

Labo Hacking (90 min)

0	Introduction	sudo ./c 2
---	--------------	------------

Ce travail pratique sous **Windows 7** illustre les attaques suivantes :

1. Crack d'un mot de passe avec l'outil Cain – **20 min**
§1.7 à §1.9 → excel (privé ou AAI)
2. Man-in-the-Middle pour voler username-password d'une session telnet – **20 min**
3. Man-in-the-Middle pour voler username-password d'une session https – **30 min**
4. Forger un paquet ARP malicieux afin de produire l'attaque ARP poisoning – **10 min**

Les §2-3-4 se font par **groupe de 2**

Important

Ce travail exige une préparation

Etudier les paragraphes 2.1, 3.1.1, 3.1.2, 3.1.4, 4.4, 5.3 et 5.4 du document
http://www.tdeig.ch/windows/Authentication_LM_NTLM.pdf

Action

Ouvrir une session utilisateur Username=**albert** password=**admin** sous Windows7
Copier le dossier [\\10.2.1.1\doclabo\Secu\Hacking](#) sur le bureau

1	Username – Password	20 min
---	----------------------------	---------------

Objectif

Tester la résistance d'un mot de passe

But 1.1

Créer 2 comptes utilisateur

Action

Ouvrir une **session administrateur**
Clic-droit sur Computer (bureau) – Manage – Continue
Sélectionner Local Users and Groups
Clic-droit sur le dossier Users – New User
Décocher User must change password at next logon
Cocher Password never expires
Create – Close

User=alice Pass=jensen
User=bob Pass=qawsed

But 1.2

Afficher le contenu du fichier SAM avec pwdump

Action

Clic-droit sur Command Prompt (bureau) – Run as administrator – Yes
Dans le dossier `C:\Users\albert\Desktop\Hacking`, exécuter
`pwdump7 -h` pour connaître les possibilités de cette commande
`pwdump7` pour afficher le contenu du fichier SAM

Résultat

Chaque ligne correspond à un compte
Les divers champs d'une ligne sont séparés par :

```
Administrator:500:NO PASSWORD*****:31D6CFE0D16AE931B73C59D7E0C089C0:::  
Guest:501:NO PASSWORD*****:NO PASSWORD*****:::  
albert:1001:NO PASSWORD*****:209C6174DA490CAEB422F3FA5A7AE634:::
```

But 1.3

Mots de passe d'un dictionnaire

Action

Clic sur `dictionary.txt` pour afficher la liste des mots de passe de ce dictionnaire

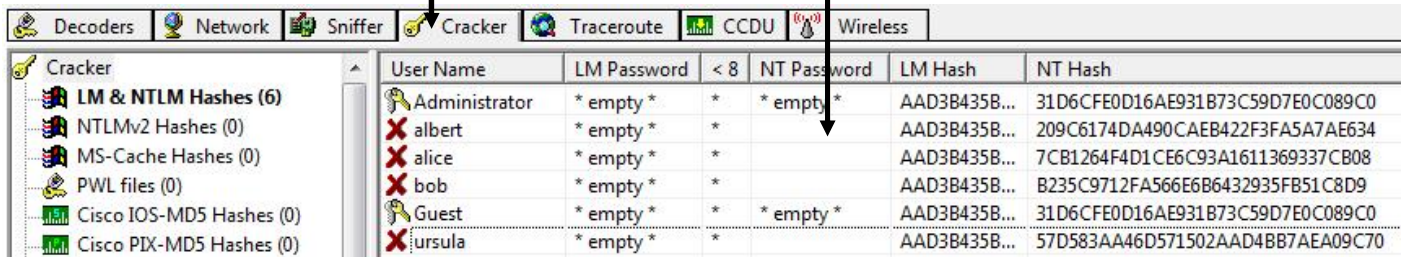
But 1.4 Lire le fichier SAM

Action

Clic-droit sur Cain (bureau) – Run as administrator – Yes

Clic sur l'onglet **Cracker** (barre d'outils)

Clic dans la **zone blanche** puis la touche « Insert » du clavier – Next



The screenshot shows the 'Cracker' tab in Cain's interface. On the left, there is a tree view with categories like 'LM & NTLM Hashes (6)', 'NTLMv2 Hashes (0)', 'MS-Cache Hashes (0)', 'PWL files (0)', 'Cisco IOS-MD5 Hashes (0)', and 'Cisco PIX-MD5 Hashes (0)'. The main area displays a table with the following columns: 'User Name', 'LM Password', '< 8', 'NT Password', 'LM Hash', and 'NT Hash'. The table contains several rows, including 'Administrator', 'albert', 'alice', 'bob', 'Guest', and 'ursula'. The 'alice' row is highlighted, and a mouse cursor is pointing at the 'NT Password' cell of that row.

