Session N°: S14

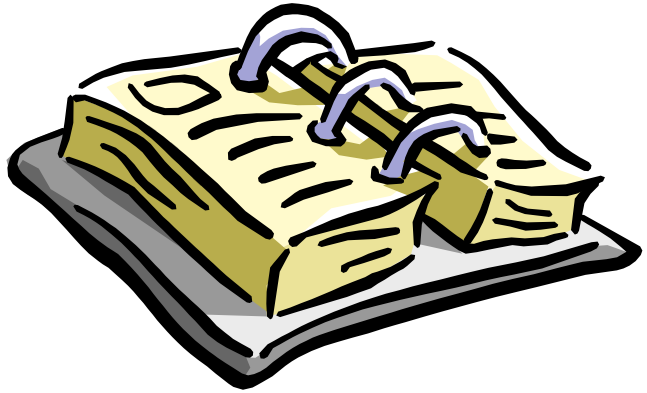
GOOGLE HACKING

Patrick Chambet
Consultant Senior
Edelweb / Groupe ON-X – http://www.edelweb.fr
http://www.chambet.com – patrick at chambet.com

EdelWeb

Planning

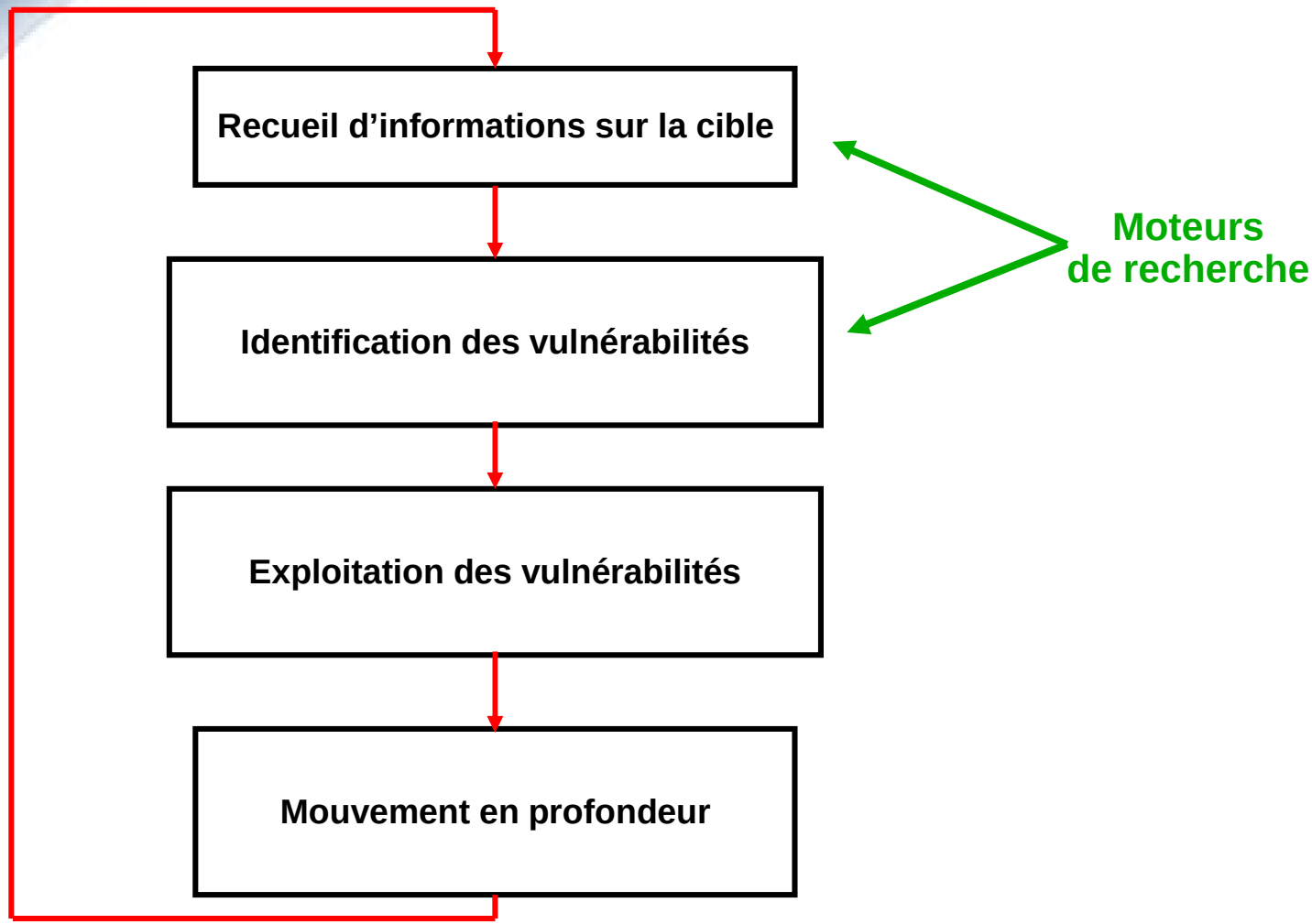
- Généralités
- Quelques exemples
- Recommandations
- Conclusion



