Tests d’intrusion
Introduction

AMUSEC
22 Mars 2024

Pour participer à la certification AMUSEC

Les cyber attaques

« Toute activité malveillante visant à collecter, perturber, refuser, dégrader ou détruire les ressources du système d'information ou l'information elle-même. » (NIST)

- En 2023, les cyber attaques représentent un danger majeur pour les états.
    - Une trentaine de collectivités territoriales attaquées, 9 hôpitaux, des universités, les attaques contre les environnements cloud ont triplé.
- En janvier 2024, vol de 33 millions de données de santé.

Croissance des attaques

- **Numérisation** de la société.
- **Phishing** de plus en plus subtiles.
- L'**IA** décuple le pouvoir de nuisance des cyber attaques. Elle permet de prédire et manipuler les comportements humains. Elle permet plus de sophistication, de rapidité et de facilité au déploiement (+ de rentabilité).
- Recours à des **solutions externalisées** qui augmentent la surface de frappe des attaquants.
- Explosion des **ransomware as a service** (RaaS). Recherche sur le dark et paiement en cryptomonnaie suffit.
- Investissement insuffisant dans la formation en cyber sécurité en France.

Solutions ?

- Pour contrer les cyber attaques, les organismes (collectivités, instituts, entreprises, etc.) doivent **réduire leurs vulnérabilités**.

- Méthode : organiser des cyber attaques contre soi-même.

Le retour d'expérience permet d'évaluer et renforcer la sécurité de l'organisation.

- Ce processus s'appelle Penetration Testing ou **test d'intrusion**.

Penetration testing

Le pentesting est une série **autorisée** d'attaques **non malveillantes** liées à la sécurité sur des **cibles** telles que
- des appareils informatiques,
- des applications,
- les ressources physiques,
- le personnel d'une organisation.

But : découvrir des **vulnérabilités** exploitables afin de mettre en place un plan d’actions permettant d’améliorer la sécurité de la cible.

Méthodes d’action identiques à celle d’un **hacker** qui opérerait une cyber attaque.

Bug bounties

Les "bug bounties" sont des **récompenses** financières versées par des organisations à des personnes ou à des groupes qui découvrent et signalent des failles dans les logiciels ou les systèmes informatiques de l'organisation.

Octobre 2021, Polygon verse $2 millions à Gerhard Wagner pour une vulnérabilité "double spend" qui aurait pu causer des ravages sur le réseau (jusqu'à $850 millions !)

Pen Test

Quand faire un Pen Test ?

- Si un **changement majeu**r est intervenu dans un environnement informatique : installation d'un nouveau système ou application ou update.
- **Régulièrement** pour s'assurer qu'aucun changement non voulu affecte la sécurité (par exemple tous les 12 mois).
- Si des standards de conformité imposent des Pen Tests (ex : PCI DSS, RGPD).

Comment ?

Il existe une méthodologie et des étapes bien définies.

Qui sont les pentesters (PT) ?

- Interne : membres de l'IT Dept de l'organisation.
- Externe : une entreprise spécialisée dans les tests d'intrusion.

Compétences requises

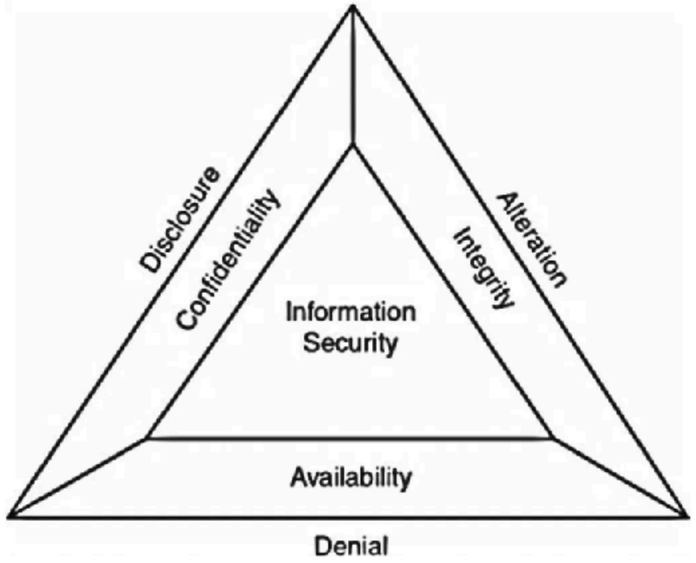
- Être curieux, créatif, astucieux, esprit critique, honnête, …
- Aimer les challenges, être tenace, psychologue, …
- Maîtriser certaines technologies (réseau, système, programmation, web, architectures, cryptanalyse, BD, stégano, …)

