

Méthodologie d'une attaque

Accès direct

- Accès direct à l'ordinateur
 - Utilisation de LiveCD et de clés USB
 - Offline NT Password & Registry Editor
 - Mise à blanc des mots de passe administrateur et ajout d'utilisateur dans le groupe administrateur locaux

```
*****
# Windows NT/2k/XP/Vista Change Password / Registry Editor / Boot CD
#
# (c) 1998-2008 Petter Nordahl-Hagen. Distributed under GNU GPL v2
#
# DISCLAIMER: THIS SOFTWARE COMES WITH ABSOLUTELY NO WARRANTIES!
#             THE AUTHOR CAN NOT BE HELD RESPONSIBLE FOR ANY DAMAGE
#             CAUSED BY THE (MIS)USE OF THIS SOFTWARE
#
# More info at: http://home.eunet.no/~pnordahl/ntpasswd/
# Email       : pnordahl@eunet.no
#
# CD build date: Sat Aug  2 00:59:36 CEST 2008
#*****

Press enter to boot, or give linux kernel boot options first if needed.
Some that I have to use once in a while:
boot nousb          - to turn off USB if not used and it causes problems
boot irqpoll        - if some drivers hang with irq problem messages
boot vga=ask        - if you have problems with the videomode
boot nodrivers      - skip automatic disk driver loading

boot:
```

Boot sur le livecd

Accès direct

- Accès direct à l'ordinateur

```
* Windows Registry Edit Utility Floppy / chntpw
* (c) 1997 - 2008 Petter N Hagen - pnoordahl@eunet.no
* GNU GPL v2 license, see files on CD
*
* This utility will enable you to change or blank the password of
* any user (incl. administrator) on an Windows NT/2k/XP/Vista
* WITHOUT knowing the old password.
* Unlocking locked/disabled accounts also supported.
*
* It also has a registry editor, and there is now support for
* adding and deleting keys and values.
*
* Tested on: NT3.51 & NT4: Workstation, Server, PDC.
*            Win2k Prof & Server to SP4. Cannot change AD.
*            XP Home & Prof: up to SP3
*            Win 2003 Server (cannot change AD passwords)
*            Vista 32 and 64 bit, Server 2008 32+64 bit
*
* HINT: If things scroll by too fast, press SHIFT-PGUP/PGDOWN ...
* =====
* There are several steps to go through:
* - Disk select with optional loading of disk drivers
* - PATH select, where are the Windows systems files stored
* - File-select, what parts of registry we need
* - Then finally the password change or registry edit itself
* - If changes were made, write them back to disk
*
* DON'T PANIC! Usually the defaults are OK, just press enter
*      all the way through the questions
*
* =====
* Step ONE: Select disk where the Windows installation is
* =====
*
* Disks:
* Disk /dev/sda: 10.7 GB, 10737418240 bytes
*
* Candidate Windows partitions found:
* 1 : /dev/sda1 10228MB (LBA), BOOT
*
* Please select partition by number or
* q = quit
* d = automatically start disk drivers
* m = manually select disk drivers to load
* f = fetch additional drivers from floppy / usb
* a = show all partitions found
* l = show probable Windows (NTFS) partitions only
* Select: f
```

Choix de la partition système

Accès direct

- Accès direct à l'ordinateur

```
* Win 2003 Server (cannot change AD passwords)
* Vista 32 and 64 bit, Server 2008 32+64 bit
* HINT: If things scroll by too fast, press SHIFT-PGUP/PGDOWN
*****
=====
There are several steps to go through:
- Disk select, with optional loading of disk drivers
- PATH select, where are the Windows systems files stored
- File-select, what parts of registry we need
- Then finally the password change or registry edit itself
- If changes were made, write them back to disk
DON'T PANIC! Usually the defaults are OK, just press enter
all the way through the questions
=====
# Step ONE: Select disk where the Windows installation is
=====
Disks:
Disk /dev/sda: 10.7 GB, 10737418240 bytes
Candidate Windows partitions found:
1 : /dev/sda1 10228MB (LBA), BOOT
Please select partition by number or
q = quit
d = automatically start disk drivers
m = manually select disk drivers to load
f = fetch additional drivers from floppy / usb
a = show all partitions found
l = show probable Windows (NTFS) partitions only
Select: [1]
Selected 1
Mounting from /dev/sda1, with assumed filesystem type FAT/UFAT/FAT32 and similar
Trying to mount FAT / UFAT / FAT32 etc
Success
=====
# Step TWO: Select PATH and registry files
=====
What is the path to the registry directory? (relative to windows disk)
[windows/system32/config] :
```

Chemin du registre

windows/system32/config

failles physiques

- Accès direct à l'ordinateur

```
=====  
# Step ONE: Select disk where the Windows installation is  
=====
```

Disk /dev/sda: 10.7 GB, 10737418240 bytes
Candidate Windows partitions found:
1 : /dev/sda1 10228MB (LBA), BOOT

Please select partition by number or
q = quit
d = automatically start disk drivers
m = manually select disk drivers to load
f = fetch additional drivers from floppy / usb
a = show all partitions found
l = show probable Windows (NTFS) partitions only
Select: [1]
Selected 1
Mounting from /dev/sda1, with assumed filesystem type FAT/VFAT/FAT32 and similar
Trying to mount FAT / VFAT / FAT32 etc
Success

```
=====  
# Step TWO: Select PATH and registry files  
=====
```

What is the path to the registry directory? (relative to windows disk)
(windows\system32\config)
EXPAND windows\system32\config

drwxr-xr-x	2	0	0	262144	Sep 24 17:56	Newsid Backup
-rwxr-xr-x	1	0	0	262144	Jan 7 13:51	default
-rwxr-xr-x	1	0	0	262144	Jan 7 13:51	sam
-rwxr-xr-x	1	0	0	13631488	Jan 7 15:39	security
-rwxr-xr-x	1	0	0	2621440	Jan 7 15:39	software
-rwxr-xr-x	1	0	0	8192	Sep 18 09:30	system
-rwxr-xr-x	15	0	0	8192	Sep 18 09:30	systemprofile
-rwxr-xr-x	1	0	0	262144	Sep 18 09:30	userdiff

Select which part of registry to load, use predefined choices
or list the files with space as delimiter
l - Password reset [sam system security]
e - RecoveryConsole parameters [software]
q = quit - return to previous
[1] :

