Pentests : réveillez-moi, je suis en plein cauchemar !

Marie BAREL – Consultant SSI /
Expertise juridique TIC

orange Business Services

- La mission du « pentesteur » : détecter et exploiter des vulnérabilités d'un SI cible
- Objectifs Client : évaluer le degré d'exposition aux menaces, mettre en lumière des voies d'accès détournées, …
- Démarche type audit « boîte noire »

  (communication d'une liste d'adresses IP ou d'une adresse de sous-réseau)
  - Phase 1 : recueil d'informations sur la cible et cartographie
  - Phase 2 : identification des vulnérabilités
  - Phase 3 : exploitation
  - Phase 4 : collecte de preuves >

  « **mission complete** »

Contexte

Introduction

Tests intrusifs, une opération à « haut risque » ?

Nature de l'évènement	Risque juridique	Mesures de protection
1. Tests sur un système sans autorisation (ex. tests « avant vente »)	Article 323-1 C.Pén. Responsabilité contractuelle Article 1382 et s. C.Civ.	Contrat : caractère obligatoire
2. Erreur sur la cible		Contrat/organisation projet : étape de validation
3. Tests sur une partie du SI hors le champ de responsabilité du client		Contrat : vérification du pouvoir du signataire
4. Dépassement du périmètre contractuel des tests		Contrat : périmètre et *durée* Organisationnel : étape de validation
5. SI cible hébergé par un tiers sur des ressources dédiées ou mutualisées		Autorisation de tiers
6. Tests impliquant l'attaque de systèmes tiers		

1. Risques liés à la cible

- L'article 323-1 du Code pénal : « le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende. »
  - Acte matériel : acceptation active (« *tous modes de pénétration* ») et passive (mise sur écoute, interception)
  - Intention frauduleuse : CA Paris, 5 avril 1994
    - **« sans droit »**
      - Absence d'autorisation (expresse ?) du maître du système : CA Toulouse, 21 janvier 1999
      - Personne non habilitée, se sachant dépourvue d'autorisation : TGI Vannes, 13 juillet 2005
    - **« en connaissance de cause »**
      - Ne pas avoir agi par erreur
      - Avoir conscience de l'irrégularité de son acte

De l'accès frauduleux

- Caractère obligatoire du contrat
- Durée et modalités des tests
  - Période de légalité des tests
  - Spécification de dates et plages horaires
- Étape de validation
  - Vérification de la qualité et du pouvoir du signataire
  - Validation Client du périmètre
    - Ex. fourniture du schéma de topologie du réseau vu de l'extérieur
- Collecte des autorisations de tiers

Mesures de protection

- **La « boîte à outils »** du chargé de test
  - **Outils « passifs »** : utilisés pendant la phase de « découverte » du SI cible
    - *Sniffers* (*Whireshark, …*)
    - Scanners de ports (*nmap*, *hping*, *netcat*, …)
    - Analyseurs DNS (*Dig*, *NSlookup*, …)
    - Scanners de vulnérabilités (*Nessus*, …)
  - **Outils « offensifs »** : utilisés pour l'exploitation de vulnérabilités
    - Librairies *d'exploits* (*Metasploit, …*)
    - Bases d'*exploits* personnels
    - Logiciels de cassage de mots de passe (*Cain&Abel*, *John the Ripper*, …)
    - …

Autres programmes : outils dédiés pour des besoins spécifiques
ex. *Kismet* et *Aircrack* pour le Wi-Fi

2. Risques liés aux outils

Nature de l'évènement	Risque juridique	Mesures de protection
7. Non maîtrise des outils entraînant une atteinte au SI Client	Responsabilité contractuelle Articles 323-2 et 323-3 Code pénal	Contrat: outils et tests autorisés, responsabilité, assurance Etape de validation
8. Attaque « d'opportunité » au cours de la période des tests	Responsabilité contractuelle (devoir de conseil, d'information et d'alerte)	Contrat/Organisation projet: - alerte sur les failles critiques - capacité Client à distinguer opérations de test / intrusion
9. Récupération sur le SI Client d'outils du Prestataire	Article 323-3-1 Code pénal	Contrat : responsabilité
10. Mise en œuvre d'outils permettant l'interception de correspondances	Article 226-15 Code pénal	Cf. risques liés aux résultats
11. Recours aux techniques de rétro conception logicielle (systèmes et applications propriétaires)	Articles 335-2 et 335-3 CPI (contrefaçon)	Autorisation de tiers

Tableau des hypothèses

- Éviter les situations à risque
  - Ex. Scans semi-automatisés s'exécutant sans surveillance ; SI truffé d'applications propriétaires aux interactions imprévisibles
- Confiance dans les outils
  - Étape de qualification des outils
- Limites des outils
  - Exemple de *nmap* cité dans MISC (HS n°1- nov. 2007)

Règle générale : pas d'implantation de charge utile susceptible de perturber le système cible !

