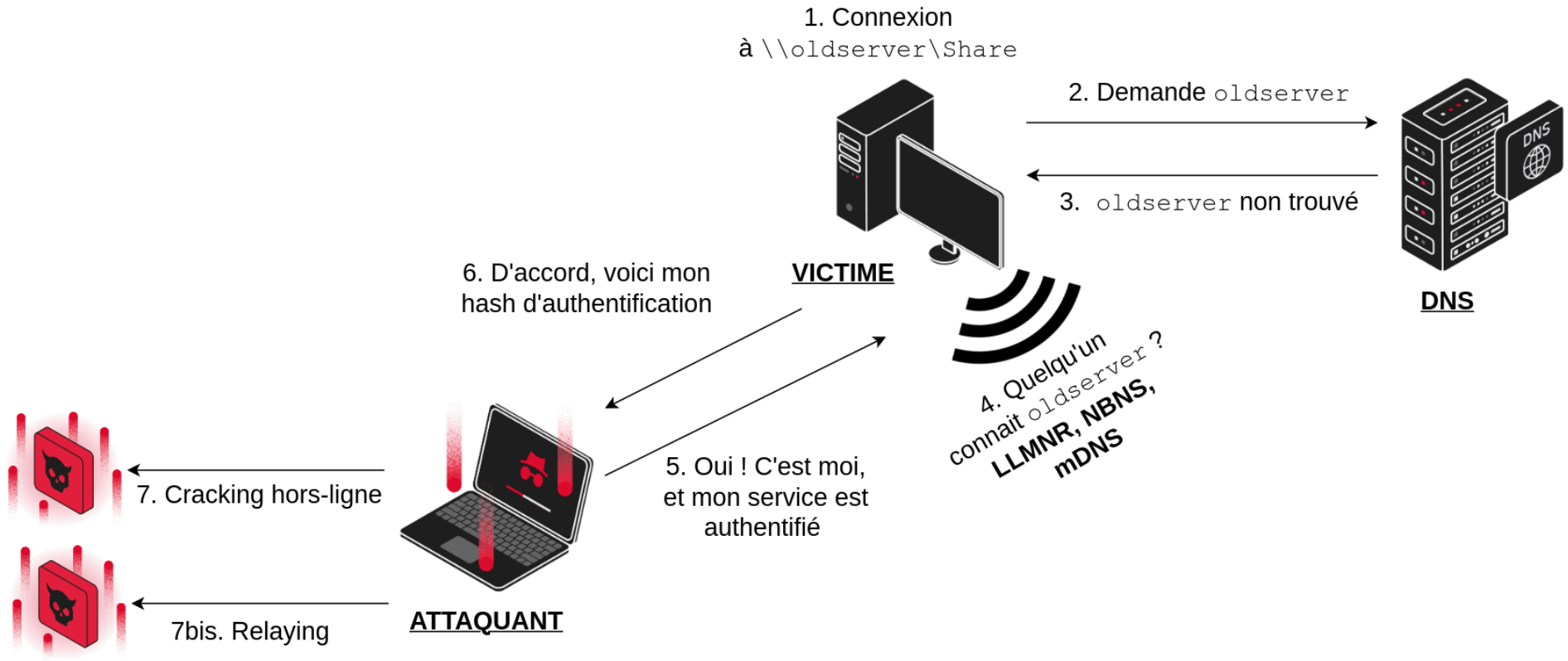
Faire du neuf avec du vieux en Active Directory

SYNACKTIV

- Attaques par **empoisonnement de protocoles locaux de résolution de noms (LLMNR, NBNS, mDNS)** :
  - Une des premières actions effectuées en interne, classiquement avec **Responder**
- Avons-nous exploré tout leur potentiel ?
  - Même des vecteurs aussi anciens peuvent faire l'objet de nouvelles recherches
  - **Deux nouvelles techniques** découvertes récemment

