

Analyser la sécurité du trafic réseau

1. Capturer le processus DORA du protocole DHCP

23648	28.919897	192.168.137.250	255.255.255.255	DHCP	342 DHCP ACK	- Transaction ID 0x3c22c697
23647	28.918574	0.0.0.0	255.255.255.255	DHCP	379 DHCP Request	- Transaction ID 0x3c22c697
23646	28.916964	192.168.137.250	255.255.255.255	DHCP	342 DHCP Offer	- Transaction ID 0x3c22c697
23643	27.909847	0.0.0.0	255.255.255.255	DHCP	345 DHCP Discover	- Transaction ID 0x3c22c697

2. Qu'est-ce que le DHCP Starvation / snooping ? Rogue DHCP ?

DHCP Starvation : Le DHCP Starvation est une attaque dans laquelle un attaquant envoie de nombreuses demandes DHCP au serveur DHCP d'un réseau. L'objectif de cette attaque est d'épuiser la pool d'adresses IP disponibles sur le serveur DHCP.

DHCP Snooping : Le DHCP Snooping est une technique de sécurité utilisée pour protéger un réseau contre les attaques de type Rogue DHCP. Il fonctionne en surveillant le trafic DHCP sur un réseau et en autorisant uniquement les réponses DHCP provenant de serveurs DHCP approuvés.

Rogue DHCP : Une attaque de Rogue DHCP survient lorsqu'un attaquant configure un serveur DHCP non autorisé sur un réseau.

3. Que se passe-t-il lors du « ipconfig /release » (windows) ? D'un point de vue sécurité quel peut être l'enjeu ?

Le système envoie une requête au serveur DHCP pour libérer l'adresse IP actuellement attribué au périphérique. Le système efface l'adresse IP actuellement attribuée et passe en mode « non connecté » pour le réseau. Toute configuration réseau, y compris les informations de la passerelle et les serveurs sont supprimés.

D'un point de vue sécurité après avoir libéré une adresse IP, un périphérique peut essayer de renouveler cette ou d'en obtenir une nouvelle en exécutant « ipconfig /renew ». Cela peut être utilisé pour tenter d'usurper une adresse IP valide sur le réseau. En libérant régulièrement et en renouvelant l'adresse IP, un périphérique peut tenter d'éviter la détection par certains systèmes de sécurité ou pare-feu qui se basent sur l'adresse IP pour identifier et surveiller les périphériques sur le réseau.

4. Quelle fonctionnalité propose CISCO pour se prémunir de ce type d'attaque ?

DHCP Snooping : Le DHCP Snooping est une fonctionnalité de sécurité qui permet aux commutateurs Cisco de surveiller le trafic DHCP sur le réseau.

Dynamic ARP Inspection : Le DAI est souvent utilisé en conjonction avec le DHCP Snooping. Il permet de surveiller et de valider les informations ARP sur le réseau.

IP Source Guard : L'IP Source Guard est une autre fonctionnalité de sécurité qui travaille en tandem avec le DHCP Snooping et le DAI. Elle permet de restreindre le trafic entrant uniquement aux adresses IP autorisées, en fonction des informations collectées par le DHCP Snooping et le DAI. Cela protège le réseau contre les adresses IP usurpées ou non autorisées.

Port Security : Cisco propose également la fonction de sécurité des ports, qui permet de limiter le nombre d'adresses MAC autorisées sur un port. Cela peut aider à prévenir les attaques de type Rogue DHCP en limitant le nombre de périphériques connectés à un port.

VLAN segmentation : Utiliser des VLAN pour isoler le trafic réseau peut également contribuer à réduire les risques liés aux attaques DHCP. Les VLANs limitent la portée des attaques potentielles.

5. Capturer une requête DNS et sa réponse

2878	9.556518	192.168.137.139	192.168.137.254	DNS	73 Standard query 0xc64a A www.google.fr
2881	9.558659	192.168.137.139	192.168.137.254	DNS	73 Standard query 0xf2c9 HTTPS www.google.fr
2883	9.563716	192.168.137.139	192.168.137.254	DNS	73 Standard query 0x7343 A www.google.fr
2884	9.563875	192.168.137.139	192.168.137.254	DNS	72 Standard query 0x23c3 A www.bing.com

6. Qu'est-ce que le DNS Spoofing ? Comment s'en protéger ?

Le terme "DNS Spoofing" fait référence à une technique utilisée par les cybercriminels pour compromettre le système de résolution de noms de domaine d'un réseau. Cette attaque a pour objectif de rediriger le trafic vers des serveurs malveillants en falsifiant les données du DNS. Les conséquences de cette attaque peuvent être graves, car elle peut entraîner l'usurpation d'identité de sites web légitimes, le détournement du trafic vers des serveurs contrôlés par l'attaquant, et ainsi exposer les utilisateurs à des attaques de phishing, de malware ou d'interception de données.

