Fiche Pentest

DE de 2022

Définir test intrusion

Objectif

Evaluer la sécurité d'un système informatique en simulant une attaque et en identifiant ses faiblesses.

Méthode

- Définition du périmètre et collecte d'information
- Analyse/Scan des vulnérabilités
- Exploitation
- Post-Exploitation
- Rapports et recommandations

Résultat

- Rapport de Vulnérabilité : Une liste détaillée des vulnérabilités découvertes, classées par sévérité.
- Impact Potentiel : Une évaluation des risques associés à chaque vulnérabilité.
- Recommandations de Sécurité : Des conseils pratiques pour corriger les failles et améliorer la sécurité globale.
- Validation des Correctifs : Une vérification des mesures correctives mises en place pour assurer leur efficacité.

Présenter les différentes étapes d'un test d'intrusion

Nom de l'étape	**Détails de l'étape**	**Outils utilisés durant l'étape**	**Éléments obtenus à la fin de cette étape**
Planification	Définir le périmètre, objectifs et méthodologies	Réunions, documentation	Plan de test, autorisations
Collecte d'informations	Recueillir des informations sur la cible	Whois, Recon-ng, dork	Carte des cibles, points d'entrée potentiels
Enumération	Identifier les failles de sécurité	Nmap, Rustscan	Liste des vulnérabilités
Exploitation	Tenter de pénétrer les systèmes via les failles trouvées	Metasploit, Burp Suite, exploit-db	Accès non autorisé, preuves d'exploitation
Post-Exploitation	Maintenir l'accès, extraire des données sensibles	Meterpreter, scripts personnalisés	Données collectées, maintien d'accès
Rapport	Documenter les découvertes et proposer des correctifs	Outils de documentation, Word, Excel	Rapport détaillé, recommandations

Approches d'un test d'intrusion

Approche	**Description**	**Objectif**	**Avantages**	**Inconvénients**
Boîte Noire	Le testeur n'a aucune information préalable sur le système testé.	Simuler une attaque externe sans connaissances internes.	Reproduit des conditions réelles d'attaque externe.	Moins efficace pour trouver toutes les vulnérabilités.
Boîte Blanche	Le testeur dispose de toutes les informations sur le système (code source, configurations, etc.).	Évaluer la sécurité en profondeur avec une connaissance complète du système.	Permet une analyse exhaustive et détaillée des vulnérabilités.	Nécessite plus de temps et d'efforts, moins réaliste pour une attaque externe.

Boîte Grise	Le testeur a une connaissance partielle du système.	Combiner les avantages des approches boîte noire et boîte blanche.	Équilibre entre réalisme et efficacité, identifie les vulnérabilités internes et externes.	Peut manquer certaines vulnérabilités cachées profondes.

Définir le scan de vulnérabilité et présenter ses différences par rapport au test d'intrusion

Scan de vulnérabilité =

- Processus automatisé qui consiste à identifier et évaluer les failles de sécurité dans un système informatique.
- Compare les configurations et versions de logiciels avec une base de données de vulnérabilités connues.

Critère	**Scan de Vulnérabilité**	**Test d'Intrusion**
Approche	Automatisée, basée sur des signatures connues.	Partiellement automatisée, simule des attaques réelles.
Objectif	Identifier les vulnérabilités connues.	Identifier et exploiter les vulnérabilités
Profondeur d'analyse	Superficielle,	Approfondie
Temps nécessaire	Court	Long
Coût	Faible	Elevé

Cours de cette année

Les étapes d'une attaque APT

1. **Accès initial**
    - Attaque web, réseau ou via interaction humaine.
    - Le but est d'infecter la cible avec un malware.
2. **Déploiement malware**
    - Déployer un agent et garder une porte d'entrée.
    - Établir une connexion avec un C2.
3. **Déplacement vertical et horizontal**
    - Scan du réseau, exploitation de vulnérabilités, accès à des informations sensibles.
    - Utilisation de tunnel pour changer de réseau.
4. **Exfiltration**
    - Identifier puis exfiltrer de façon chiffrée les informations sensibles de l'entreprise.
5. **Persistance**
    - Maintenir son accès au réseau sur le long terme, et supprimer ses traces.