Choix de l'action à exécuter

propose d'effacer un mot de passe

failles physiques

- Accès direct à l'ordinateur

```
What to do? [1] -> 3
SOFTWARE-hive not loaded, and there's where RecoveryConsole settings are
<>=====<> chntpw Main Interactive Menu <>=====<>
Loaded hives: <sam> <system> <security>
 1 - Edit user data and passwords
 2 - Syskey status & change
 3 - RecoveryConsole settings
 9 - Registry editor, now with full write support!
 q - Quit (you will be asked if there is something to save)

What to do? [1] -> 9
Simple registry editor. ? for help.
> q

<>=====<> chntpw Main Interactive Menu <>=====<>
Loaded hives: <sam> <system> <security>
 1 - Edit user data and passwords
 2 - Syskey status & change
 3 - RecoveryConsole settings
 9 - Registry editor, now with full write support!
 q - Quit (you will be asked if there is something to save)

What to do? [1] -> 1
===== chntpw Edit User Info & Passwords =====
RID  -- Username ----- Admin?  -- Lock? --
01f4  Administrator      ADMIN   dis/lock
03e3  ASPNET               ADMIN   dis/lock
01f5  HelpAssistant         ADMIN   dis/lock
03e2  rexor                 ADMIN   dis/lock
03ee  single_user            ADMIN   dis/lock

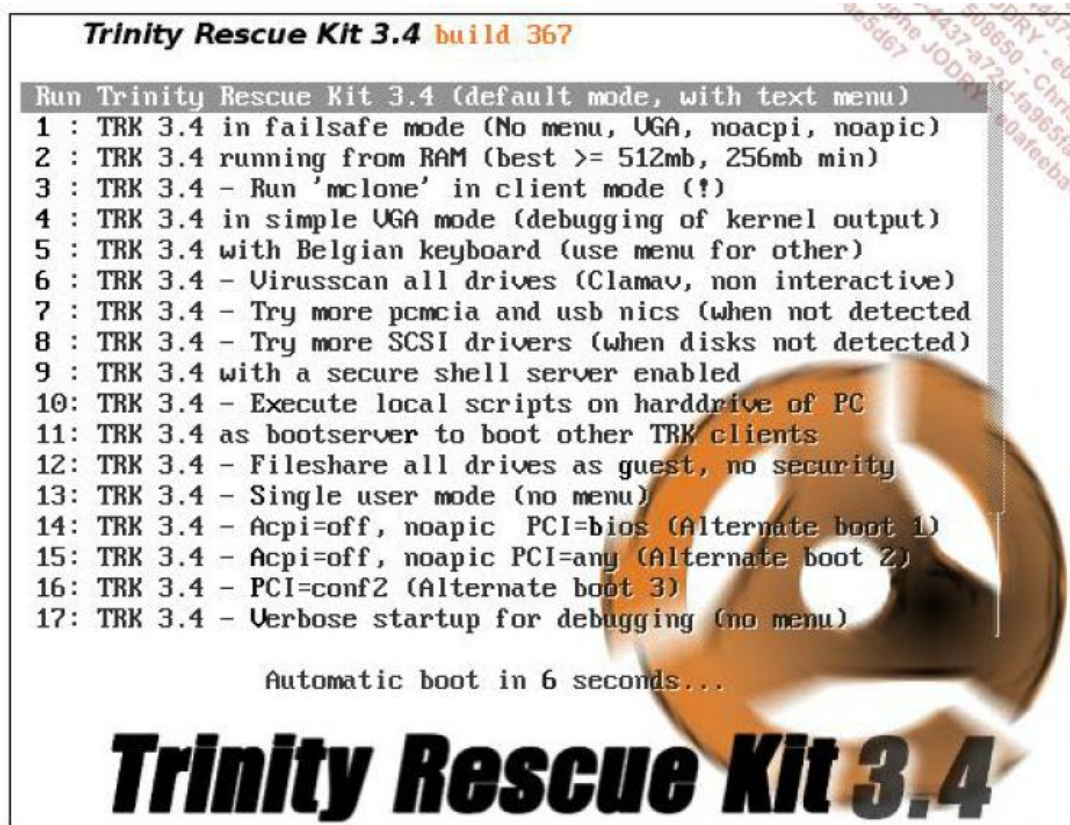
Select: ? - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator]
```

Reset du mot de passe administrateur

On quitte avec « ! », « q » et « y », l'écran suivant proposera de vérifier l'intégrité des disques, ignorer.

Accès direct

- Accès direct à l'ordinateur
 - Trinity Rescue Kit



Accès direct

- Accès direct à l'ordinateur
 - Trinity Rescue Kit

```
Trinity Rescue Kit easy menu
| Welcome
| TRK Help -->
| Keyboard layout selection -->
| Windows password resetting -->
| Mount all local filesystems
| Unmount all local filesystems
| Virus scanning -->
| Windows junkfile cleaning -->
| Mclone: computer replication over the network -->
| Backup and restore utilities-->
| Run a windows fileserver -->
| Run an ssh server
| Set an ip-address on the first adapter
| TRK Network boot server
| Trinity Remote Support (contact us first)
| Ethernet packet sniffing -->
| Try detecting more harddisk controllers
| Try detecting more USB and PCMCIA network adapters
| Midnight Commander
| Go to a shell
| Go to a shell and save all output to /tmp/terminal.out
| Quit this menu
| Poweroff computer
| Reboot without ejecting CD / usb stick

Use winpass to reset your password. Recommended is to just remove the password. This is the most
sure method.
You can also restore your original password database here.
```


Accès direct

- Accès direct à l'ordinateur
 - Trinity Rescue Kit

```
Trinity Rescue Kit easy menu
| Welcome
| TRK Help -->
| Keyboard layout selection -->
| Windows password resetting -->
| Mount all local filesystems
| Unmount all local filesystems
| Virus scanning -->
| Windows junkfile cleaning -->
| Mclone: computer replication over the network -->
| Backup and restore utilities-->
| Run a windows fileserver -->
| Run an ssh server
| Set an ip-address on the first adapter
| TRK Network boot server
| Trinity Remote Support (contact us first)
| Ethernet packet sniffing -->
| Try detecting more harddisk controllers
| Try detecting more USB and PCMCIA network adapters
| Midnight Commander
| Go to a shell
| Go to a shell and save all output to /tmp/terminal.out
| Quit this menu
| Poweroff computer
| Reboot without ejecting CD / usb stick

Use winpass to reset your password. Recommended is to just remove the password. This is the most
sure method.
You can also restore your original password database here.
```

Accès direct

- Accès direct à l'ordinateur
 - Trinity Rescue Kit

```
----- chntpw Edit User Info & Passwords -----  
| RID |----- Username -----| Admin? | Lock? --|  
| 01f4 | Administrateur             | ADMIN  |          |  
| 01f5 | Invit@                     |        | dis/lock |  
| 03e9 | SUPPORT_388945a0           |        | dis/lock |  
  
Select: ! - quit, . - list users, 0x<RID> - User with RID (hex)  
or simply enter the username to change: [Administrateur]  
  
RID      : 0500 [01f4]  
Username: Administrateur  
fullname:  
comment  : Compte d'utilisateur d'administration  
homedir  :  
  
User is member of 1 groups:  
00000220 = Administrateurs (which has 1 members)  
  
Account bits: 0x0210 =  
[ ] Disabled           | [ ] Homedir req.      | [ ] Passwd not req. |  
[ ] Temp. duplicate    | [X] Normal account    | [ ] NMS account     |  
[ ] Domain trust ac    | [ ] Wks trust act.    | [ ] Srv trust act   |  
[X] Pwd don't expir    | [ ] Auto lockout      | [ ] (unknown 0x08)  |  
[ ] (unknown 0x10)     | [ ] (unknown 0x20)    | [ ] (unknown 0x40)  |  
  
Failed login count: 0, while max tries is: 0  
Total login count: 6  
  
- - - - User Edit Menu:  
1 - Clear (blank) user password  
2 - Edit (set new) user password (careful with this on XP or Vista)  
3 - Promote user (make user an administrator)  
(4 - Unlock and enable user account) [seems unlocked already]  
q - Quit editing user, back to user select  
Select: [q] > 1  
Password cleared!  
  
Select: ! - quit, . - list users, 0x<RID> - User with RID (hex)  
or simply enter the username to change: [Administrateur] _
```