Introduction

Empoisonnement de protocoles locaux de résolution de noms 101



Empoisonnement LLMNR, NBNS, mDNS

Introduction

Ce qui va suivre

SYNACKTIV

- Techniques présentées relatives à l'exploitation du **relaying**
- Utiles afin d'obtenir un accès initial au sein de l'AD
- Plan de la présentation :
  1. Technique n°1 : améliorer les capacités de **relaying NTLM** en déclenchant une authentification HTTP depuis une connexion SMB
  2. Technique n°2 : effectuer du **relaying Kerberos** avec LLMNR
  3. **Combiner** les deux techniques

Relayer, c'est mieux en HTTP

Forcer le client SMB Windows à fallback vers WebDav

Relayer, c'est mieux en HTTP

SYNACKTIV

La prépondérance des clients SMB lors des attaques par empoisonnement LLMNR/NBNS/mDNS

- Lors des attaques par empoisonnement LLMNR/NBNS/mDNS, beaucoup d'authentifications de **clients SMB** reçues
  - Prévalence du protocole SMB
  - Connexions automatiques à des shares qui n'existent plus
  - Typos dans les URI SMB

```
$ python3 Responder.py -I eth0
[...]
[*] [LLMNR]  Poisoned answer sent to 192.168.123.17 for name oldserver
[SMB] NTLMv2-SSP Client   : 192.168.123.17
[SMB] NTLMv2-SSP Username : CORP\adove
[SMB] NTLMv2-SSP Hash     : adove::CORP:7c942a248d0b8bb2:8B6376D3588A6E3471894EA9C5A0AB74:0101[...]0000000
```

Relayer, c'est mieux en HTTP

SYNACKTIV

La prépondérance des clients SMB lors des attaques par empoisonnement LLMNR/NBNS/mDNS

- Authentification pouvant être effectuée par des comptes machines
- Dans ce cas, **pas de possibilité de cracker les hashes obtenus**
- **Possibilités de relai assez restreintes**

Relayer, c'est mieux en HTTP

Le potentiel mitigé du protocole SMB pour le relai NTLM

SYNACKTIV

- Le relai NTLM permet d'utiliser les services de l'AD **avec l'identité du compte relayé**
  - Piéger la victime pour déclencher son authentification NTLM auprès de votre service
  - Demande d'un challenge NTLM au service cible
  - Transmission du challenge du service cible à la victime, qui le chiffre
  - Transmission du challenge chiffré au service cible, attaquant authentifié
- Mécanismes de protection : **signature**, **channel binding**

Relayer, c'est mieux en HTTP

Le potentiel mitigé du protocole SMB pour le relai NTLM

SYNACKTIV

- L'implémentation des mécanismes de protection et donc les possibilités de relai dépendent :
  - Du protocole utilisé par la victime (**client**)
  - Du service cible (**serveur**)
- Exigences par défaut de mécanismes d'intégrité des clients et serveurs **assez variées**

Relayer, c'est mieux en HTTP

Le potentiel mitigé du protocole SMB pour le relai NTLM

SYNACKTIV

- Un service cible particulièrement intéressant pour le relai est le service **LDAP**
- Relayer vers LDAP ouvre beaucoup de possibilités :
  - **Énumération** de toutes les informations de l'AD (ldeep, bloodhound)
  - Utilisateurs et politique de mot de passe pour **password spraying**
  - **Création d'un compte machine** pour accès authentifié
  - Compromission de machines par **shadowcreds** ou **RBCD**

Relayer, c'est mieux en HTTP

Le potentiel mitigé du protocole SMB pour le relai NTLM

SYNACKTIV

- Par défaut, le service LDAP implémente la signature **lorsque le client supporte ce mécanisme**
- **Ce qui est malheureusement le cas du client SMB Windows**
- Impossibilité de relayer une authentification SMB vers les services LDAP/LDAPS

```
$ python3 examples/ntlmrelayx.py -t ldap://192.168.123.10 -smb2support
[...]

[*] Servers started, waiting for connections
[*] SMBD-Thread-5 (process_request_thread): Received connection from 192.168.123.17, attacking target ldap://192.168.123.10
[!] The client requested signing. Relaying to LDAP will not work! (This usually happens when relaying from SMB to LDAP)
```