Généralités

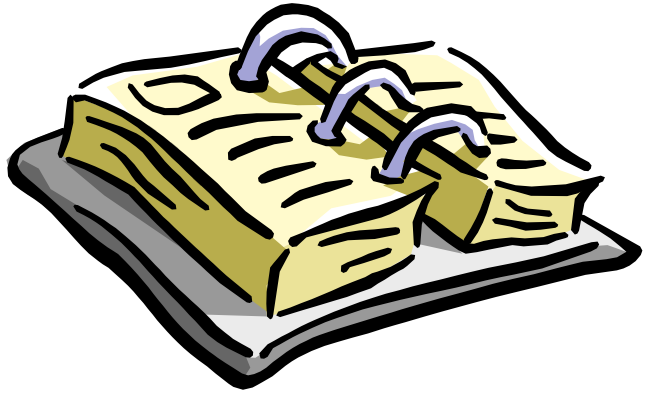
- Le recueil d'informations est la première étape lors d'un test d'intrusion (ou d'une attaque réelle)
- Les moteurs de recherche sont des outils de test évidents et très utilisés par les attaquants
  - Passifs
  - Furtifs
  - Utilisent l'énorme « mémoire » d'Internet
    - Cache de Google
    - Google groups
    - http://www.archive.org

Déroulement d'une intrusion



Planning

- Généralités
- Quelques exemples
- Recommandations
- Conclusion



Quelques exemples (1/7)

- Identification passive de la nature du serveur Web
- Détection invisible des proxies HTTP et FTP sortants de l'entreprise
- En-têtes SMTP
  - Plus besoin d'envoyer un faux mail ou un mail à un utilisateur inexistant !
- Accès à des fichiers sensibles ou d'anciennes versions de pages Web retirés des serveurs Web mais toujours présents dans le cache de Google

