



Sécurité des S.I.

V. Brague – B. Grapeloup – M. Raissi

Janvier 2021

Introduction

Whoami

> Valentin

- Différents postes:

- Administration
- SoC Interne
- Réponse sur incident
- Sensibilisation auprès d'utilisateurs
- Pentest
- Hunting
- Bientôt RedTeam !



Sommaire

- ▶ Introduction
- ▶ Sécurité des systèmes
- ▶ Sécurité des applications
- ▶ Détection d'attaques
- ▶ Attaque sur infrastructure

Organisation de la sécurité dans une entreprise

- ▶ Les politiques de sécurité (PSSI)
 - ▶ Politique de Sécurité des Systèmes d'Information
- ▶ Les documents techniques
 - ▶ Politique de mot de passe
 - ▶ Gestion des mises à jour
 - ▶ Guide de journalisation d'évènements
- ▶ Audits
 - ▶ Organisation
 - ▶ Technique

Les vulnérabilités et le système CVE

Vulnérabilité : faiblesse permettant de porter atteinte à l'**intégrité**, la **confidentialité** ou la **disponibilité**



Créent en 1999 un **système international de référencement** des vulnérabilités

CVE-YYYY-XXXXX
année - identifiant

Chaque vulnérabilité se voit attribuer un **score de criticité sur 10** nommé CVSS.

CVE-2017-0144 : vulnérabilité dans le protocole SMBv1, exploitée par la NSA (outil « EternalBlue »)

CVE-2020-1472 (ZeroLogon) : vulnérabilité dans le protocole d'authentification Netlogon permettant de devenir administrateur d'un domaine Windows



@CVEnew



Sécurité des systèmes

Architecture des S.I.

Le réseau d'un S.I. d'entreprise est constitué de **différents sous-réseaux** et de différents **équipements réseau**.

Pourquoi diviser le réseau en sous-réseaux, plutôt que d'avoir un seul réseau ?

- Confiner les problèmes réseau et optimiser le trafic

Exemple : tempêtes de broadcast

- Confiner les intrusions potentielles

Exemple : empêcher un intru connecté à la prise d'une salle de réunion d'accéder aux postes des utilisateurs

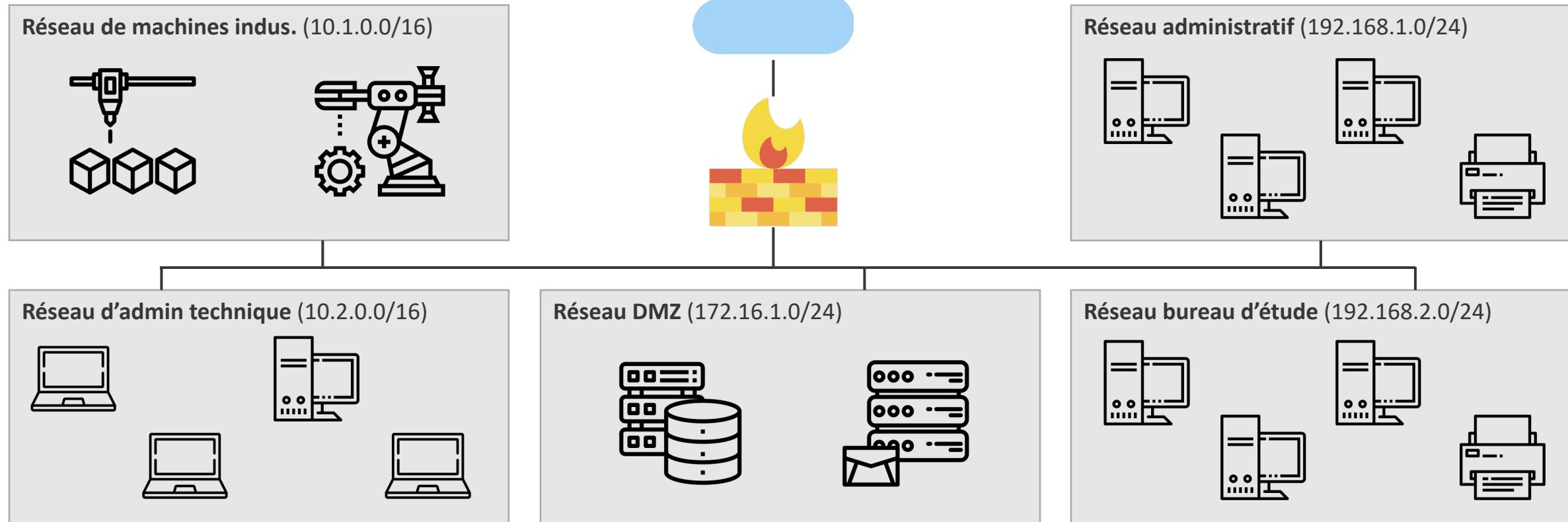
- Assurer des facilités de gestion opérationnelle

Exemple : bloquer le sous-réseau du service comptabilité d'accéder au sous-réseau des machines industrielles

Un **pare-feu** permet de gérer la communication entre sous-réseaux, mais aussi de/vers Internet.

Architecture des S.I.

Exemple de schéma d'architecture réseau



1. Qu'est-ce qu'une zone DMZ, quelle est sa particularité ?
2. Que peut-on dire sur les classes d'adressage de ce réseau ?

Architecture des S.I.

Un pare-feu fonctionne à l'aide de **règles de flux** autorisant ou bloquant les flux réseau qui lui parviennent.

Un flux réseau peut être autorisé ou bloqué selon différents **critères**, notamment :

- L'adresse IP ou le réseau source
- Le port source
- L'adresse IP ou le réseau de destination
- Le port de destination
- Le protocole (TCP ou UDP)

Les métadonnées de chaque paquet qui arrive à un pare-feu sont comparées aux différentes règles.

Chaque règle est évaluée une par une, dans l'ordre, jusqu'à ce que l'une corresponde au paquet.

Une dernière règle (parfois implicite) bloque les paquets qui ne correspondent à aucune règle précédente.

Architecture des S.I.

Exemple d'une table de règles de flux **partielle** (*préfixes des alias : N_ = Network, S_ = Serveur*)

ID	IP SOURCE	PORT SOURCE	IP DEST.	PORT DEST.	PROTOCOLE	ACTION
1	Any	Any	Ce pare-feu	53	UDP	AUTORISER
2	Any	Any	Ce pare-feu	123	Any	AUTORISER
3	N_Bureaux	Any	Any	80, 443	TCP	AUTORISER
4	N_Bureaux	Any	S_MAIL	587, 993	TCP	AUTORISER
5	N_Admin	Any	N_Machines_Indus	992	TCP	AUTORISER
[...]						
100	Any	Any	Any	Any	Any	BLOQUER

Remarque : la toute dernière règle #100 est parfois implicite chez certains éditeurs de solutions de pare-feu.

- 
1. Pourquoi le port source de chacune de ces règles est-il « Any » ?
 2. À quoi servent chacune de ces règles ?
 3. Le réseau de machines industrielles peut-il surfer sur le web ?
 4. Le bureau d'étude peut-il se connecter au serveur email de l'entreprise situé dans la DMZ ? Recevoir des mails de l'extérieur ?
 5. Le réseau administratif peut-il accéder au réseau de machines ?

Architecture des S.I.

Conseils pour concevoir sa table de règles de flux

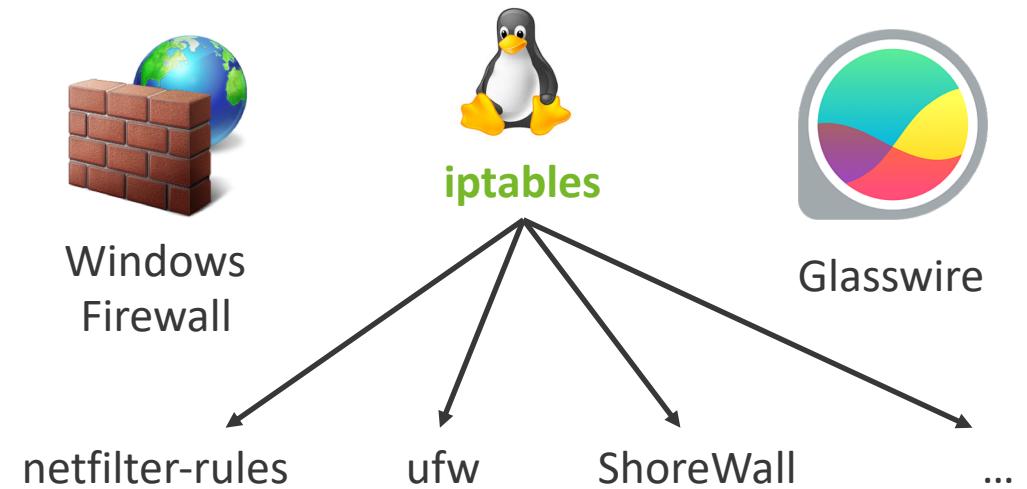
- D'abord comprendre et lister les besoins métiers, puis les traduire « informatiquement » par la suite
Exemple : « la comptabilité doit accéder à Internet » => « le réseau 192.168.1.0 doit accéder à 80/443 TCP »
- Faire des règles aussi nominales que possible
Exemple : ne pas définir dans la même règle l'accès à des ports web et des ports mail
- Organiser les règles par catégories
Certaines solutions de pare-feu le permettent pour des commodités de gestion
- Avoir une politique de nommage documentée pour les alias, avec des préfixes ou suffixes
Exemple : N_ pour les réseaux, S_ pour les serveurs, P_ pour les postes de travail...
- Commenter les règles
Certaines solutions de pare-feu le permettent, mais attention à ne pas sur-commenter des choses évidentes !
- Journaliser les bonnes règles
On journalise en général les règles de blocage pour permettre de dissocier les accès légitimes des attaques

Architecture des S.I.

De la théorie simple à la « vraie vie »...

- Les pares-feux sont aujourd’hui ***stateful*** (par opposition à ***stateless***) : les communications retour sont gérées
- L’action « Bloquer » peut en fait être déclinée en **Drop** ou **Reset**
- Possibilité de **journaliser** le trafic qui passe par tout ou partie des règles
- Les pare-feu modernes (NGFW = Next-Gen FW) offrent des possibilités supplémentaires pour le **filtrage**
- Les pare-feu modernes offrent des **fonctionnalités** supplémentaires

Un pare-feu peut être **matériel** (équipement réseau propre) ou **logiciel** (installé sur chaque machine).



Durcissement des configurations

Les sujets abordés :

- Politique de mot de passe
- Gestion des mises à jour
- Gestion des accès
- Désactivation des services non utilisés
- Restriction réseau au niveau des hôtes
- Sécurisation des services exposés

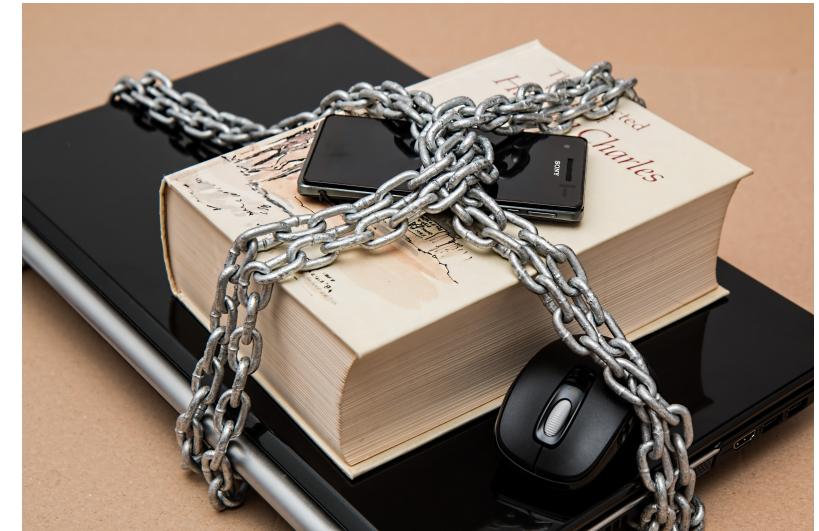
Durcissement des configurations système

Politique de mot de passe

Elle est la base commune définissant les règles d'acceptation d'un mot de passe suivant un nombre de règles.