Spectre très large ; demande plusieurs années de pratique intensive.

Certifications :

- Entreprises : PASSI (ANSSI), CREST (label anglo-saxon), …
- Pentesters : OSCP (Offensive Security Certified Professional), CEH (Certified Ethical Hacker), CompTIA Pentest+, …

CIA et DAD



Modèle pour la sécurité des SI :
CIA triad : Confidentiality, Integrity, Availability.
Les 3 principaux services qui garantissent la sécurité des biens.

L’antithèse de CIA triad :
DAD triad : Disclosure, Alteration, Destruction/Denial triad.

DAD est l’objectif ultime du hacker.

Différentes approches

- **Black box** : le pentester ne connait aucune information non publique sur la cible.
- **White box** : il reçoit tous les détails de l’environnement réseau, y compris les configurations des serveurs et les services qu'ils exécutent, un diagramme de réseau montrant les différents segments du réseau et les applications, ainsi que les informations sur les adresses IP.
- **Grey box** : il reçoit un nombre d’informations limité (ex @IP).

Les équipes

Red team : effectue le test. Son but est de montrer qu'une suite d'actions peut amener un utilisateur externe à causer des dommages importants à l'entreprise ciblée.

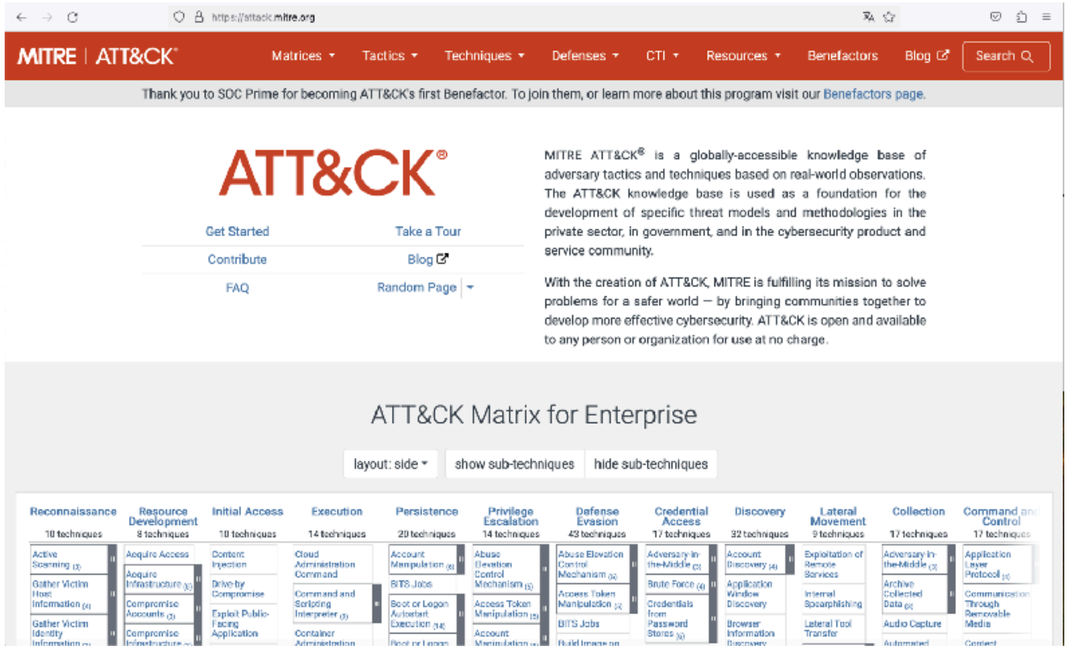
Blue team (si existe) : en charge de la sécurité de l'organisation.
Son but est défendre, en détectant et contrecarrant les attaques de Red team.