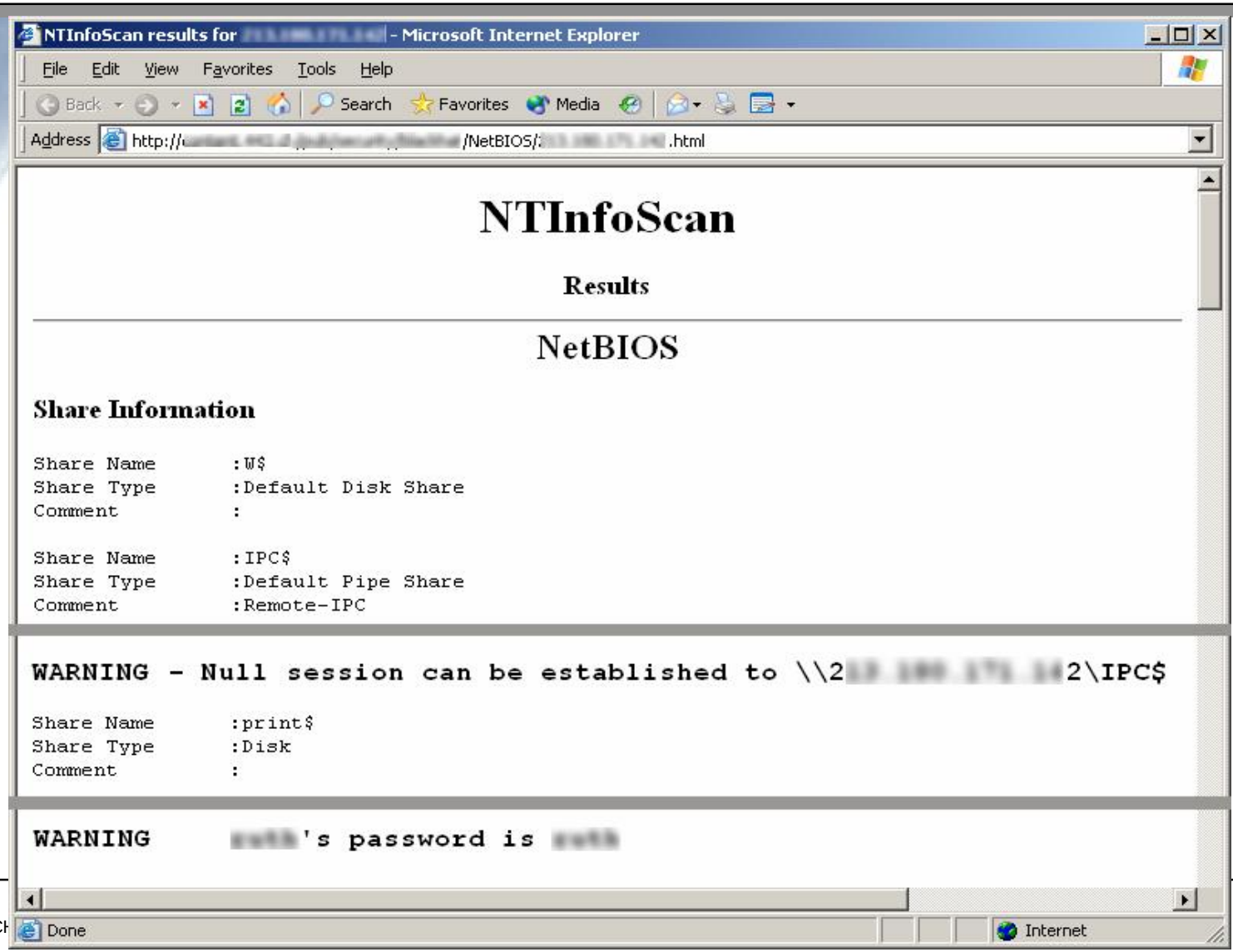
Quelques exemples (2/7)

- Caractères spéciaux
  - `"toto1.toto2" +toto –titi`
- Mots-clés Google très utiles
  - `filetype:abc`
  - `site:toto.com`
  - `intext:toto`
  - `[all]intitle:toto`
  - `[all]inurl:toto`
  - `link:www.toto.com`
  - `cache:www.toto.com/titi.html`
  - `related:www.toto.com/titi.html`
  - `phonebook:Bill Gates+WA`
  - `define:toto`

Quelques exemples (3/7)

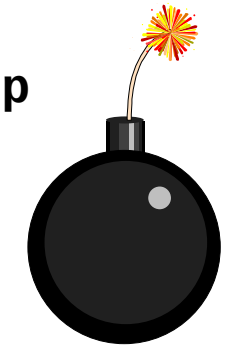
- Parcourir un site « offline »
  - `site:toto.com` -> renvoie toutes les pages en cache du site toto.com
  - Scanner de CGI furtif
- Découverte de mots de passe
  - `"Index of" htpasswd / passwd`
  - `filetype:xls username password email`
  - `"WS_FTP.LOG"`
  - `"config.php"`
  - `allinurl: admin mdb`
  - `service filetype:pwd` (FrontPage)

Quelques exemples (4/7)



Quelques exemples (5/7)

- Recherche de données utiles pour un attaquant
  - `"robots.txt" "Disallow:" filetype:txt`
  - `inurl:_vti_cnf` (FrontPage files)
  - `allinurl:winnt/system32/`
  - `allinurl:/msadc/Samples/selector/showcode.asp`
  - `allinurl:/examples/jsp/snp/snoop.jsp`
  - `allinurl:phpinfo.php`
  - `ipsec filetype:conf`
  - `intitle:"error occurred" ODBC request WHERE (SELECT|INSERT)`
  - `"mondomaine.com" nessus report`
  - `"report generated by"`
  - `"Terminal Services Web Connection"`



Quelques exemples (6/7)