Les principales problématiques étant :

- Utilisation de mots de passe à faible entropie
- Réutilisation de mots de passe à travers plusieurs services
- Non renouvellement du mot de passe
- Faible variation des mots de passes lors du renouvellement
- Stockage insécurisé des mots de passe



Durcissement des configurations système

Politique de mot de passe

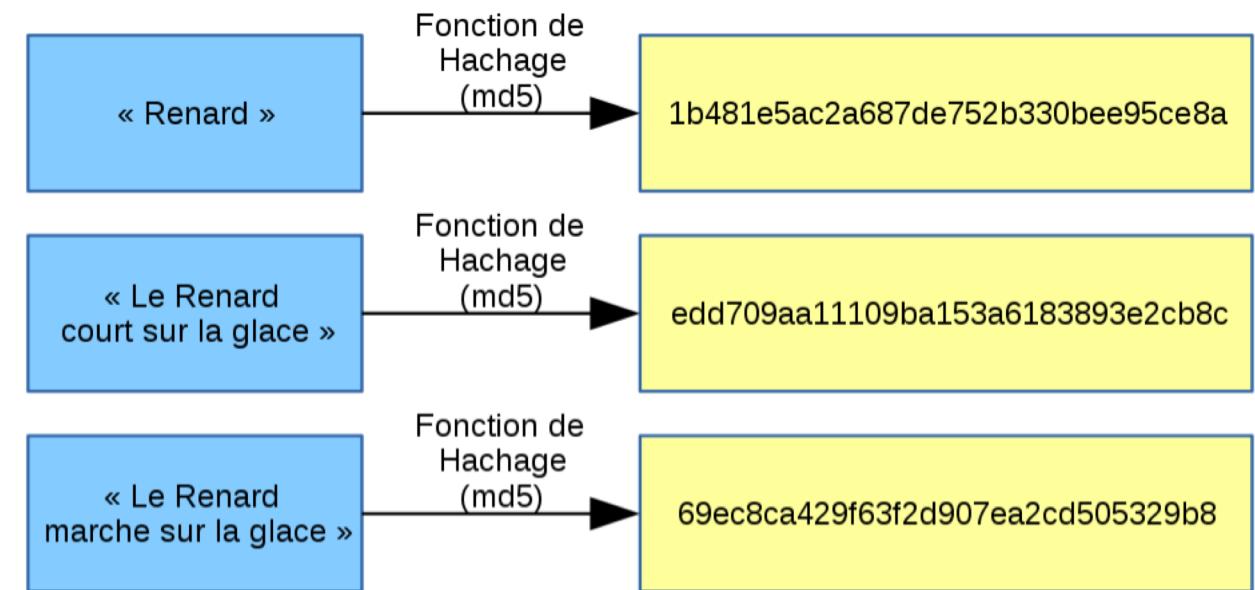
Le « hashage », est une fonction mathématique permettant de calculer une empreinte numérique permettant d'identifier une donnée de manière unique.

Plusieurs cas d'usages :

- Mots de passe
- Identifier un fichier
- Vérifier l'intégrité d'une donnée

Plusieurs fonctions :

- Md5
- Sha1, sha256, sha512



Durcissement des configurations système

Politique de mot de passe

Les principales attaques :

- BruteForce
- PasswordSpraying
- RainbowTable

Les outils :

- John The Ripper
- Hashcat
- THC Hydra
- Patator

123456
password
12345678
qwerty
123456789
12345
1234
111111
1234567
dragon
123123
baseball
abc123
football
monkey
letmein
696969
shadow
master
666666
qwertyuiop
...



awesome@company.com

Durcissement des configurations système

Politique de mot de passe

Les principales attaques :

- BruteForce
- PasswordSpraying
- RainbowTable

Quelques statistiques :

- 65% des personnes réutilisent un mot de passe pour plusieurs comptes
- 13% des personnes utilisent le même mot de passe pour l'ensemble de leurs comptes.
- Même en ayant connaissance des risques, 59% des personnes réutilisent un mot de passe pour plusieurs comptes.
- 42% des entreprises compromises en 2019 l'ont été via des mots de passe faibles.
- 48% des personnes utilisent des mots de passe identiques pour leurs comptes personnels et leurs comptes professionnels.

Durcissement des configurations système

Politique de mot de passe

Les principales attaques :

- BruteForce
- PasswordSpraying
- RainbowTable

Comment s'en prémunir :

- Ne pas réutiliser un mot de passe pour plusieurs comptes
- Utiliser un gestionnaire de mots de passe
- Utiliser des mots de passe avec une complexité importante
 - + de 8 caractères
 - Chiffres et caractères spéciaux
 - Majuscules et minuscules
- Changer régulièrement le mot de passe

Du point de vue système :

- Limiter le nombre de tentatives par comptes
- Mettre en place de la supervision de sécurité
- Imposer une politique de sécurité aux utilisateurs

Durcissement des configurations système

Politique de mot de passe

Les principales attaques :

- BruteForce
- PasswordSpraying
- RainbowTable

Les outils :

- John The Ripper
- Hashcat
- THC Hydra
- Patator

123456
password
12345678
qwerty
123456789
12345
1234
111111
1234567
dragon
123123



[awesome@company.com](#)
[cto@company.com](#)
[hr@company.com](#)
[Jean-daniel@company.com](#)
[Rene@company.com](#)
[michel@compagny.com](#)

Durcissement des configurations système

Politique de mot de passe

Les principales attaques :

- BruteForce
- PasswordSpraying
- RainbowTable

Comment s'en prémunir :

- Ne pas réutiliser un mot de passe pour plusieurs comptes

Du point de vue système :

- Limiter le nombre de tentatives pour une même IP
- Mettre en place une surveillance de sécurité

Durcissement des configurations système

```
[ssh]
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 6
```

Configuration Fail2Ban

```
Status
|- Number of jail:      1
`- Jail list:  sshd
root@localhost:~# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed:      6
| `- File list:          /var/log/auth.log
`- Actions
| |- Currently banned:  3
| |- Total banned:       3
| `- Banned IP list:    185.220.102.6 104.236.239.60 197.211.1.6
```

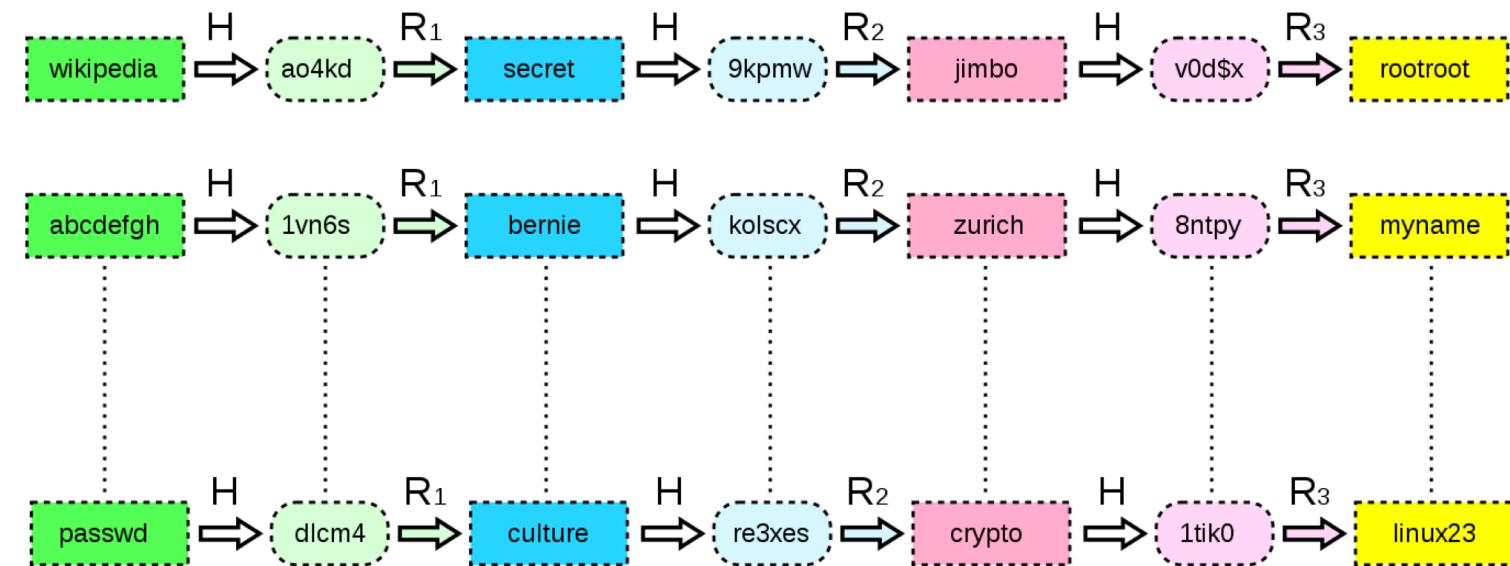
Status Fail2Ban

Durcissement des configurations système

Politique de mot de passe

Les principales attaques :

- BruteForce
- PasswordSpraying
- RainbowTable



Durcissement des configurations système

Politique de mot de passe

Les principales attaques :

- BruteForce
- PasswordSpraying
- RainbowTable

Comment s'en prémunir :

- Limiter le risque de compromission de la base de donnée.
- Utiliser des fonctions de hashage plus complexe à calculer.
- Utiliser un « sel » pour complexifier les tentatives d'utilisation de rainbow table.
- Contraindre les utilisateurs à une politique de mot de passe forte.

Durcissement des configurations système

Sous Linux il est possible de gérer une politique de mot de passe localement avec PAM.

```
#  
# Password aging controls:  
#  
#      PASS_MAX_DAYS   Maximum number of days a password may be used.  
#      PASS_MIN_DAYS   Minimum number of days allowed between password changes.  
#      PASS_WARN_AGE    Number of days warning given before a password expires.  
#  
PASS_MAX_DAYS    99999  
PASS_MIN_DAYS    0  
PASS_WARN_AGE    7
```

/etc/login.defs

```
minlen=12 maxrepeat=3 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 difok=4 reject_username  
enforce_for_root
```

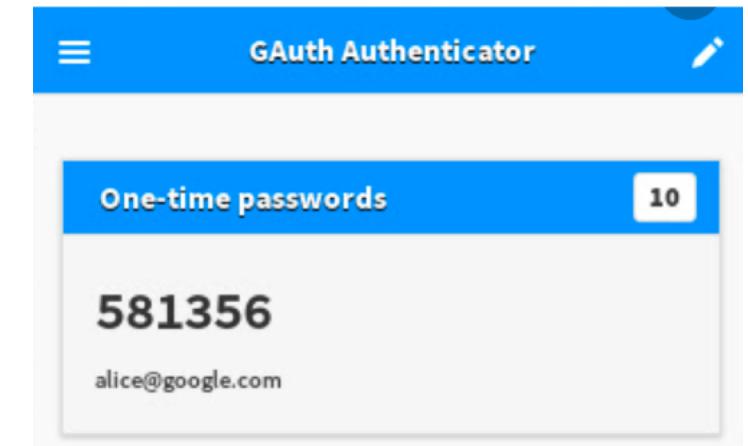
/etc/pam.d/common-password

Durcissement des configurations système

Politique de mot de passe

Les alternatives ou compléments aux mot de passe :

- Token physiques
 - Yubikey
 - RSA
- Token logiques
 - Google Authenticator
 - KeePass
- Reconnaissance biométrique
 - Empreintes
 - Reconnaissance faciale (Alicem)



Durcissement des configurations système

Gestion des mises à jour

Elle est la base définissant les processus et les règles de mise à jour de l'ensemble des éléments d'un Système d'information.

Les composants non mis à jour :

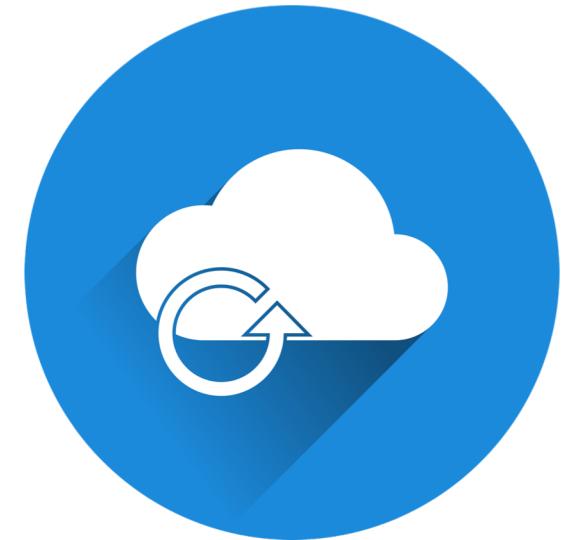
- Sont un des vecteurs préférés par les attaquants
- Sont des attaques plus ou moins triviales
- Sont souvent la porte d'entrée dans le système d'information

Durcissement des configurations système

Gestion des mises à jour

Un exemple de processus de mise à jour :

- Inventaire du parc précis
- Scan de vulnérabilité
- Validation que les patchs correspondent, et ne cassent rien d'existant
- Utilisation de moyen automatique pour pousser les mises à jour



Durcissement des configurations système

Gestion des accès

Elle est la base définissant les droits dont chaque compte hérite en fonction de son rôle.