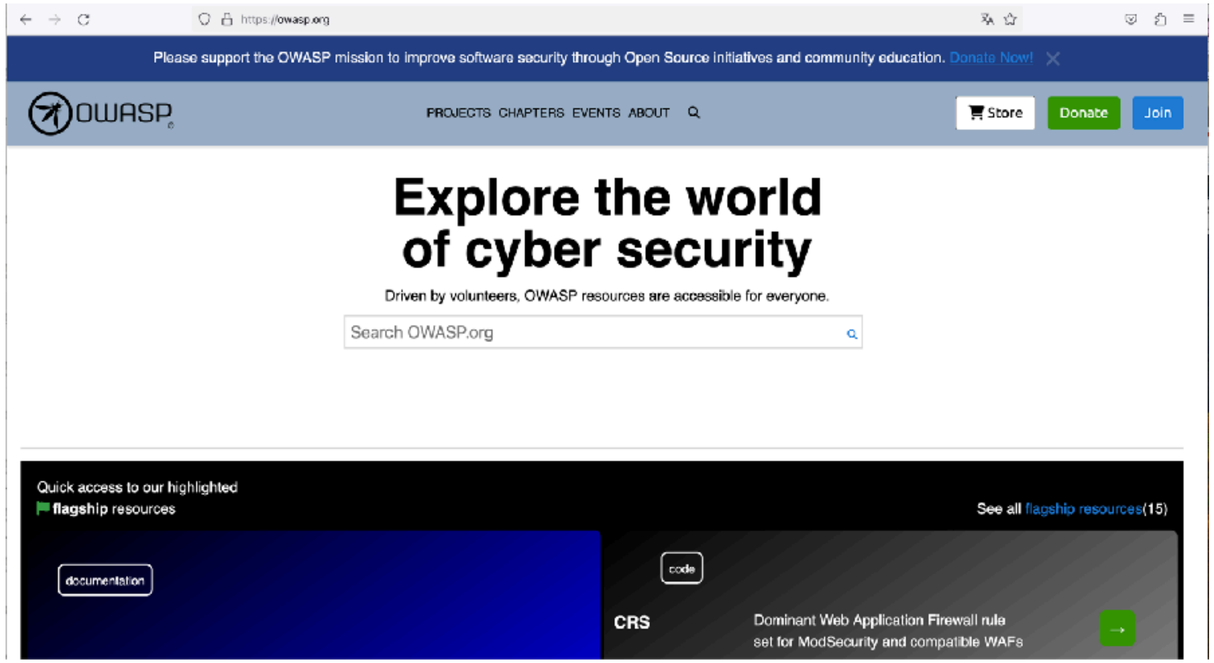
Purple team (si requis) : combinaison de membres de la Red et de la Blue team.
Son rôle est de coordonner les activités de pen-testing et superviser les relations red-blue team.

Other stakeholders : management, development, legal.

