# Attaques SSH en “brute-force”

- De quoi s'agit-il ?
- Analyse typologique
- Analyse de risque
- Comment réagir ?

# De quoi s'agit-il ?

- Premières traces en Mai 2005
- Tentatives de login via SSH sur des comptes dont l'existence est probable
- Probablement des scripts avec des dictionnaires
- Un grand nombre de tentatives pour chaque attaque :
  - d'une centaine à plusieurs milliers de tentatives (plus de 600 pour chaque source IP en moyenne)

# Extraits de logs :

/var/log/messages

```
Sep  3 18:20:24 nangate sshd(pam_unix)[871]: check pass; user unknown
Sep  3 18:20:24 nangate sshd(pam_unix)[871]: authentication failure; logname= uid=0 euid=0
      tty=NODEVssh ruser= rhost=by214eb.eas.asu.edu
Sep  3 18:23:41 nangate sshd(pam_unix)[1025]: authentication failure; logname= uid=0 euid=0
      tty=NODEVssh ruser= rhost=by214eb.eas.asu.edu  user=root
```

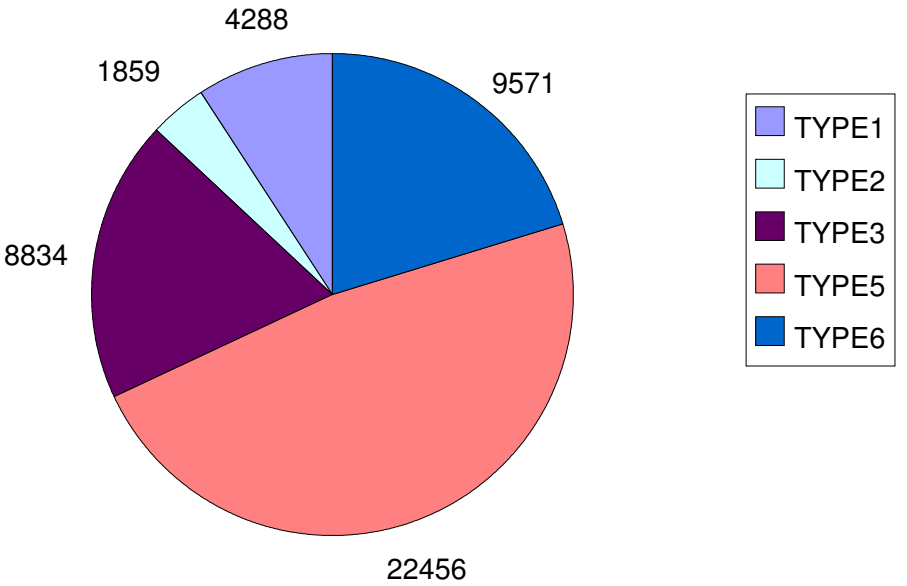
/var/log/secure

```
Sep  3 18:20:19 nangate sshd[871]: Illegal user staff from 149.169.227.108
Sep  3 18:20:26 nangate sshd[871]: Failed password for illegal user staff from 149.169.227.108
      port 33761 ssh2
Sep  3 18:21:17 nangate sshd[902]: Failed password for ftp from 149.169.227.108
      port 35651 ssh2
```

# Analyse typologique

- Données LPSC (*) :
  - dates : 18 mai au 8 Août 2006
  - 47008 tentatives, soit près de 4000 par semaine !
- Classification :
  - TYPE1 : root
  - TYPE2 : system account
  - TYPE3 : well-known account
  - TYPE5 : login/login
  - TYPE6 : login/password

Répartition par types d'attaques




(*) Données collectées au LPSC par Jean Mirasolo et Bernard Boutherin

# Origine des attaques

- Données LPSC :
  - 74 sources IP différentes pour les 47008 tentatives
  - CN (Chine) et US (USA) en majorité
  - 80% des réseaux d'origine présentent une adresse de messagerie (e-mail,abuse) pour recueillir les plaintes.

# Analyse de risque

- nombre de machines exposées (accessible de l'internet en SSH) ?
- probabilité de trouver le mot de passe d'un compte existant à priori (root,...) ?
- probabilité de trouver le compte d'un utilisateur et le bon mot de passe ?