Relayer, c'est mieux en HTTP

SYNACKTIV

Le meilleur potentiel de relai des clients HTTP

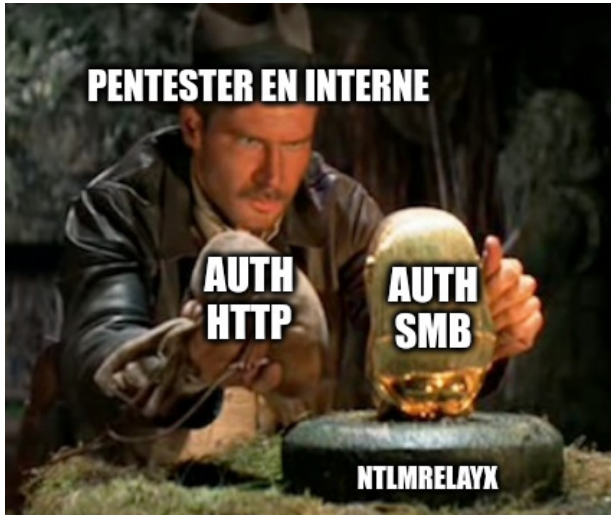
- La plupart des clients HTTP **ne supportent pas la signature des échanges**
- Possibilité, par défaut, de relayer les authentifications HTTP vers LDAP/LDAPS
- Malheureusement, les authentifications HTTP sont **plus rares**

```
1  $ python3 examples/ntlmrelayx.py -t ldap://192.168.123.10 -smb2support
2  [...]
3
4  [*] Servers started, waiting for connections
5  [*] HTTPD(80): Client requested path: /a
6  [*] HTTPD(80): Connection from 192.168.123.17 controlled, attacking target ldap://192.168.123.10
7  [*] HTTPD(80): Authenticating against ldap://192.168.123.10 as CORP/ADOVE SUCCEED
8  [*] Enumerating relayed user's privileges. This may take a while on large domains
9  [*] Dumping domain info for first time
10 [*] Domain info dumped into lootdir!
```

Relayer, c'est mieux en HTTP

Le dilemme

- Situation inconfortable lors de l'empoisonnement de résolution de noms :
  - **Beaucoup d'authentifications SMB** avec possibilités de relaying restreintes
  - **Peu d'authentifications HTTP** avec de bonnes possibilités de relaying
- Et s'il était possible de **transformer les authentifications SMB en authentifications HTTP ?**



Relayer, c'est mieux en HTTP

Faire fallback le client SMB Windows vers WebDav

SYNACKTIV

- **WebClient service** est le client HTTP WebDav Windows
- Découverte que le client SMB Windows tente de **fallback vers WebClient** si ce dernier est disponible et si des codes d'erreur spécifiques lui sont retournés :
  - `STATUS_LOGON_FAILURE` (0xc000006d)
  - `STATUS_BAD_NETWORK_NAME` (0xc00000cc)

Relayer, c'est mieux en HTTP

Faire fallback le client SMB Windows vers WebDav

SYNACKTIV

- Comportement standard Responder (**ACCESS_DENIED**), pas de fallback :

30	3.355664	fe80::21bb:3ade:e5b…	fe80::5054:ff:fe48:…	TCP	74 51593 → 445 [ACK] Seq=1 Ack=1 Win=2108160 Len=0
31	3.355702	fe80::21bb:3ade:e5b…	fe80::5054:ff:fe48:…	SMB	147 Negotiate Protocol Request
32	3.355835	fe80::5054:ff:fe48:…	fe80::21bb:3ade:e5b…	TCP	74 445 → 51593 [ACK] Seq=1 Ack=74 Win=64768 Len=0
33	3.355982	192.168.123.16	192.168.123.18	LLMNR	110 Standard query response 0x3272 AAAA idonotexist AAAA fe80::5054:ff:fe48:ed98
34	3.357297	fe80::5054:ff:fe48:…	fe80::21bb:3ade:e5b…	SMB2	314 Negotiate Protocol Response
35	3.357338	fe80::21bb:3ade:e5b…	fe80::5054:ff:fe48:…	SMB2	308 Negotiate Protocol Request
36	3.357531	fe80::5054:ff:fe48:…	fe80::21bb:3ade:e5b…	SMB2	314 Negotiate Protocol Response
44	3.359162	fe80::21bb:3ade:e5b…	fe80::5054:ff:fe48:…	SMB2	240 Session Setup Request, NTLMSSP_NEGOTIATE
47	3.359699	fe80::5054:ff:fe48:…	fe80::21bb:3ade:e5b…	SMB2	412 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
48	3.359977	fe80::21bb:3ade:e5b…	fe80::5054:ff:fe48:…	SMB2	711 Session Setup Request, NTLMSSP_AUTH, User: CORP\AD01-WKS1$
49	3.397057	fe80::5054:ff:fe48:…	fe80::21bb:3ade:e5b…	SMB2	150 Session Setup Response, Error: STATUS_ACCESS_DENIED
50	3.397202	fe80::21bb:3ade:e5b…	fe80::5054:ff:fe48:…	TCP	74 51593 → 445 [RST, ACK] Seq=1111 Ack=895 Win=0 Len=0