Collecte d'informations DNS : L'attaquant commence par collecter des informations sur les serveurs DNS utilisés par la cible.

Attaque de l'enregistrement DNS : L'attaquant envoie de fausses informations DNS aux serveurs DNS de la cible, en essayant de remplacer ou de corrompre les enregistrements DNS existants. Cela peut se faire en envoyant des réponses DNS falsifiées avant que les réponses légitimes ne parviennent aux serveurs DNS de la cible.

Mise en cache des enregistrements falsifiés : Les serveurs DNS de la cible peuvent mettre en cache les enregistrements DNS falsifiés, ce qui signifie que même si l'attaque n'a réussi qu'une seule fois, l'impact peut persister pendant un certain temps, car les systèmes continueront à utiliser les données corrompues en cache.

Pour se protéger contre le DNS Spoofing il faut :

Faire des mises à jour régulières.

Mise en place de la validation DNSSEC qui est une extension du DNS qui permet de vérifier l'authenticité des données DNS.

Utilisations de serveur DNS fiable.

Mise en place de pare-feu

Surveillance et détection des anomalies.

7. Qu'est-ce que DNS Sec ? DNS over TLS / HTTPS ?

DNSSEC (Domain Name System Security Extensions) : DNSSEC est une extension du DNS qui vise à garantir l'authenticité et l'intégrité des données DNS. Il fonctionne en ajoutant des signatures numériques aux enregistrements DNS, ce qui permet aux clients DNS de vérifier que les données DNS n'ont pas été modifiées en transit.

DNS over TLS : DNS over TLS est un protocole qui chiffre le trafic DNS entre le client DNS et le serveur DNS en utilisant le protocole TLS, le même protocole de chiffrement utilisé pour sécuriser les connexions HTTPS. Le DoT ajoute une couche de confidentialité aux requêtes DNS, empêchant les tiers de surveiller ou d'intercepter le trafic DNS non chiffré.

DNS over HTTPS : DNS over HTTPS est une autre technologie qui chiffre le trafic DNS, mais au lieu d'utiliser TLS, elle utilise HTTPS pour encapsuler les requêtes DNS. Il s'agit d'une approche basée sur le navigateur, où les requêtes DNS sont traitées via HTTPS, généralement par des serveurs DNS publics.

8. Dans quels cas trouve-t-on du DNS sur TCP ?

Réponse DNS volumineuse

Transferts de zone DNS

Requêtes DNS sécurisées

Clients ou réseaux restrictifs

Protection contre les attaques

9. Capturer un flux HTTP

```
17583 142.482843 87.248.205.0 192.168.137.139 HTTP 614 HTTP/1.1 206 Partial Content (application/x-chrome-extension)
```

10. Qu'est-ce que le HTTP Smuggling ? Donner un exemple de CVE

Le HTTP Request Smuggling est une vulnérabilité de sécurité qui peut permettre à un attaquant de manipuler ou de détourner des requêtes HTTP dans le but de provoquer une interprétation incorrecte de ces requêtes par un serveur web. Cela peut entraîner des comportements inattendus, la divulgation de données sensibles ou des attaques d'injection.

Un exemple de CVE lié au HTTP Request Smuggling est CVE-2019-9515. Cette vulnérabilité a été découverte dans certains serveurs proxy et implique l'interprétation incorrecte des en-têtes HTTP Transfer-Encoding et Content-Length par le proxy. L'attaquant peut alors provoquer un déni de service ou injecter des requêtes malveillantes en exploitant cette vulnérabilité.

11. Comment mettre en place la confidentialité pour ce service ?

Chiffrement HTTPS, Configuration sécurisée du serveur Web, gestion des certificats, protection contre les attaques SSL/TLS, Mise à jour des logiciels, pare-feu et filtrage des adresses IP, contrôle d'accès et authentification, surveillance et audit, protection contre les injections SQL et XSS, politiques de confidentialité.