Trinity Rescue Kit 3.4

Accès direct

- Accès direct à l'ordinateur
 - Dumper la base SAM avec Backtrack



Accès direct

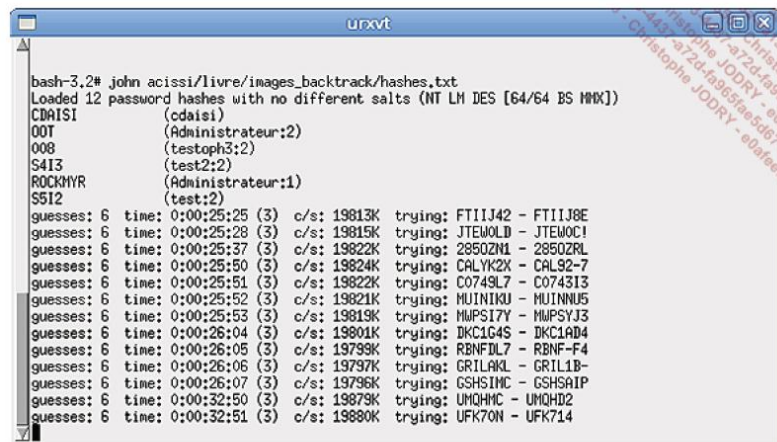
- Accès direct à l'ordinateur
 - Dumper la base SAM avec Backtrack

```
samdump2 /mnt/<partition>/Windows/System32/config/SYSTEM  
/mnt/Windows/System32/config/SAM> hash.txt
```

```
root@bt:~# samdump2 /mnt/hda2/Windows/System32/config/SYSTEM /mnt/hda2/Windows/System32/co  
nfig/SAM > hash-7.txt  
root@bt:~# cat hash-7.txt  
Administrateur:500:aad3b435b51404eeaad3b435b51404ee:6f9b6aa9a8f8033cef006d45ff5d0230:::  
Invit0:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
rezor:1000:aad3b435b51404eeaad3b435b51404ee:6f9b6aa9a8f8033cef006d45ff5d0230:::  
titi:1002:aad3b435b51404eeaad3b435b51404ee:36aa83bdcab3c9fdaf321ca42a31c3fc:::  
root@bt:~# █
```

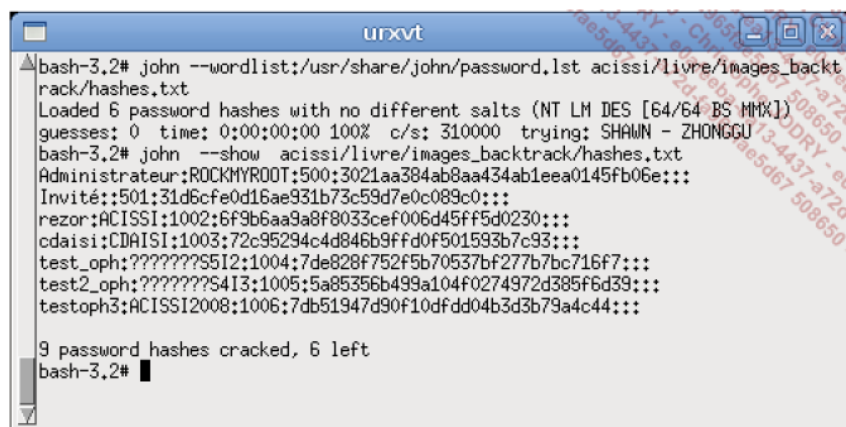
failles physiques

- Accès direct à l'ordinateur
 - John the Ripper



```
urxvt
bash-3.2# john acissi/livre/images_backtrack/hashes.txt
Loaded 12 password hashes with no different salts (NT LM DES [64/64 BS MMX])
CDaISI (cdaisi)
00T (Administrateur:2)
008 (testoph3:2)
S4I3 (test2:2)
ROCKMYR (Administrateur:1)
SSI2 (test:2)
guesses: 6 time: 0:00:25:25 (3) c/s: 19813K trying: FTIIJ42 - FTIIJ8E
guesses: 6 time: 0:00:25:28 (3) c/s: 19815K trying: JTEW0LD - JTEW0C1
guesses: 6 time: 0:00:25:37 (3) c/s: 19822K trying: 28502NL - 28502RL
guesses: 6 time: 0:00:25:50 (3) c/s: 19824K trying: CALYK2K - CAL92-7
guesses: 6 time: 0:00:25:51 (3) c/s: 19822K trying: C0749L7 - C0743I3
guesses: 6 time: 0:00:25:52 (3) c/s: 19821K trying: MUINIKU - MUINNU5
guesses: 6 time: 0:00:25:53 (3) c/s: 19819K trying: MWPSI7Y - MWPSYJ3
guesses: 6 time: 0:00:26:04 (3) c/s: 19801K trying: DKC1G4S - DKC1AD4
guesses: 6 time: 0:00:26:05 (3) c/s: 19799K trying: RBNF7L7 - RBNF-F4
guesses: 6 time: 0:00:26:06 (3) c/s: 19797K trying: GRILAKL - GRIL1LB
guesses: 6 time: 0:00:26:07 (3) c/s: 19796K trying: GSHSINC - GSHSAIP
guesses: 6 time: 0:00:32:50 (3) c/s: 19879K trying: UMQHMC - UMQHD2
guesses: 6 time: 0:00:32:51 (3) c/s: 19880K trying: UFK7ON - UFK714
```