User Name	LM Password	< 8	NT Password	LM Hash	NT Hash
Administrator	* empty *	*	* empty *	AAD3B435B...	31D6CFE0D16AE931B73C59D7E0C089C0
albert	* empty *	*		AAD3B435B...	209C6174DA490CAEB422F3FA5A7AE634
alice	* empty *	*		AAD3B435B...	7CB1264F4D1CE6C93A1611369337CB08
bob	* empty *	*		AAD3B435B...	B235C9712FA566E6B6432935FB51C8D9
Guest	* empty *	*	* empty *	AAD3B435B...	31D6CFE0D16AE931B73C59D7E0C089C0
ursula	* empty *	*		AAD3B435B...	57D583AA46D571502AAD4BB7AEA09C70

Cain affiche le contenu du fichier SAM

But 1.5 Cracker le mot de passe d'alice avec le dictionnaire

Action

Sélectionner la ligne alice – clic droit – Dictionary Attack – NTLM hashes

Clic droit dans la zone « Dictionary » - Add to list – C:\...\Dictionary.txt

Start

But 1.6 Cracker le mot de passe de bob avec la méthode dictionnaire puis *brute-force*

Action

Refaire l'opération précédente (attaque par dictionnaire) avec bob mais ne pas oublier de faire un « reset » avec clic droit sur la zone « Dictionary » - Reset initial file position

Pour l'attaque en brute force, clic droit sur bob – Brute-Force-Attack – NTLM Hashes

Limiter le jeu de caractères utilisés aux lettres

Start

Observer la valeur affichée pour Current password

Question 1a Quelle est la valeur moyenne du Key Rate

Question 1b Appuyer simultanément sur Ctrl Maj Esc pour répondre à la question
Quelle est la charge CPU affichée par le Task Manager – onglet Performance ?

Action Utiliser la calculette CryptMe pour effectuer les §1.7 à 1.9 à domicile
Elle se trouve sur le site web www.tdeig.ch dans le dossier contenant les documents du cours

But 1.7 Puissance de calcul de Charly

Utiliser la calculette CryptMe – onglet Attaques pour estimer la puissance de calcul de votre ennemi

Comparer les valeurs affichées avec votre mesure 1a

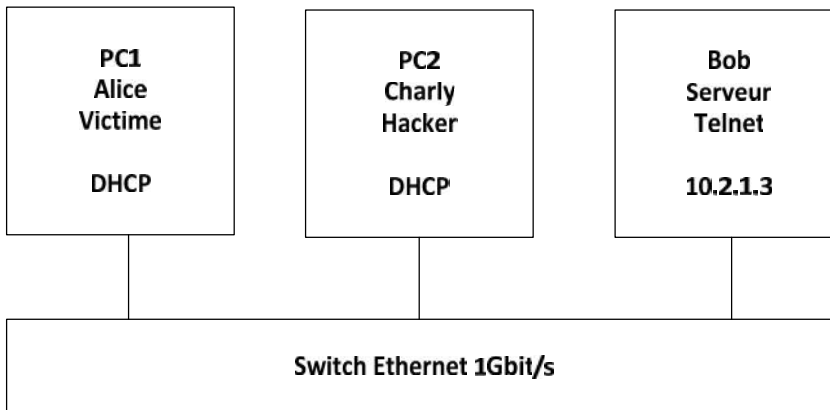
But 1.8 Résistance du mot de passe

Action Utiliser la calculette CryptMe – onglet Résistance

But 1.9 Longueur du mot de passe

Action Utiliser la calculette CryptMe – onglet Longueur du mot de passe

Réseau PC1 (victime Alice), PC2 utilisé par Charly et le serveur 10.2.1.3 (Bob) sont reliés par un commutateur Ethernet. Le serveur DHCP fournit des adresses en 10.2.2.X