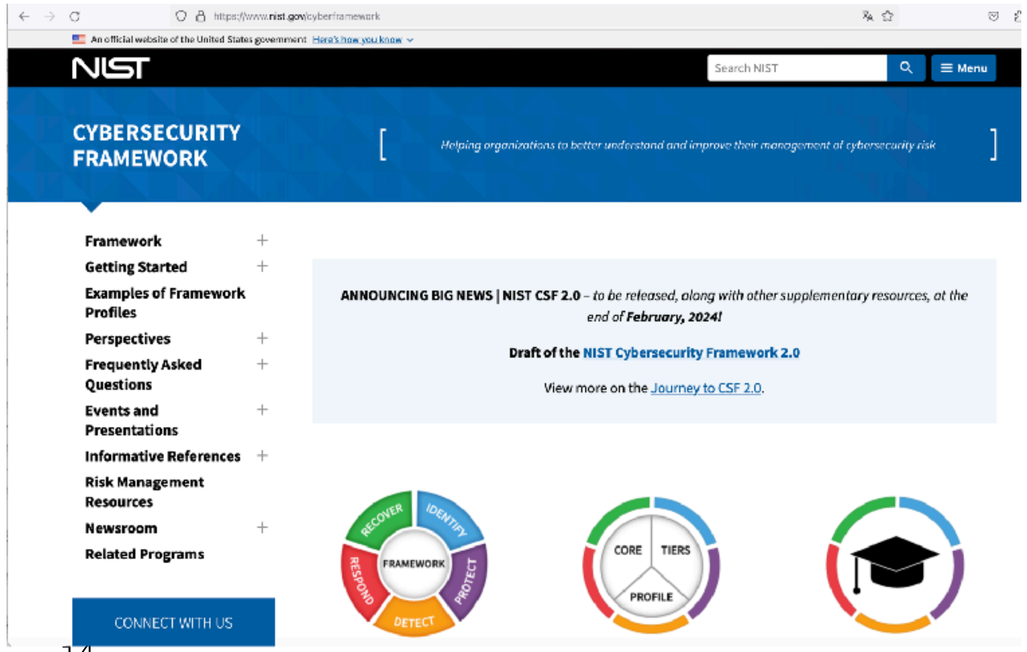
Standards et méthodologies

- **MITRE** ATT&CK Framework
  - Infos complètes et actualisées sur les menaces cyber.
  - Database de vulnérabilités (CVE).
- **OWASP :** Open Web Application Security Project
  - Méthodologies, documentations, outils de test pour le web.
  - OWASP TOP10 (vulnérabilités les plus connues et contremesures)
- **NIST** (National Institute of Standard and Technology)
  - Agence dept du commerce, définit le cadre de la cyber.
- **PTES** : Penetration Testing Execution Standard
  - Méthodologie du pentest en 7 phases.
- …





Quelques site web Intéressants



Les phases du Pen-Test

- **Planification et délimitation du champ d'application**
  Signature de contrat, définitions des cibles, objectif du test, les équipes, les méthodes (black, white, …), ROE : Rules Of Engagement (choses à faire et à ne pas faire).
- **Collecte d'information et analyse de vulnérabilité**
  Collecte passive et active, utilisation de logiciel de vulnérabilité, ingénierie sociale.
- **Attaque et exploit**
  Exploiter les vulnérabilités (passwd cracking, SQL injection, contournement d'accès, attaque physique, …)
- **Rapport et communication des résultats**
  Actions effectuées, résultats, recommandations, nettoyage.

Planification et délimitation du champ d’application

(Phase 1)

Importance du Pré-engagement

Autorisation du propriétaires des ressources

- Autorisation d'un tiers s'il héberge des ressources.
- Autorisation du cloud provider si des ressources sont sur un cloud.

Les contrats protègent les acteurs :
Service level agreement (SLA), statement of work (SOW), master service agreement (MSA), non disclosure agreement (NDA) …

Clauses de non-responsabilité

- **Point-in-time assessment** : le test se fait sur l'état du système au temps de la signature.
- **Comprehensiveness** : le test est basé sur les types de tests autorisés par le client et les vulnérabilités connues à ce moment-là.
- Des outils d'intrusion peuvent induire des dommages.

QCM !