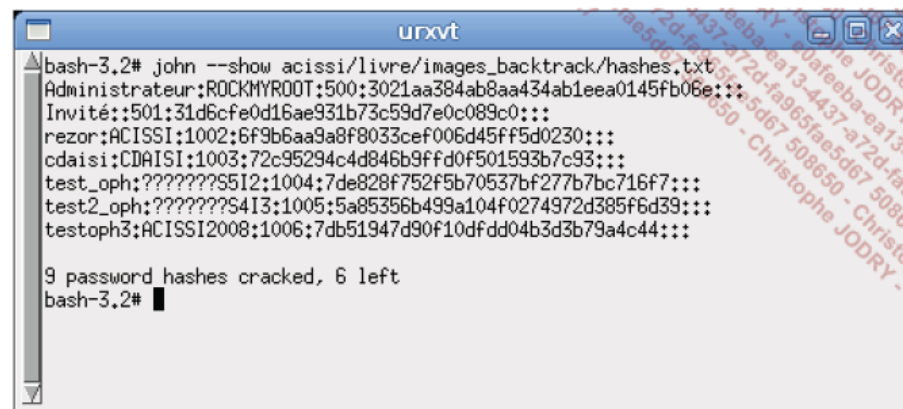
Le perceur de mot de passe John The Ripper



```
urxvt
bash-3.2# john --wordlist:/usr/share/john/password.lst acissi/livre/images_backtrack/hashes.txt
Loaded 6 password hashes with no different salts (NT LM DES [64/64 BS MMX])
guesses: 0 time: 0:00:00:00 100% c/s: 310000 trying: SHAWN - ZHONGGU
bash-3.2# john --show acissi/livre/images_backtrack/hashes.txt
Administrateur:ROCKMYROOT:500:3021aa384ab8aa434ab1eea0145fb06e:::
Invité::501:31d6cfe0d16ae931b73c59d7e0c089c0:::
rezor:ACISSI:1002:6f9b6aa9a8f8033cef006d45ff5d0230:::
cdaisi:CDaISI:1003:72c95294c4d846b9ff0f501593b7c93:::
test_oph:???????S5I2:1004:7de828f752f5b70537bf277b7bc716f7:::
test2_oph:???????S4I3:1005:5a85356b499a104f0274972d385f6d39:::
testoph3:ACISSI2008:1006:7db51947d90f10dfdd04b3d3b79a4c44:::

9 password hashes cracked, 6 left
bash-3.2#
```

"Brute force" en mode dictionnaire



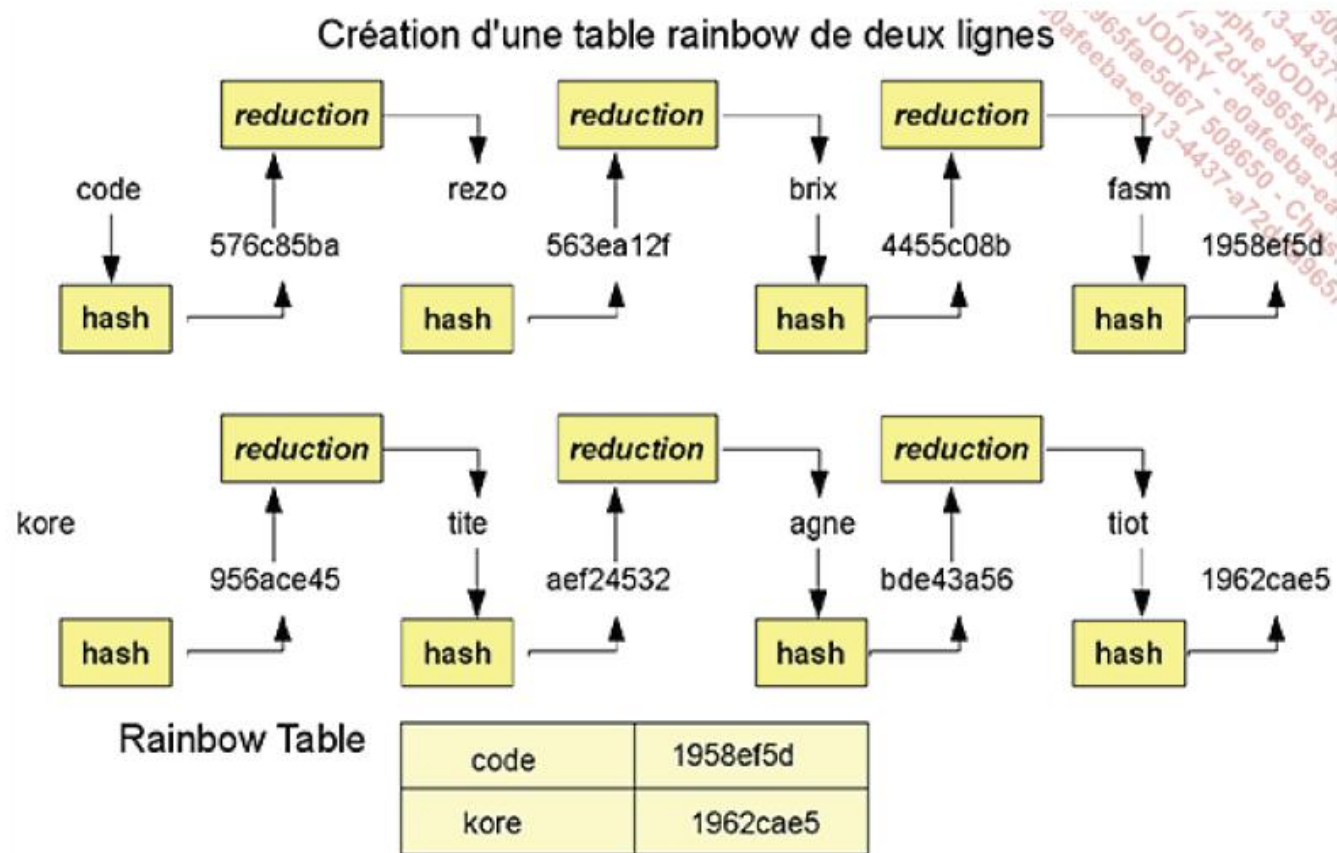
```
urxvt
bash-3.2# john --show acissi/livre/images_backtrack/hashes.txt
Administrateur:ROCKMYROOT:500:3021aa384ab8aa434ab1eea0145fb06e:::
Invité::501:31d6cfe0d16ae931b73c59d7e0c089c0:::
rezor:ACISSI:1002:6f9b6aa9a8f8033cef006d45ff5d0230:::
cdaisi:CDaISI:1003:72c95294c4d846b9ff0f501593b7c93:::
test_oph:???????S5I2:1004:7de828f752f5b70537bf277b7bc716f7:::
test2_oph:???????S4I3:1005:5a85356b499a104f0274972d385f6d39:::
testoph3:ACISSI2008:1006:7db51947d90f10dfdd04b3d3b79a4c44:::

9 password hashes cracked, 6 left
bash-3.2#
```

Visualisation de l'avancement du crack

Accès direct

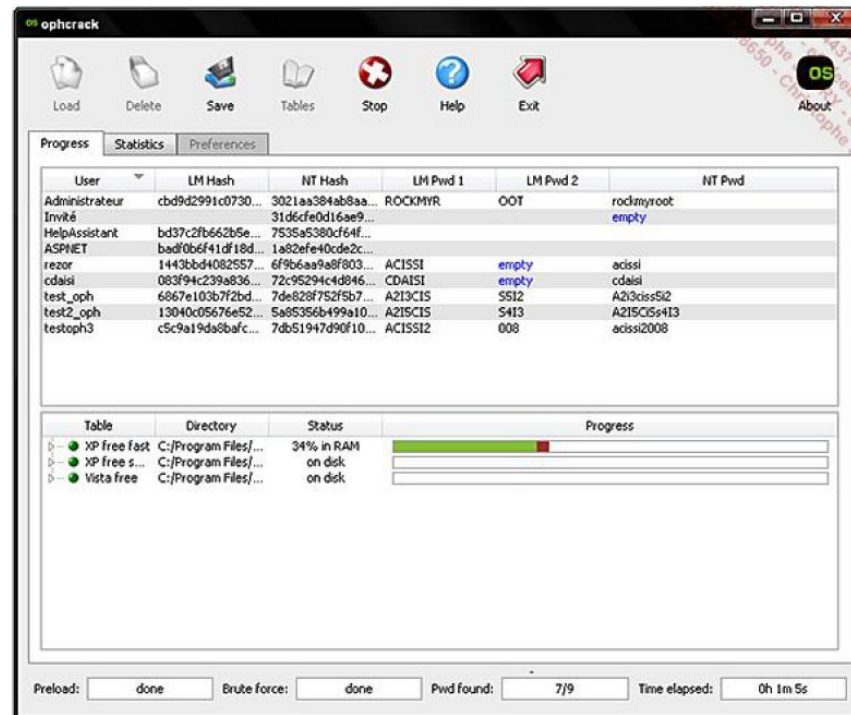
- Accès direct à l'ordinateur
 - Table Rainbow