Quelques exemples :

- Comptes locaux
 - Règle de nommage
 - Limiter les comptes génériques
- Raccordement à un référentiel commun, LDAP
 - AGDLP Pour Windows
 - Règle de nommage
 - Revue régulière des droits
 - Désactivation des comptes inactifs



Durcissement des configurations système

Désactivation de services non utilisés

L'exposition de services qui ne sont pas utilisés augmente la surface d'attaque.

Il est recommandé de laisser que les services nécessaires au bon fonctionnement du système, ou de l'application.



Durcissement des configurations système

Mise en place de restriction réseau au niveau des hôtes

La mise en place d'un pare-feu au niveau de l'hôte peut ressembler à la dernière défense limitant des accès illicites

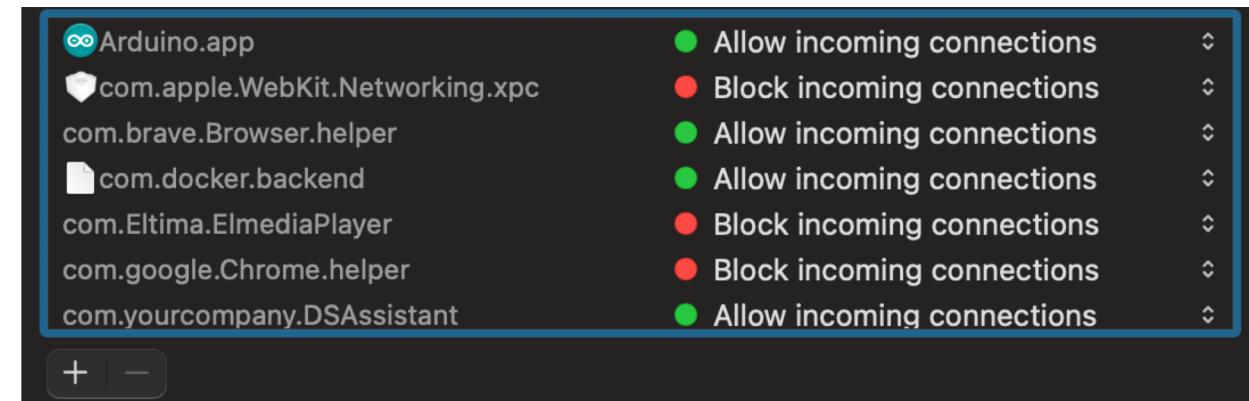
Quelques exemples :

- Si un pare-feu venait à être trop permissif, cela limiterait l'impact
- Limiter les mouvements lateraux d'attaquants
- N'exposer que les services utilisés pour limiter la surface d'attaque



Durcissement des configurations système

Nativement, l'ensemble des Systèmes d'exploitation ont un pare-feu local.



Nom du programme	Zone	Protocole : P...	Connecté à	Date et heure
C:\Windows\System32\sass.exe		TCP :49475		11/9/2016 11:06:09 AM
C:\Windows\System32\sass.exe		TCPv6 :49475		11/9/2016 11:06:09 AM
C:\Windows\System32\services.exe		TCP :49412		11/9/2016 11:06:01 AM
C:\Windows\System32\services.exe		TCPv6 :49412		11/9/2016 11:06:01 AM
C:\Windows\System32\spoolsv.exe		TCP :49410		11/9/2016 11:06:01 AM
C:\Windows\System32\spoolsv.exe		TCPv6 :49410		11/9/2016 11:06:01 AM
C:\Windows\System32\wininit.exe		TCP :49408		11/9/2016 11:06:00 AM
C:\Windows\System32\wininit.exe		TCPv6 :49408		11/9/2016 11:06:00 AM

Durcissement des configurations système

```
# Generated by iptables-save v1.6.0 on Wed Jan 20 20:59:00 2021
*raw
:PREROUTING ACCEPT [24005949:91948567716]
:OUTPUT ACCEPT [603588:138214153]
COMMIT
# Completed on Wed Jan 20 20:59:00 2021
# Generated by iptables-save v1.6.0 on Wed Jan 20 20:59:00 2021
*nat
:PREROUTING ACCEPT [147680:6140295]
:INPUT ACCEPT [139503:5648824]
:OUTPUT ACCEPT [2961:202133]
:POSTROUTING ACCEPT [12372:756208]
:DOCKER - [0:0]
-A PREROUTING -m addrtype --dst-type LOCAL -j DOCKER
-A OUTPUT ! -d 127.0.0.0/8 -m addrtype --dst-type LOCAL -j DOCKER
-A POSTROUTING -s 172.25.0.0/16 ! -o br-2d468bc56e50 -j MASQUERADE
-A POSTROUTING -s 172.24.0.0/16 ! -o br-729329f1f38c -j MASQUERADE
-A POSTROUTING -s 172.23.0.0/16 ! -o br-9d0205451be6 -j MASQUERADE
-A POSTROUTING -s 172.17.0.0/16 ! -o docker0 -j MASQUERADE
-A POSTROUTING -s 172.23.0.2/32 -d 172.23.0.2/32 -p tcp -m tcp --dport 443 -j MASQUERADE
-A POSTROUTING -s 172.23.0.2/32 -d 172.23.0.2/32 -p tcp -m tcp --dport 80 -j MASQUERADE
```

Exemple d'iptables sous Linux.

Durcissement des configurations système

Il existe plusieurs outils pour gérer le Firewall d'un hôte linux :

Considérés comme le « backend »

- IPTables
- Nftables

```
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
```

To	Action	From
--	-----	----
22/tcp	ALLOW IN	Anywhere
Anywhere on eth0	ALLOW IN	192.168.0.0/16
25/tcp	ALLOW IN	Anywhere
80/tcp	DENY IN	Anywhere
22/tcp (v6)	ALLOW IN	Anywhere (v6)
25/tcp (v6)	ALLOW IN	Anywhere (v6)
80/tcp (v6)	DENY IN	Anywhere (v6)

Considérés comme le « frontend »

- UFW
- Firewalld

Durcissement des configurations système

Sécurisation des services utilisés

Un service exposé se doit d'être sécurisé au maximum pour limiter des utilisations illicites.

Quelques exemples :

- Mise en place de HTTPS
- Limiter le nombre de requêtes par secondes
- Uniquement autoriser les connexions en SSH avec un certificat



Durcissement des configurations système

En résumé :

- La sécurité se joue à plusieurs niveau.
- Les choix sont toujours à adapter en fonction des risques que l'on souhaite couvrir.
- Chaque mise en place de composants, services... nécessite une réflexion avec la sécurité en tête pour limiter au maximum toute exposition.

TP01 – Sécurisation d'une machine

La société "Télécom 3000" est en recherche d'un administrateur système et sécurité suite à la démission soudaine et inexpliquée de son ancien administrateur.

Kyan était en train d'installer un nouveau serveur qui allait permettre de délivrer un nouveau service pour l'entreprise.

Seul l'OS et le SSH ont été installés, Kyan avait laissé des indications sur le travail qu'il était en train de mener sur ce serveur, votre rôle est de le reprendre et de le finir.

Sécurité des applications

Étude d'attaques web courantes

Top 10 de l'OWASP



- Établit un classement régulier des 10 vulnérabilités les plus courantes sur le web
- Fournit des **exemples d'exploitation** et donne des **conseils détaillés pour s'en prémunir**
- Tout développeur web devrait connaître ce classement !



La sécurité doit être gérée dès le début d'un projet, et non arriver comme un « vernis » sur la fin.

OWASP

Echelle de risque :

- Exploitabilité
- Prévalence de la faille
- Déetectabilité de la faille
- Impacts techniques
 - Traçabilité
 - Confidentialité
 - Intégrité
 - Disponibilité

Threat Agents	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impacts	Business Impacts
App. Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	SEVERE: 3	App / Business Specific
	AVERAGE: 2	COMMON: 2	AVERAGE: 2	MODERATE: 2	
	DIFFICULT: 1	UNCOMMON: 1	DIFFICULT: 1	MINOR: 1	

Threat Agents / Attack Vectors		Security Weakness		Impacts	
App. Specific	Exploitability: 3	Prevalence: 2	Detectability: 3	Technical: 3	Business ?
Almost any source of data can be an injection vector, environment variables, parameters, external and internal web services, and all types of users. Injection flaws occur when an attacker can send hostile data to an interpreter.	Injection flaws are very prevalent, particularly in legacy code. Injection vulnerabilities are often found in SQL, LDAP, XPath, or NoSQL queries, OS commands, XML parsers, SMTP headers, expression languages, and ORM queries. Injection flaws are easy to discover when examining code. Scanners and fuzzers can help attackers find injection flaws.	Injection can result in data loss, corruption, or disclosure to unauthorized parties, loss of accountability, or denial of access. Injection can sometimes lead to complete host takeover. The business impact depends on the needs of the application and data.			
Is the Application Vulnerable?			How to Prevent		
<p>An application is vulnerable to attack when:</p> <ul style="list-style-type: none"> * User-supplied data is not validated, filtered, or sanitized by the application. * Dynamic queries or non-parameterized calls without context-aware escaping are used directly in the interpreter. * Hostile data is used within object-relational mapping (ORM) search parameters to extract additional, sensitive records. * Hostile data is directly used or concatenated, such that the SQL or command contains both structure and hostile data in dynamic queries, commands, or stored procedures. <p>Some of the more common injections are SQL, NoSQL, OS command, Object Relational Mapping (ORM), LDAP, and Expression Language (EL) or Object Graph Navigation Library (OGNL) injection. The concept is identical among all interpreters. Source code review is the best method of detecting if applications are vulnerable to injections, closely followed by thorough automated testing of all parameters, headers, URL, cookies, JSON, SOAP, and XML data inputs. Organizations can include static source (SAST) and dynamic application test (DAST) tools into the CI/CD pipeline to identify newly introduced injection flaws prior to production deployment.</p>			<p>Preventing injection requires keeping data separate from commands and queries.</p> <ul style="list-style-type: none"> * The preferred option is to use a safe API, which avoids the use of the interpreter entirely or provides a parameterized interface, or migrate to use Object Relational Mapping Tools (ORMs). <p>Note: Even when parameterized, stored procedures can still introduce SQL injection if PL/SQL or T-SQL concatenates queries and data, or executes hostile data with EXECUTE IMMEDIATE or exec().</p> <ul style="list-style-type: none"> * Use positive or "whitelist" server-side input validation. This is not a complete defense as many applications require special characters, such as text areas or APIs for mobile applications. * For any residual dynamic queries, escape special characters using the specific escape syntax for that interpreter. <p>Note: SQL structure such as table names, column names, and so on cannot be escaped, and thus user-supplied structure names are dangerous. This is a common issue in report-writing software.</p> <ul style="list-style-type: none"> * Use LIMIT and other SQL controls within queries to prevent mass disclosure of records in case of SQL injection. 		
Example Attack Scenarios			References		
<p>Scenario #1: An application uses untrusted data in the construction of the following vulnerable SQL call:</p> <pre>String query = "SELECT * FROM accounts WHERE custID='" + request.getParameter("id") + "'";</pre> <p>Scenario #2: Similarly, an application's blind trust in frameworks may result in queries that are still vulnerable, (e.g. Hibernate Query Language (HQL)):</p> <pre>Query HQLQuery = session.createQuery("FROM accounts WHERE custID='" + request.getParameter("id") + "'");</pre> <p>In both cases, the attacker modifies the 'id' parameter value in their browser to send: ' or '1'='1. For example:</p> <p>http://example.com/app/accountView?id=' or '1='1</p>			<p>OWASP</p> <ul style="list-style-type: none"> * OWASP Proactive Controls: Secure Database Access * OWASP ASVS: V5 Input Validation and Encoding * OWASP Testing Guide: SQL Injection, Command Injection, and ORM Injection * OWASP Cheat Sheet: Injection Prevention * OWASP Cheat Sheet: SQL Injection Prevention * OWASP Cheat Sheet: Injection Prevention in Java * OWASP Cheat Sheet: Query Parameterization * OWASP Automated Threats to Web Applications – OAT-014 		