But 2.1 Trouver les adresses Ethernet & IP d'Alice et Charly

Noter ces valeurs

- Alice (PC1) : Ethernet = IP =
- Charly (PC2) : Ethernet = IP =
- Bob Ethernet = IP = 10.2.1.3

Question 2a Comment avez-vous procédé ?
Expliquer votre méthodologie

But 2.2 Utiliser l'outil Cain pour effectuer l'attaque *ARP poisoning*

Action Suivre les étapes décrites dans les pages 7 à 9 de ce document

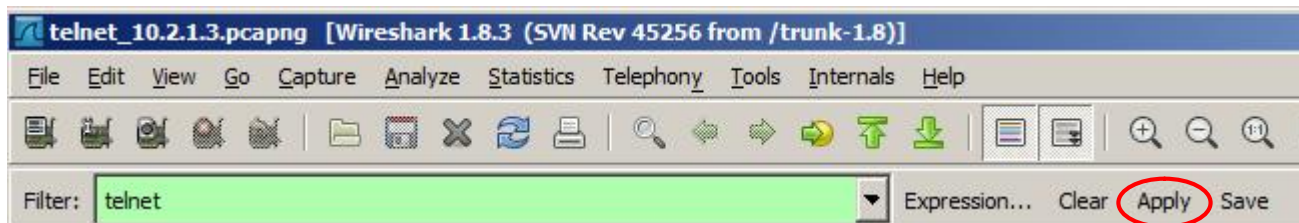
Alice établit une connexion **telnet** (Command Prompt) sur le serveur 10.2.1.3 avec username = **test** et password = **123**

Question 2b Lors de l'attaque ARP poisoning, quelle est l'entrée erronée présente dans le cache ARP d'Alice ?

Question 2c Cain a-t-il récupéré les paramètres username-password ? Si oui pourquoi ?

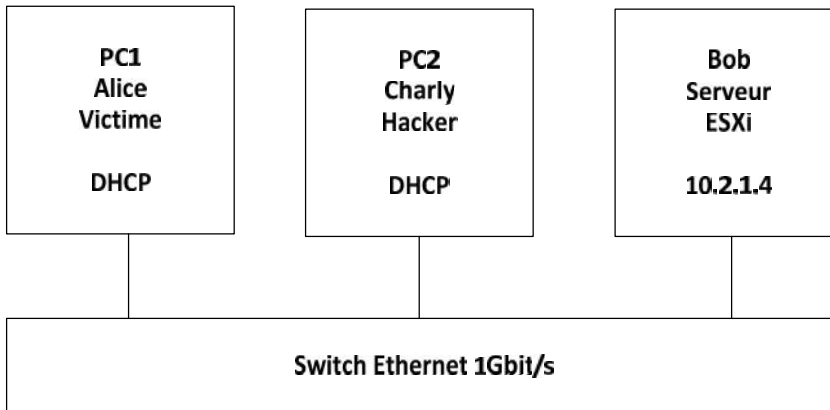
But 2.3 Analyse Wireshark telnet_10.2.1.3

Action Ouvrir l'acquisition telnet_10.2.1.3.pcap



Question 2d Dans quels paquets se trouvent username et password ?

Réseau PC1 (victime Alice), PC2 utilisé par Charly et le serveur ESXi 10.2.1.4 (Bob) sont reliés par un commutateur Ethernet. Le serveur DHCP fournit des adresses en 10.2.2.X