Génération d'une table rainbow de deux lignes

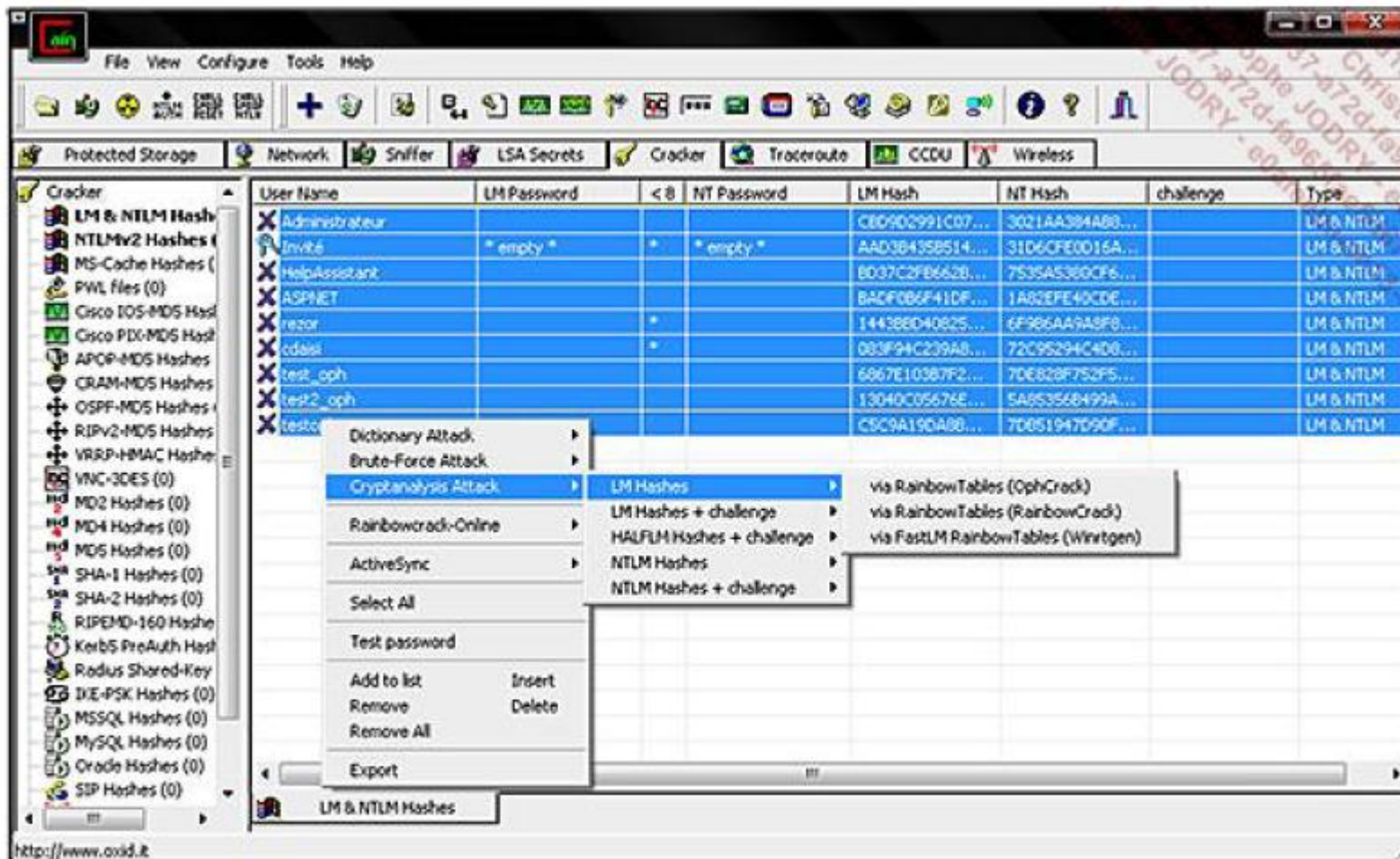
Accès direct

- Accès direct à l'ordinateur
 - Table Rainbow
 - Pour les générer: rtgen ou winrtgen ou site freerainbowtables
 - L'arme absolu: OPHCRACK



failles physiques

- Accès direct à l'ordinateur
 - L'arme absolu n° 2: logiciel Cain&Abel



Accès direct

- Accès direct à l'ordinateur
 - Les Keyloggers



Les keyloggers matériels



Insérés entre clavier et UC, ils sont très discrets



Le keylogger modulaire est invisible

Accès direct

- Accès direct à l'ordinateur
 - Les contremesures aux outils LiveCD?
 - Les contremesures aux keyloggers?

Social engineering

- Social engineering
 - Utiliser la pièce fragile qu'est l'humain
 - Ramy Badir: « Un ordinateur sécurisé est un ordinateur entreposé dans un hangar, et débranché »
 - Kevin Mitnick: « Je pourrais toujours trouver une personne assez aimable pour brancher l'ordinateur ! »
 - Exemple d'attaque:

Social engineering

Atravers S.A. est une multinationale de fabrication de jeux vidéo. Son siège social est situé dans un quartier réputé de Paris, et comme dans beaucoup d'autres entreprises, c'est là-bas que se prennent beaucoup de décisions. Jérôme le sait bien et se dit qu'une telle situation pourra lui permettre d'accéder à une copie du jeu vidéo dont la sortie est prévue pour dans quelques semaines.