Exemple d'APT

Chine : APT1

Russie : APT28 (fancy bear) /29

Corée du nord : APT38 lazarus

20/21	FTP (File Transfer Protocol)	Transfert de fichiers
22	SSH (Secure Shell)	Connexion sécurisée à distance
53	DNS (Domain Name System)	Conversion des noms de domaine en IP
80	HTTP (Hypertext Transfer Protocol)	Accès aux pages web
123	NTP (Network Time Protocol)	Synchronisation de l'horloge
143	IMAP (Internet Message Access Protocol)	Réception des e-mails
389	LDAP (Lightweight Directory Access Protocol)	Annuaire et gestion des postes sur le réseau
443	HTTPS (HTTP Secure)	Accès aux pages web de manière sécurisée
445	SMB (Server Message Block)	Partage de fichiers et d'imprimantes
636	LDAPS (LDAP Secure)	Annuaire et gestion des postes sur le réseau de manière sécurisée
3306	MySQL	Base de données
3389	RDP (Remote Desktop Protocol)	Accès bureau à distance

L'exploitation

/etc/passwd => shell

/etc/shadow => stockages des mdp

Shell

Bind Shell = attaquant qui initie une connexion sur un serveur distant

Reverse Shell = serveur distant qui initie une connexion sur la machine de l'attaquant

Reverse > Bind car :

- – Pour outrepasser les protections de parefeu qui bloquent les connexions entrantes
- – ne pas ouvrir de port sur la machine cible

Outils de reverse shell = netcat / bash

Vulnérabilité Web

Le javascript (JS) est un langage qui permet de crée des pages web dynamiques.

Il va être utiliser pour faire des injection XSS au moment où le site va interpréter le code JS.

Les injection XSS se font généralement au niveau des pages de login, des formulaires …

Ainsi on va pourvoir voler les informations de connexions (cookie de session) aux utilisateurs.

Il existe trois types d'injection XSS :

- XSS Stocké (Stocké dans la BDD du site)
- XSS Reflected (Injecté dans la requête HTTP)
- XSS DOM Based (injecté dans la page HTML coté client)

Le SQL, langage de programmation des bases de données relationnelles.

On y fait des injections SQL (SQLI). Avec pour but d'injecter du code coté serveur.

On le fait dans des champs de la base de données qui vont permettre de retrouver des données utiles (bancaire, login …)

Les IDOR (Insecure direct object reference) sont des vulnérabilités qui permettent à n'importe quel utilisateur d'accéder à la base de données (genre le champ de login de votre CDI) ou bien via une url.

Pour ce genre d'attaque on peut utiliser BurpSuite qui est très complet

Crackage mot de passe

Actuellement il est souvent recommandé d'avoie un mot de passe de **8 charactères avec majuscule, minuscule, chiffre et charactère spéciale**. Le problème est qu'en 2023 cela ne prend que **5 min pour cracker ce genre de mot de passe**. C'est pour cela qu'on trouve régulièrement une demande de **12 charactères**, ainsi il faut environ **226 ans** pour cracker

Les différents types d'attaque de mdp :

- Par dictionnaire : utiliser une liste de mot (rockyou.txt)
- Par combinaison : utiliser deux listes de mots
- Par brute-force : tester toutes les combinaisons
- Par masque : on applique un masque sur une liste de mot (1234 ...)
- Par association : on compare le dictionnaire à un hash

Deux logiciels présentés :

- Hashcat :

  "Complexe" mais avec beaucoup d'option d'utilisation et utilise la carte graphique (grosse puissance potentiel)

- JohnTheRipper :

  Simple mais avec peu d'option, utilise la puissance CPU

Ce qu'il faut revoir selon le proff

Slides 6 à 30

Reverse shell et elevation de privilèges

slides 62, 54, 32

Failles : différents types xss

Objectif pentest

Qu'est-ce que le pentest ?

– Chercher des failles et des vulnérabilités dans les systèmes d'information

– Évaluer la maturité d'un système d'information

– Renforcer la sécurité des systèmes d'informations

– Restituer les vulnérabilités au clien

Statistiques

Fréquence des attaques

53% des entreprises interrogées ont déjà subit une attaque

Combien de temps caché ?

En moyenne il faut 200 jours avant que les attaquants soient découverts. Parfois ils ne le sont pas du tout.

Attaques de l'intérieur

Une fois sur 10, les attaquants sont de mèches avec une personne de l'entreprise.

Quel est le prix ?

En France, en 2023, le coût médian d'une attaque est de 15 640€

Réputation

En 2023, 25% des entreprises ont vu un impact sur leur marque et réputation après une attaque.

Futures attaques

Les entreprises novices en sécurité ont dépensé 3 fois plus dans la cyber qu'en 2021