Injection

Injection SQL : manque de sécurisation des saisies utilisateur permettant de manipuler la base de données

Nom d'utilisateur

Mot de passe

```
SELECT *  
FROM users  
WHERE user_id = 'algosecure'  
AND password = 'motdepasse';
```

Nom d'utilisateur

Mot de passe

```
SELECT *  
FROM users  
WHERE user_id = 'algosecure'  
AND password = '' OR '1'='1'';
```

Impacts potentiels :

- Connexion à un compte sans en connaître le mot de passe
- Récupération de données
- Modification ou suppression de données
- Exécution de commandes sur le système (prise de contrôle)

Injection

Ne jamais avoir confiance dans les données récupérées

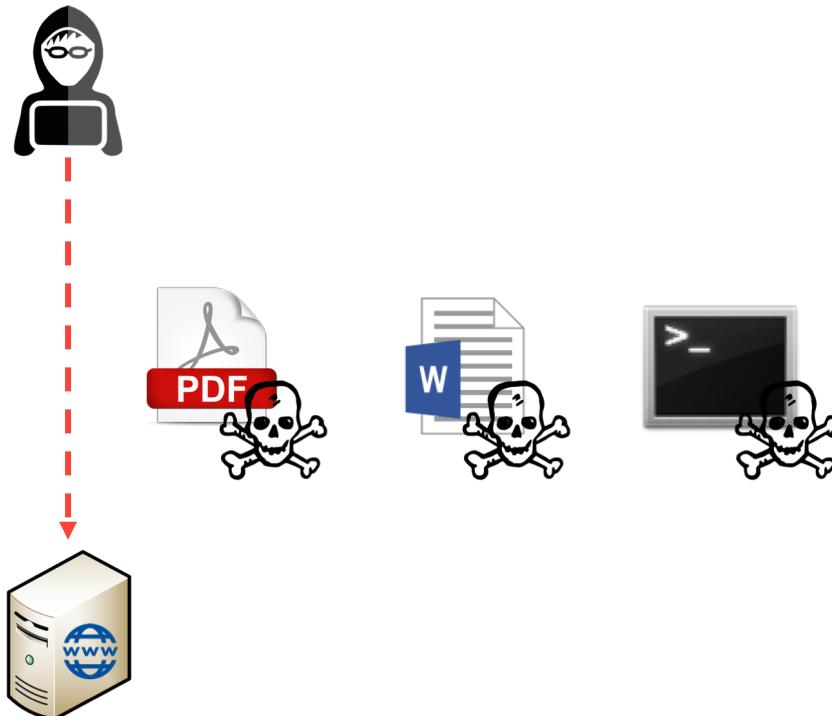
Deux axes importants :

- Côté client
 - Validation locale
 - N'envoie que les données validées
 - Plus agréable pour l'utilisateur
 - **Validation locale**
- Côté serveur
 - Validation des données avant traitement, stockage...
 - Limite les actes malveillants
 - Attention aux filtres utilisés



Injection

Envoi de fichiers non sécurisé : manque de vérifications sur les fichiers uploadés



L'attaquant est en mesure d'envoyer des fichiers malveillants sur le serveur.

Impacts potentiels :

- Modification du contenu du site (défacement, manipulation)
- Exécution de commandes sur le système (prise de contrôle)

Broken Authentication

Toutes les fonctions gérant :

- Authentification
- Sessions

Les différentes attaques :

Authentification :

- Bruteforce
- Password Spraying
- Comptes par défaut

Sessions :

- Vol / réutilisation de cookies
- Abus du processus de réinitialisation du mot de passe
- MFA Absent ou contournable

Comment s'en prémunir :

- Méthodes anti-bruteforce
- Limiter l'usage de comptes génériques
- Sécuriser l'usage des cookies
- Implémentation du MFA

Sensitive Data Exposure

Concerne la mauvaise gestion des données sensibles.

Les impacts potentiels :

- MITM
- Vol de données non chiffrées
- Vol de données faiblement protégées
- Récupération de données techniques

Comment s'en prémunir :

- Chiffrer les données sensibles
- Stocker les données indispensables et rien d'autre
- Hash, salt and pepper
- Utiliser des suites de chiffrements fiables
- Générer et stocker les secrets utilisés pour le chiffrement
- Gérer les retours d'erreur

Broken Access Control

Concerne la vérification des droits avant l'accès à des ressources.

Les impacts potentiels :

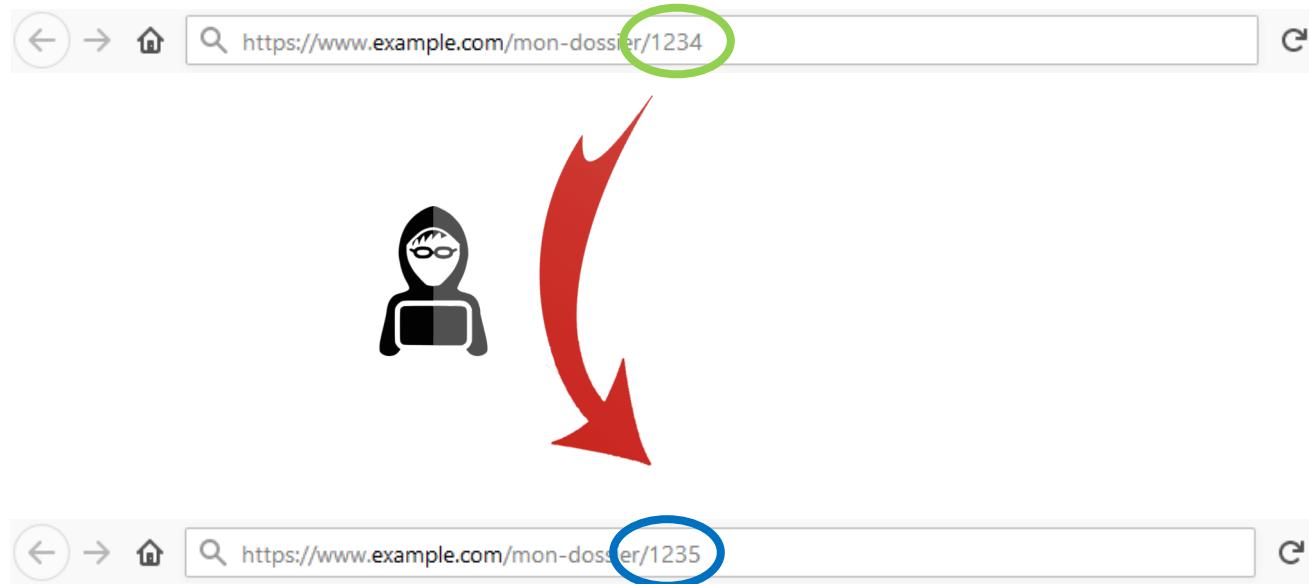
- Accès aux informations d'autres comptes
- Accès à des pages pour des comptes à fort privilège
- Elévation de privilège

Comment s'en prémunir :

- Authentifier les utilisateurs sur l'ensemble des pages
- Limiter l'affichage d'ID dans l'URL ou les requêtes
- Valider les droits côté serveur

Étude d'attaques web courantes

Manque de contrôle d'accès ou IDOR (Insecure Direct Object Reference) : accès illégitime à des données



Impacts potentiels :

- Accès aux données d'un autre utilisateur
- Accès aux fonctionnalités d'administration

L'attaquant accède à des ressources qui ne lui appartiennent pas en modifiant un simple identifiant.

Security Misconfiguration

Il s'agit de défaut de configurations à différents niveaux de l'application.

Les impacts potentiels :

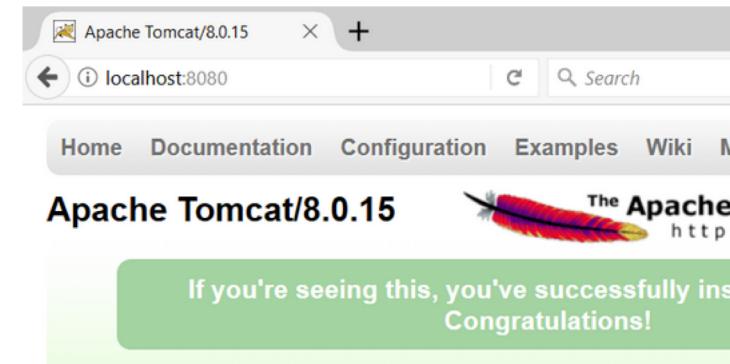
- Exploitation de pages par défaut
- Exploitation de dossiers / fichiers non protégés
- Fuite d'information
- Exposition de services non utilisés

Comment s'en prémunir :

- Processus de durcissement des configurations
- Le minimum d'installations
- Segmentation logique ou physique des applications
- Utilisation des header de sécurité (ex: HSTS, Content-Security-Policy)
- Processus / outils de vérification du durcissement

Security Misconfiguration

Exploitation de pages par défaut :



Exploitation de fichiers ou dossiers non protégés :

Index of /includes/

..		
auth.php	23-Jun-2020 08:18	-
auth.php.swp	22-Jun-2020 13:24	1373

Fuite d'information :

```
Not Found
The requested URL /page.html was not found on this server.
Apache/2.2.3 (Unix) mod_ssl/2.2.3 OpenSSL/0.9.7g DAV/2 PHP/5.1.2 Server at localhost Port 80
```

Security Misconfiguration

Exposition de services d'administration ou plus largement vulnérables

SHODAN

Explore | Pricing | Enterprise Access | New to Shodan? | Login or Register

Exploits | Maps | Images

TOTAL RESULTS
2,413,287

TOP COUNTRIES

Country	Count
China	868,352
United States	466,193
Germany	92,994
Brazil	79,859
Russian Federation	59,699

TOP SERVICES

Service	Count
RDP	2,392,117
RDP (3388)	20,576
SMB	365
Citrix	149
8081	13

TOP ORGANIZATIONS

Organization	Count
Tencent cloud computing	432,987
Amazon.com	127,991
Tencent Cloud Computing (Beijing) Co.	55,179
Beijing Baidu Netcom Science and Technology Co.	42,037
China Telecom jiangsu	33,582

TOP OPERATING SYSTEMS

Operating System	Count
Windows 7 or 8	9,029
Windows XP	2,492
Windows 6.1	182
Linux 3.x	126
Unix	80

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

182.16.53.18
NETSEC
Added on 2019-06-04 08:45:39 GMT
Hong Kong, Cheung Sha Wan

Remote Desktop Protocol
\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00

123.207.56.43
Tencent cloud computing
Added on 2019-06-04 08:45:34 GMT
China, Beijing

SSL Certificate
Issued By:
- Common Name:
Issued To:
- Common Name:
Supported SSL Versions
TLSv1, TLSv1.1, TLSv1.2
Diffie-Hellman Parameters
Fingerprint: RFC2409/Oakley Group 2

103.232.188.89
Shanghai Anchang Network Security Technology Co.,L
Added on 2019-06-04 08:45:41 GMT
China

SSL Certificate
Issued By:
- Common Name: XS1037114461
Issued To:
- Common Name: XS1037114461
Supported SSL Versions
TLSv1, TLSv1.1, TLSv1.2

5.8.88.16
m0g9t5hmpemuhot.morene.host
MoreneHost
Added on 2019-06-04 08:45:27 GMT
Netherlands

SSL Certificate
Issued By:
- Common Name: WIN-344VU98D3RU
Issued To:
- Common Name: WIN-344VU98D3RU
Supported SSL Versions
TLSv1, TLSv1.1, TLSv1.2