Atravers .- « Société Atravers, bonjour »

Jérôme .- « Bonjour, ici Charles, du service informatique, au siège de Paris. Comment allez-vous ? »

Atravers .- « Ça va très bien, merci. »

Jérôme .- « Dites, on va devoir interrompre l'accès assez longtemps dans l'après-midi, pour des raisons de maintenance, et j'essaie de dresser une liste des gens à rétablir rapidement, pour que le travail puisse se faire correctement. Est-ce que vous pouvez travailler sans le téléphone et l'accès Internet durant l'après-midi ? »

Atravers .- « Cela me semble difficile, un standard sans Internet ni téléphone. Attendez, vous me faites peur, j'ai beaucoup de travail cet après-midi, des appels téléphoniques à passer, des réservations à effectuer, avec la sortie prochaine du jeu, on doit boucler toutes les tâches rapidement. Vous ne pouvez pas plutôt couper le week-end ? »

Jérôme .- « Malheureusement non, il faut vraiment qu'on intervienne aujourd'hui. Pour des raisons de sécurité nous devons changer pas mal de choses sur les serveurs et il faut faire cela rapidement. Mais rassurez-vous, c'est pour cela que j'appelle, cela peut très bien ne durer que quelques minutes pour vous. »

Atravers .- « Très bien, comment faire pour que ça aille vite ? »

Jérôme .- « Bien il me faut simplement deux ou trois renseignements, pour savoir quels serveurs vous utilisez, et puis votre nom d'utilisateur et votre mot de passe pour qu'on rétablisse votre connexion dès le début de l'après-midi. »

Atravers .- « J'utilise le G: et parfois aussi F:, mais le G: est le plus important parce que c'est sur celui-ci que l'on a les documents pour le travail ici. Mon nom d'utilisateur est josephine.gerard, par contre on a une note qui dit de ne jamais fournir le mot de passe ici, même au service informatique. Vous avez changé d'avis ? »

Jérôme .- « Pour le mot de passe, non, nous changeons simplement de serveur, les autres employés devront remettre leur mot de passe au fur et à mesure, cela va prendre plusieurs heures parce qu'il faut qu'on appelle chaque service. Pour aller plus vite, je vais remettre le vôtre directement, et avec un peu de chance vous pourrez travailler dès votre retour du déjeuner. »

Atravers - « D'accord, en effet, je comprends. Mon mot de passe est F4SMTDB3mm. Pourrais-je le changer une fois votre opération terminée ? »

Jérôme - « Tout à fait ! »

Jérôme termine alors les discussions avec les questions anodines.

Jérôme a obtenu des informations, mais surtout le mot de passe d'un employé sur le système d'information de la société. Il lui faudra maintenant utiliser ces informations, pour tenter une escalade de privilège par exemple, à moins que la société en question ne limite pas les accès aux données techniques.

Au cours de cet échange, Jérôme a dû faire preuve de répondant, pour diminuer l'inquiétude de la collaboratrice face à l'idée de donner son mot de passe. Mais le plus important, c'est que la personne lui a fourni les informations dans l'espoir d'être aidée, alors même que le but de Jérôme est tout l'inverse.

Social engineering

- Social engineering
 - Formes d'attaques
 - La plus simple et la plus frontale
 - Indirecte ou complexe
 - Techniques utilisées
 - Les médias:
 - Téléphone: simple et anonyme
 - Mails de phishing
 - SMS
 - TailGating
 - Psychologie
 - Absence de méfiance
 - Ignorance
 - Crédulité
 - Altruisme et besoin d'aide
 - Intimidation

Social engineering

- Social engineering
 - Profil de l'attaquant
 - Ce sont des appels téléphoniques, des discussions où il faut manipuler les personnes en inspirant divers sentiments au gré des besoins; faut savoir s'exprimer et jouer sur les intonations.
 - Charisme, audace, mais aucune place à l'improvisation: l'attaque est toujours préparée avec graphique représentant tout les directions que pourrait prendre la conversation.
 - Imposteur, menteur
 - Limier
 - Minutieux
 - Profil de la cible
 - Point d'entrée de l'entreprise; Si possible non sensibilisée au Social Engineering
 - Ou service informatisé mais non informatique

Social engineering

- Social engineering
 - Contre-mesures:
 - Classification des données: constitution d'une matrice qui régit les accès aux informations. (différence entre données et informations?)
 - Classer les informations en fonction de la catégorie:
 - Financière; juridique; technique; publique
 - Puis classer des personnes dans des groupes, avec quel accès à quel catégorie
 - Enfin, classer les informations par voie d'accès: écrit, mail, téléphone
 - Principes utilisées par l'armée française: Public, Restreint, confidentiel défense, secret défense, très secret défense.
 - Sensibilisation du personnel

Attaques à distance

- Anonymat obligatoire car tout acte de piratage répréhensible par la loi:
 - Adresse IP
 - Comment?
 - Rebond sur un autre système (prise de main à distance sur d'autre PC avant d'attaquer etc... -> cf BOTNET
 - Utilisation de proxy. Exemple TOR ou JonDonym

Connaître sa victime

- Les outils

- Netcat

- Netcat permet de créer soit un client soit un serveur. Ce programme permet de faire rapidement de l'envoi de fichiers, de créer une porte dérobée, des ordinateurs zombies et bien plus, et ce, sans avoir besoin de recourir à un langage.

- Nmap:

- Scanner de port; prise d'empreinte TCP/IP
 - Capable de déterminer l'OS, la topologie d'un réseau...

```
Starting Nmap 4.76 ( http://nmap.org ) at 2009-05-13
00:10 CEST
Interesting ports on 192.168.0.11:
Not shown: 1995 closed ports
PORT      STATE      SERVICE
22/tcp    open       ssh
80/tcp    open       http
111/tcp   open       rpcbind
68/udp    open|filtered dhcpd
111/udp   open|filtered rpcbind
5353/udp  open|filtered zeroconf
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.17 - 2.6.25
Network Distance: 0 hops
```

- Scapy

- Metasploit

- Metasploit intègre une base d'exploits (plus d'une centaine), c'est-à-dire de codes usant de vulnérabilités, pour exécuter arbitrairement une commande sur une machine.

L'attaque par le réseau

- Rappel :

Netstat permet de connaître les services et ports ouverts sur votre machine, ainsi que les différents états des connexions.

Lancez **netstat -a**

Les états :

- **ESTABLISHED** : connexion établie
- **SYN_SENT & SYN_RECV** : connexion en cours d'établissement
- **CLOSE** : socket fermé
- **CLOSE_WAIT** : socket en attente de fermeture
- **LISTEN** : un service est ouvert sur ce port