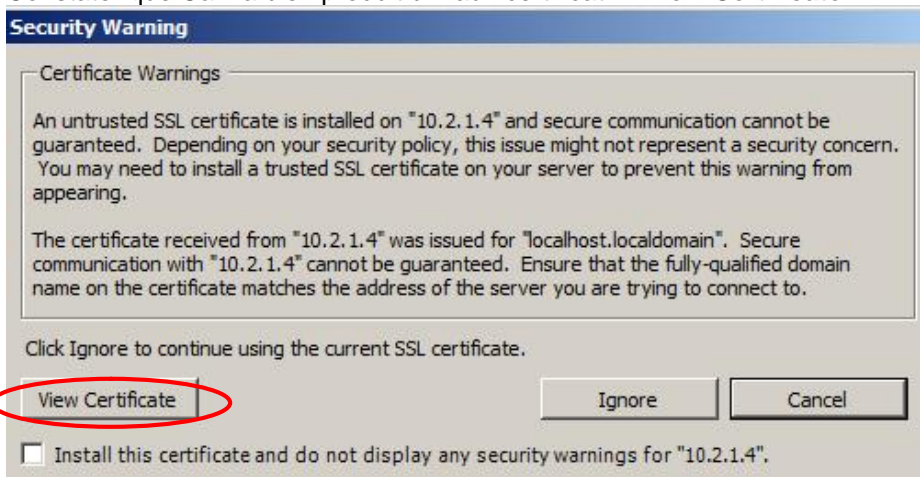
Objectifs Utiliser l'outil Cain pour effectuer l'attaque *ARP poisoning*

Action Effectuer un ping pour contrôler la disponibilité du serveur ESXi
Suivre les étapes décrites dans les [pages 7 à 9 de ce document](#)

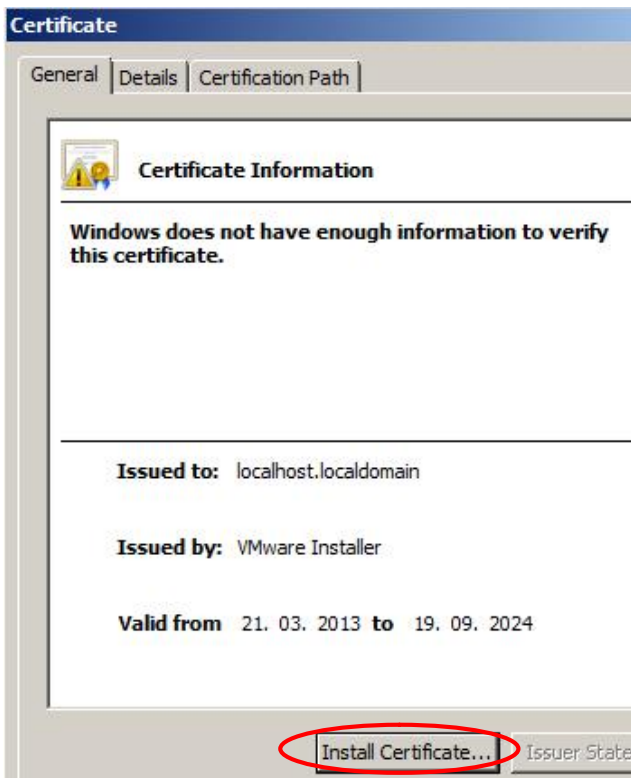
Sur le PC Alice, utiliser vSphere (raccourci bureau) pour se connecter au serveur ESXi en SSL
Login = root Password = 12345678