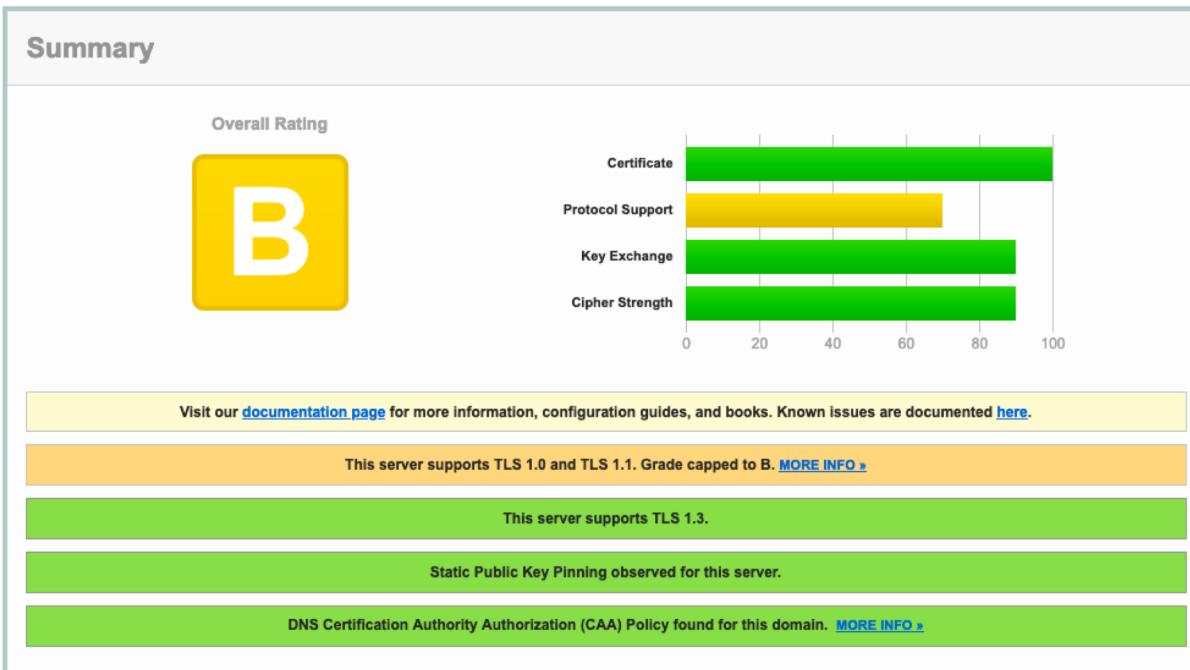
Security Misconfiguration

Outils de vérification du durcissement :

SSL Report: [google.com](#) (216.58.194.206)

Assessed on: Fri, 15 Jan 2021 15:48:08 UTC | HIDDEN | [Clear cache](#)

[Scan Another »](#)



SSLabs de qualys

```
root@kali:~# sslscan 10.7.7.5
Kali Linux  Kali Docs  Kali Tools
Version: 1.11.10-static
OpenSSL 1.0.2-chacha (1.0.2g-dev)

Testing SSL server 10.7.7.5 on port 443 using SNI name 10.7.7.5

  TLS Fallback SCSV:
Server does not support TLS Fallback SCSV

  TLS renegotiation:
Secure session renegotiation supported

  TLS Compression:
Compression enabled (CRIME)

  Heartbleed:
TLS 1.2 not vulnerable to heartbleed
TLS 1.1 not vulnerable to heartbleed
TLS 1.0 not vulnerable to heartbleed

  Supported Server Cipher(s):
Preferred TLSv1.0 256 bits DHE-RSA-AES256-SHA DHE 1024 bits
Accepted  TLSv1.0 256 bits AES256-SHA
Accepted  TLSv1.0 128 bits DHE-RSA-AES128-SHA or network DHE 1024 bits
Accepted  TLSv1.0 128 bits AES128-SHA
Accepted  TLSv1.0 128 bits RC4-SHA
Accepted  TLSv1.0 128 bits RC4-MD5
Accepted  TLSv1.0 112 bits EDH-RSA-DES-CBC3-SHA DHE 1024 bits
Accepted  TLSv1.0 112 bits DES-CBC3-SHA
Preferred SSLv3 256 bits DHE-RSA-AES256-SHA DHE 1024 bits
Accepted  SSLv3 256 bits AES256-SHA
Accepted  SSLv3 128 bits DHE-RSA-AES128-SHA DHE 1024 bits
Accepted  SSLv3 128 bits AES128-SHA
Accepted  SSLv3 128 bits RC4-SHA
Accepted  SSLv3 128 bits RC4-MD5
Accepted  SSLv3 112 bits EDH-RSA-DES-CBC3-SHA DHE 1024 bits
Accepted  SSLv3 112 bits DES-CBC3-SHA
```

ssllscan

Cross-Site Scripting (XSS)

Il s'agit d'un manque de sécurisation des saisies utilisateur permettant de manipuler un autre utilisateur ou les données affichées.

Impacts potentiels :

- Imitation d'une page de login
- Keylogger
- Modification du contenu du site
- Récupération du cookie de connexion

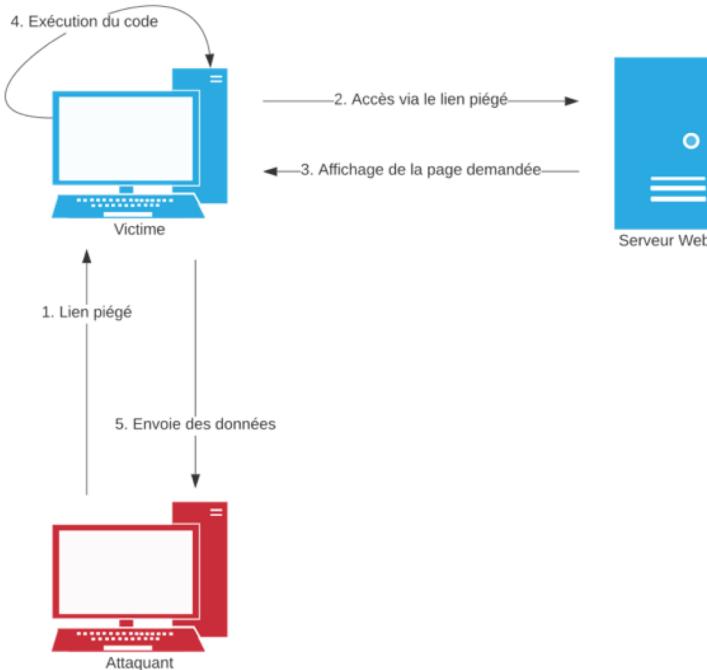
Comment s'en prémunir :

- Utilisation de framework échappant les caractères utilisés dans les XSS
- Mise en place de filtrage des entrées utilisateur
- Utilisation de CSP
- Utilisation du header 'httponly'

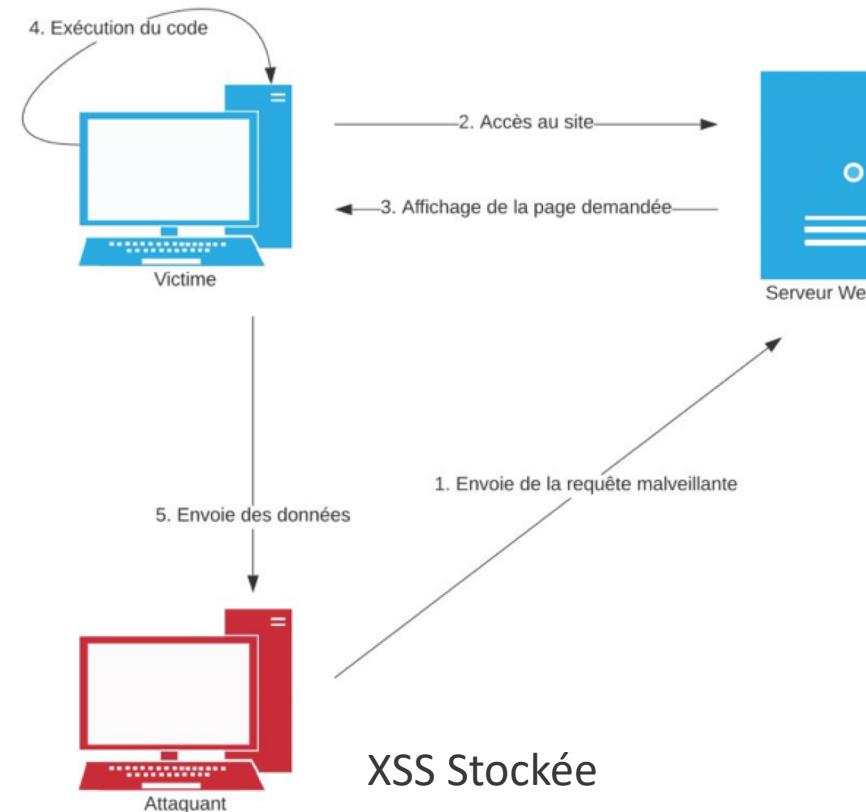
Cross-Site Scripting (XSS)

Les différents types de XSS :

- **XSS Réfléchies**
- **XSS Stockées**
- XSS dans le DOM (Document Object Model)



XSS Réfléchie



Component with known vulnerabilities

Il s'agit d'un défaut de mise à jour des composants de l'application.

Les vecteurs :

- Exploitation documentée
- Code d'exploitation

Comment s'en prémunir :

- Suivre les mises à jour des éditeurs
- Avoir un inventaire des versions des composants
- N'utiliser que le strict minimum
- Ne récupérer les sources que par des canaux sécurisés et surs.

```
root@kali:~# searchsploit -t java windows ↵
-----
Exploit Title

-----
Apple Safari 3.2.3 (Windows x86) - JavaScript 'eval' Remote Denial of Service
Citrix Metaframe for Windows NT 4.0 TSE 1.8 - Java ICA Environment Denial of Service
Microsoft Windows Media Player 7.0 - '.wmz' Arbitrary Java Applet
Microsoft Windows Media Player 7.0 - JavaScript URL
Veritas NetBackup 6.0 (Windows x86) - 'bpjava-msvc' Remote Command Execution
```

Insufficient Logging & Monitoring

Il s'agit d'un défaut de traçabilité et de surveillance des applications.

Les vecteurs :

- Absence de logging
- Absence de surveillance

Comment s'en prémunir :

- Mettre en place de la traçabilité sur les actions à risque
- Horodater, et formater les évènements facilitant l'investigation
- Mise en place de systèmes de détection

Insufficient Logging & Monitoring

Lors de la mise en place de traçabilité :

- Qui ?
- Quand ?
- Où ?
- Comment ?

Points complémentaires :

- Centralisation des évènements
- Création de règles en temps réel

```
[16/Jan/2021:05:51:22 +0000] - - 301 - GET http ██████████ "/" [Client 3.17.190.209] [Length 166] [Gzip -] [Sent-to 172.26.0.2] "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko; compatible; BW/1.1; bit.ly/2W6Px8S) Chrome/84.0.4147.105 Safari/537.36" "-"
[16/Jan/2021:05:51:22 +0000] - 200 200 - GET https ██████████ "/" [Client 3.17.190.209] [Length 844] [Gzip -] [Sent-to 172.26.0.2] "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko; compatible; BW/1.1; bit.ly/2W6Px8S) Chrome/84.0.4147.105 Safari/537.36" "-"
[16/Jan/2021:05:51:22 +0000] - - 301 - GET http ██████████ /robots.txt" [Client 3.17.190.209] [Length 166] [Gzip -] [Sent-to 172.26.0.2] "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko; compatible; BW/1.1; bit.ly/2W6Px8S) Chrome/84.0.4147.105 Safari/537.36" "-"
[16/Jan/2021:05:51:23 +0000] - 200 200 - GET https ██████████ /robots.txt" [Client 3.17.190.209] [Length 844] [Gzip -] [Sent-to 172.26.0.2] "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko; compatible; BW/1.1; bit.ly/2W6Px8S) Chrome/84.0.4147.105 Safari/537.36" "-"
[16/Jan/2021:05:51:23 +0000] - - 400 - - https ██████████ "-" [Client 3.17.190.209] [Length 0] [Gzip -] [Sent-to ] "-" "-"
```

Autres points

Quelques points complémentaires :

- Utiliser des librairies revues et validées, vérifier le reste des codes réutilisés.
- Faire de la veille technique.
- Utiliser des container ne signifie pas qu'on est à l'abri d'attaques.
- Gestion des erreur non verbeuse (ex: mauvais mot de passe même si l'utilisateur n'existe pas).

TP02 – Sécurisation des application



Mise en œuvre et compréhension de la sécurité des applications via WebGoat.

Récupérer et lancer le docker : `docker run -e TZ=Europe/Amsterdam webgoat/goatandwolf`

Attention, lancer ce docker **seulement** sur une machine locale.