12. Qu'est-ce qu'une PKI ?

Une PKI, ou Infrastructure à Clé Publique (en anglais, Public Key Infrastructure), est un ensemble de procédures, de protocoles, de normes, de logiciels et de matériels qui permettent de gérer, de distribuer, de stocker et de révoquer des clés de chiffrement, principalement des paires de clés publiques et privées, pour assurer la sécurité des communications électroniques et des transactions sur un réseau.

13. Capturer un mot de passe FTP ou Telnet

tcp.stream eq 323					
No.	Time	Source	Destination	Protocol	Length
1460..	3653.859641	192.168.137.140	192.168.137.139	TELNET	
1460..	3653.911028	192.168.137.139	192.168.137.140	TCP	
1460..	3653.911588	192.168.137.140	192.168.137.139	TELNET	
1460..	3653.958199	192.168.137.139	192.168.137.140	TCP	
1460..	3654.797180	192.168.137.139	192.168.137.140	TELNET	
1460..	3654.837891	192.168.137.140	192.168.137.139	TCP	
1460..	3655.072105	192.168.137.139	192.168.137.140	TELNET	
1460..	3655.072281	192.168.137.140	192.168.137.139	TCP	
1460..	3655.250139	192.168.137.139	192.168.137.140	TELNET	
1460..	3655.250332	192.168.137.140	192.168.137.139	TCP	
1460..	3655.357976	192.168.137.139	192.168.137.140	TELNET	
1460..	3655.358260	192.168.137.140	192.168.137.139	TCP	
1460..	3655.749151	192.168.137.139	192.168.137.140	TELNET	
1460..	3655.749349	192.168.137.140	192.168.137.139	TCP	
1460..	3655.854188	192.168.137.139	192.168.137.140	TELNET	
1460..	3655.854362	192.168.137.140	192.168.137.139	TCP	
1460..	3656.086207	192.168.137.139	192.168.137.140	TELNET	
1460..	3656.086403	192.168.137.140	192.168.137.139	TCP	
1460..	3656.287495	192.168.137.139	192.168.137.140	TELNET	
1460..	3656.287679	192.168.137.140	192.168.137.139	TCP	
1460..	3656.647125	192.168.137.139	192.168.137.140	TELNET	

```

BenDeb login: ...TToottool1123344..
Password: Toto132.....1234.

Login incorrect
BenDeb login: BBeenn
Password: Toto1234.

Login incorrect
BenDeb login: bbeenn
Password: Toto1234.

Linux BenDeb 4.19.0-25-amd64 #1 SMP Debian 4.19.289-2 (2023-08-08) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
ben@BenDeb:~$

```

14. Comment mettre en place la confidentialité pour ce service ?

Utilisez SSH à la place, chiffrement supplémentaire, autorisation d'accès strictes, comptes d'utilisateurs sécurisés, surveillez les activités, mise à jour et correctifs, isoler le serveur telnet.

15. Capturer un handshake TLS – puis déchiffrer le trafic avec votre certificat

```
EXPORTER_SECRET ad0bd404b2b72995bddb1d175bc644c206741373fd8a0f5b3c8d5d081886cd46 6aad239d890be21d4bfd4b9bb96e1ccea74fe11609e7dc088a7e8266d
CLIENT_HANDSHAKE_TRAFFIC_SECRET 609c36addb42ff90dc76c379ec2792585f0a79f92eb90cddfddfb50134de9db a69cf80a176f24bc0d1bb99347ad1dfb4d4d87bee
SERVER_HANDSHAKE_TRAFFIC_SECRET 609c36addb42ff90dc76c379ec2792585f0a79f92eb90cddfddfb50134de9db 2aee82bac258fb651fdfa3ebad08042da65e1eb7c
CLIENT_TRAFFIC_SECRET_0 609c36addb42ff90dc76c379ec2792585f0a79f92eb90cddfddfb50134de9db 918e6f392ec725ef4e7cbcd85f1a44c25bef0e83cc2c7b184
SERVER_TRAFFIC_SECRET_0 609c36addb42ff90dc76c379ec2792585f0a79f92eb90cddfddfb50134de9db 38d99fe1de0bcab8b3eea2a3e2df3f90ede4531b5c6e678e
```