Constater que Cain a bien produit un faux certificat → **View Certificate**



Installer ce certificat

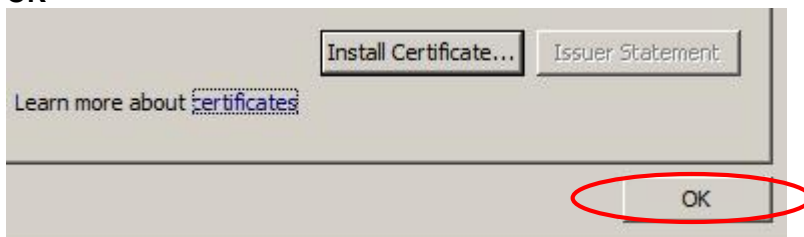


Next – Next – Finish

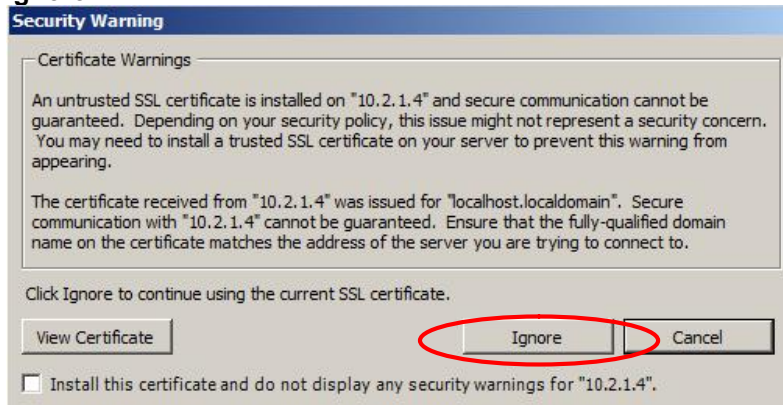
Confirmer



OK



Ignore



Documents Aidez-vous au besoin des documents ci-dessous pour répondre aux questions
http://www.oxid.it/ca_um/topics/apr-https.htm
http://www.oxid.it/ca_um/topics/certificates_collector.htm
http://www.oxid.it/ca_um/topics/sniffer_related_faqs.htm
http://www.oxid.it/ca_um/topics/apr_related_faqs.htm

Question 3a Qui a généré le certificat reçu par Alice ?

Question 3b Contrôler avec un navigateur la présence du certificat

Question 3c Quelles sont les différences entre ce certificat et celui envoyé par Bob ?

Question 3d Quelle est la procédure pour retrouver le username-password dans Caïn ?

Question 3e Comment contrer cette attaque ?

4	Forger un paquet ARP malicieux afin de produire l'attaque ARP poisoning	10 min
----------	--	---------------

Introduction L'outil Colasoft permet de forger (construire) un paquet.
Il est très utile lors de tests spécifiques ... et lors d'attaques.

Rappel Le cache ARP est mis à jour dynamiquement grâce au couple d'adresses source Ethernet – IP présentes dans l'en-tête ARP (voir ex 1)

Configuration Vous avez besoin de 2 PC sous Windows 7 pour les scénarios suivants :

- **Alice = Victime = PC1**
- **Bob = 10.2.1.1**
- **Charly = Hacker = PC2**

But 4.1 **Afficher le contenu du cache ARP de la victime Alice**

Remarque Par défaut, PC1 et PC2 obtiennent leur configuration IP par DHCP.
Le service DHCP, fourni par le firewall pfSense, attribue l'adresse IP 10.2.2.X en fonction de l'adresse Ethernet reçue dans la demande selon une liste blanche qui sera étudiée au prochain labo.

Action Sur **PC1 (Alice)**,
`ping 10.2.1.1` Pour tester la connexion avec ce serveur
`arp -a` Pour connaître le contenu du cache ARP

Q_4a Quelle est l'adresse Ethernet du serveur 10.2.1.1 ?

But 4.2 **Corrompre la table ARP de la victime Alice**

Forger le paquet **ARP response** capable de créer l'entrée IP=10.2.1.1 : Eth = aa:bb:cc:dd:ee:ff dans le cache ARP de **PC1**

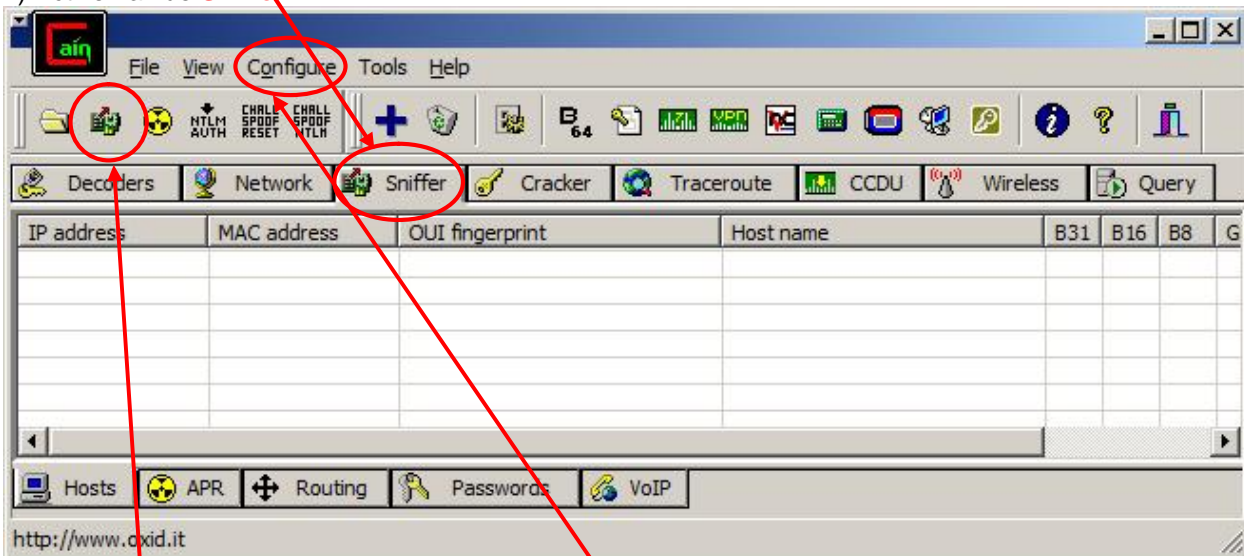
Action Sur **PC2 (Charly)**,
Exécuter `pktbuilder_1.0.1.177.exe` avec les droits admin
Bouton Add
Select Template: ARP Packet – Ok

