INTITULÉ : HACKING ET SECURITE - NIVEAU 1

PRÉNOM : ARTHUR

NOM : MENDJANA

Qualification des Services Intellectuels OPQF

Fédération de la Formation Professionnelle

Présentation du Module

❑ **Public concerné** :

Techniciens informatique, gestionnaires de parc, techniciens d'exploitation, techniciens de maintenance…

❑ **Objectifs :**

Pirates et attaques informatiques : savoir les repérer et les contrer

❑ **Modalités pédagogiques :**

Cours magistral / Exercices / Travaux pratiques

❑ **Prérequis**

Connaissance de la structure matérielle et architecturale d'un ordinateur

PROGRAMME

1- ENVIRONNEMENT ET ACTEURS

- Objectif d'une attaque et scénario d'attaque
- Les techniques d'attaques : code vandale, intrusion, usurpation d'identité, DDOS, ...
- Rappel de protocole TCP/IP

2- MATÉRIEL DE SÉCURISATION

- Sécurisation des accès physique (802.1X)
- ACL de niveau 2 et 3
- Firewall et règles de filtrage
- La Translation d'adresse NAT et le PAT
- DMZ et multi-DMZ
- Surveillance par IDS/IPS et logs
- Architecture réseau sécurisée

PROGRAMME

3- SÉCURISATION DES ÉCHANGES

- Notion de cryptographie
- Fonctions de hachage
- SSL
- VPN réseau

4- PANORAMA DES TECHNIQUES DE HACKING

- Social Engineering ; Failles physiques (accès aux locaux, BIOS, …)
- Collecte d'information : (footprintig, fingerprinting, découverte réseau, recherche de faille)
- Vol de session (TCP Hijacking) ; Appel à procédures distantes
- Élévation de privilèges et permissions ; Gestion des mots de passe et cracking (brut force)

4- PANORAMA DES TECHNIQUES DE HACKING

4-1 Social Engineering

C'est une technique qui a pour but d'extirper des informations à des personnes sans qu'elles ne s'en rendent compte. Contrairement aux autres attaques. La seule force de persuasion est la clé de voûte de cette attaque. Il y a quatre grandes méthodes de social engineering : par téléphone, par lettre, par internet et par contact direct.

Par téléphone

Le hacker vous contactera par téléphone. C'est la technique la plus facile. Son but est d'avoir le renseignement le plus rapidement possible. Un bon hacker aura préparé son personnage et son discours. Il sera sûr de lui. Il sera très persuasif dans le timbre de sa voix. Certains hackers ont quelques techniques pour parfaire leur crédibilité, comme jouer sur un magnétophone une cassette préalablement enregistrée de bruits de bureau, ou encore utiliser un matériel qui change le timbre de la voix pour imiter celle d'une secrétaire.

Comment parer cette méthode ?

Si vous recevez un coup de fil d'une personne que vous ne connaissez pas : Ne donnez aucun renseignement. Restez dans le vague, et débarrassez vous de lui : soit vous mettez un terme à cet appel, soit demandez une confirmation par écrit (par fax) de la demande.
Par fax, on obtient le numéro appelant, et il est donc facile de l'identifier. Et ainsi, on garde une trace écrite, cela pouvant être d'une grande importance pour déposer une plainte.
Malheureusement, un bon hacker vous aura étudié avant, et se fera passer pour un client, un fournisseur, ou un de vos collègue situé dans un autre bureau dans le cas d'une grande entreprise. Pire encore, il attaquera au moment le plus propice pour lui : par exemple, lorsque le responsable d'un client est en vacances. Il devient très dur alors, de se douter d'une mauvaise intention...

4-1 Social Engineering

Par courrier postal

Le hacker vous fera une lettre très professionnelle. Au besoin, il n'hésitera pas à voir un imprimeur pour avoir du papier à lettre comportant un logo, un filigrane, téléphone, fax, email... Il utilisera très certainement une boîte postale pour l'adresse de sa société fictive.

Comment parer cette méthode ?

L'idéal serait de filtrer tout le courrier entrant de l'entreprise. Pour chaque source inconnue de l'entreprise, il faudrait faire une vérification de l'existence réelle de celle-ci.

Par internet

Le social engineering par internet est semblable à celui par téléphone. Le hacker se fera facilement passer pour un opérateur système, un responsable informatique ou un ingénieur système.

Comment parer cette méthode ?

Comme pour le téléphone, ne donnez pas de renseignements à quelqu'un que vous ne connaissez pas. Mais par internet, c'est plus facile de donner de la crédibilité, tant il y a de noms de domaines et d'adresses emails farfelus. Il n'est donc pas facile de faire la part des choses. Une bonne étude de la gestion de l'extranet et de la mise en place d'une structure matérielle et personnelle adéquate est la meilleure solution.