No.	Time	Source	Destination	Protocol	Length	Info
4014	18.098069	157.240.202.1	192.168.137.139	HTTP2	806	HEADERS[11]: 200 OK, HEADERS[11]: 200 OK
4015	18.098069	157.240.202.1	192.168.137.139	HTTP2	1487	DATA[5] (text/css)
4018	18.098069	157.240.202.1	192.168.137.139	HTTP2	1029	DATA[11] (text/css)
4022	18.099785	157.240.202.1	192.168.137.139	HTTP2	180	DATA[17] (text/css)
4025	18.101748	157.240.202.1	192.168.137.139	HTTP2	573	DATA[19] (text/css)
4027	18.101946	157.240.202.1	192.168.137.139	HTTP2	292	HEADERS[21]: 200 OK

>	Ethernet II, Src: VMware_98:60:73 (00:0c:29:98:60:73), Dst: VMware_fc:28:cc (00:50:56:fc:28:cc)
>	Internet Protocol Version 4, Src: 192.168.137.139, Dst: 157.240.202.35
>	Transmission Control Protocol, Src Port: 50837, Dst Port: 443, Seq: 1225, Ack: 31835, Len: 170
>	Transport Layer Security
>	TLSv1.3 Record Layer: Application Data Protocol: HyperText Transfer Protocol 2
>	Opaque Type: Application Data (23)
>	Version: TLS 1.2 (0x0303)
>	Length: 165
>	[Content Type: Application Data (23)]
>	Encrypted Application Data: 7e6f52bf39e3ee13299bdfde69e25d1d993c1cc7fe6b44540bc57b4c3aff0e2a9461!
>	[Application Data Protocol: HyperText Transfer Protocol 2]
>	HyperText Transfer Protocol 2
>	Stream: HEADERS, Stream ID: 3, Length 139, GET /security/hsts-pixel.gif
>	Length: 139
>	Type: HEADERS (1)
>	> Flags: 0x25, Priority, End Headers, End Stream
>	0... .. = Reserved: 0x0
>	.000 0000 0000 0000 0000 0000 0000 0011 = Stream Identifier: 3
>	[Pad Length: 0]
>	1... .. = Exclusive: True
>	.000 0000 0000 0000 0000 0000 0000 0000 = Stream Dependency: 0
>	Weight: 146
>	[Weight real: 147]
>	Header Block Fragment: 82418994642c673f55c87a7f870491610525b6193e989d0942d59bc9685e634bcbcac7c9...
>	[Header Length: 680]
>	[Header Count: 15]
>	> Header: :method: GET
>	> Header: :authority: facebook.com

16. Qu'est-ce qu'une autorité de certification (AC) racine ? Qu'est qu'une AC intermédiaire.

Une Autorité de Certification racine, également connue sous le nom de "Root Certificate Authority" en anglais, est la plus haute autorité de certification dans une infrastructure à clé publique. Une AC racine est responsable de la signature numérique des certificats d'autres autorités de certification, créant ainsi une chaîne de confiance pour vérifier l'authenticité des certificats émis par des autorités de certification intermédiaires ou d'autres entités.

Une Autorité de Certification Intermédiaire, également appelée "Intermediate Certificate Authority" en anglais, est une composante d'une infrastructure à clé publique (PKI) qui se situe entre l'Autorité de Certification Racine et les utilisateurs finaux ou les serveurs. Contrairement à l'AC racine, l'AC intermédiaire n'a pas le même niveau de confiance dans la chaîne de certification. Au lieu de cela, elle émet des certificats pour les entités spécifiques, comme des sites Web ou des utilisateurs, en utilisant la clé privée associée à l'AC intermédiaire.