# Comment réagir

- S'assurer que les mots de passe sont solides
- Limiter les machines exposées
- Limiter les comptes exposés
- Plainte à “abuse”
- Détecter et bloquer les tentatives d'attaques par brute-force
- Limiter les dégâts en cas de succès

# Solidité des mots de passe

- Sous la responsabilité des utilisateurs, mais :
  - Campagne d'éducation
  - Détection des mots de passe trop simples (John-the-Ripper)
  - Dispositifs imposant une certaine qualité des mots de passe (password strength enforcement)
- Une solution radicale : n'autoriser que les logins basés sur une paire de clés.
  - Qui protège sa clé privée par un mot de passe ?
  - Comment dépose t'on sa clé publique sur un serveur SSH inaccessible par login classique ?

# Limiter machines et comptes exposés

- Machines :
  - machines cibles : le minimum (passerelle pour le labo ?)
  - contrôle de l'origine des connexions (listes blanches)
- Comptes :
  - politique de fermeture des comptes
  - as-t on besoin que le compte root puisse être accédé directement ?

# Plainte à “abuse”

- Pratiquée par Bernard Boutherin
  - 95 protestations depuis début 2006
  - 85% sans réponse
  - 12 réponses automatiques, 2 réponses utiles
- Contre :
  - le temps nécessaire pour écrire le mail (automatisation ?)
- Pour :
  - prévient l'administrateur du site distant
    (si il y quelqu'un qui s'en occupe et s'il est de bonne foi)

# Limiter l'escalade...

- corriger les vulnérabilités permettant l'escalade de privilège
  - pas toujours facile (mise à jour kernel = recompiler les modules)
  - au moins sur les machines exposées
- surveillance renforcée (tripwire, alarmes sur les logs,...)
- zone DMZ pour les machines exposées ?

# Détection et blocage des tentatives

- Systèmes basés sur iptables :
  - Daemon-Shield, ssdfilter, Fail2Ban,
- Systèmes basés sur Tcp-Wrappers :
  - DenyHosts, sshblock.sh
- Port-Knocking
- Pam_abl (auto-blacklist)

# Solution expérimentée : Pam_abl

- Module PAM (Pluggable Authentication Modules)
- Enregistre les échecs sur un même compte ou depuis une même adresse IP
- Interdit l'accès si un seuil nb echecs/période est dépassé.
- Exemple de configuration :

```
#/etc/sysconfig/pam_abl.conf
#debug
host_db=/var/lib/abl/hosts.db
host_purge=12h
host_rule=*/sshd:10/1h,30/1d
```

# Pam_abl en action

/var/log/secure :

```
Sep  4 09:56:33 nangate pam_abl[17415]:
Blocking access from host-200-110-95-106.telconet.net to service sshd, user rpcuser
Sep  4 09:56:37 nangate pam_abl[17418]:
Blocking access from host-200-110-95-106.telconet.net to service sshd, user rpm
Sep  4 10:33:43 nangate pam_abl[21097]:
Blocking access from host-200-110-95-106.telconet.net to service sshd, user NOUSER
```

- Quelques statistiques (du 13 Août au 13 Septembre 2006) :
  - 16788 tentatives SSH bloquées par pam_abl
  - dont 2489 sur des comptes existants (root compris)
  - dont 2207 sur le compte root

# Pam_abl : Bilan

- Complètement «  transparent  » pour les utilisateurs
  - Aucun utilisateur ne s'est vu bloqué à la suite d'une erreur de mot de passe  (grâce à des seuils généreux!)
- Une protection efficace
  - Plus aucune chance de réussite au delà du seuil réglé
- Simple à mettre en oeuvre
  - tire parti de la modularité des PAMs
  - pas besoin de toucher à sshd

# Conclusion

- La stratégie “plainte systématique” peut-elle faire diminuer les attaques ?
  - le taux de réponses laisse penser le contraire mais c'est utile cependant.
- Les pirates sont-ils en train de s'adapter ?
  - de plus en plus de tentatives isolées, sur root, notamment
- Conserver l'accessibilité de nos services pour nos utilisateurs nomades tout en les protégeant (air connu!)
  - la bonne solution doit être efficace sans gêner les utilisateurs.

OpenOffice.org

# Références

- Whitedust : Recent SSH Brute-Force Attacks (by A.St Onge)
  http://www.whitedust.net/article/27/Recent%20SSH%20Brute
- Whitedust : SSH Brute-Force Attacks: Update (by A.St Onge)
  http://www.whitedust.net/article/34/SSH%20Brute-Force%20
- Samhain Labs: Defending against brute force ssh attacks
  http://la-samhna.de/library/brutessh.html
- PAM_ABL
  http://www.hexten.net/pam_abl/
- Port-Knocking
  http://www.portknocking.org/