Techniques de Hacking – N1

SEC-HACK

TECHNIQUES DE HACKING – NIVEAU 1

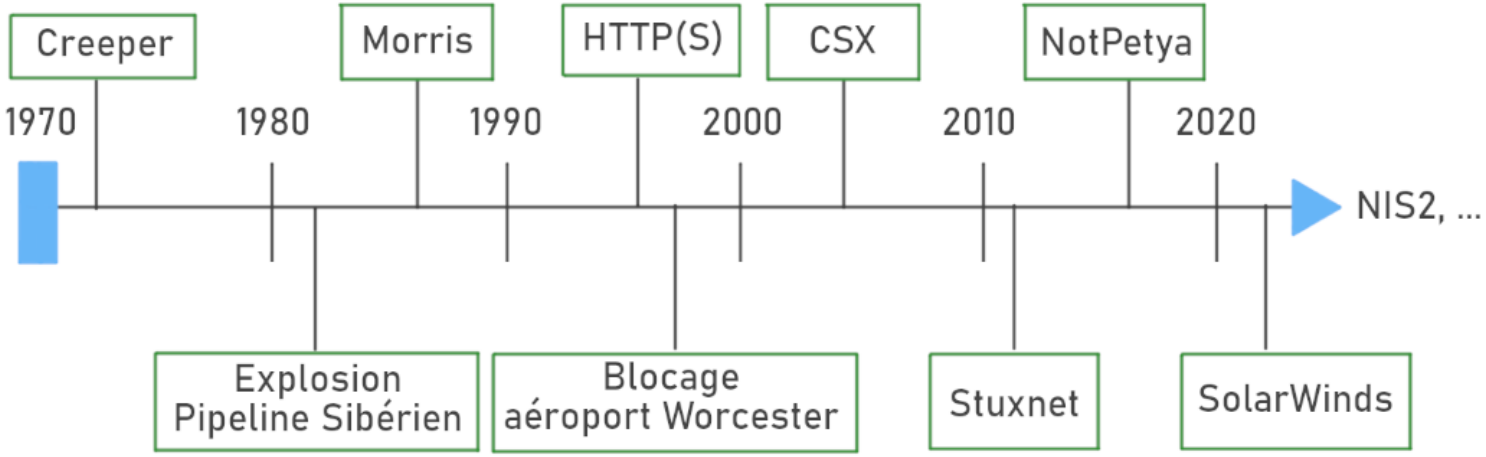
LES FONDAMENTAUX

Techniques de Hacking Niveau 1 – Les Fondamentaux

- L’histoire et la nomenclature
- Organisation des acquis
- La veille en cybersécurité
- Les principaux types d’attaques
- Les différentes phases d’une attaque (Kill Chain)

- Un peu d'histoire

Les premières attaques informatiques remontent aux premiers systèmes déployés. Il aura cependant fallu attendre un grand nombre d'incidents pour arriver à la « maturité cyber » que nous avons aujourd'hui.



- Terminologies et Définitions

On considère tout évènement non prévu dans le fonctionnement normal d'un système d'information comme évènement de sécurité.

Un incident de sécurité (cyber attaque) est un évènement indésirable impactant directement l'un des points fondamentaux de la sécurité d'une donnée :

- Confidentialité
- Intégrité
- Disponibilité

Note : Un évènement aléatoire (panne matérielle, incendie, …) est également considéré comme étant un incident de sécurité.

L’objectif du pentesting est de tester et analyser les mesures de défenses mises en œuvre au niveau du système d'information dans un but de protection des assets informatiques et surtout des données qu'ils hébergent et traitent.

L'idée est de venir opérer ces tentatives de "piratage" avec une approche éthique et de ainsi rester dans un contexte légal.

Les entreprises et autres professionnels qui fournissent ce genre de services le font dans un contexte spécifique et borné dans le cadre d'une mission.

Les limites de ce que le pentester est en droit de faire (quelles machines attaquer, quels types d'attaques, quelles limites d'exploitation, ...) est d'ailleurs généralement pleinement défini lors d'une réunion de cadrage pré-pentest.

L'éthique de travail réside donc dans le respect de ce cadrage et des limitations imposées. On distingue 3 catégories de hackers en fonction de leurs intentions :

White Hat : Il s'agit des hackers qui restent dans le droit chemin. Leur objectif est de mettre leurs compétences au profit des autres. Il s'agit classiquement des pentesteurs et autres cadres de pentest légaux.