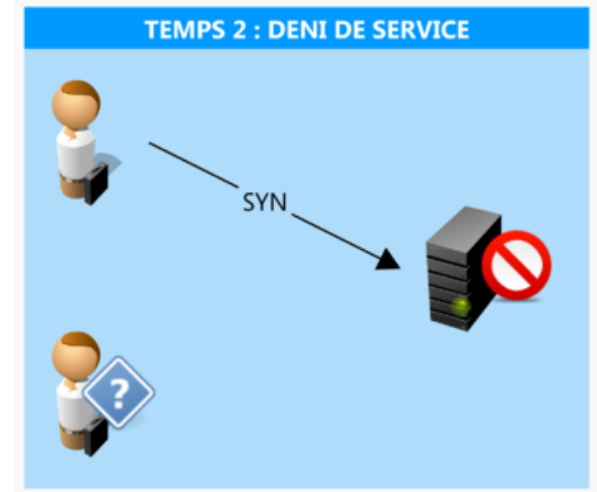
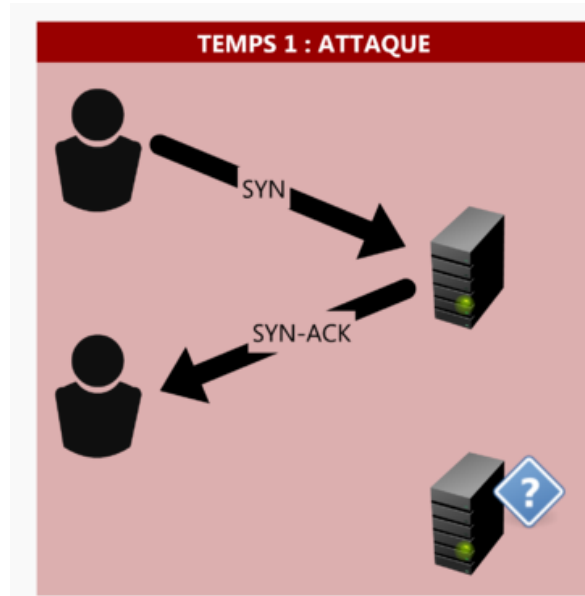
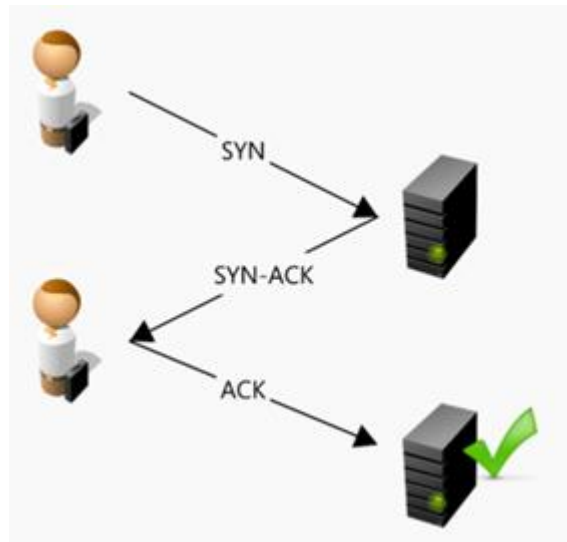
L'attaque par le réseau

- Dos et DDoS:

- Un DoS (Denial of Service) est une attaque de déni de service. Le but d'un déni de service est de faire tomber un serveur.
- L'attaque par Syn flood est l'une des attaques les plus répandues, elle consiste à demander des connexions et ne pas y répondre. Lors d'une demande de connexion, le serveur est en attente et bloque pendant un certain temps une partie de ses ressources pour cette nouvelle connexion.
- Le but est d'envoyer plus de demandes de connexion qu'il ne peut en traiter dans un temps donné. Le serveur ne pourra plus subvenir au besoin des vrais clients.
- L'outil hping2 permet d'effectuer ce genre d'attaque. Nous pouvons l'installer via la commande `apt-get install hping2`.
- Exemple de tentative de DoS sur le port 80 à l'adresse IP : ipserveur
- `hping2 ipserveur -I eth0 -q -i u1 -S --rand-source -p 80 &`
- Le DDoS (Distributed Denial of Service) est similaire au DoS, mais l'attaque se fait à partir de plusieurs machines.
- Une attaque DoS est simple à contrer, il suffit d'établir une règle dans le pare-feu afin de bloquer l'adresse IP attaquante. Dans le cas d'un DDoS cela se complique énormément.

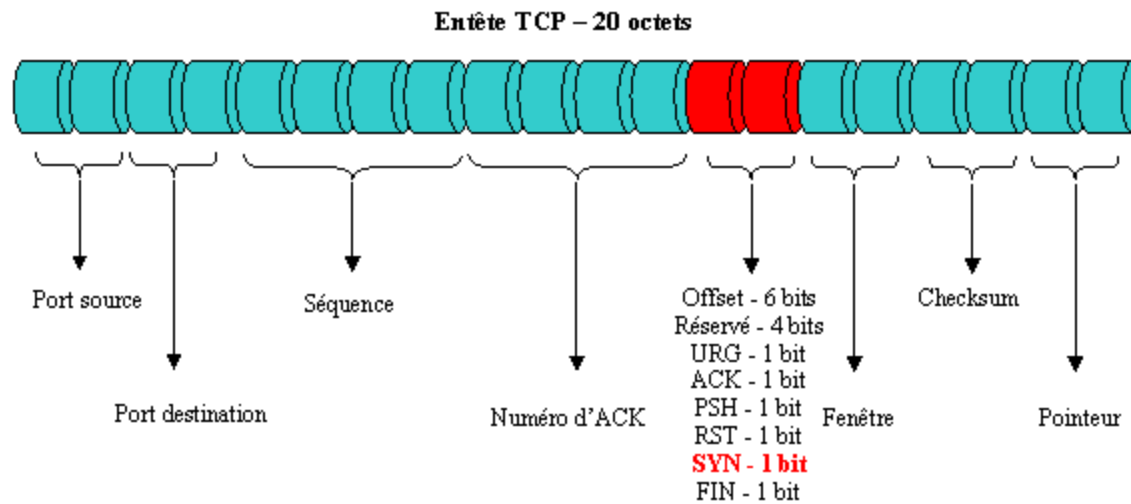
L'attaque par le réseau

- Syn Flood:



L'attaque par le réseau

- Syn Flood:



L'attaque par le réseau

- Syn Flood:

La cible recevant la synchronisation TCP mémorise cette demande nécessitant donc de la mémoire et du processeur. Voici l'état des connexions d'un Windows XP avant la réception d'un Synflood :

```
C:\WINDOWS\System32\cmd.exe
C:\>netstat -nao

Connexions actives

Proto  Adresse locale      Adresse distante    Etat
TCP    0.0.0.0:21          0.0.0.0:0           LISTENING           1472
TCP    0.0.0.0:135         0.0.0.0:0           LISTENING           696
TCP    0.0.0.0:445         0.0.0.0:0           LISTENING           4
TCP    0.0.0.0:1027        0.0.0.0:0           LISTENING           1472
TCP    0.0.0.0:1400        0.0.0.0:0           LISTENING           956
TCP    0.0.0.0:3389        0.0.0.0:0           LISTENING           872
TCP    10.10.101.4:139     0.0.0.0:0           LISTENING           4
UDP    0.0.0.0:445         *:*:                1472
UDP    0.0.0.0:3456        *:*:                872
UDP    10.10.101.4:123     *:*:                4
UDP    10.10.101.4:137     *:*:                4
UDP    10.10.101.4:138     *:*:                4
UDP    127.0.0.1:123       *:*:                872

C:\>
```