Relayer, c'est mieux en HTTP

Faire fallback le client SMB Windows vers WebDav

SYNACKTIV

- Avec un code d'erreur spécifique (**STATUS_LOGON_FAILURE**), fallback :

112	3.825687	192.168.123.18	192.168.123.16	SMB2	302 Negotiate Protocol Request
114	3.827079	192.168.123.16	192.168.123.18	SMB2	216 Negotiate Protocol Response
115	3.827629	192.168.123.18	192.168.123.16	SMB2	220 Session Setup Request, NTLMSSP_NEGOTIATE
116	3.828833	192.168.123.16	192.168.123.18	SMB2	329 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
117	3.829201	192.168.123.18	192.168.123.16	SMB2	621 Session Setup Request, NTLMSSP_AUTH, User: CORP\AD01-WKS1$
118	3.830563	192.168.123.16	192.168.123.18	SMB2	139 Session Setup Response, Error: STATUS_LOGON_FAILURE
141	3.879759	fe80::21bb:3ade:e5b…	fe80::5054:ff:fe48:…	HTTP	209 OPTIONS /abcd/ HTTP/1.1
144	3.881485	fe80::5054:ff:fe48:…	fe80::21bb:3ade:e5b…	HTTP	294 HTTP/1.1 200 OK
163	3.910281	fe80::21bb:3ade:e5b…	fe80::5054:ff:fe48:…	HTTP	239 PROPFIND /abcd/ HTTP/1.1
168	3.911729	fe80::5054:ff:fe48:…	fe80::21bb:3ade:e5b…	HTTP	92 HTTP/1.1 401 Unauthorized (text/html)
179	3.914042	fe80::21bb:3ade:e5b…	fe80::5054:ff:fe48:…	HTTP	322 PROPFIND /abcd/ HTTP/1.1 , NTLMSSP_NEGOTIATE
180	3.915011	fe80::5054:ff:fe48:…	fe80::21bb:3ade:e5b…	HTTP	871 HTTP/1.1 401 Unauthorized , NTLMSSP_CHALLENGE (text/html)
181	3.916238	fe80::21bb:3ade:e5b…	fe80::5054:ff:fe48:…	HTTP	906 PROPFIND /abcd/ HTTP/1.1 , NTLMSSP_AUTH, User: CORP\AD01-WKS1$
182	3.919766	fe80::5054:ff:fe48:…	fe80::21bb:3ade:e5b…	HTTP	226 HTTP/1.1 200 OK

Relayer, c'est mieux en HTTP

Faire fallback le client SMB Windows vers WebDav

SYNACKTIV

- Pré-requis :
  - **WebClient service en cours d'exécution** sur la machine
  - Certaines actions ne déclenchent pas le fallback

Relayer, c'est mieux en HTTP

Démonstration

SYNACKTIV

- **Démonstration** : exploiter le fallback WebClient pour effectuer une attaque par **shadowcreds** depuis une authentification SMB

Relayer, c'est mieux en HTTP

Démonstration

Relayer, c'est mieux en HTTP

Implémentation dans Responder

SYNACKTIV

- Possibilité de changer le code d'erreur directement implémenté dans Responder par **`BlWasp`**

```
$ python3 Responder.py -I eth0 -E
```