App.wooclap.com/PENTEST1

Collecte d’information et analyse de vulnérabilité

(Phase 2)

Collecte d’informations

(Information Gathering)

Exemples de types d’informations collectées

- Adresses Email, N° Téléphone (pour attaques social engineering)
- Adresses IP de la cible.
- Les systèmes qui fonctionnent ou qui sont à l’arrêt.
- Les ports ouverts ou fermés.
- Les logiciels utilisés et leurs versions.
- Les logiciels fonctionnent-ils sur le cloud ou en local ?

Collecte d’informations

- **Passive** : ressources publiques d’internet (noms d’@IP, personnes potentiellement cibles, information sur le système, etc.). Pas de connexion directe à l’organisation (évite suspicion).
  - Ex : réseaux sociaux, moteur de recherche, …
- **Active** : utilise des outils qui se connectent avec l’organisation pour obtenir des infos sur le système (ex : scan).
  - Ex : scan de ports (nmap), …

Collecte d'informations passive : OSINT

(Open Source Intelligence)

- Outils OSINT organisés en catégories :
  https://osintframework.com/
- Moteurs de recherches (google, bing, DuckDuckGo…)
- Inspection des metadata des documents
  (Exiftool, Metagoofil, FOCA,…)
- Inspecter les anciennes versions des sites web :
  https://web.archive.org/
- Social Media Scraping : utiliser Facebook, Twitter, Linkedin pour en déduire des informations potentiellement sensibles

Collecte d’informations passive (suite)

Strategic Search Engine Analysis

- www.shodan.io : informations sur les appareils connectés à Internet.
- www.censys.io : idem + indication géographique.
- www.exploit-db.com/google-hacking-database (GHDB).
- www.cve.org : common vulnerabilities and exposures.
- www.cwe.org : common weakness enumeration.
- Guide pour test d’intrusion : NIST SP 800-115.
- Outils en ligne de commande : whois, Recon-ng, theHarvester, Maltego,…

Collecte d’informations passive
Résumé

- C’est une étape très importante qu’il ne faut pas négliger.
- Elle permet d’avoir des informations sur
  - des @mails, des noms de responsables et leurs responsabilités, des localisations,
  - des sous traitances,
  - le réseau, les serveurs (web, DNS Mail, …),
  - Éventuellement les softwares et versions,
  - …
- Elle permet de rester discret (pas de connexion à la cible).

QCM !

App.wooclap.com/PENTEST1

Collecte active (1)

Connexion directe à la cible

- @IP et N° de ports ouverts.
- Version de l'OS.
- Logiciels et leurs versions.
- Information sur la topologie du réseau (zenmap, SNMP).
- Information de routage (tracert, traceroute, …).
- Information sur les serveurs web.
- Présence de proxys.
- Information sur les techniques de détection de la cible.
- Hébergement externe d'une partie de l'infrastructure.
- Etre le plus discret possible.

Collecte active avec nmap (2)

La cible est directement attaquée. En général, la cible est une machine (host).

Quels hôtes sont en lignes ?

```
nmap -sP 192.168.1.0/24
```

Ping sweep (ICMP)

Quels sont les services ouverts ?

```
nmap -sT 192.168.1.35
```

(SYN, SYN-ACK, ACK)

Three-way handshake

Focus sur un ou plusieurs ports

```
nmap -sT 192.168.1.35 -p 80,443
```

Ce host est-il un serveur web ?

Moins de traffic (SYN, SYN-ACK)

```
sudo nmap -sS 192.168.1.35
```

SYN scan

Collecte active avec nmap (3)

Teste les ports ouverts pour déterminer le service en écoute et sa version :

```
nmap -sV 192.168.1.35
```

Quel OS tourne sur la cible ?

```
nmap sS —O 192.168.1.35
```

-O : OS qui tourne sur la cible
-o : écrit le résultat dans un fichier

Réduction du traffic (le ping en moins)

```
nmap -sS -Pn 192.168.1.0/24
```

Ralentir le scan pour rester discret

```
nmap -A -T0 192.168.1.35
```

-A donne les versions et l'OS

-T0 : très lent (paranoid)
...
-T5 : très rapide (insane)