Réaliser les modules : A1, A2, A3, A5 et A7

Détection d'attaques

Définition d'un évènement

Un évènement, quel qu'il soit est l'enregistrement d'une action réalisée sur un système d'information.

Un évènements peut venir de différents équipements :

- Application
- Système
- Equipements spécifiques (ex: IOT, systèmes industriels...)

Un évènement peut être utile dans de multiples cas :

- Débug d'outils, de configurations...
- Traçabilité dans un cadre légal ou réglementaire
- Investigation suite à un incident de sécurité
- Corrélation en temps réel

Définition d'un évènement

```
Jan 18 20:56:35 stock sshd[19038]: Failed password for invalid user ftpuser from 71.214.62.135 port 56662 ssh2
Jan 18 20:56:35 stock sshd[19038]: pam_unix(sshd:auth): check pass; user unknown
Jan 18 20:56:38 stock sshd[19038]: Failed password for invalid user ftpuser from 71.214.62.135 port 56662 ssh2
Jan 18 20:56:38 stock sshd[19038]: Received disconnect from 71.214.62.135 port 56662:11: disconnected by user [preauth]
Jan 18 20:56:38 stock sshd[19038]: Disconnected from 71.214.62.135 port 56662 [preauth]
Jan 18 20:56:38 stock sshd[19038]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=71.214.62.135
```

Logs d'authentification sur Linux

An account was successfully logged on.

Subject:	SYSTEM
Security ID:	WIN-GGB2ULGC9G0\$
Account Name:	WORKGROUP
Account Domain:	0x3E7
Logon Information:	
Logon Type:	2
Restricted Admin Mode:	-
Virtual Account:	No
Elevated Token:	Yes
Impersonation Level:	Impersonation
New Logon:	
Security ID:	CONTOSO\Administrator
Account Name:	Administrator
Account Domain:	WIN-GGB2ULGC9G0
Logon ID:	0x8DCDC
Linked Logon ID:	0x0
Network Account Name:	-
Network Account Domain:	-
Logon GUID:	{00000000-0000-0000-0000-000000000000}

Log système sous Windows

assistantd (SiriCore) ERROR

Subsystem: com.apple.siri Category: Database Details 2021-01-18 22:03:55.236622+0100

```
-[SiriCoreSQLiteDatabase openWithError:] success = 0, error = Error Domain=SiriCoreSQLiteDatabaseErrorDomain
Code=2 UserInfo={NSFilePath=<private>, NSUnderlyingError=0x7fad8aae9cf0 {Error
Domain=SiriCoreSQLiteAPIErrorDomain Code=14 UserInfo={NSLocalizedDescription=<private>,
SiriCoreSQLiteAPIErrorExtendedCode=14}}}
```

Log applicatif sous MacOS

Les différentes catégories de logs

Il est possible de catégoriser les logs :

- Log applicatifs
- Logs systèmes
- Logs de sécurité

En fonction des systèmes, un degré de criticité est associé :

- Error
- Warning
- Information

Cette catégorisation permet d'appliquer des filtres pour trouver les informations intéressantes.

Format et traitement des évènements

Un format d'évènement est une structure de données qui permet l'analyse et le parsing.

Il existe un grand nombre de format de logs, les principaux étant :

- Syslog
- JSON
- Windows Event Log

Le fait d'avoir des données structurées permet de les parser et de pouvoir faire des recherches efficaces et en tirer des informations.

Le parsing peut s'apparenter à un découpage des données pour les stocker, les indexer et les rendre accessibles.

Gestion des évènements

Il est possible de gérer les évènements de plusieurs manières :

- Stockage en local des évènements
- Stockage à distance
- Stockage à distance et traitement par une solution de type SIEM

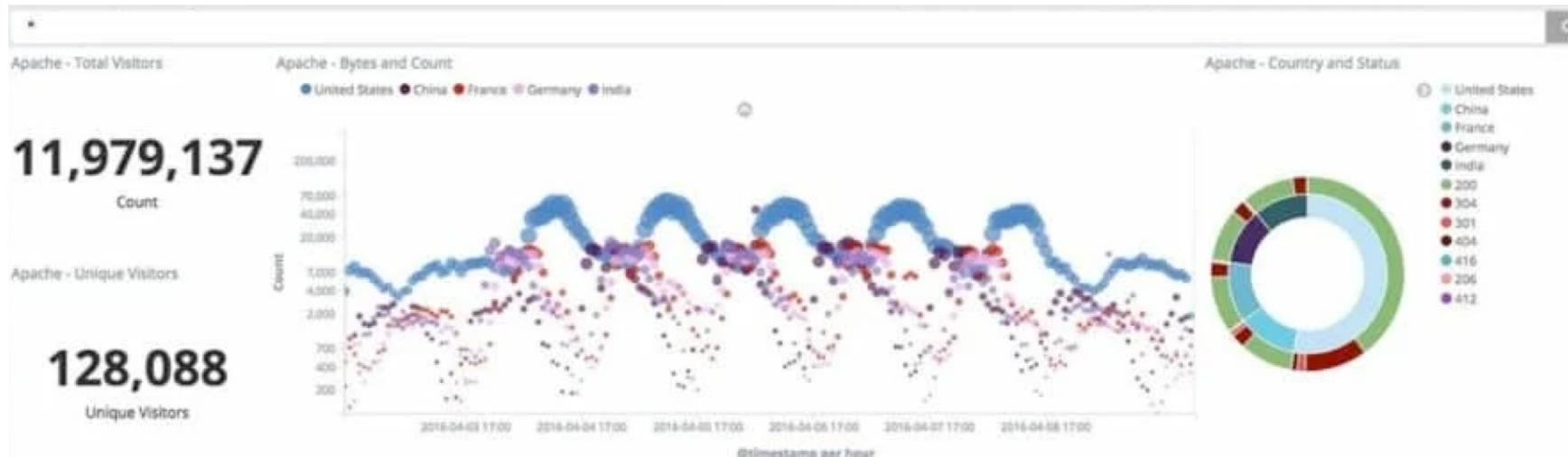
Beaucoup d'outils existent pour manipuler les évènements :

- cat / grep / less / more...
- lnav
- Splunk
- ELK

Gestion des évènements

```
Nov 16 00:04:19 Tim-Stacks-iMac Spotlight[731]: XPC connection was invalidated
Nov 16 00:04:19 Tim-Stacks-iMac SpotlightNetHelper[734]: [SLSUGGESTIONS] PRSSearchSession received an HTTP error
Nov 16 00:04:28 Tim-Stacks-iMac Quicksilver[1190]: Remote hosts could not be loaded from ~/hosts: The file does
Nov 16 00:04:57 Tim-Stacks-iMac com.apple.SecurityServer[89]: Killing auth hosts
Nov 16 00:04:57 Tim-Stacks-iMac com.apple.SecurityServer[89]: Session 100589 destroyed
Nov 16 00:05:08 Tim-Stacks-iMac com.apple.SecurityServer[89]: Killing auth hosts
Nov 16 00:05:08 Tim-Stacks-iMac com.apple.SecurityServer[89]: Session 100590 destroyed
Nov 16 00:07:29 Tim-Stacks-iMac CalendarAgent[392]: [com.apple.calendar.store.log.caldav.core dav] [Refusing to p
Nov 16 00:07:59 --- last message repeated 1 time ---
Nov 16 00:09:12 Tim-Stacks-iMac WindowServer[237]: _CGXRemoveWindowFromWindowMovementGroup: window 0x174 is not
192.0.2.33 - - [16/Nov/2015:08:01:43 +0000] "PUT /index.html HTTP/1.0" 200 571424 "-" "-"
192.0.2.55 - - [16/Nov/2015:08:01:43 +0000] "GET /index.html HTTP/1.0" 200 101575 "http://lnav.org/download.html
Nov 16 08:01:44 frontend3 server[121]: Successfully started helper
Nov 16 08:01:44 frontend3 server[121]: Handling request fb475cec-6812-437f-b9f4-7d7ce71f801f
Nov 16 08:01:44 frontend3 server[123]: Handling request fb475cec-6812-437f-b9f4-7d7ce71f801f
```

LNAV



Kibana

Création d'alerte

Une fois l'ensemble des évènements récupérés, il est possible de créer des alertes selon des critères définis.

Dans le cadre d'une application web, créer une alerte si les conditions suivantes sont réunies :

- 10 tentatives de connexions échouées sur 2 minutes sur un compte
- 10 tentatives de connexion échouées sur 2 minutes sur plusieurs comptes depuis une même IP
- Connexion depuis une IP en dehors de France
- Connexion à des heures non ouvrées
- ...

Surveillance réseau

Les alertes basées sur les évènements d'une application ou d'un système sont intéressantes, mais elles ne représentent qu'une vue partielle des données échangées.

```
[17/Jan/2021:14:40:26 +0000] - 200 200 - POST https npm.poneyquitousse.fun "/api/tokens" [Client 127.0.0.1:137] [Length 583] [Gzip -] [Sent-to 172.25.0.2] "Mozilla/5.0 (Macintosh  
; Intel Mac OS X 10.16; rv:84.0) Gecko/20100101 Firefox/84.0" "https://npm.poneyquitousse.fun/login"
```

Il manque les informations importantes contenues dans le POST.

Certains équipements ou solutions permettent d'inspecter le traffic réseau pour récupérer ces informations.

Il faut le voir comme une source complémentaire d'information permettant de détecter des attaques plus évoluées et impossibles à voir avec des évènements applicatif standard.

Surveillance réseau

Cette détection peut être mise en place via une sonde au niveau du réseau, ou directement sur les hôtes avec des logiciels spécifiques.

```
[**] [1:36636:3] EXPLOIT-KIT Angler exploit kit index uri request attempt [**]
[Classification: Attempted User Privilege Gain] [Priority: 1]
02/05-21:28:29.166073 10.41.245.114:49278 -> 86.106.93.167:80
TCP TTL:128 TOS:0x0 ID:4292 IpLen:20 DgmLen:457 DF
***AP*** Seq: 0x34E6A38B Ack: 0xF40F5004 Win: 0x100 TcpLen: 20
```

Il existe deux modèles principaux pour ce type de détection :

- Via signature
 - Utilisation de REGEX avec des signaux spécifiques
- Via détection d'écart de comportements
 - Utilisation de Machine Learning ou Intelligence Artificielle

Surveillance réseau

Qu'est-ce qu'un NIDS ?

Network Intrusion Detection System

Est un équipement réseau passif permettant de détecter des attaques via l'analyse de trames réseaux.

Qu'est-ce qu'un NIPS ?

Network Intrusion Prevention System

Est un équipement réseau actif permettant de bloquer des attaques via l'analyse de trames réseaux.

