

Sécurité dans les réseaux informatiques

Attaques : Physique

Comprendre les attaques pour mieux se défendre

Mohamed Mejri

October 27, 2016

Si on a un accès physique à un ordinateur, que peut-on faire?

Contourner l'authentification, changer le mot de passe, ajouter d'autres comptes, installer un keylogger (espion logiciel ou matériel), etc.



Accès physique à l'ordinateur

Ordinateur éteint et BIOS protégé : changer des mots de passe

- ouvrir l'ordinateur et réinitialiser la mémoire BIOS. Exemple ôter la batterie pendant quelques minutes et la remettre (ne fonctionne pas si l'ordinateur possède une eeprom dans laquelle il stocke le mot de passe)



Accès physique à l'ordinateur

Ordinateur éteint et BIOS non protégé

- Quand le système d'exploitation est en cours d'exécution, il protège l'accès au fichier de mots de passe
- 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
Utiliser un outil comme UNetbootin (<http://unetbootin.sourceforge.net/>) pour créer un USB amorçable (des versions "live" de Kali et autres distributions Linux)
- Ensuite, on monte le disque dur locale (celui qui contient les dossiers du Windows)
- Après, on peut modifier le contenu de ce fichier (modifier le mot de passe d'un utilisateur, ajouter un utilisateur, etc.) ou le récupérer pour briser certains mots de passe hachés

Accès physique à l'ordinateur

Ordinateur éteint et BIOS non protégé : Accéder à la base SAM via un livecd Backtrack ou Kali

- Pour ce faire, on démarre la machine sur Kali ou Backtrack livecd (appuyer sur F12 pour choisir le média du démarrage)
- Kali et Backtrack ne donne pas directement l'accès au disque dur de la machine cible. Car le livecd utilise un "ram disk" : une partie de la mémoire vive comme mémoire de masse.
- Pour accéder au disque dur de la cible, il faut le "monter"

```
fdisk -l  (visualiser les répartitions)
mkdir /mnt/sda1 (créer un point de montage dans /mnt)
mount /dev/sda1 /mnt/sda1 (monter la partition dans cet exemple c'est /dev/sda1)
cd /mnt/sda//WINDOWS/system32/config (aller jusqu'au fichier SAM)
```

- Certaines versions de Windows chiffrent le fichier SAM, mais la clé est souvent stockée sur le disque dur. Un outil comme BkHive permet de la récupérer
- Remarque : Windows donne la possibilité de mettre la clé de cryptage du fichier SAM sur un support externe, mais dans ce cas on aura besoin de ce disque pour tout démarrage

Accès physique à l'ordinateur

Ordinateur éteint et BIOS non protégé : changer des mots de passe

- Une fois, on a accès au fichier mots de passe hachés, on utilise l'outil chntpw

- Lancer chntpw en mode interactif

```
chntpw -i /mnt/sda1/WINDOWS/system32/config/SAM
```

- La commande nous affiche la liste d'utilisateurs

The screenshot shows a terminal window with the following text:

```
* SAM policy limits;
Failed logins before lockout is: 0
Minimum password length: 6
Password history count: 10
RID ----- Username ----- Admin? ----- Lock? -----
01f4 Administrator           ADMIN      dis/lock
03e6 alakhani                ADMIN      dis/lock
01f5 Guest                   ADMIN      dis/lock
03ea HomeGroupUser$          ADMIN      dis/lock
```

root@kali:~/media/EC08E20208E29ABA/Windows/System32/config#

- Choisir un de ces utilisateurs et taper la commande suivante pour modifier son mot de passe

```
chntpw -u "utilisateur_cible" /mnt/sda1/WINDOWS/system32/config/SAM
```

- La commande nous affiche le menu suivant



- Éliminer un mot de passe ou le modifier
- Tout le travail peut se faire dans moins que 5 min

Accès physique à l'ordinateur

Ordinateur éteint et BIOS non protégé : changer des mots de passe

- Utilisation de Offline NT Password & Registry Editor : un logiciel de 4 Mo disponible sur livecd et USB et qui permet d'ajouter des utilisateurs ou de modifier leurs mots de passe incluant celui de l'administrateur (Windows, NT, Windows 7, 2000, XP, 2003, 2008 et Vista).