Black Hat : Il s'agit de "criminels", l'objectif est de mettre en défaut une infrastructure et chercher à faire du profit (financier principalement) sur la base de ces attaques.

Grey Hat: Il s'agit d'une catégorie intermédiaire entre les deux premières, leur objectif est de mettre leurs compétences au profit des autres mais sans s'en se soucier de la loi ou de l'éthique (par exemple attaquer un site malveillant, ...)

Avant de commencer tout pentest, il est donc nécessaire de définir les bornes, les limitations et surtout les engagements à respecter dans le cadre des tests. Tous ces éléments sont placés au sein du ROE (Rules of Engagement).

Ce document comporte l'ensemble de ces éléments notamment :

- L'autorisation explicite de perpétrer des attaques sur la cible (protection légale)
- Les bornes et les cibles qui doivent être attaquées. Dans de nombreux cas, l'objectif va être de restreindre le périmètre de l'attaque à certains serveurs et/ou applications mais pas l'intégralité du système d'information
- Les règles qui doivent être suivies. Par exemple, l'interdiction de causer un déni de service sur la production, d'opérer du phishing, autoriser le MITM, ...

- Organisation des acquis

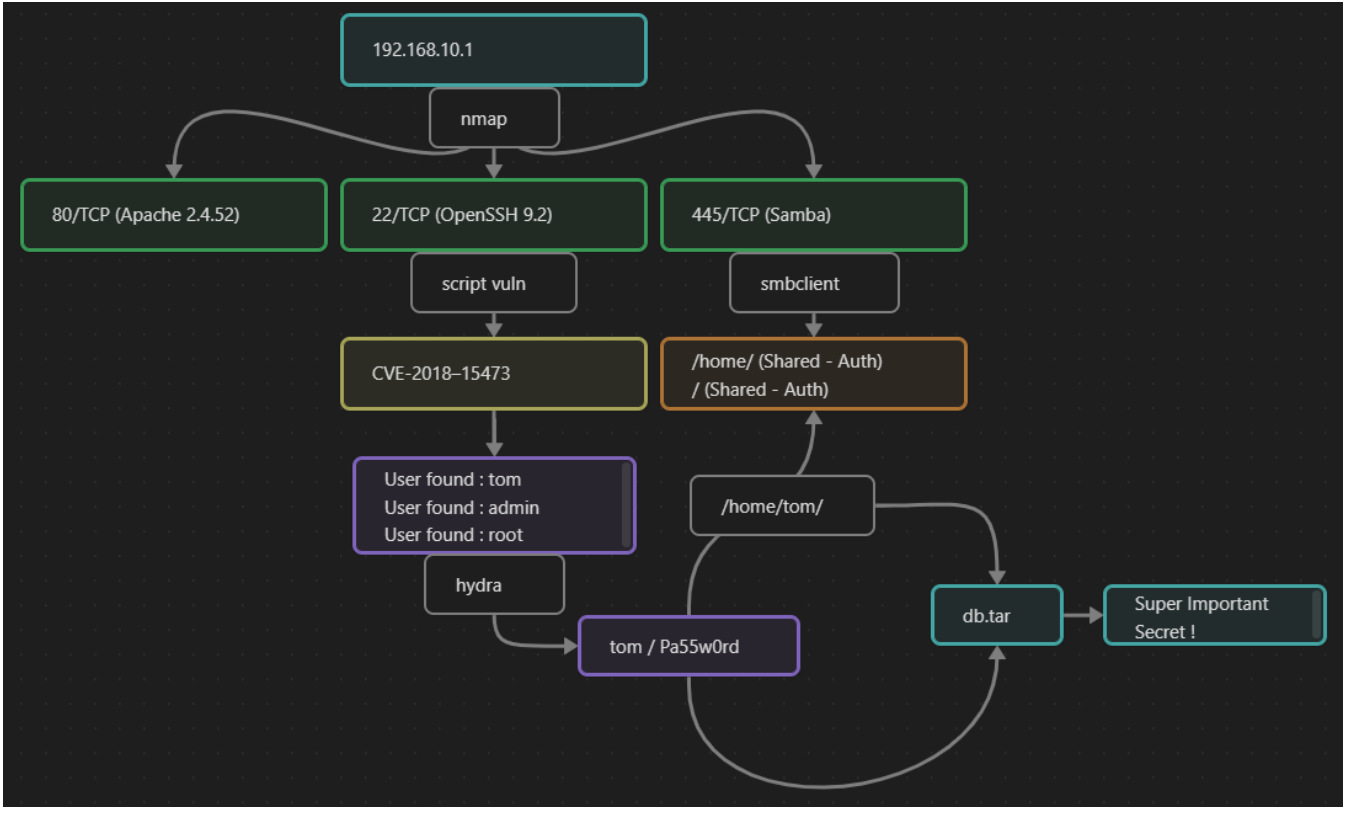
Dès le lancement d'un pentest, il sera également nécessaire de bien organiser son travail.