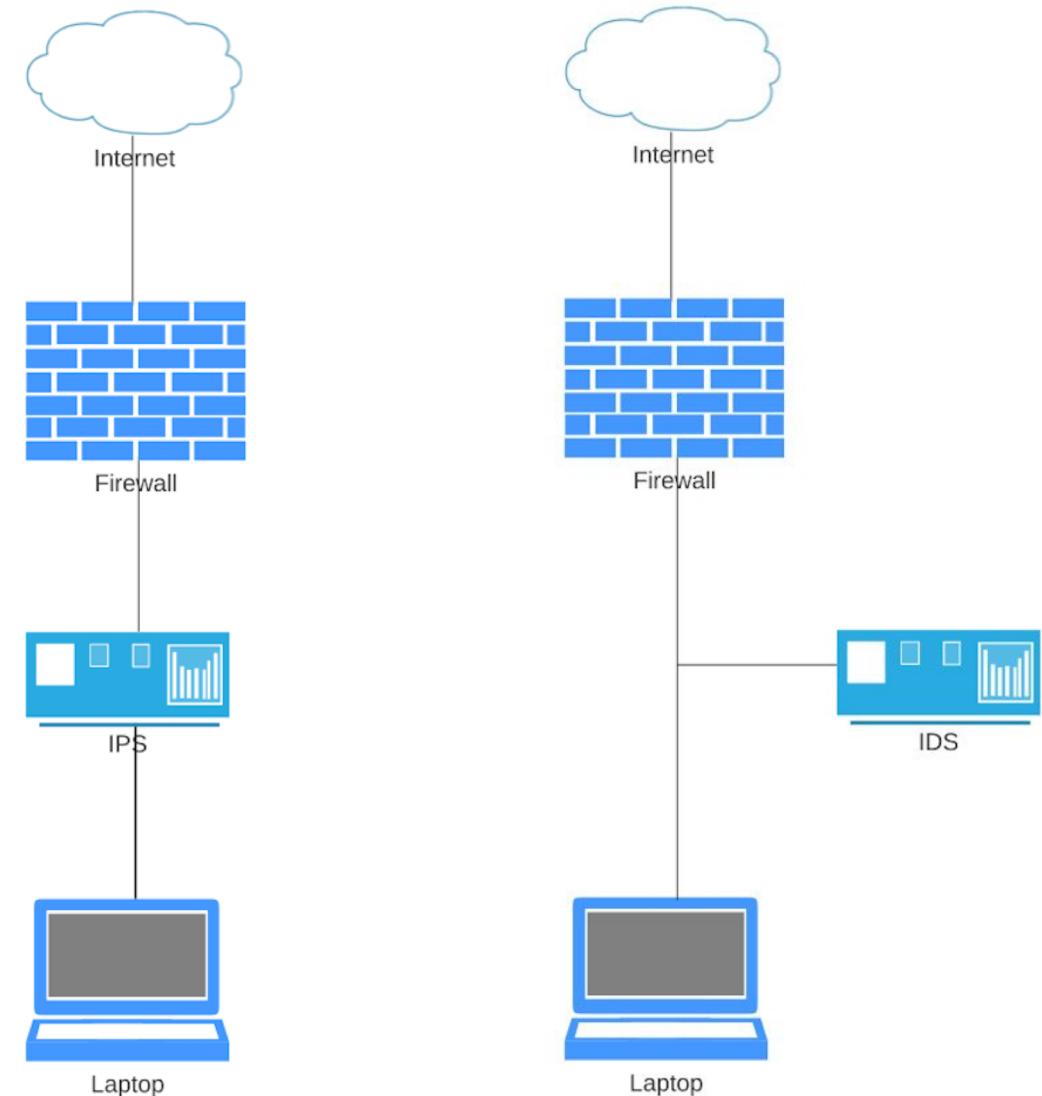
Surveillance réseau

Comment ces équipements sont positionnés ?

L'IPS est positionné en coupure, il bloque et alerte sur les échanges considérés comme malveillants.

L'IDS est positionné en série, il constate et alerte sur les échanges considérés comme malveillants.

Il existe aussi les HIPS et HIDS, ils s'agit du même concept mais installé directement sur le serveur.



En résumé

- Il n'existe pas de solution miracle et omnisciente.
- Une bonne base de sécurisation et de suivi de mise à jour sera toujours plus intéressant que de la détection.
- Un bon logging, et la gestion de l'archivage permet d'offrir des capacités de réponse sur incident.
- La détection en temps réel est importante dans les grandes entreprises, ou SI complexes.
- Lors de la mise en place ou du développement d'une application, il faut toujours se poser ces questions :
 - Qui ?
 - Quand ?
 - Quoi ?
 - Où ?
 - Comment je vais mettre à disposition ces informations.

Attaques sur infrastructure

Hacking Ethique

Le **hacking** est initialement la bidouille et l'**expérimentation**, dont les motivations sont la passion, le jeu, le plaisir, l'échange et le partage. Il s'apparente en partie au **piratage informatique**. Dans ce cas, c'est une pratique visant à un échange « discret » d'**informations** illégales ou confidentielles. Cette pratique, établie par les **hackers**, apparaît avec les premiers **ordinateurs domestiques**. Le **hacking** est ainsi, plus généralement, un ensemble de techniques permettant d'exploiter les possibilités, failles et vulnérabilités d'un élément ou d'un groupe d'éléments matériels ou humains.

[wikipedia.com](https://fr.wikipedia.org/wiki/Hacking)

Il existe 3 types de hackers :

- **WhiteHat**, ce sont des hackers éthique. Ils suivent un cadre légal et préviennent les éditeurs lors de la découvertes de failles dans leurs solutions.
- **GreyHat**, ce sont des hackers qui peuvent suivre ou non une éthique. Ils se situent entre les WhiteHat et les BlackHat.
- **BlackHat**, ce sont des hackers qui ne suivent aucune éthique et sont mal intentionnés.

Hacking Ethique

Pratique du hacking lorsqu'elle n'est pas malveillante et encadrée.

Les moyens techniques utilisés sont identiques.

Les différents cadres légaux étant :

- **Bug bounty**, autorisation sur un périmètre restreint à des chercheurs en cyber sécurité.
- **Test d'intrusion**, encadrement contractuel avec une entreprise ou un individu.
- **Divulgation responsable**, lors de la découverte d'une faille, un lapse de temps est entendu entre l'entreprise et le chercheur avant divulgation complète.

L'aspect juridique de la sécurité



Il est **interdit de s'introduire et/ou de se maintenir frauduleusement** dans un système d'information.



Atteintes aux systèmes de traitement automatisé de données
(Articles 323-1 à 323-8 du Code Pénal)

La volonté « bienveillante » de rapporter des failles sans vouloir porter atteinte n'exonère pas d'une condamnation.



« Affaire Bluetouff » : Olivier Laurelli, a.k.a. Bluetouff, accède en 2012 à des fichiers sensibles et insuffisamment protégés d'une agence gouvernementale via une simple recherche Google (« *google dorks* »). Il récupère des fichiers sensibles, environ 8 Go, puis parcourt l'arborescence du site. Il est condamné en 2014 à 3000€ d'amende, et son pourvoi en cassation est rejeté en 2015.

☞ <https://www.nextinpath.com/article/18067/95165-affaire-bluetouff-cour-cassation-consacre-vol-fichiers-informatiques>

Pentest et Redteam

Pentest

Méthodologie permettant de mettre à l'épreuve d'un hacker éthique une application ou un périmètre restreint.

En règle général, une entreprise fait appel aux services d'une autre entreprise spécialisée en sécurité informatique pour réaliser cette prestation.

Les principaux avantages :

- Permet de tester la robustesse d'une application.
- Donne un avis externe sur l'implémentation de la solution.
- Permet de répondre à des critères réglementaires, légaux.
- Prestation abordable pour une grande partie des entreprises

Les principaux désavantages :

- Mission souvent courte (1 à 2 semaines)
- Périmètre très restreint qui ne permet pas d'avoir une approche globale du risque à l'échelle de l'entreprise.

Pentest et Redteam

Redteam

Méthodologie permettant de mobiliser une équipe sur une durée moyenne à longue sur le périmètre entier de l'entreprise.

Le but principal sera de compromettre l'entreprise, ou d'accéder à des secrets en utilisant tous les moyens à disposition. De l'attaque informatique, au social engineering en passant par l'intrusion physique.

Les principaux avantages :

- Permet d'avoir une approche globale du risque sur l'entreprise.
- Permet d'avoir une vue précise des possibilités d'un groupe d'attaquant sur l'entreprise.
- Permet aux attaquants de passer plus de temps pour élaborer des techniques plus évoluées.

Les principaux désavantages :

- Prestation qui va coûter plus d'argent et de temps.
- N'a pas une démarche exhaustive sur les vulnérabilités existantes sur le SI.

Méthodologie pour les tests d'intrusion

Il existe 3 formes de pentest :

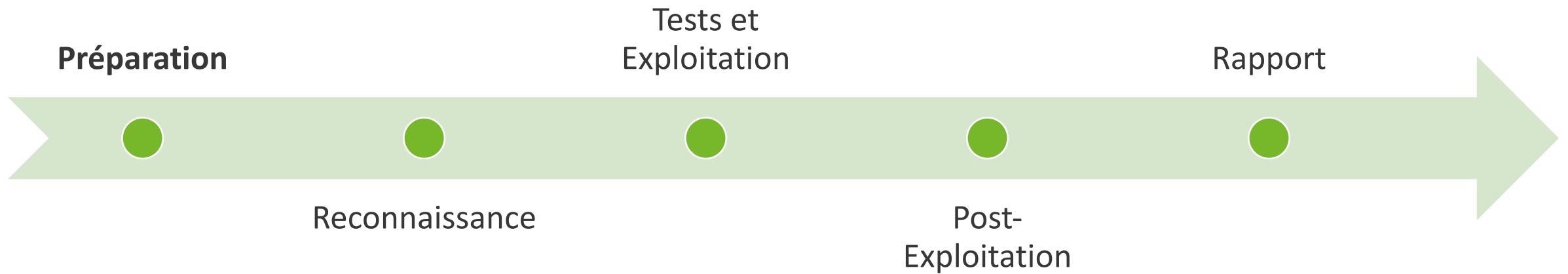
- **BlackBox**, l'attaquant n'a aucune information sur la cible en dehors de l'application à viser.
- **GreyBox**, l'attaquant à quelques informations ainsi qu'un compte, souvent utilisateur.
- **WhiteBox**, l'attaquant a toute la documentation ainsi qu'une grande partie des droits sur la solution.

Ces 3 formes permettent d'accomplir différents objectifs :

- **BlackBox**, permet de se mettre dans le cas d'une menace externe avec aucune informations spécifique. (Un attaquant externe)
- **GreyBox**, permet de se mettre dans le cas d'une menace interne avec des informations et possiblement un compte à faible privilèges. (Un utilisateur malveillant)
- **WhiteBox**, permet de se mettre dans le cas d'une menace interne avec de fort privilèges. (Un administrateur malveillant)

Ces 3 formes sont souvent réalisées au cours d'un même pentest, ce qui permet d'offrir une vue précise sur les risques encourus par la solution.

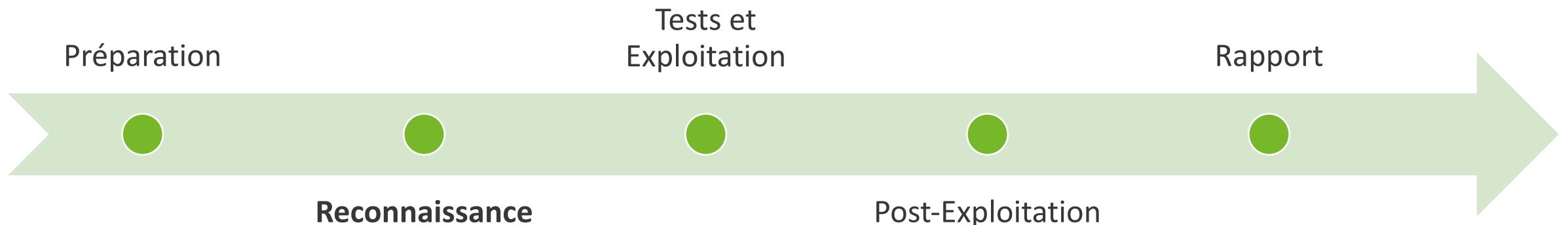
Méthodologie pour les tests d'intrusion



La préparation consiste à :

- Définir le périmètre de l'attaque.
- Définir le type de pentest.
- Définir le type de rendu.
- Définir le contrat avec l'entreprise.

Méthodologie pour les tests d'intrusion

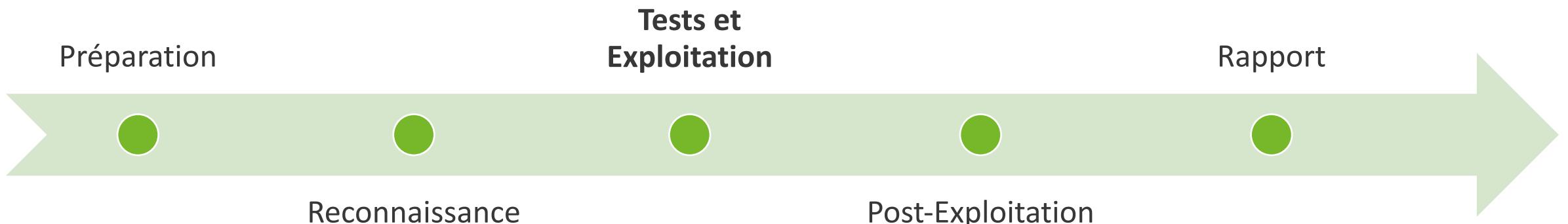


La reconnaissance consiste à récupérer un maximum d'informations sur la cible, qu'elles soient techniques ou organisationnelles.