Q_4b Quelles valeurs donner aux divers champs ?

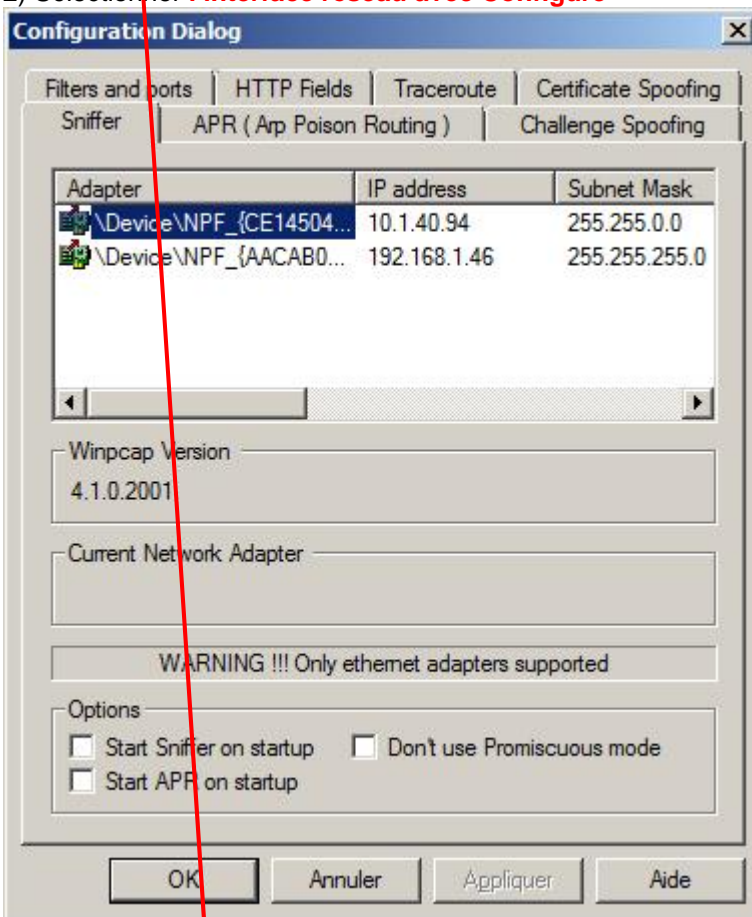
Test Clic droit sur le paquet n°1 à droite – Send Selected Packet
Contrôler l'effet dans le cache ARP d'Alice

