Distribution EOLE - Tâche #31471

Scénario # 30987 (Terminé (Sprint)): faire un POC MINTM Amon 2.8.1

Activation du MITM sur 2.8.1

12/31/2020 11:41 AM - Benjamin Bohard

Status:	Fermé	**Start date:**	11/09/2020
Priority:	Normal	**Due date:**	
Assigned To:	Benjamin Bohard	**% Done:**	100%
Target version:	Prestation Cadoles MEN 52-01 (Noël)	**Estimated time:**	0.00 hour
		Spent time:	0.00 hour

Description

History

#1 - 12/31/2020 11:45 AM - Benjamin Bohard

Quelques références utilisées pour activer le MITM sur squid :

- https://wiki.squid-cache.org/ConfigExamples/Intercept/SslBumpWithIntermediateCA
- https://docs.diladele.com/faq/squid/sslbump_squid_windows.html
- https://docs.diladele.com/administrator_guide_stable/install/ubuntu18/squid.html

#2 - 12/31/2020 11:56 AM - Benjamin Bohard

- File 02squid.conf.patch added

- File 01squid.conf.patch added

Compilation de squid

Comme suggéré dans les documents consultés, la version de squid distribuée par Ubuntu ne semble pas être compatible avec la fonctionnalité de MITM : l'option ssl-bump n'est pas reconnue.

Recompilation du paquet distribué par Ubuntu en modifiant le rules (ajout des options --enable-ssl et --enable-ssl-crtd et remplacement de --with-gnutls par --with-openssl, la pertinence de cette dernière substitution restant à vérifier) :
https://owncloud.cadoles.com/owncloud/public.php?service=files&t=110e53e7e81d5d2faadf760fe4597ebd

Génération d'une clé et d'un certificat permettant d'émettre des certificats

```
openssl genrsa 4096 > /etc/squid/signingCA.key
openssl req -new -x509 -days 3650 -key /etc/squid/signingCA.key -out /etc/squid/signingCA.crt
cp /etc/squid/signingCA.crt /etc/squid/chain.pem
chown proxy:proxy /etc/squid/signingCA.key /etc/squid/signingCA.crt /etc/squid/chain.pem
```

Le changement de propriétaire n'est peut-être pas nécessaire, par contre, la présence de la chaîne semble l'être. Un essai en ne renseignant que le certificat signingCA.key dans la configuration n'était pas concluant.

Configuration de squid

Voir les patchs joints. Ajout des options aux lignes http_port et ajout d'acl basiques

```
http_port 3128 ssl-bump generate-host-certificates=on dynamic_cert_mem_cache_size=4MB cert=/etc/squid/signingC
A.crt key=/etc/squid/signingCA.key cafile=/etc/squid/chain.pem
```

```
acl step1 at_step SslBump1
```

```
acl step2 at_step SslBump2
acl step3 at_step SslBump3
ssl_bump bump all
```

Préparation du répertoire des certificats

```
/usr/lib/squid/security_file_certgen -c -s /var/spool/squid/ssl_db -M 4MB
```

Ce répertoire appartient à root.

#3 - 12/31/2020 05:21 PM - Benjamin Bohard

- Status changed from Nouveau to En cours

#4 - 01/05/2021 03:00 PM - Emmanuel GARETTE

- Status changed from En cours to Résolu

#5 - 01/06/2021 05:21 PM - Emmanuel GARETTE

- % Done changed from 0 to 100

#6 - 01/08/2021 10:37 AM - Fabrice Barconnière

- Status changed from Résolu to Fermé

- Remaining (hours) set to 0.0

Files

01squid.conf.patch	974 Bytes	12/31/2020	Benjamin Bohard
02squid.conf.patch	988 Bytes	12/31/2020	Benjamin Bohard