Faire du relai Kerberos via LLMNR

Implémentation du relai Kerberos sur Responder et krbrelayx

Faire du relai Kerberos via LLMNR

Relai Kerberos 101

SYNACKTIV

- Authentification Kerberos :
  - Demande d'un **TGT** au KDC
  - Utilisation du TGT pour demander un **ST** pour le service cible
  - Utilisation du ST pour construire un **AP-REQ** envoyé au service cible
- **Aucun mécanisme inhérent à Kerberos n'empêche le relai d'un AP-REQ**
- Mêmes protections que pour NTLM : signature et channel binding

Faire du relai Kerberos via LLMNR

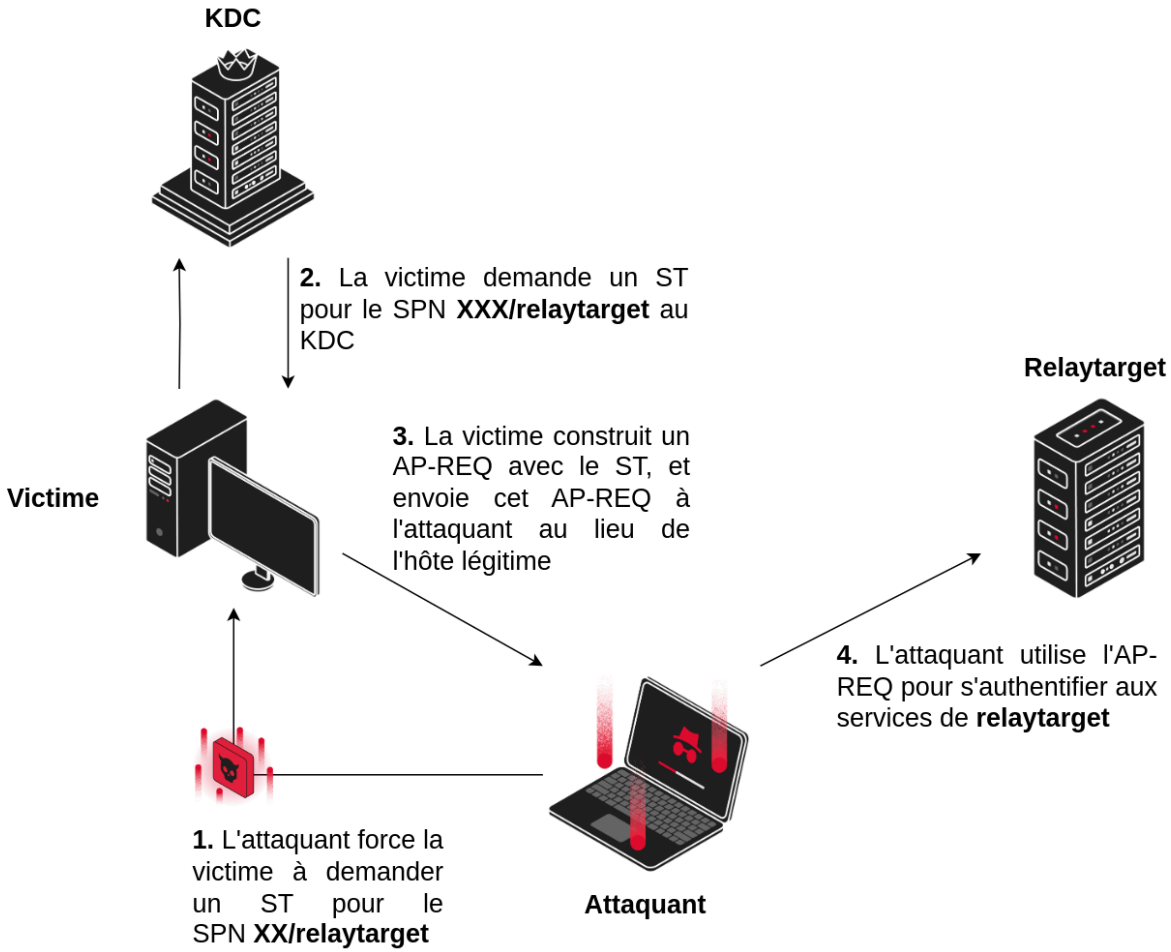
Relai Kerberos 101

SYNACKTIV

- Pour effectuer du relai Kerberos, il faut :
  - Forcer la victime à construire un AP-REQ pour un service arbitraire
  - Forcer la victime à envoyer l'AP-REQ à l'attaquant au lieu du service voulu
- Un peu plus complexe que le relai NTLM