4-1 Social Engineering

Par contact direct

C'est le social engineering le plus dur de la part du hacker. Il sera équipé pour que vous n'y voyez que du feu : costard, cravate, très classe, très propre, attaché-case , agenda rempli, documents divers, carte de visite, badge... Si le hacker prend de tels risques, c'est qu'il est déterminé à obtenir les renseignements souhaités. Il sera donc très persuasif.

Comment parer cette méthode ?

Cela est très difficile, car vous avez été directement confronté au charisme du hacker. S'il a réussi, vous êtes persuadé de son honnêteté. Cependant, lors d'une discussion, n'hésitez pas à demander un maximum de renseignements "concrets" (nom de votre interlocuteur, nom et adresse de la société, etc), pour, par la suite, vérifier auprès des organismes compétents l'existence réelle de votre interlocuteur. N'hésitez pas à téléphoner à la société pour savoir si la personne existe, et si elle est au courant qu'elle vous a vu ces dernières heures...

4-2 Collecte d'information (footprintig, fingerprinting)

La reconnaissance ou collecte d’informations est la première phase d’un test de pénétration (Pentest) qui consiste à obtenir des informations précises sur votre cible sans pour autant révéler votre présence ou vos intentions, d’apprendre comment fonctionne la société et de déterminer la meilleure façon d’y pénétrer.

La reconnaissance est l’art de collecter des informations sur une cible avec ou sans son accord, en entrant en contact ou non avec elle. C'est ainsi que nous pouvons distinguer 2 types de reconnaissance:

- La reconnaissance passive (Le footprinting)

- La reconnaissance active (Le fingerprinting)

4-2 Collecte d'information (footprintig, fingerprinting)

- La reconnaissance passive (Le footprinting)
  Lors de la reconnaissance passive des informations sont collectées passivement et indirectement afin de découvrir des informations sur notre cible sans entrer en contact avec leurs systèmes. Cela peut permettre de savoir qui sont les responsables du réseau, l'hébergeur, le type de serveur web, le système d'exploitation de la cible, …
  NB: Lors de son exécution vous ne risquez pas de vous faire repérer car on utilise des informations publiques.

  Outils & Techniques:
- www.whois.net,
- toolbar.netcraft.com/site_report,
- Maltego

4-2 Collecte d'information (footprintig, fingerprinting)

La reconnaissance active (Le fingerprinting)
Durant la reconnaissance active, il y a une interaction directe avec les systèmes d'informations(SI) de la cible afin d'avoir d' amples informations sur elle.
NB: Lors de son exécution il y a un risque de se faire repérer par des systèmes de détection d'intrusion(IDS) ou des systèmes de prévention d'intrusion(IPS). Ce qui peut être défavorable dans le travail d'un auditeur discret/professionnel.

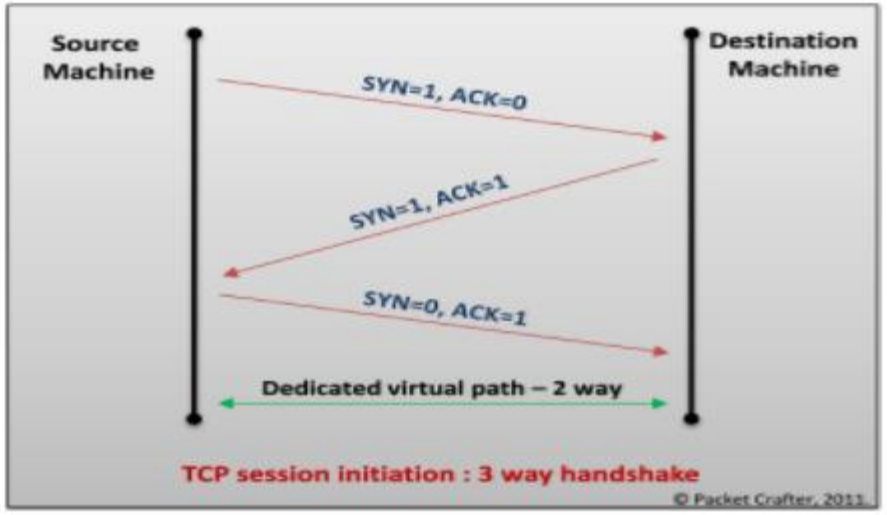
Outils & Techniques:
- Ingénierie sociale
- Nmap
- SMTP bounce back
- Shoulder sniffing

4-3 Vol de session (TCP Hijacking)

TCP garantit la livraison des données et garantit également que les paquets seront livrés dans le même ordre dans lequel ils ont été envoyés.