17. Connectez-vous sur <https://taisen.fr> et affichez la chaîne de confiance du certificat

```
C:\Users\cozebe01>openssl s_client -showcerts -connect taisen.fr:443
CONNECTED(000001B4)
depth=2 C = US, O = Internet Security Research Group, CN = ISRG Root X1
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=1 C = US, O = Let's Encrypt, CN = R3
verify return:1
depth=0 CN = taisen.fr
verify return:1
---
Certificate chain
 0 s:CN = taisen.fr
  i:C = US, O = Let's Encrypt, CN = R3
  a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
  v:NotBefore: Sep 14 12:58:07 2023 GMT; NotAfter: Dec 13 12:58:06 2023 GMT
```

```
1 s:C = US, O = Let's Encrypt, CN = R3
  i:C = US, O = Internet Security Research Group, CN = ISRG Root X1
  a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
  v:NotBefore: Sep  4 00:00:00 2020 GMT; NotAfter: Sep 15 16:00:00 2025 GMT
```

```
2 s:C = US, O = Internet Security Research Group, CN = ISRG Root X1
  i:O = Digital Signature Trust Co., CN = DST Root CA X3
  a:PKEY: rsaEncryption, 4096 (bit); sigalg: RSA-SHA256
  v:NotBefore: Jan 20 19:14:03 2021 GMT; NotAfter: Sep 30 18:14:03 2024 GMT
```

```
Server certificate
subject=CN = taisen.fr
issuer=C = US, O = Let's Encrypt, CN = R3
---
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: RSA-PSS
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 4441 bytes and written 391 bytes
Verification error: unable to get local issuer certificate
---
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Server public key is 2048 bit
This TLS version forbids renegotiation.
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 20 (unable to get local issuer certificate)
---
```

18.Capturer une authentification Kerberos

3 0.004160	192.168.47.100	192.168.47.105	KRB5	322 AS-REQ
4 0.005223	192.168.47.105	192.168.47.100	KRB5	1425 AS-REP
5 123.611943	192.168.47.100	192.168.47.105	KRB5	1614 TGS-REQ
6 123.615018	192.168.47.105	192.168.47.100	KRB5	1542 TGS-REP

19. Quels sont les flags TCP

Les drapeaux TCP, également appelés "flags" en anglais, sont des indicateurs binaires dans l'en-tête des paquets TCP qui servent à contrôler et à signaler divers aspects de la communication TCP. Les drapeaux TCP sont essentiels pour établir, maintenir et terminer une connexion TCP entre des périphériques. Voici une liste des principaux drapeaux TCP :

URG (Urgent Pointer) : Le drapeau URG indique que le champ pointeur urgent est valide. Cela signifie que des données urgentes suivent dans le segment. Le pointeur urgent indique la position du dernier octet de données urgente.

ACK (Acknowledgment) : Le drapeau ACK indique que le champ numéro d'acquittement (Acknowledgment Number) est valide. Il confirme que le périphérique a reçu avec succès les données jusqu'à l'octet spécifié dans le champ d'acquittement.

PSH (Push) : Le drapeau PSH indique au récepteur de pousser les données dans l'application destinataire, plutôt que d'attendre de recevoir un volume maximal de données avant de les transmettre.

RST (Reset) : Le drapeau RST est utilisé pour réinitialiser une connexion TCP. Il indique que la connexion est terminée anormalement ou qu'il y a un problème de communication.

SYN (Synchronize) : Le drapeau SYN est utilisé pour initialiser une connexion TCP. Lorsqu'un appareil souhaite établir une connexion, il envoie un segment TCP avec le drapeau SYN.

FIN (Finish) : Le drapeau FIN est utilisé pour terminer une connexion TCP de manière ordonnée. Lorsque les deux périphériques ont fini d'échanger des données, ils envoient un segment TCP avec le drapeau FIN pour indiquer la fin de la communication.

20. Capturer une authentification RDP

6	0.119014	192.168.100.128	192.168.100.10	RDP	101 Cookie: msthash=Administr, Negotiate Request
7	0.123804	192.168.100.10	192.168.100.128	RDP	73 Negotiate Response
24	6.606001	192.168.100.128	192.168.100.10	RDP	101 Cookie: msthash=Administr, Negotiate Request
25	6.612439	192.168.100.10	192.168.100.128	RDP	73 Negotiate Response
62	6.725308	192.168.100.128	192.168.100.10	RDPUDP	1274 SYN,CORRELATIONID,SYNEX
63	6.726368	192.168.100.10	192.168.100.128	RDPUDP	1274 SYN,SYNEX
65	6.835252	192.168.100.128	192.168.100.10	RDPUDP2	1049 AOA,DUMMY
66	7.053551	192.168.100.10	192.168.100.128	RDPUDP2	1060 ACK,OVERHEAD,DELAYACK,AOA,DUMMY
67	7.053721	192.168.100.10	192.168.100.128	RDPUDP2	1049 AOA,DUMMY
68	7.053897	192.168.100.10	192.168.100.128	RDPUDP2	1049 AOA,DUMMY
69	7.053897	192.168.100.10	192.168.100.128	RDPUDP2	1049 AOA,DUMMY
70	7.054021	192.168.100.10	192.168.100.128	RDPUDP2	1049 AOA,DUMMY
71	7.054158	192.168.100.10	192.168.100.128	RDPUDP2	1049 AOA,DUMMY