Faire du relai Kerberos via LLMNR

Relai Kerberos 101



Faire du relai Kerberos via LLMNR

Relai Kerberos 101

SYNACKTIV

- Jusqu'ici, 2 techniques implémentées :
  - **Relai Kerberos over DNS** (Dirk-jan Mollema) — mitm6/krbrelayx
  - **Relai Kerberos over SMB** (James Forshaw) — implémenté par Hugo Vincent dans krbrelayx

Faire du relai Kerberos via LLMNR

Relai Kerberos 101

SYNACKTIV

- Jusqu'ici, 2 techniques implémentées :
  - **Relai Kerberos over DNS** (Dirk-jan Mollema) — mitm6/krbrelayx
  - ~~**Relai Kerberos over SMB** (James Forshaw) — implémenté par Hugo Vincent dans krbrelayx~~ ➜ Ne fonctionne plus depuis le patch de CVE-2025-33073

Faire du relai Kerberos via LLMNR

Relayer Kerberos over LLMNR

SYNACKTIV

- Recherche de **James Forwshaw** (2021) mentionne **un vecteur supplémentaire potentiel via LLMNR**
- Lié à la manière dont les **clients HTTP Windows** effectuent l'authentification Kerberos (browsers, .NET, WebClient)
- SPN demandé par ces clients tiré du `answer name` de la réponse DNS