Afin de garantir que les paquets sont livrés dans le bon ordre, TCP utilise des paquets de reconnaissance (ACK) et des numéros de séquence pour créer une « connexion complète en duplex fiable entre deux points de terminaison », les paramètres se référant aux hôtes communicants.
La connexion entre le client et le serveur commence par une poignée de main à trois.

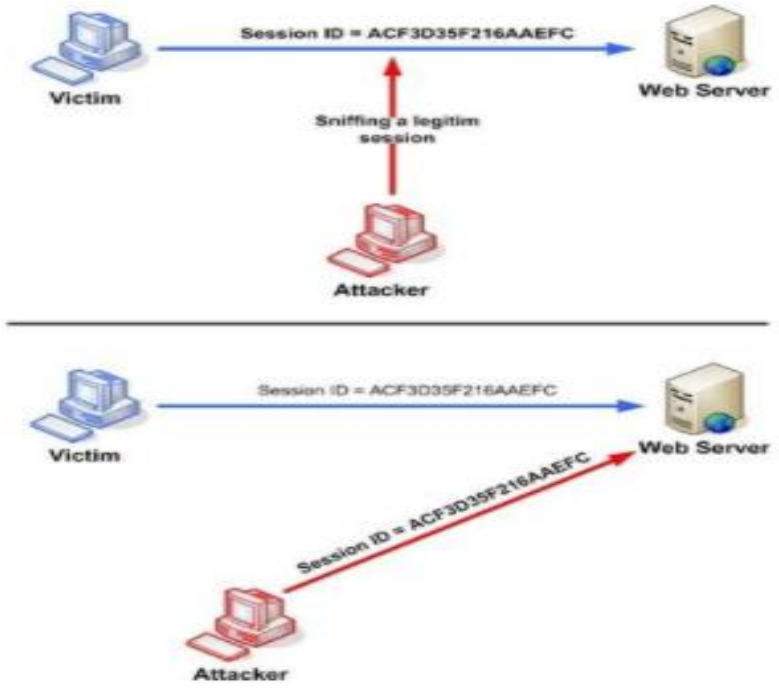
Après la poignée de main, il s'agit simplement d'envoyer des paquets et d'incrémenter le numéro de séquence pour vérifier que les paquets sont envoyés et reçus.



4-3 Vol de session (TCP Hijacking)

L'objectif du piratage de session TCP est de créer un état où le client et le serveur sont incapables d'échanger des donnée, lui permettant de forger des paquets acceptables pour les deux extrémités, qui imitent les paquets réels.

Ainsi, l'attaquant est en mesure de prendre le contrôle de la session



4-4 Élévation de privilèges et permissions ; Gestion des mots de passe et cracking (brut force)

LES ATTAQUES PAR BRUTE-FORCE : COMMENT ÇA MARCHE ?

Les attaques par brute-force consistent à trouver un mot de passe ou une clé à travers des tentatives successives. Il s'agit donc de casser le mot de passe en **tentant des combinaisons successives** jusqu'à trouver la bonne.
Cela peut aller de tentatives alphanumériques : a, aa aaa, ab, abb, abbb etc.
ou partir d'un dictionnaire de mot de passe les plus souvent utilisés.

Les services des serveurs sur internet sont particulièrement visés à travers des ordinateurs qui envoient des requêtes successives sur internet.
Dans ce cas précis, des noms d'utilisateurs courants sont tentés : root, admin, administrator, demo, john etc.
Et des mots de passe courant : 1234, admin, etc

Des ordinateurs infectés envoient des requêtes en continuent pour tenter de trouver des comptes en ligne "faciles".
On distingue donc les attaques ***online*** qui s'attaquent à des services internet (WEB, FTP, SSH, Mail).

Les attaques dit ***offline***, pour casser un mot de passe d'un zip, d'un utilisateur d'un OS ou autres.
Ces attaques locales peuvent aussi viser des comptes en ligne récupérés.. ou un hash d'un compte administrateur récupéré par une injection SQL

4-4 Élévation de privilèges et permissions ; Gestion des mots de passe et cracking (brut force)

QUELQUE ATAQUE PAR BRUTE FORCE

Cracker mot de passe Windows par Brute-Force

Il existe bien entendu des outils pour cracker un mot de passe Windows.
S'il s'agit d'une perte de mot de passe, il est beaucoup plus rapide de changer ce dernier, au lieu de tenter de le trouver
Ophcrack est par exemple un programme qui permet de cracker les mots de passe Windows.

Ophcrack se base sur les tables arc-en-ciel pour cracker ces hash et ainsi trouver le mot de passe de l'utilisateur Windows