Collecte active (4)

Website reconnaissance

- **Crawling** website : explorer le site, ses liens et répertoires pour découvrir sa structure. Peut être manuel ou utiliser des outils automatiques.
- **Scraping** website : extraction des données utiles révélées par le crawling.
- Inspection manuelle des liens en utilisant le fichier robots.txt. Exemple : https://www.ibm.com/robots.txt
- **Outils** : wget (download websites), msfcrawler (Metasploit), Black Widow (open source), w3af (open source), Burp Suite Spider (application Java, PortSwigger Ltd).

Collecte active (5)

- **Packet interception**

Sniffer les packets (Wireshark, TCPDump, …)

- **Crafting**

Sonder les ensembles de règles des pare-feu pour trouver des points d'entrée dans la cible (par exemple en envoyant des packets SYN avec la commande hping3).

- Vol de **Tokens**

Utilisés dans l’authentification ou l’autorisation. Wireshark peut être utilisé.

- **Détecter les défenses de la cible**

Load balancer, Web Application Firewall (WAF), anti virus, firewall.

Collecte active Résumé

- La reconnaissance active inclut l'utilisation de **scanners** pour trouver des hosts ayant d'éventuelles vulnérabilités.
- Le scanner à connaître : **nmap**.
- Web site reconnaissance : **crawling** (spidering) un site pour analyser ses liens et directories et découvrir sa structure.
- Les outils à connaître : **wget**, **msfcrawler**, **Black Widow**, **Burp Suite** Spider.
- Le **sniffing** permet d'intercepter ARP traffic, obtenir des tokens, détecter les systèmes de défense (load balancers, firewalls).
- Outils à connaître : **Wireshark** (sniffing), **hping3** (crafting).
- **Rester discret** : scanner 1 cible à la fois, réduire le nombre de ports à scanner, changer les IP ou MAC des machines régulièrement.

QCM !

App.wooclap.com/PENTEST1

Recherche des vulnérabilités

- Les **informations collectées** sont analysées.
- Certaines informations peuvent faire apparaitre des **faiblesses** impactant potentiellement la confidentialité, l'intégrité ou la disponibilité du système.
- La phase suivante consiste à rechercher des **vulnérabilités** connues (recensées).
- On appelle ça « **vulnerability scanning** » en anglais et il existe des outils puissants pour faire ce travail.

Principaux types de vulnérabilités

- Logiciels non patchés.
- Trop de comptes avec privilèges admin.
- Configuration par défaut : exemple login password.
- Permissions par défaut : l'accès aux objets doit suivre la politique de sécurité choisie.
- Certificat SSL/TLS : invalide, périmé, …
- Vulnérabilité du web : SQL injection, XSS, …
- Vulnérabilité humaine.
- …

Principaux outils de scans

Principaux outils de scan paramétrables qui recherchent des vulnérabilités connues :

- **Nikto, OWASP ZAP** : open source web app.
- **Nessus** : commercial, version gratuite limitée. Nessus collecte les infos et classe les vulnérabilités.
- **OpenVAS** : alternative gratuite à Nessus.
- **Burp Suite** : commercial mais très utilisé par les pros.
- **SQLmap** : open source pour les attaques injection SQL.
- WPScan : open source pour les sites WordPress.
- Scout Suite : audit de sécurité pour le cloud.
- …

Vulnérabilités des app web

2 principales techniques pour tester les app :

- **Static app security testing (SAST)** : analyse le code à la recherche de vulnérabilités. Aussi appelé « white box testing ».
- **Dynamic app security testing (DAST)** : analyse d'un app qui tourne (pas d'accès au code).