Utilisation du logiciel Cain 4.9.36

1) Activer la vue **Sniffer**



2) Sélectionner l'interface réseau avec **Configure**

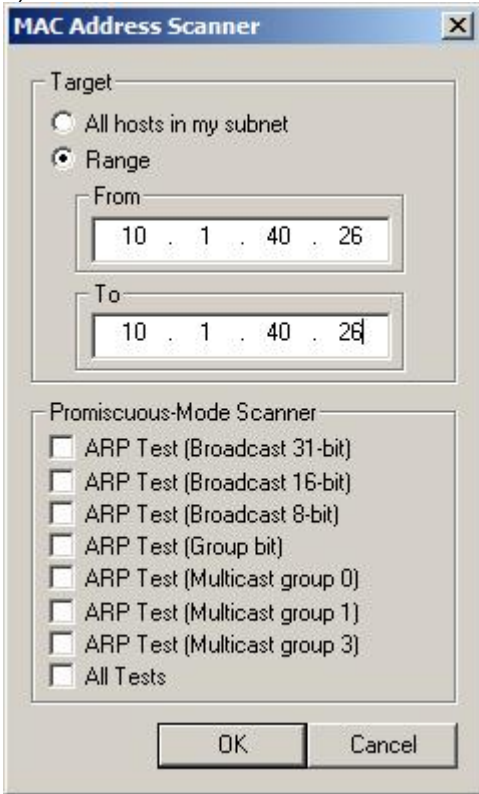


3) Activer le **Sniffer**



4) Ajouter les **éléments**

5) Sélectionner l'adresse IP d'Alice = 10.1.40.26

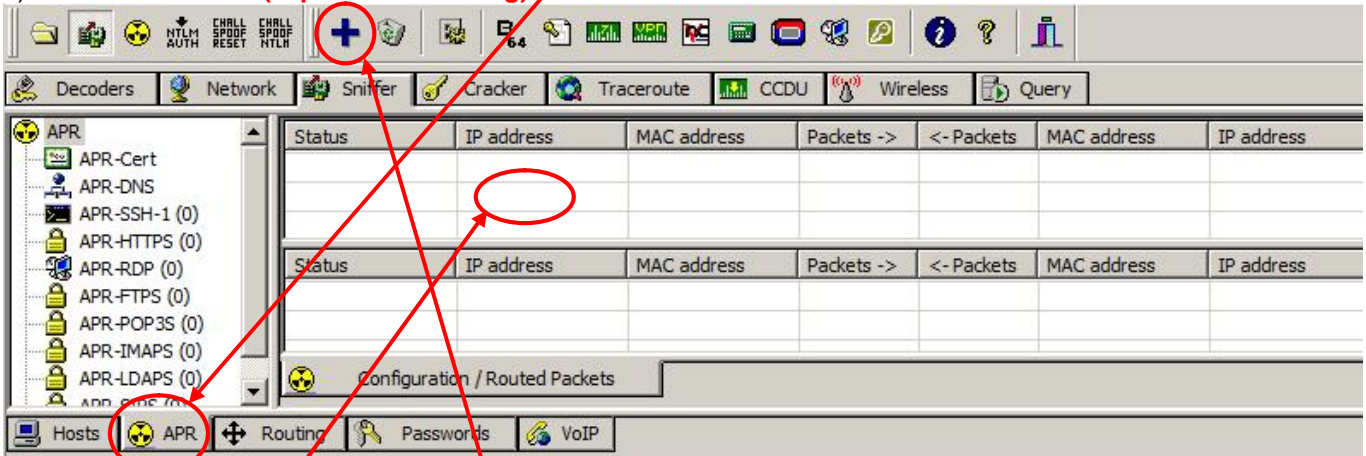


6) idem pour l'adresse IP de Bob

Dans mon cas

IP address	MAC address
10.2.2.7	E0CB4E252FB1
10.2.2.26	5404A6D18CDB

7) Activer la vue APR (Arp Poison Routing)



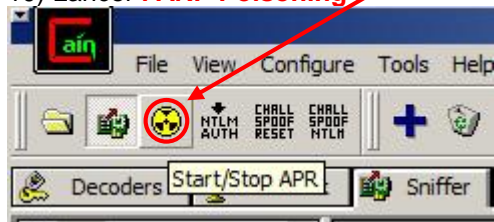
8) Sélectionner la zone puis Ajouter

9) Dans mon cas . Alice = 10.2.2.26 et Bob = 10.2.2.7

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Idle	10.2.2.26	5404A6D18CDB			E0CB4E252FB1	10.2.2.7

Appelez le prof pour qu'il valide cette attaque !