- Booter la machine sur le livecd
- Choisir la partition (en cas où il y a un double boot windows)
- Donner le répertoire dans lequel se trouve le registre
C:\Windows\System32\Config
- Choisir le menu qui permet d'éditer des mots de passe

Accès physique à l'ordinateur

Ordinateur éteint et BIOS non protégé : changer des mots de passe

- Utilisation de Offline NT Password & Registry Editor :

```

chntpw version 0.99.6.110511 (C) Peltier N Haze
SMB name (from header): \SystemRoot\System32\Config\SAM
File size: 62144 (1490880) bytes containing 1 page(s) type is i (headerspace)
Used for data: 26621656 blocks/bytes, unused 82728 blocks/bytes.

HOST KEY at [0] name (from header): SYSTEM
File size: 1194394 (4498980) bytes containing 814 page(s) type is h (headerspace)
Used for data: 553120 blocks/bytes, unused 1059 blocks/bytes.

HOST KEY at [1] name (from header): \SystemRoot\System32\Config\SECURITY
File size: 2560 (10240) bytes containing 1 page(s) type is B (headerspace)
Used for data: 873435648 blocks/bytes, unused 575120 blocks/bytes.

SMB policy limits:
Minimum password length: 8
Maximum password length: 128
Password history: count: 2

<=====> chntpw Main Interactive Menu <=====>
Loaded hives: (SMB) \System\ (SECURITY)
1 - Edit user data and passwords
2 - Registry editor, now with full write support!
q - Quit (you will be asked if there is something to save)

What to do? [1] ->

===== chntpw Edit User Info & Passwords ====
RID - ----- Username ----- Admin? - Look? --
0x0 - Administrator          | No      | No
0x0 - NPAPI                   | No      | No
0x0 - Guest                   | No      | No
0x0 - Assistant                | No      | No
0x0 - Instructor                | No      | No
0x0 - SUPPORT_388945a0          | No      | No
                                          | dis/lock | dis/lock
                                          | dis/lock | dis/lock

Select: f - quit   - list users, 0x<RID> - User with RID <RID> [Administrator]
or simply enter the username to change (Administrator) Administrator

```

- Trinity Rescue Kit : même chose que Offline NT Password mais fonctionnant sur Windows 7, Windows 8, Vista, XP, Windows Server 2003, 2008 et 2012.
- Kon-boot : un live CD qui permet de contourner l'authentification Windows (XP, Vista 32 bits, Windows 7 et Windows 8 32 bits, Windows Server 2003, 2008 et 2012 32 bits) et Linux (Gentoo, Debian, Ubuntu, Fedora)

Accès physique à l'ordinateur

Ordinateur éteint et BIOS non protégé : Dumper la base SAM et dévoiler des mots de passe

- Modifier le mot de passe d'un administrateur ou d'un autre utilisateur est rapidement détectable
- Il vaut mieux dévoiler des mots de passe valides et les utiliser
- Une fois le disque dur de la cible est monté, on utilise un outil comme samdump2 pour récupérer le fichier SAM c:\Windows\system32\config\SAM
- Pour ce faire, on utilise la commande suivante

```
samdump2 /mnt/sda1/Windows/system32/config/SYSTEM /mnt/sda1/Windows/system32/config/SAM >hash7.txt
```

- Le résultat est récupéré dans le fichier hash7.txt et contient les mots de passe haché de Windows qu'on pourrait briser via des outils comme John the Ripper, OPHCRACK, Cain & Abel

```
john /tmp/mot_de_passe_chiffree.txt -format=nt
```

Le format nt est pour NTLM

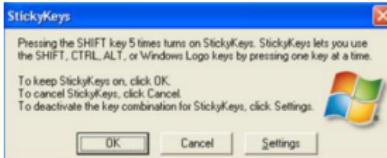
Accès physique à l'ordinateur

Ordinateur éteint et BIOS non protégé : Autres techniques

→ Utiliser le Firewire pour contourner l'authentification de Windows.