Maîtrise des outils

Nature de l'évènement	Risque juridique	Mesures de protection
12. Alerte de sécurité déclenchée par une opération de test en cours	Dépôt de plainte	Contrat : autorisation de réalisation de tests intrusifs Organisation projet : données d'identification
13. Atteintes au SI cible	Responsabilité contractuelle	Contrat : méthodes autorisées Étape de validation
14. Accès à et/ou révélation d'informations confidentielles	Responsabilité contractuelle	Contrat : confidentialité
15. Accès à des données personnelles des Utilisateurs du SI audité	Art. 226-15 Code Pénal Art. 9 C.Civ.	Contrat : confidentialité Organisationnel : information préalable ?
16. Découverte de la présence de données pénalement répréhensibles	Article 1382 Code civil (faute) Complicité en raison du silence ?	Principe de transparence (art. 5, Charte FPTI)

3. Risques liés aux résultats

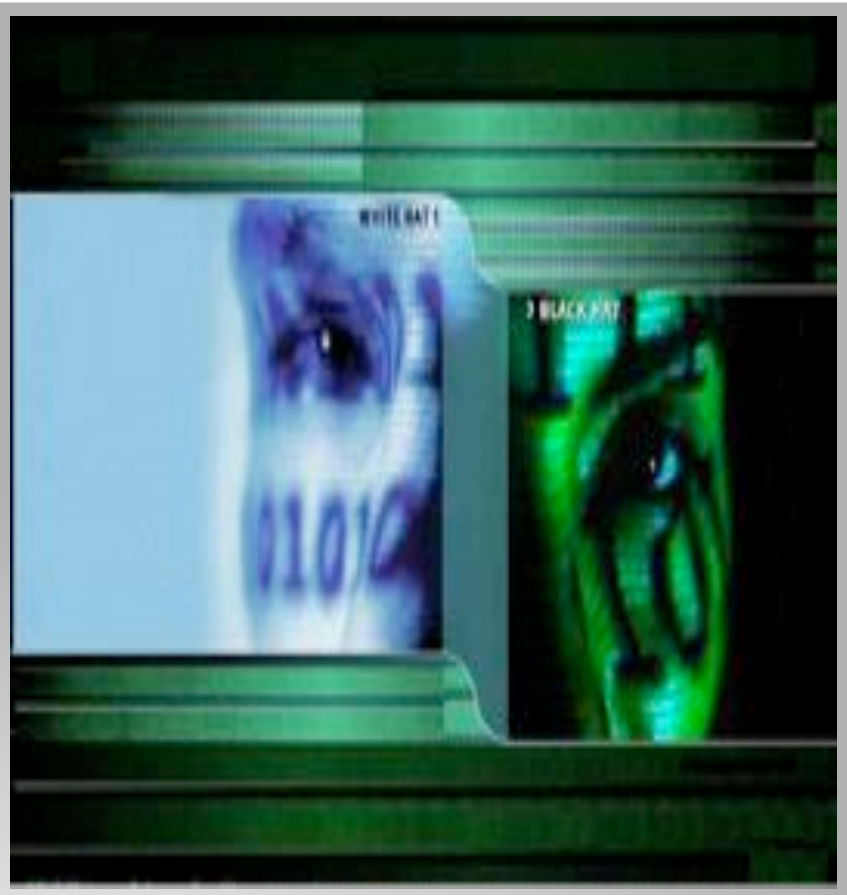
- Cas des contenus illictes :
  - Le Prestataire informe le Client de toute **pratique illicite ou anormale** qu'il aurait pu constater lors du déroulement des tests intrusifs (art. 5 Charte FPTI)

- Cas des contenus à caractère personnel
  - Un Client **ne peut valablement autoriser** l'accès au contenu de fichiers et de correspondances privées
  - L'auditeur doit se garder d'accéder au contenu de fichiers ou messages **portant une indication manifeste de leur nature privée**

Cas d'accès à des contenus

- Le contrat : des **dispositions clés** garantissant le bon déroulement de la prestation

- Charte de la FPTI et **déontologie** du Prestataire



Bilan

Du contrat à l'éthique

RETEX d'un RSSI …

- Les tests intrusifs ne peuvent être réalisés « sans aide externe »
- Le **périmètre à tester** doit être déterminé non pas en fonction de la valeur que vous accordez à un système, mais de la valeur que les attaquants peuvent leur accorder
- Le rapport doit certes mesurer les faiblesses, mais aussi mettre en avant les forces de sécurisation des systèmes : **des tests intrusifs aux tests de solidité !**

Conclusion

Contact

Marie BAREL
Consultant SSI
Expertise juridique TIC

Silicomp-AQL orange Business Services
marie.barel@aql.fr


Questions