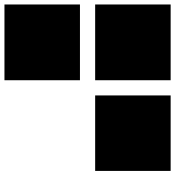
SYNACKTIV
DIGITAL SECURITY

# Outils et techniques pour les attaques ciblées

*Retours d'expériences sur la conception et la réalisation de tests d'intrusion « Red-Team »*

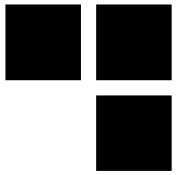
Présenté 17/03/2014
Pour JSSI OSSIR 2014
Par Renaud Feil

# Agenda



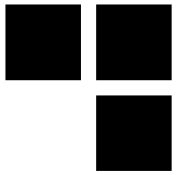
- **Objectif :**
  - Présenter des outils et des techniques pouvant être mis en œuvre pour simuler une attaque ciblée dans un contexte professionnel
- **L'objectif choisi :**
  - Accéder au réseau interne
- **Trois vecteurs d'attaques proposés :**
  - Envoi d'e-mails malveillants
  - Ingénierie sociale pour récupérer des identifiants d'accès distants
  - Intrusion physique en vue de connecter un *implant* sur le réseau
- **Avertissement :**
  - Respecter les contraintes légales et les règles d'éthique
  - Anonymiser les informations personnelles dans le rapport

# Evolution des tests d'intrusion



- **Un peu d'histoire :**
  - 1967 : *Joint Computer Conference* par les experts de la RAND Corporation et de la NSA
  - 1971 : *tiger teams* & James P. Anderson pour l'USAF
  - 1995 : premiers tests d'intrusion commerciaux en France
- **Aujourd'hui :**
  - Multiplication des méthodologies et des certifications
  - Intégration des tests d'intrusion dans les cycles de développement
  - La sécurité n'est pas totalement un échec
- **Limites :**
  - L'intégration des tests d'intrusion dans le cycle de développement des applications limite leur aspect réaliste
  - La sécurité d'une application ou d'un système n'est pas la sécurité de l'organisation dans son ensemble

# Définitions



- **Attaques ciblées :**
  - Reconnaissance préalable et planification en fonction de la cible
  - Objectifs définis : récupérer de l'information, détourner des processus métiers
  - Opération courte durée (*Hunting)* ou longue durée (*Farming)*
- **Tests d'intrusion *Red-Team* :**
  - Simuler une attaque ciblée de courte durée
  - Interactions légères avec les membres de l'organisation ciblée
  - Périmètre large
  - Fenêtre de test plus longue que dans un test d'intrusion conventionnel

# Reconnaissance et planification

- **Objectifs :**
  - Identifier les systèmes accessibles sur Internet
  - Créer un organigramme simplifié de la société
  - Identifier les implantations physiques
  - Récupérer des coordonnées téléphoniques et des e-mails
  - Sélectionner les meilleurs scénarios pour les prises de contact
  - Faire valider les scénarios par le commanditaire
- **Critères de choix d'un bon scénario :**
  - Efficience (résultat optimal pour une faible complexité)
  - Faible risque de découverte
  - En cas de soupçon par un interlocuteur, *plausible deniability*

# Outils pour la reconnaissance

- **Moteurs de recherches et réseaux sociaux :**
  - Google, Google Maps & Street View, mais aussi les autres moteurs de recherche !
  - LinkedIn, Facebook, et équivalents locaux
  - Bases *whois*, énumération DNS
  - Recherche itérative et complète
- **Autres outils :**
  - *theHarvester* : Récupération d'e-mails, etc.

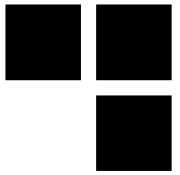
    *$ python theHarvester.py -d domaine.com -b all*
  - *Metagoofil* : Récupération des métadonnées des documents bureautiques

    *$ python metagoofil.py -d synacktiv.com -t pdf,doc,xls,ppt,odp,ods,docx,xlsx,pptx -l 200 -n 50 -o tmp -f results.html*

# Reconnaissance++

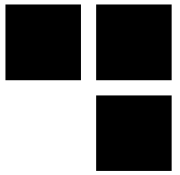
- **Compromettre un système vulnérable exposé sur Internet ?**
  - Est-il vraisemblablement connecté, directement ou indirectement, au WAN ciblé ?
  - Pourrait-t-il stocker des mots de passe identiques à ceux du réseau ciblé ?
  - Est-ce que son nom DNS est dans un domaine pouvant être utilisé dans le cadre d'une campagne de phishing ?
  - Est-ce que des membres de l'organisation cible s'y connectent régulièrement (attaque dite « du point d'eau ») ?