La collecte des données que l'on va venir opérer pendant notre pentest peut impliquer énormément de contenu et de relations entre ces éléments, il est donc fréquent de commencer par organiser ces éléments sous la forme d'une « MindMap » ou équivalent.

Cette cartographie va nous permettre de conserver toutes les découvertes mais aussi assurer la mise en relation de celles-ci.

C'est notamment particulièrement nécessaire pendant des phases de scan de surface ou d'OSINT.

Exemple : Cartographie simple



- La veille en cyber sécurité

La veille consiste à surveiller constamment les menaces potentielles qui pèsent sur les systèmes d'information d'une entreprise.

La démarche consiste à collecter, analyser et partager des informations sur les différents sujets d'intérêts pour mieux suivre et comprendre :

- Les vulnérabilités émergentes
- Les intrusions et grands évènements de sécurité
- Les menaces et les risques informatiques
- Les tendances d'utilisation d'outils et de méthodes au sein des systèmes d'informations

Il existe différentes sources de flux RSS ainsi que des sociétés proposant des rapports de CTI annuels.

- ANSSI : Alertes et vulnérabilités émergentes avec le CERT-FR (+ documentations techniques)
- ENISA : Réseau de CSIRT, coordination locale vers les CERT
- MISP (Malware Information Sharing Platform) : Informations sur les malwares et les acteurs de la menace
- FireEye : Analyse avancée sur les APT
- Verizon / Thales : Enquête sur les violations de données

- CIS : Guide de sécurisation de systèmes et d'applications
- Mozilla / Qualys : Meilleures pratiques d'utilisation de SSL
- NIST NVD : Recensement de toutes les vulnérabilités connues
- ….

Il existe un grand nombre de plateformes et autres livres blancs pour tous les usages et les suivis que l'on souhaite opérer.

Il est également important de rester alerte sur les informations en temps réel sur les réseaux sociaux notamment (X, LinkedIn, …).

- Les principaux types d'attaques

1) Les logiciels malveillants (malware)

Pour atteindre un objectif d'attaque (impact sur l'un des points du CIA), il est généralement nécessaire pour un attaquant de déployer une application / bout de code malveillant sur la machine cible.

Il existe plusieurs types de malwares (Trojan, Ransomware, Spyware, …) en fonction de l'objectif ciblé (qui peut également être la simple persistance sur le système).

Note : De nos jours, la grande majorité des attaques (~86%) sont dites « malware-free » à cause des forts taux de détection proposés par les EDR modernes.

- Les principaux types d'attaques

2) Les attaques par ingénierie sociale

Pour être en mesure de déployer sa payload (malware), il est fréquent de passer par des stratégies d'ingénierie sociale (inviter la cible à cliquer sur un lien ou à ouvrir un fichier).

L'ingénierie sociale consiste à exploiter la confiance qu'une personne va placer en nous ou dans les informations que nous allons lui transmettre afin de lui faire suivre un schéma d'actions (arnaque au président, …).

Note : De nouvelles techniques de phishing émergent (QR code piégé, …) et parfois grandement facilitées par l'utilisation d'IA (pour la voix notamment)

- Les principaux types d'attaques

3) Attaques sur les réseaux

D'un point de vue technique, il existe une très vaste surface d'attaque à disposition d'un attaquant. En effet, les mécanismes réseaux (TCP/IP) ont été pensés dans un premier temps pour l'efficacité opérationnelle et en aucun cas pour la sécurité.

Le stack TCP/IP que l'on retrouve sur toutes les machines aujourd'hui présente des vulnérabilités et mécanismes exploitables à tous les niveaux de fonctionnement de celui-ci.