Utilisation de Nessus et SQLmap

CVSS : Common Vulnerability Scoring System

Sévérité de la vulnérabilité : CVSS base score
[0-4[: Low ; [4-7[: Medium ; [7-10[: High : 10 : Critical

CVSS Vector information Vector. Exemple :
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Version

Attack Vector : Network
Attack Complexity : Low
Priviledges required : None
User interaction : None

Scope : Changed
Confidentiality : High
Integrity : High
Availability : High

QCM !

App.wooclap.com/PENTEST1

Attaque et exploit

(Phase 3)

Méthodes d’exploitation

- Après avoir recueilli des informations sur les cibles et identifié les vulnérabilités potentielles, on peut passer à la phase d'exploitation.
- L'exploitation consiste à exécuter des exploits contre les vulnérabilités découvertes (possible objectif : escalade des privilèges).
- Avec un peu de chance le scan peut donner une vulnérabilité exploitable avec un outil automatisé comme **metasploit**.
- Des scanners comme Nessus produisent ces informations.

Quelles vulnérabilités exploiter ?

La selection de la vulnérabilité dépend du « statement of work » et « Rules of engagement » et de Owasp Top 10 et de son score CVSS

- Classées CRITICAL ou HIGH.
- Dont il existe une exploitation connue (des scanners comme NESSUS indiquent si un code peut être utilisé pour exploiter la vulnérabilité).
- Dont la complexité (AC) est Low ou Medium.
- Qui peuvent permettre un remote shell (par ex : VNC).

BD d’exploitations

Où trouver les codes d’exploitation des vulnérabilités ?

- **Exploit Database**
  https://exploit-db.com
- **Vulnerability and Exploit Database** (Rapid7, intégré à Metasploit)
  https://www.rapid7.com/db
- NIST National Vulnerability Database (**NVD**)
  https://nvd.nist.gov
- …

Exploitation : étapes à suivre

1. Tentative de connexion à la cible en utilisant la vulnérabilité. Par exemple, si elle est liée à SSH, essayer une connexion SSH.
2. Fournir les données attendues par la cible pour la connexion.
3. Fournir ou contourner login password.
4. Une fois connecté, penser à charger un code qui permettra de rétablir facilement la connexion (persistence).
5. Effectuer des reconnaissances.
6. Recueillir des données.
7. Prendre des mesures pour dissimuler sa présence sur la cible.
8. Nettoyer quand l’exploitation est finie.

Metasploit (Rapid7)

C’est un framework qui permet d’effectuer ces étapes.
Utilisation :

- Start the console (commande `msfconsole`).
- Lister les exploits (`show exploits`).
- Choose an exploit to use (`use` …).
- Configure parameters needed by the exploit (`show options`, puis `set` …).
- Choose a payload if needed.
- Run the exploit (`exploit`).

Démo concernant Eternal blue avec Metasploit

QCM !

App.wooclap.com/PENTEST1

Rapport et communication des résultats

(Phase 4)

- Quand et comment communiquer ?
- Suggérer des stratégies de remédiation.
- Rédaction et traitement du rapport final.
- Activités postérieures à la remise du rapport.

Well-defined communication path

Le NDA (nondisclosure Agreement) définit les contacts adhoc :

- **Primary contact**: responsable de la coordination journalière et de la gestion du test.
- **Technical contact**: pour fournir un support technique.
- **Emergency contact**: le contact en cas d'urgence. La découverte d'une attaque en cours est un cas d'urgence.

Communication triggers

Les principaux déclencheurs sont

- **Critical findings** : les failles de sécurité critiques doivent être signalées au contact adhoc.
- **Stage completion** : à la fin de chaque étape du pentest, rencontrer le client pour un compte rendu.
- **Indicators of a prior compromise** (IOC) : le pentester a les preuves que le système a été compromis. Il faut en informer immédiatement les parties prenantes (stakeholders).