# Protéger son organisation contre les opérations de reconnaissance



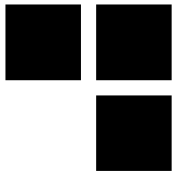
- **Prévenir :**
  - Recensement et protection ou fermeture des systèmes accessibles depuis Internet
  - Sensibilisation aux risques liés aux réseaux sociaux
- **Surveiller :**
  - Surveillance pro-active régulière pour identifier les informations accessibles publiquement sur l'organisation
  - Élimination des informations les plus sensibles

# Envoi d'e-mails malveillants



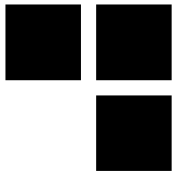
- **Objectifs :**
  - Compromettre un poste de travail pour établir un tunnel vers le réseau interne
  - Puis passer en tests d'intrusion interne en ayant déjà un poste de travail compromis
- **Cibler les interfaces de l'entreprise qui *doivent* ouvrir les pièces jointes :**
  - Service commercial : appel d'offre
  - Service marketing : plaquette pour participer à un salon
  - RH : candidature
- **Avertissement : éviter la compromission d'un ordinateur personnel**
  - Vérification de l'en-tête HTTP *User-Agent* et de l'adresses IP source
  - Test du domaine Windows d'appartenance de la machine
- **Avertissement 2 : éviter l'escalade en cas de détection**
  - En-tête SMTP spécifique pour prévenir l'investigateur qu'il s'agit d'une simulation

# Outils de *spear phishing*



- **Déroulement :**
  - Serveur de contrôle
  - Exécutable
  - Document Office contenant une macro
  - Lien vers un serveur web
  - Réservation et utilisation d'un nom de domaine crédible (*masociete-sa.com*)
  - Exploit client fiable (navigateur, JVM, Flash, Acrobat)
  - Peu importe les *0-days* !
  - Contournement de l'antivirus en utilisant un code sur-mesure (ou une *obfuscation* d'un code existant)
  - Choix du canal de communication avec Internet (HTTP CONNECT avec réutilisation du mot de passe sur le serveur proxy, DNS, SMTP)
  - Utilisation d'un certificat développeur

# Protéger son organisation contre les attaques ciblées par e-mails



- **La sensibilisation atteint ses limites**
- **Importance des mesures de protection techniques :**
  - *Top 35 Strategies to Mitigate Targeted Cyber Intrusions*
  - *« At least 85% of the targeted cyber intrusions that the Australian Signals Directorate (ASD) responds to could be prevented by following the Top 4 mitigation strategies »*

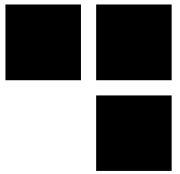
    *1) Application whitelisting*

    *2) Patch applications such as Java, PDF viewers, Flash, web browsers and Microsoft Office*

    *3) Patch operating system vulnerabilities*

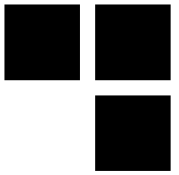
    *4) Restrict administrative privileges*

# Ingénierie sociale



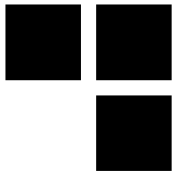
- **Objectifs :**
  - Récupérer un mot de passe permettant d'accéder au réseau interne depuis Internet (information *primaire*)
  - Récupérer des informations facilitant les autres étapes de l'intrusion (information *secondaire*)
- **Choix des cibles :**
  - Assistants département (nombreux contacts)
  - Nouveaux arrivants
  - *Help desk*
- **Important :**
  - Répéter les différents scénarios de conversations possibles
  - *Caller ID spoofing*
  - Itération des appels vers différents contacts avec à chaque fois plus d'informations

# Protéger son organisation contre l'ingénierie sociale



- **C'est là que la sensibilisation rentre en jeu :**
  - On ne donne pas son mot de passe au téléphone !
  - Procédure de remontée d'alerte et de corrélation
- **Importance de la sensibilisation du *Help desk* :**
  - Support de la hiérarchie en cas de refus d'une demande risquée d'un VIP
  - *Scripts* pour harmoniser les contrôles d'identité et légitimer le refus en cas de suspicion
- **Privilégier les technologies d'authentification forte ne pouvant pas être communiquées par téléphone :**
  - Biométrie, cartes à puce, etc.