Messages d'appel à l'aide

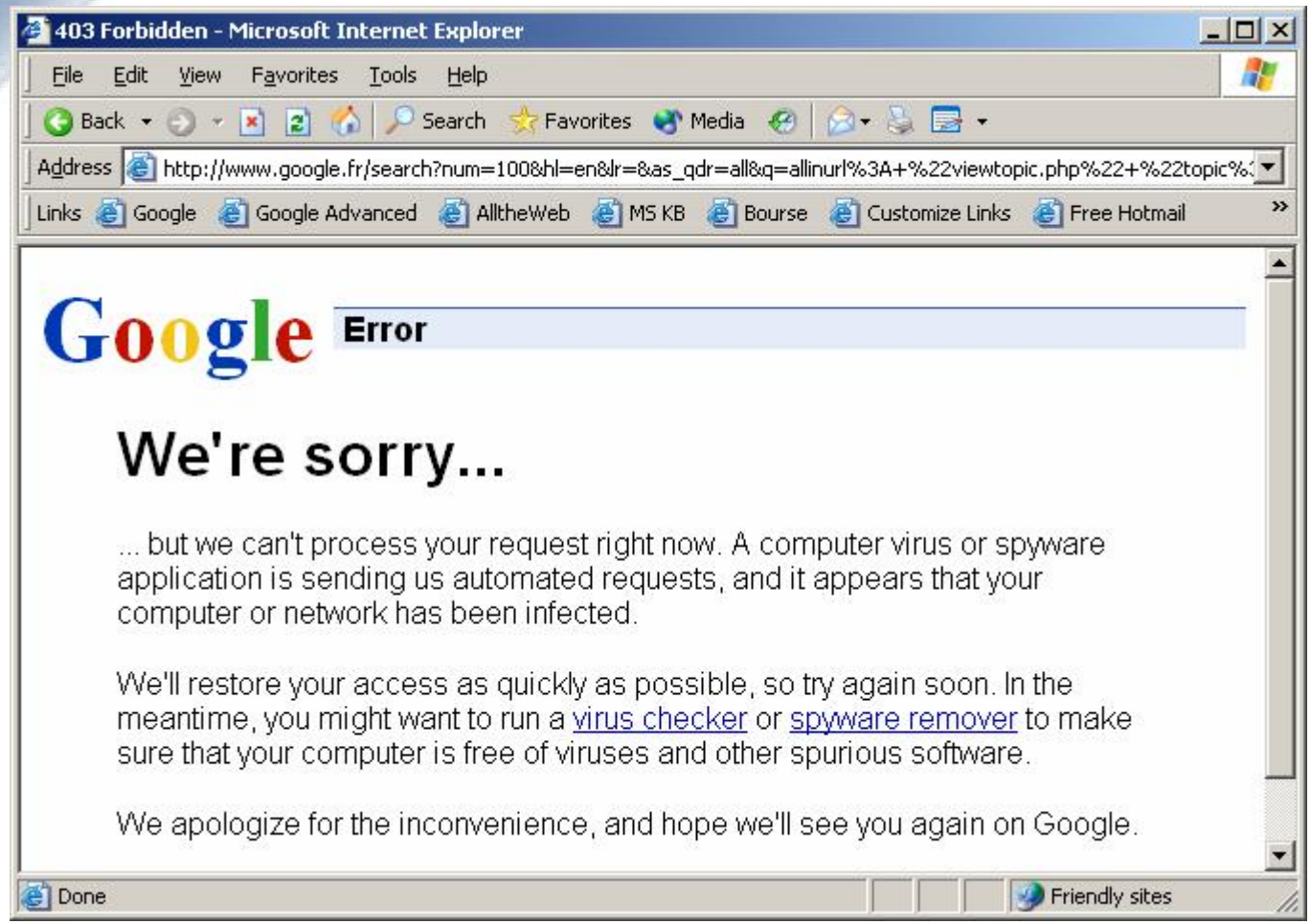
```
"I have the net-to-net configuration:

                  x.x.x.202    x.x.x.31
Localhost================Router================Remotehost
x.x.x.205                                          x.x.x.32

I work on Linux Red Hat 2.4.18 with x509 patched freeswan
1.99. I have updated my ipsec.conf configuration file with:
"conn net-to-net
     left=x.x.x.x
     (...)
"
The password is: (bip)
My problem is the following: (…)
Please, help me quickly !
Thanks a lot,
Jack"
```

Quelques exemples (7/7)