- L'idée de faire passer une machine pirate Linux bien préparée comme étant un périphérique : un stockage Firewire, un iPod, etc.
- On exploite le fait que l'utilisation de périphériques est "plug and play" : l'installation se fait automatiquement même si la session est verrouillée

→ Escalader le privilège avec StickyKeys : Appuyer 5 fois sur "shift" dans l'écran de logon et une boîte de dialogue StikyKeys apparaît



- Le programme qui lance StickyKeys se trouve dans `c:\window\system32\sethc.exe`
- Si on l'efface et on met `cmd.exe` à sa place tout en le renommant `sethc.exe`, on aura, après 5 "shift" sur l'écran de logon, un interpréteur de commandes avec des privilège root

Accès physique à l'ordinateur keylogger



PS2 keylogger



USB keylogger



Wi-fi keylogger



Keylogger intégré au clavier



Bluetooth keylogger



VideoGhost

Keylogger pour capture d'écran

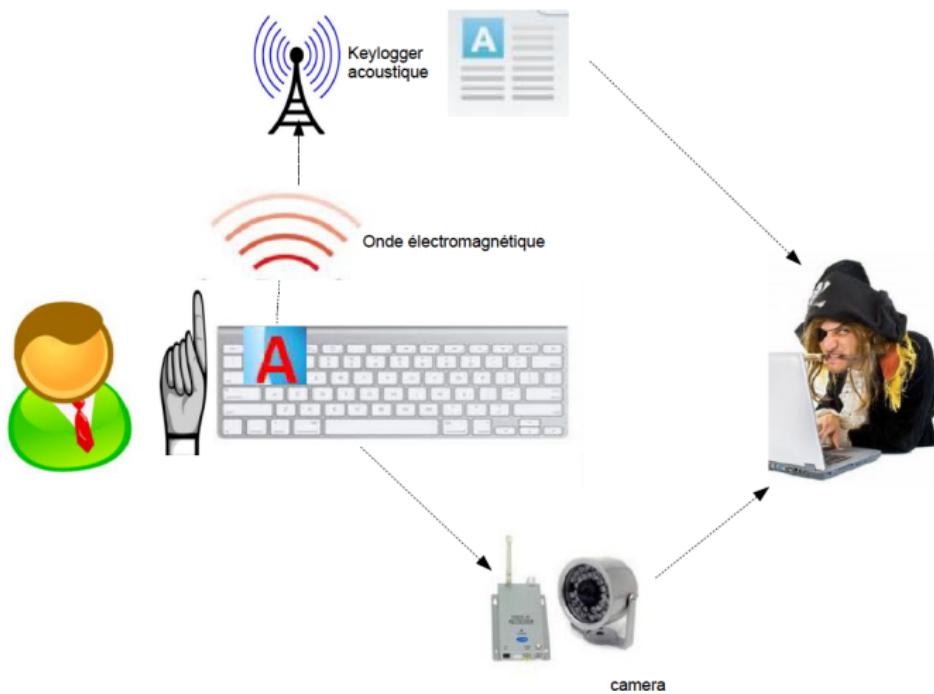


SerialGhost

Wi-Fi

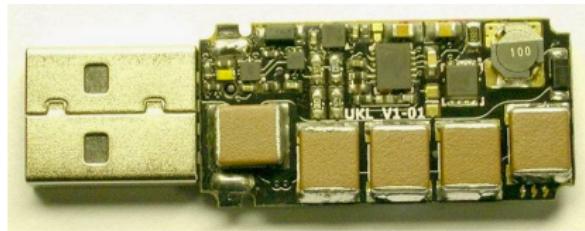
Accès physique à l'ordinateur

Autres keylogger



Accès physique à l'ordinateur

Une clé USB qui endomage votre ordinateur (USB Killer)



Killer 2.0 est équipé de condensateurs qui se chargent à -220V puis vident la charge accumulée sur les câbles d'alimentation du port USB jusqu'à ce que la machine décède. Ce qui ne prend pas bien longtemps.

source :

<http://hightech.bfmtv.com/internet/usb-killer-la-cle-usb-qui-tue-automatiquement-votre-ordinateur-921513.html>