Exemples d'attaques : MITM, DDoS, DHCP Spoofing, ARP Poisoning, CAM Poisoning, …

- Les principaux types d'attaques

4) Attaques sur les identités

Si un utilisateur ne tombe pas dans le piège tendu par du phishing ou autre technique d'ingénierie sociale, un attaquant est toujours en mesure de récupérer ses accès par un autre moyen.

Par exemple :

- OSINT (recherche de credentials leak)
- Génération d'un dictionnaire dédié
- Attaque par force brute

- Les principaux types d'attaques

5) Vulnérabilités applicatives

La dernière grande catégorie d'attaque contient l'essentiel des vulnérabilités existantes.

La plupart des éléments exploitables se trouvent au sein des services et applications mis à disposition des utilisateurs.

Ces attaques peuvent être dues à un code source présentant des problèmes (SQLi, BufferOverflow, …) mais également à des questions d'obsolescence (cryptographique notamment).

- Les différentes phases d'un attaque

En fonction des règles définies pendant le cadrage, le pentest peut prendre une grande quantité de direction, il n'existe donc pas une approche unique.

La méthodologie dépend donc du type de ressource ciblé (infrastructure réseau, service web, ...) mais il réside des points communs dans l'ensemble des attaques que l'on va venir opérer.

On peut donc qualifier une approche générale constituée des 3 étapes suivantes :

- Collecte d'informations
- Découverte / Scan
- Exploitation

Collecte d'informations :

Il s'agit de la première étape, le renseignement. L'objectif n'est ici pas de scanner le moindre système mais plutôt de collecter les informations publiquement disponible sur une organisation.

Lorsque cette étape est nécessaire, c'est généralement à des fins de pentest en boite noire.

C'est principalement en opérant de l'OSINT que l'on pourra récupérer des informations qui nous serons utiles par la suite (organisation de la cible, personnel, ...)

Découverte / Scan :

Cette étape consiste à la fois en la découverte des systèmes présent mais surtout des services et des informations qu'il est possible de récupérer concernant ceux-ci.

On va s'intéresser ici surtout à tout ce qui est de l'ordre de la footprint (empreinte). La plupart des applications laissent à disposition des informations potentiellement sensibles qui peuvent être découvertes (type de service, système d'exploitation hôte, numéros de version).

Toutes ces informations vont être utiles pour rechercher des failles connues en corrélant notamment les numéros de version avec des bases de données de vulnérabilités.

Exploitation :

Une fois que l'on possède une grande variété d'informations sur les systèmes cibles, l'étape finale consiste soit en l'utilisation d'un exploit public soit dans l'orchestration d'un contournement de la logique logicielle.

C’est dans notre phase de découverte que l’on corrélera les informations de versions découvertes avec des bases de données de vulnérabilités à la recherche d’un exploit.

Le contournement logiciel en tant que tel consistera en une étape plus complexe qui devra être opérée en grande partie manuellement et sera nécessaire uniquement si il n’existe pas d’exploit public de disponible.

Ces 3 étapes constituent donc la base de notre test de pénétration. Cependant, une exploitation réussie ne signifie pas, dans la majorité des cas, une compromission complète.

Il est courant de ne récupérer que des permissions partielles ou un accès à une machine intermédiaire ne contenant aucune donnée ou information exploitable.

La première étape qui vient suivre ce modèle de test de pénétration est donc la recherche de l'élévation de privilège qui consiste en la rechercher d'un moyen d'étendre ses accès au sein d'une machine. Cette élévation peut s'opérer soit :

- De manière horizontale : Accès à un autre compte possédant des privilèges équivalents
- De manière verticale : Accès aux privilèges d'un autre groupe de permissions

Une fois qu'un attaquant se retrouve dans un modèle de "post-exploitation", plusieurs objectifs supplémentaires peuvent être visés (pivot, gathering, ...)

- Pivoter : Rechercher d'autre hôtes pouvant être attaqués depuis la machine initialement infectée

- Forer : Rechercher des informations supplémentaires sur l'hôte infecté une fois notre élévation de privilège réussie

- Couvrir : Supprimer les traces de la compromission initiale et potentiellement des actions menées par la suite (altération des journaux systèmes et applicatifs, …)

Il s'agit la d'une méthodologie "standard", certains domaines nécessiteront une approche légèrement différente. Pour une vision plus complète => MITRE ATT&CK

TECHNIQUES DE HACKING – NIVEAU 1

TRAVAUX PRATIQUES