# Intrusions physiques



- **Objectifs :**
  - Connecter un *implant* sur le réseau interne pour établir un tunnel de communication sur Internet
  - Récupérer des mots de passe dans les locaux
- **Deux équipes :**
  - Équipe terrain
  - Équipe Internet
- **Choix de l'intervenant « terrain » :**
  - Expertise et complémentarité des profils
  - Sérieux
- **Critères de choix du scénario :**
  - Taille de l'entreprise
  - Mesures de sécurité physique observables (mécaniques, électroniques et humains)
  - Risques physiques liés à l'intrusion
  - Possibilité ou non de dégrader les mesures de sécurité en place

# Quelques scénarios

- **Branchement d'un *implant* :**
  - Suivre une personne qui rentre, portable à la main, en disant « je suis dans le lobby, j'arrive dans 1 minute »
  - Arriver tôt (avant l'équipe IT), avec un T-shirt imprimé au logo de la société qui fait la maintenance des imprimantes
- **Outils complémentaires :**
  - Kit d'ouverture de serrures ou clonage RFID
  - *Keyloggers* matériels
  - *Implant* à connecter au réseau interne
  - Outils d'attaque sur *Firewire* ou USB
  - Clé USB émulant un clavier (*Teensy*)

# Remarque sur le branchement de clés USB inconnues...

- **Courrier connecté *Webkey* par La Poste :**
  - *« Création de trafic sur un site Internet grâce à la Webkey, un support innovant et créatif qui renforce l'efficacité du courrier »*
  - *« Vous permettez à votre client de naviguer en toute sécurité en apposant la garantie «antivirus» avec un support USB à contenu limité »*

Courrier connecté
webkey

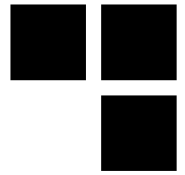
# Connexion à l'implant

- **Coordination des équipes :**
  - Affichage LED :

    *# echo 1 > /sys/class/leds/plug\:green\:health/brightness*
  - Envoi SMS :

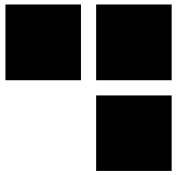
    *# gsmsendsms -d /dev/ttyUSB0 0612345678 "dhcp lease obtained"*
- **Établissement du tunnel entre l'implant et l'équipe Internet :**
  - Cas simple : couverture 2G / 3G / 4G
  - Sinon protocole de configuration automatique et recherche d'établissement d'un tunnel

# Connexion à l'implant



- **Tests successifs de différentes techniques :**
  - Contournement si nécessaire d'un filtrage par MAC ou d'un NAC (branchement en coupure derrière une imprimante)
  - DHCP
  - Écoute réseau et sélection d'une adresse IP disponible
  - Recherche de la route par défaut
  - Recherche d'un serveur de relais HTTPS ou DNS

# Protéger son organisation contre les intrusions physiques



- **La sensibilisation des employés atteint ses limites**
- **Mais importance de la formation du service de sécurité physique :**
  - Détection des comportements à risque pour les systèmes informatiques
  - Tenue d'un journal des incidents
- **Mesures de sécurité physiques :**
  - « Contrôle de l'unicité de passage » (éviter le talonnage)
  - Bloquer les prises réseaux dans les endroits accessibles au public
- **Mesures de sécurité informatiques :**
  - Détection du branchement d'appareils inconnus sur le réseau interne
  - Alerte et investigation en cas de comportement suspect
  - Interdire le branchement de périphériques USB non-autorisés

# Faire face aux attaques ciblées

- **Sensibilisation : succès et échecs**
  - Ingénierie sociale : Possible de faire comprendre qu'il ne faut pas donner son mot de passe par téléphone :-)
  - Intrusion physique : Difficile de demander aux salariés d'interpeller les personnes sans badge dans des locaux :-(
  - Mails piégés : Difficile d'empêcher les utilisateurs de ne pas ouvrir les pièces jointes ou de suivre les liens dans des e-mails « normaux » :-(
- **Importances des mesures de prévention techniques**
- **Tester et mesurer les progrès :**
  - Les métriques n'indiquent pas un niveau de sécurité
  - Elles donne un niveau d'avancement des travaux qui peuvent (ou non) contribuer au niveau de sécurité
- **Il y a des *success story* dans certaines organisations**

# AVEZ-VOUS DES QUESTIONS ?

MERCI DE VOTRE ATTENTION,

SYNACKTIV
DIGITAL SECURITY