Et voici après la réception des demandes de SYN :

```
C:\WINDOWS\System32\cmd.exe
C:\>netstat -nao

Connexions actives

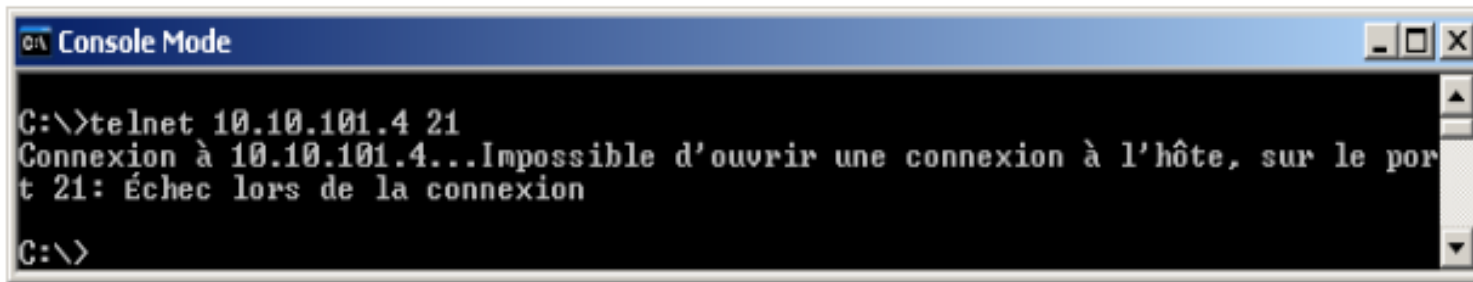
Proto  Adresse locale      Adresse distante    Etat
TCP    0.0.0.0:21          0.0.0.0:0           LISTENING           1472
TCP    0.0.0.0:135         0.0.0.0:0           LISTENING           696
TCP    0.0.0.0:445         0.0.0.0:0           LISTENING           4
TCP    0.0.0.0:1027        0.0.0.0:0           LISTENING           1472
TCP    0.0.0.0:1400        0.0.0.0:0           LISTENING           956
TCP    0.0.0.0:3389        0.0.0.0:0           LISTENING           872
TCP    10.10.101.4:21      41.87.113.37:6436    SYN_RECEIVED        1472
TCP    10.10.101.4:21      52.27.144.38:36466   SYN_RECEIVED        1472
TCP    10.10.101.4:21      54.142.99.119:10799  SYN_RECEIVED        1472
TCP    10.10.101.4:21      94.130.209.157:50495 SYN_RECEIVED        1472
TCP    10.10.101.4:21      98.64.203.101:6976   SYN_RECEIVED        1472
TCP    10.10.101.4:21      113.146.100.187:20324 SYN_RECEIVED        1472
TCP    10.10.101.4:21      144.95.169.90:22118  SYN_RECEIVED        1472
TCP    10.10.101.4:21      186.136.158.10:19551 SYN_RECEIVED        1472
TCP    10.10.101.4:139     0.0.0.0:0           LISTENING           4
UDP    0.0.0.0:445         *:*:                1472
UDP    0.0.0.0:3456        *:*:                872
UDP    10.10.101.4:123     *:*:                4
UDP    10.10.101.4:137     *:*:                4
UDP    10.10.101.4:138     *:*:                4
UDP    127.0.0.1:123       *:*:                872

C:\>
```

La cible passe les requêtes reçues en SYN_RECEIVED. Cet état est temporaire, le temps de durée de vie est variable en fonction de la pile IP.

L'attaque par le réseau

- Syn Flood:



```
C:\>telnet 10.10.101.4 21
Connexion à 10.10.101.4...Impossible d'ouvrir une connexion à l'hôte, sur le port 21: échec lors de la connexion
C:\>
```

* testé depuis la machine ayant effectuée le Synflood

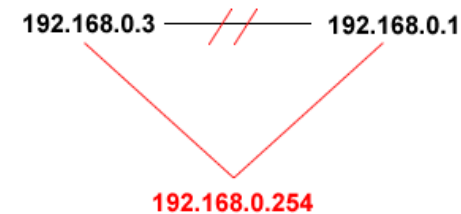
L'attaque par le réseau

- Man In The Middle

- Théorie:

- L'attaque de l'homme du milieu ou Man In The Middle (MITM), est une attaque utilisant au moins trois ordinateurs.

- Deux ordinateurs communiquent ensemble, un troisième au milieu casse la liaison entre les deux ordinateurs, et se fait passer pour l'autre entité, il intercepte et renvoie les communications et peut de plus les modifier.



- Chaque ordinateur, routeur sur un réseau possède une adresse Mac. Chaque entité possède une table ARP, celle-ci permet de stocker la relation Adresse IP/Adresse Mac des ordinateurs du réseau.

- Nous pouvons lister cette table via la commande : `arp -a`

```
user@ordi:~$ arp -a
nas-02-81-77.local (192.168.0.12) à 00:0d:a2:17:17:17 [ether] sur eth0
? (192.168.0.254) à 00:07:cb:00:00:00 [ether] sur eth0
```

- L'attaque a pour but de falsifier sur les ordinateurs du réseau la relation adresse Mac/adresse IP afin de pouvoir réceptionner et retransmettre les données. Cela est possible grâce à la table ARP qui met en cache cette association.

L'attaque par le réseau

- Failles Wi-Fi

- Cracker un réseau WEP

- Outil: la suite Aircrack

- Cracker un réseau WPA

- Outil: pyrit . Cassage du mot de passe par dictionnaire. Plus complexe que le WEP.

- Téléphonie sur IP

- La Voix sur IP a connu un essor important en France pour les entreprises, mais aussi pour les particuliers grâce notamment à la vulgarisation des offres Triple Play. Le phreaking, la technique de piratage dédiée à la téléphonie se rapproche donc inévitablement du hacking. En effet, si la téléphonie utilise le réseau informatique, elle hérite de ses faiblesses.

- Écoute de conversation:

- VOIPONG permet l'enregistrement en fichier wav d'une conversation voip
 - présent sur le live CD Backtrack

- Usurpation de ligne

- Package sipcrack (live CD Backtrack)

L'attaque applicative

- Par le Web

- Motivations de l'attaquant:

- Rendre le site indisponible, c'est un DoS (Denial of Service). Les raisons peuvent être multiples comme mettre en difficulté un concurrent commercial ou juste pour jouer, pour prouver une certaine maîtrise technique.
 - Modifier le contenu d'un site pour compromettre la réputation.
 - Récupérer des informations non autorisées.
 - Prendre le contrôle du serveur dans l'objectif de lancer une attaque sur un autre serveur en tout anonymat, ou encore pour avoir une base d'attaque de l'entreprise où se situe le serveur.
 - ...
 - Les raisons des attaques sont très diverses, du simple adolescent qui veut s'amuser ou prouver sa compétence technique aux terroristes qui peuvent paralyser une entreprise ou récupérer des données sensibles.

Méthodes CEH



Méthode et outillage SANS 560

Reconnaissance

Whois

DNS

- Nslookup
- DIG

Metadonnees

- Exiftools
- Strings

Scanning

TCPDUMP

WIRESHARK

NMAP

SCAPY

NESSUS

NSE

Exploitation et Post- Exploitation

METASPLOIT

NETCAT

Password Attack

JOHN THE
RIPPER

OPHCRACK

CAIN & ABEL

Wireless et Web App

Aircrack ng

Cowpatty

Nikto

??

Autres méthodes

- PTES
- OSSTMM
- NIST Special Publication 800-115
- OWASP

Comment s'entraîner?

- Damn Vulnerable Linux: <http://www.damnulnerablelinux.org>
- Damn Vulnerable Web App: <http://www.dvwa.co.uk>
- <http://google-gruyere.appspot.com/>
- <https://www.hacking-lab.com/>
- <http://insecure.org/> pour les outils.
- <http://pentestlab.org/10-vulnerable-web-applications-you-can-play-with/>