Autres raisons de communiquer : demande de modification du scope, demande d'infos supplémentaires, demande spécifique, …

Findings and remediations

- **Shared local administrator credentials**: Utiliser un mot de passe différent par machine.
- **Weak password complexity**: Renforcer la politique de passwords. Utiliser des filtres (proactifs, réactifs).
- **Plain text passwords**: Chiffrer les passwords !
- **No multifactor authentication**: implémenter MFA surtout dans les environnements Cloud (par ex Office 365).
- **SQL injection**: « sanitize user input » ou utiliser « parameterize queries » (aussi appelé « prepared statement »)
- **Unnecessary open services**: notion de « System hardening ». Eliminer ce qui n'est pas nécessaire (ports, comptes,…), chiffrer les communications (TLS, IPSec, …)

Contrôles administratifs

Vérifier que

- des mécanismes de contrôles d’accès sont utilisés (ex RBAC).
- Il existe un règlement de sécurité et qu’il est appliqué.
- Il existe une politique concernant la complexité minimale des passwords.
- les programmeurs suivent le cycle de développement sécurisé des logiciels et mettent en œuvre la sécurité à toutes les phases du cycle de vie de l'application.

Contrôles opérationnels communs

- **Job rotation**. Plusieurs personnes peuvent effectuer une tâche donnée. Détecter les activités frauduleuses d'un précédent employé à ce poste.
- **Time-of-day restrictions**. Les restrictions horaires consistent à limiter l'accès aux installations ou aux ressources du réseau aux heures de travail.
- **Mandatory vacations**. Permet de détecter tout acte répréhensible sur le lieu de travail ou toute activité frauduleuse.
- **User training**. La sensibilisation des employés peut réduire considérablement les risques d'incident de sécurité.

Contrôles physiques courants

- **Access control vestibule**. Vérifier que l’accès aux endroits sensibles n’est donné qu’aux personnes autorisées.

- **Video surveillance**. Des caméras de vidéosurveillance doivent être installées dans l'ensemble de l'établissement pour surveiller l'activité à l'intérieur de l'établissement et à toutes les entrées et sorties.

Rédaction du rapport (1)

- **Titre** et **table des matières**.
- **Executive summary**. Pour les cadres supérieurs ou l'équipe de direction. Il est écrit en dernier. Contient les **informations clés**, méthodologie utilisée, les tâches clés effectuées et une vue d'ensemble des conclusions et des résultats.
- **Scope details**.
- **Methodology**. Types de tests, comment les attaques ont été menées. Les procédés pour identifier et évaluer les risques, les métriques utilisées.

Rédaction du rapport (2)

- **Findings and remediation**. Discuter des **problèmes** de sécurité constatés et des **mesures correctives** à prendre pour résoudre chaque problème de sécurité. L’évaluation des risques doit comprendre une analyse sur l’**impact business** (BIA).

- **Conclusion**. Résumer les résultats et identifier les parties d'un test typique qui n'ont pas été incluses dans l'évaluation et que l'entreprise pourrait vouloir effectuer à l’avenir. Par ex. recommender un futur test « social engineering ».

- **Appendix**.

Protection du rapport

- Le rapport doit être **chiffré** lorsque stocké ou envoyé.
- L'accord original de pentest doit spécifier la **durée** pendant laquelle le pentester a une copie du rapport en sa possession.
- Celle-ci doit être conservée en lieu sûr.
- Une fois que le rapport n'est plus nécessaire, l'organisme de pentesting doit **supprimer** en toute sécurité les copies numériques et déchiqueter les copies papier.

Post-engagement cleanup

- **Removing shells**: Supprimer tous les programmes shell installés lors de l'exécution du pentest.
- **Removing tester-created credentials**: Veiller à supprimer tous les comptes d'utilisateurs créés pendant le pentest. Cela inclut les comptes de portes dérobées (backdoors).
- **Removing tools**: Supprimer tous les outils logiciels qui ont été installés.

Le reste des taches est principalement d’ordre administratif.

Last QCM !

App.wooclap.com/PENTEST1