> Frame 6: 101 bytes on wire (808 bits), 101 bytes captured (808 bits) on interface \Device\NPF_{F1A9442C-1C16-45D4-ABB4-E9F3F44F8F46}, id 0	0000 00
> Ethernet II, Src: VMware_19:20:57 (00:0c:29:19:20:57), Dst: VMware_19:7e:0d (00:0c:29:19:7e:0d)	0010 00
> Internet Protocol Version 4, Src: 192.168.100.128, Dst: 192.168.100.10	0020 64
> Transmission Control Protocol, Src Port: 50172, Dst Port: 3389, Seq: 1, Ack: 1, Len: 47	0030 20
> TPCKT, Version: 3, Length: 47	0040 00
> ISO 8073/X.224 COTP Connection-Oriented Transport Protocol	0050 68
> Remote Desktop Protocol	0060 00
Routing Token/Cookie: Cookie: msthash=Administr	
Type: RDP Negotiation Request (0x01)	
> Flags: 0x00	
Length: 8	
> requestedProtocols: 0x0000000b, TLS security supported, CredSSP supported, CredSSP with Early User Authorization Result PDU supported	
...1 = TLS security supported: True	
...1 = CredSSP supported: True	
...0 = RDSTLS supported: False	
...1 = CredSSP with Early User Authorization Result PDU supported: True	

21. Quelles sont les attaques connues sur NetLM ?

Le protocole NetLM, également connu sous le nom de LM Hash (pour Lan Manager Hash), était un mécanisme de hachage de mot de passe utilisé dans les anciennes versions de Windows pour stocker les mots de passe des utilisateurs. Cependant, le LM Hash était connu pour être vulnérable et a depuis été largement abandonné au profit de mécanismes de hachage de mot de passe plus sécurisés.

Les vulnérabilités liées au LM Hash ont donné lieu à plusieurs attaques et techniques d'attaque. Voici quelques-unes des attaques connues sur NetLM :

Rainbow Tables : Les attaquants peuvent utiliser des tables arc-en-ciel (rainbow tables) précalculées pour accélérer la récupération des mots de passe en fonction des hachages LM. Étant donné que les hachages LM sont basés sur une méthode de hachage faible et prévisible, ils sont vulnérables à ce type d'attaque.

Forçage par dictionnaire : Les attaquants peuvent effectuer des attaques par force brute en essayant une multitude de mots de passe possibles en utilisant les hachages LM pour vérifier si le mot de passe est correct.

Attaques par division en blocs : Les attaquants peuvent diviser les hachages LM en blocs plus petits et les attaquer individuellement pour trouver le mot de passe.

Attaques par collisions : Les attaquants peuvent rechercher des collisions entre les hachages LM, ce qui peut révéler des mots de passe.

Utilisation de logiciels de récupération de mot de passe : Des outils de récupération de mot de passe spécifiques peuvent être utilisés pour exploiter les vulnérabilités du LM Hash.

22. Capturer une authentification WinRM

→	2834	632.482774	192.168.137.139	192.168.137.10	HTTP	317	POST /wsman HTTP/1.1 , NTLMSSP_NEGOTIATE
←	2835	632.483717	192.168.137.10	192.168.137.139	HTTP	412	HTTP/1.1 401 , NTLMSSP_CHALLENGE
→	2837	632.484840	192.168.137.139	192.168.137.10	HTTP	1895	POST /wsman HTTP/1.1 , NTLMSSP_AUTH, User: ais.fr\cozebe01 (application/http-spnego-session-encrypted)
→	2840	632.543392	192.168.137.10	192.168.137.139	HTTP	833	HTTP/1.1 200 (application/http-spnego-session-encrypted)

▼ Hypertext Transfer Protocol

> POST /wsman HTTP/1.1\r\n

Connection: Keep-Alive\r\n

Content-Type: multipart/encrypted;protocol="application/HTTP-SPNEGO-session-encrypted";boundary:

> [truncated]Authorization: Negotiate TlRMTVNTUAADAAAAGAAYAJIAAAASARIBqgAAAAwADABYAAAAEAAQAGQAAAJ

User-Agent: Microsoft WinRM Client\r\n

> Content-Length: 1841\r\n

Host: 192.168.137.10:5985\r\n

23. Capturer une authentification SSH ou SFTP

381	118.394501	192.168.137.139	192.168.137.140	SSHv2	87	Client: Protocol (SSH-2.0-OpenSSH_for_Windows_8.1)
383	118.400727	192.168.137.140	192.168.137.139	SSHv2	95	Server: Protocol (SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u3)
385	118.406532	192.168.137.139	192.168.137.140	SSHv2	1446	Client: Key Exchange Init
386	118.406651	192.168.137.140	192.168.137.139	SSHv2	1134	Server: Key Exchange Init
387	118.407880	192.168.137.139	192.168.137.140	SSHv2	102	Client: Elliptic Curve Diffie-Hellman Key Exchange Init
388	118.410747	192.168.137.140	192.168.137.139	SSHv2	506	Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys
396	122.043202	192.168.137.139	192.168.137.140	SSHv2	70	Client: New Keys

24. Intercepter un fichier au travers du protocole SMB

49	5.341733	192.168.100.128	192.168.100.10	SMB2	358	Create Request File: L'oiseau.txt
50	5.348919	192.168.100.10	192.168.100.128	SMB2	378	Create Response File: L'oiseau.txt
51	5.349367	192.168.100.128	192.168.100.10	SMB2	378	GetInfo Request FILE_INFO/SMB2_FILE_EA_INFO File: L'oiseau.txt;GetInfo Request FILE_INFO/SMB2_FILE_STREAM_INFO File: L'oiseau.txt;GetInfo Request SEC_INFO/SP...
52	5.349947	192.168.100.10	192.168.100.128	SMB2	346	GetInfo Response;GetInfo Response;GetInfo Response
53	5.350666	192.168.100.128	192.168.100.10	SMB2	171	Read Request Len:30 Off:0 File: L'oiseau.txt
54	5.351151	192.168.100.10	192.168.100.128	SMB2	168	Read Response

> Frame 54: 168 bytes on wire (1344 bits), 168 bytes captured (1344 bits) on interface \Device\NPF_{F1A9442C-1C16-45D4-AE}	0000	00 0c 29 19 20 57 00 0c	29 19 7e 0d 08 00 45 00	..): W...)...E
> Ethernet II, Src: VMware_19:7e:0d (00:0c:29:19:7e:0d), Dst: VMware_19:20:57 (00:0c:29:19:20:57)	0010	00 9a 0b fa 40 00 00 06	a4 88 c0 a8 64 0a c0 a8@... ..d...
> Internet Protocol Version 4, Src: 192.168.100.10, Dst: 192.168.100.128	0020	64 00 01 bd c3 25 c7 03	0d 18 03 b4 2e 1a 50 18	d....%... ..,P
> Transmission Control Protocol, Src Port: 445, Dst Port: 49957, Seq: 385, Ack: 395, Len: 114	0030	20 12 92 b5 00 00 00 00	00 6e fe 53 dd 42 40 00n-SMB@
> NetBIOS Session Service	0040	01 00 00 00 00 00 08 00	01 00 39 00 00 00 00 009.....
> SMB2 (Server Message Block Protocol version 2)	0050	00 00 3d 00 00 00 00 00	00 00 ff fe 00 00 05 00
> Data (30 bytes)	0060	00 00 19 00 00 00 00 40	00 00 5e 00 3e 72 25 4b@...>r%K
	0070	57 19 a7 03 0f 65 0f b1	08 30 11 00 50 00 1e 00	W...e...o P...
	0080	00 00 00 00 00 00 00 00	00 00 63 6f 75 63 6f 75a[oucou
	0090	20 6a 65 20 73 75 69 73	20 75 6e 20 70 65 74 65	...je suis un peti
	00a0	74 20 6f 69 73 65 61 75		t oiseau

25. Comment protéger l'authenticité et la confidentialité d'un partage SMB ?

Utiliser le protocole SMB sécurisé, chiffrement SMB, Authentification sécurisée, Contrôle des autorisations, filtrage IP, Pare-feu, chiffrement des disques, auditez les accès, mises à jour régulières, gestions des mots de passe, utilisation de VPN.