10) Lancer l'ARP Poisoning

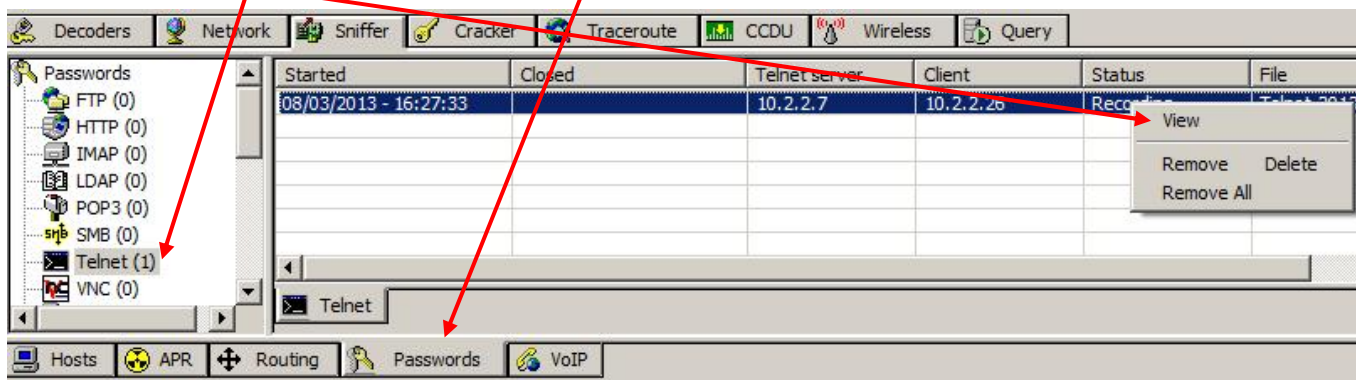


11) Observer le changement d'état

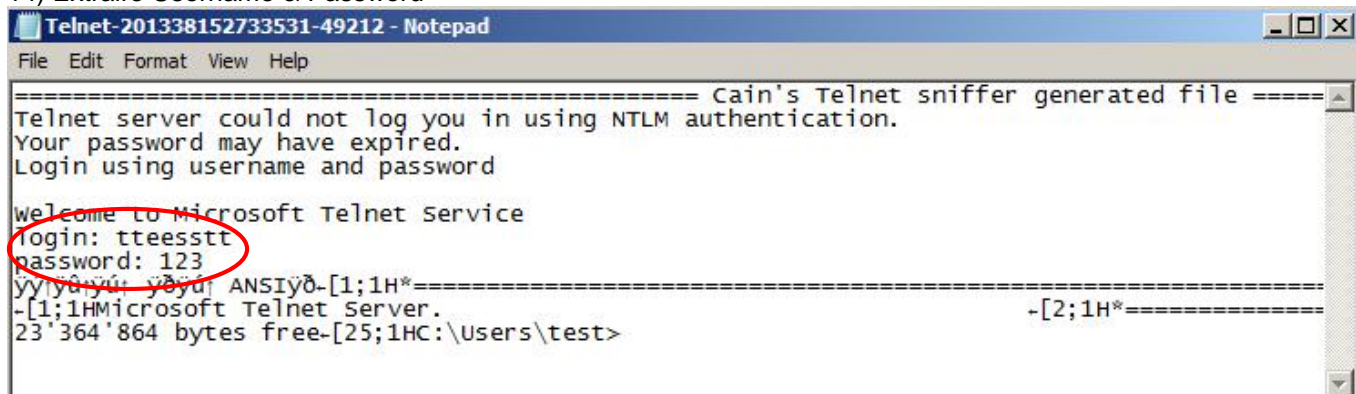
Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	10.2.2.26	5404A6D18CDB	0	0	E0CB4E252FB1	10.2.2.7

12) Alice établit une session telnet

13) Observer le résultat dans la vue Passwords



14) Extraire Username & Password



Liens

- http://www.oxid.it/ca_um/
- http://www.oxid.it/ca_um/topics/promiscuous-mode_scanner.htm
- http://www.oxid.it/ca_um/topics/mac_scanner.htm
- http://www.oxid.it/ca_um/topics/configuration.htm
- http://www.oxid.it/ca_um/topics/route_table_manager.htm
- http://www.oxid.it/ca_um/topics/apr.htm
- http://www.oxid.it/ca_um/topics/apr-https.htm

User Manual