Faire du relai Kerberos via LLMNR

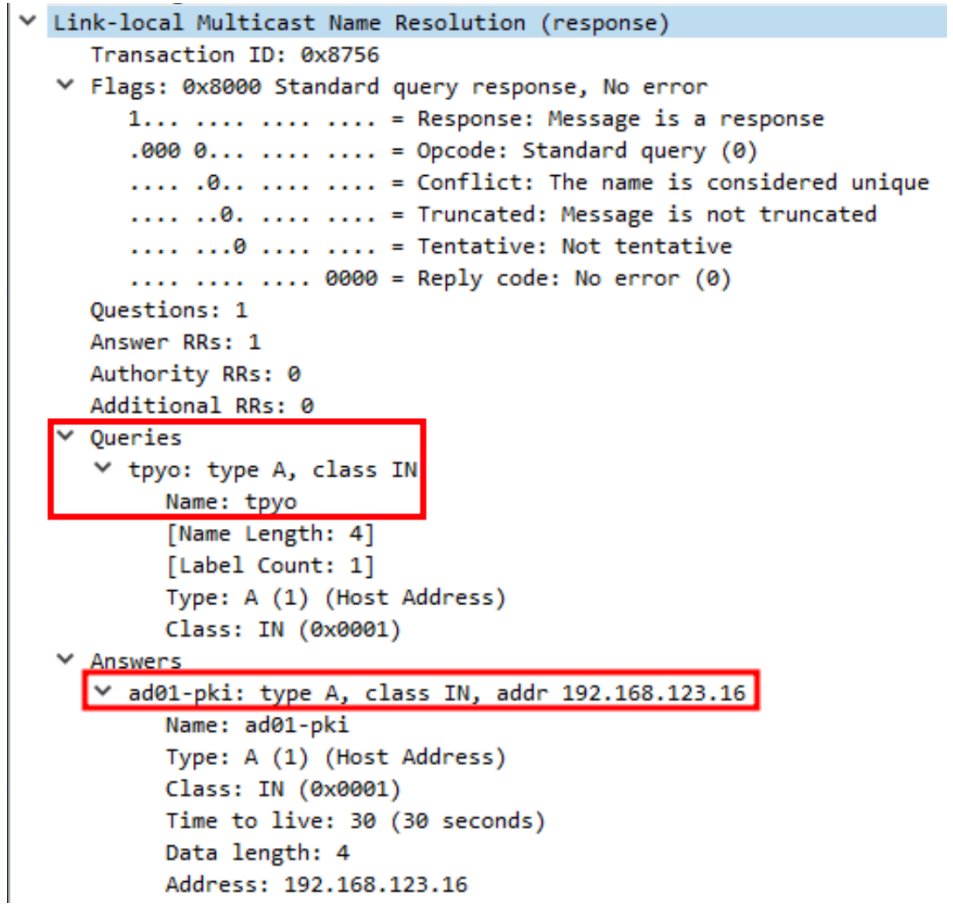
Relayer Kerberos over LLMNR

SYNACKTIV

- Attaque :
  1. L'attaquant effectue du poisoning LLMNR
  2. Un client HTTP sur le réseau local échoue à résoudre un nom d'hôte
  3. L'attaquant répond en LLMNR. Il indique :
     - Que le **`answer name`** est la cible du relai (diffère de la query)
     - Que l'IP est celle de la machine attaquante
  4. La victime demande un ST pour la cible du relai à partir du **`answer name`**
  5. Elle construit un AP-REQ et l'envoie à l'IP de attaquant, qui le relai

Faire du relai Kerberos via LLMNR

Relayer Kerberos over LLMNR



Exemple d'une réponse LLMNR pour effectuer du relai Kerberos

Faire du relai Kerberos via LLMNR

Relayer Kerberos over LLMNR

SYNACKTIV

- Implémentation dans **`Responder`** et **`krbrelayx`** début 2025 (mergé dans main)
- Utilisation du flag `-N` pour spécifier un answer name arbitraire :

```
$ python3 Responder.py -I eth0 -N ad01-pki
```

Faire du relai Kerberos via LLMNR

Relayer Kerberos over LLMNR

SYNACKTIV

- **Démonstration** : Relayer l'authentification Kerberos d'un client SMB vers le service SMB d'une autre machine

Faire du relai Kerberos via LLMNR

Relayer Kerberos over LLMNR

Faire du relai Kerberos via LLMNR

Relayer Kerberos over LLMNR

SYNACKTIV

- Cas d'utilisation :
  - Authentification NTLM désactivée sur le service cible
  - Impossibilité d'utiliser le relai over DNS
- Limitations :
  - Nécessité d'utiliser LLMNR (non fonctionnel avec mDNS et NBNS)
  - Limité au réseau local
  - Fonctionne uniquement avec les **clients HTTP**, et non SMB

Ça c'est de l'empoisonnement de résolution de noms!

Utiliser le fallback WebDav pour effectuer du relai Kerberos

Ça c'est de l'empoisonnement de résolution de noms !

SYNACKTIV

Utiliser le fallback WebDav pour effectuer du relai Kerberos

- Il est possible de **combiner les deux techniques présentées**
- Le relai Kerberos over LLMNR ne fonctionne qu'avec les clients HTTP
- Possibilité d'exploiter le fallback vers WebDav pour effectuer du relai Kerberos à partir d'une authentification SMB
- Utilisation des deux nouvelles capacités de Responder

Ça c'est de l'empoisonnement de résolution de noms !

SYNACKTIV

Utiliser le fallback WebDav pour effectuer du relai Kerberos

- **Démonstration** : Déclencher le fallback WebDav afin de relayer l'authentification Kerberos d'une machine vers le service ADCS, et compromettre la machine

Ça c'est de l'empoisonnement de résolution de noms !

SYNACKTIV

Utiliser le fallback WebDav pour effectuer du relai Kerberos

Conclusion

Conclusion

SYNACKTIV

- Même les vecteurs d'attaque aussi anciens que l'empoisonnement LLMNR, NBNS et mDNS peuvent encore surprendre
- L'exploitation Active Directory est une **combinaison de primitives d'exploitation**
- Avoir une vue globale de ces primitives et de leur articulation est important, au-delà de les maîtriser individuellement

SYNACKTIV

https://www.linkedin.com/company/synacktiv

https://x.com/synacktiv

https://synacktiv.com