- **Les éléments de recherche peuvent être construits pour y inclure des vulnérabilités et des exploits connus**
  - **Exemple: vulnérabilité phpBB et vers Santy.A et .B**
    - **http://www.google.com/search?num=100&hl=en&lr=&as_qdr=all&q=allinurl%3A+%22viewtopic.php%22+%22{choix aléatoire entre "t", "p" et "topic“}%3D[nombre aléatoire entre 0 et 30000]%22&btnG=Search**
    - **Tentative d’exploitation de la vulnérabilité phpBB Remote URLDecode Input Validation (BID 11672)**

- **Outils automatisés de recherche de vulnérabilités**
  - **SiteDigger 2.0 de FoundStone**
    - **http://www.foundstone.com/resources/proddesc/sitedigger.htm**
    - **Nécessite l’installation de GoogleAPI**
  - **Athena**
    - **http://www.buyukada.co.uk/projects/athena/**

Exemple: ver Santy (réaction de Google)

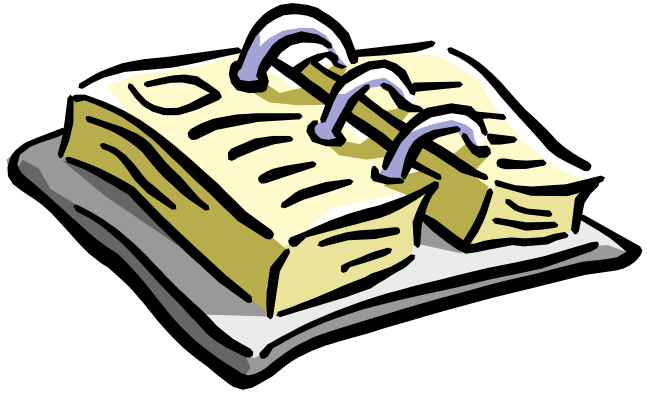


Effets indirects

- **Social engineering**
  - **Identification d'ex-employés, maintenant dans des entreprises concurrentes**
  - **Informations personnelles sur les administrateurs et les salariés d'une entreprise**
    - **Hobbies**
    - **Compétences**
    - **Niveaux d'expertise et de motivation**
    - **Amis et réseaux relationnels**
    - **Etc.**

Planning

- Généralités
- Quelques exemples
- Recommandations
- Conclusion



Recommandations (1/2)

- **Sur vos serveurs Web**
  - **Appliquez les derniers correctifs de sécurité et sécurisez le serveur (HTTP + PHP + …)**
  - **Désactivez le directory browsing**
  - **Ne placez pas de données sensibles sans authentification**
    - **Même dans un répertoire caché**
  - **Ne faites pas confiance à du masquage d'URL basé sur des scripts, du java ou des ActiveX**
  - **Analysez les requêtes Google qui ont conduit vers des données sensibles sur votre site et modifiez-le en conséquence**
    - **Logs HTTP, header « Referer: »**
    - **Honeypots Web et honeytokens**
      - **GHH: http://ghh.sourceforge.net/**

Recommandations (2/2)

- **Contrôlez le contenu de Google**
  - Informations sur votre entreprise
  - Informations sur vos utilisateurs et employés
  - Liens pointant vers vos sites Web
  - Organisez une veille régulière
- **Demandez à Google de supprimer certains résultats de recherche de son cache**
  - http://www.google.com/remove.html

Conclusion

- Google s'avère être l'allié des pen-testers et des attaquants
  - Et même des vers
- Il est important de faire attention aux informations présentes sur le Web à propos de votre entreprise
  - Une veille régulière est nécessaire
- N'hésitez pas à demander la modification ou la suppression d'une information vous concernant

Liens

- Google
  - Google APIs: http://www.google.com/apis/
  - Retrait de résultats: http://www.google.com/remove.html
- http://www.hackingspirits.com/eth-hac/papers/ Demystifying%20Google%20Hacks.pdf
- “Googledorks”
  - http://johnny.ihackstuff.com/index.php?module=prodreviews
- http://www.searchlores.org/
- http://www.theregister.co.uk/2001/11/28/the_google_attack_engine/
- Outils
  - Athena: http://www.buyukada.co.uk/projects/athena/
  - SiteDigger 2.0: http://www.foundstone.com/resources/proddesc/sitedigger.htm
  - GHH: http://ghh.sourceforge.net/

Questions / réponses