Deux types de reconnaissances existent :

- **Passive**, le but est de ne laisser aucune trace visible pour la cible. Cela peut passer par des Google Dorks, la visite des sites de l'entreprise, la récupération de données techniques sur les versions utilisées, les noms de domaines, les données qui ont pu fuiter...
- **Active**, le but est de récupérer des informations sur des cibles intéressantes avec des outils qui peuvent laisser des traces. Cela peut passer par la réalisation de scan réseau, l'énumération de dossier sur un site...

Méthodologie pour les tests d'intrusion



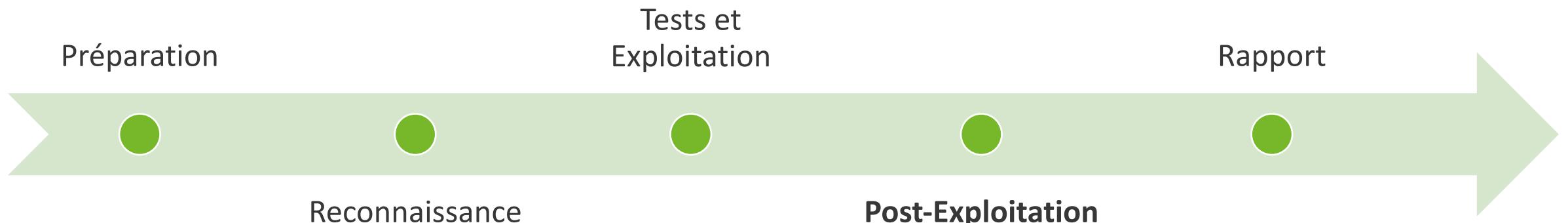
La phase de tests et d'exploitation correspond aux premières tentatives automatisées ou manuelles pour trouver le vecteur d'entrée, la faille à exploiter.

On va retrouver ici l'ensemble des techniques, outils et connaissances mobilisables pour trouver le premier vecteur de compromission.

En fonction de type de cible, les outils et les connaissances peuvent fortement varier.

Il est important durant cette phase de collecter l'ensemble des preuves lors de l'exploitation de vulnérabilité. Ces preuves seront utilisées lors de la rédaction du rapport.

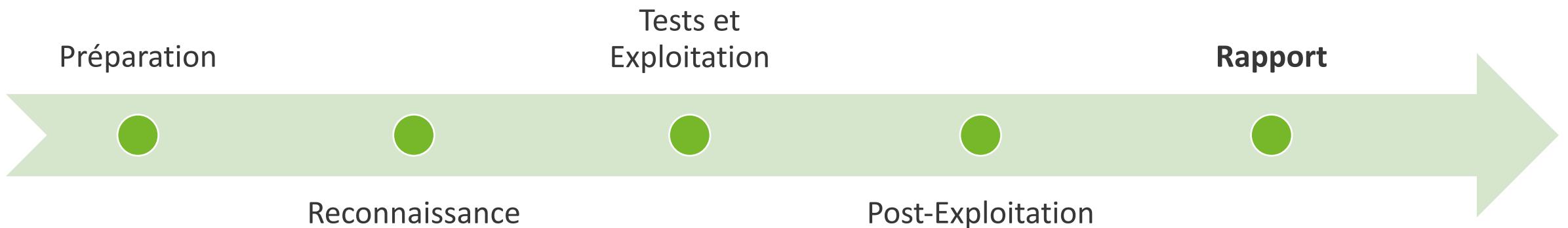
Méthodologie pour les tests d'intrusion



La phase de post-exploitation correspond à :

- L'élévation de privilèges.
- La récupération d'informations supplémentaires (base de données, informations sensibles...).
- Exfiltration des données.
- La latéralisation et la compromission d'autres systèmes.
- La mise en place de mécanismes de persistance.
- Suppression des traces de l'attaque.

Méthodologie pour les tests d'intrusion



Le rapport est le document traçant l'ensemble des actes réalisés, les systèmes compromis ainsi que les pistes permettant de corriger les failles.

Il est généralement composé de deux parties :

- Le résumé compréhensible (peu technique). Permettant aux personnes non techniques de comprendre rapidement et simplement la portée de l'attaque.
- Le détail technique comprenant : les failles, leurs criticités, les preuves... Permettant aux personnes administrant la solution de comprendre comment corriger les failles.

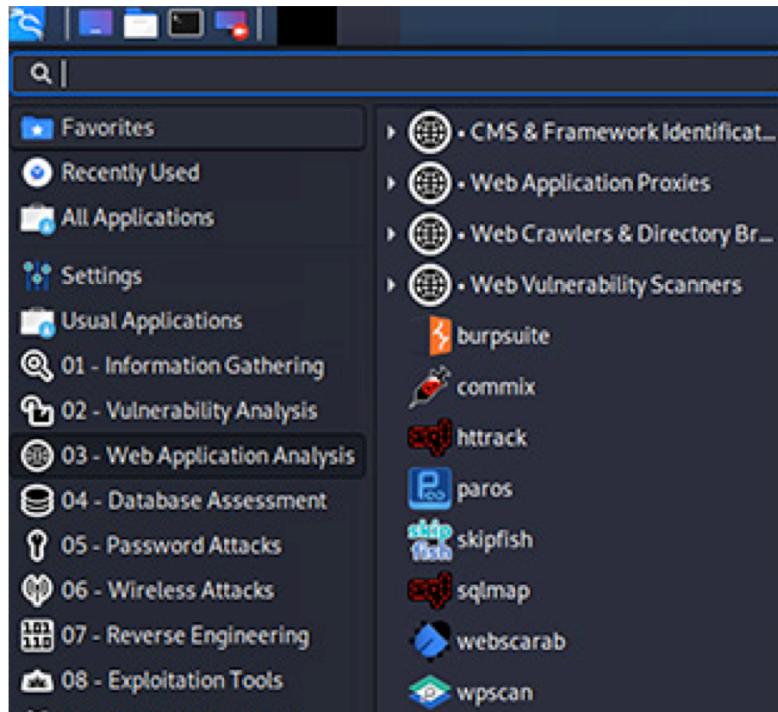
Les outils pour les tests d'intrusion

Il existe un nombre important d'outils permettant de faire de la reconnaissance, de l'exploitation, de la mise en place de persistance...

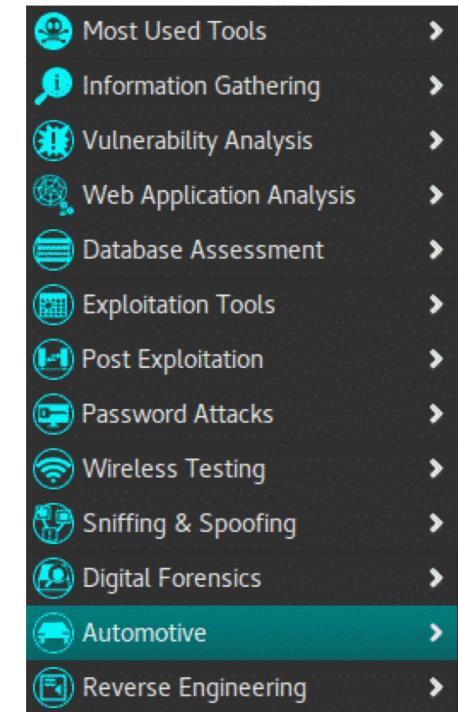
Deux systèmes d'exploitations regroupent un nombre important de ces outils



Kali Linux



Parrot OS



Les outils pour les tests d'intrusion

Reconnaissance Active

Nmap, permet de faire du scan de port sur un ou plusieurs hôtes.



Il est possible de connaître les ports ouverts sur une machine, et donc de trouver des services sans avoir une connaissance préalable de la cible.

Exemple : nmap **-sS** **-sV** **-O** 127.0.0.1

Scan SYN

Scan avec détection de version pour les services découverts

Détection de version de l'OS

```
Starting Nmap 4.20 ( http://insecure.org ) at 2007-01-26 00:18 CET
Interesting ports on 192.168.1.65:
Not shown: 1692 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
1234/tcp  open  hotline
6112/tcp  open  dtspc

Nmap finished: 1 IP address (1 host up) scanned in
5.622 seconds
root@siteduzero:~#
```

Les outils pour les tests d'intrusion

Reconnaissance Active

SSLScan, Permet de vérifier les configurations SSL/TLS d'un site.

Majoritairement utilisé pour des failles permettant de compromettre la confidentialité des données.

Exemple : sslscan monserveur.fr

```
OpenSSL 1.0.2k-dev xx XXX xxxx
Testing SSL server https://monserveur.fr on port 443

  TLS Fallback SCSV:
Server supports TLS Fallback SCSV

  TLS renegotiation:
Session renegotiation not supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLS 1.2 not vulnerable to heartbleed
TLS 1.1 not vulnerable to heartbleed
TLS 1.0 not vulnerable to heartbleed

  Supported Server Cipher(s):
Preferred TLSv1.2 256 bits ECDHE-RSA-AES256-SHA384      Curve P-256 DHE 256
Accepted   TLSv1.2 128 bits ECDHE-RSA-AES128-SHA256       Curve P-256 DHE 256
Accepted   TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384    Curve P-256 DHE 256
```

Les outils pour les tests d'intrusion

Reconnaissance Active

WhatWeb, permet de connaitre les technologies utilisées sur un site web.

Principalement utilisé dans les phases de Reconnaissance initiales.

Exemple : whatweb monserveur.fr

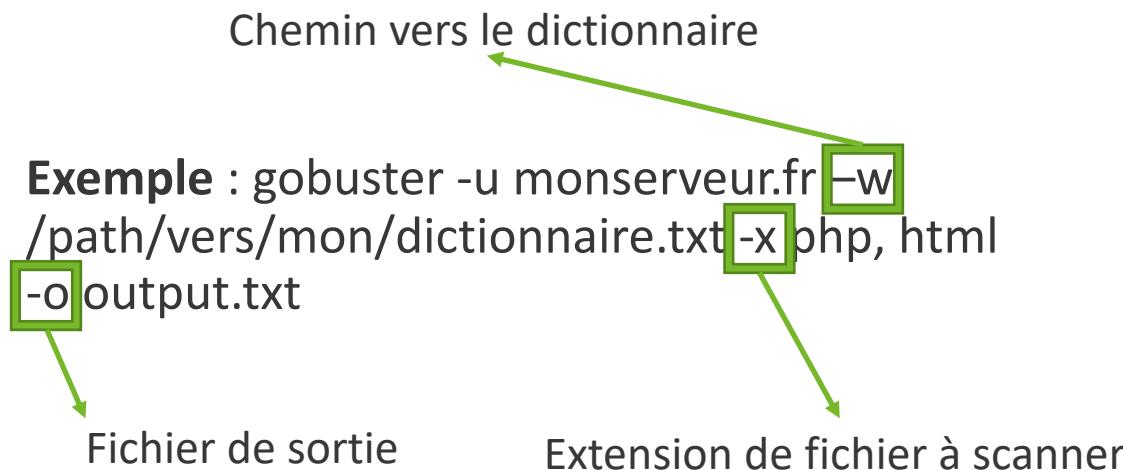
```
root@kali:~# whatweb www.facebook.com
/usr/lib/ruby/1.9.1/rubygems/custom_require.rb:36:in `require': iconv will be deprecated in the future, use String#encode instead.
http://www.facebook.com [302] Country[IRELAND][IE], IP[31.13.79.246]
, RedirectLocation[https://www.facebook.com/], UncommonHeaders[x-fb-debug]
https://www.facebook.com/ [200] Country[IRELAND][IE], HTML5, IP[31.13.79.246], Meta-Refresh-Redirect[/?_fb_noscript=1], PasswordField[pass,reg_passwd__], Script, UncommonHeaders[strict-transport-security,x-frame-options,x-xss-protection,x-content-type-options,x-fb-debug], X-Frame-Options[DENY], X-XSS-Protection[0]
https://www.facebook.com/?_fb_noscript=1 [200] Cookies[noscript], Country[IRELAND][IE], HTML5, IP[31.13.79.246], PasswordField[pass,reg_passwd__], Script, UncommonHeaders[strict-transport-security,x-frame-options,x-xss-protection,x-content-type-options,x-fb-debug], X-FRAME-Options[DENY], X-XSS-Protection[0]
```

Les outils pour les tests d'intrusion

Reconnaissance Active

Gobuster, permet d'effectuer de l'énumération de domaine, d'URI (fichiers et dossiers).

Permet principalement dans les phases de reconnaissances actives de trouver des fichiers et dossiers sur un serveur Web en se basant sur une liste locale.

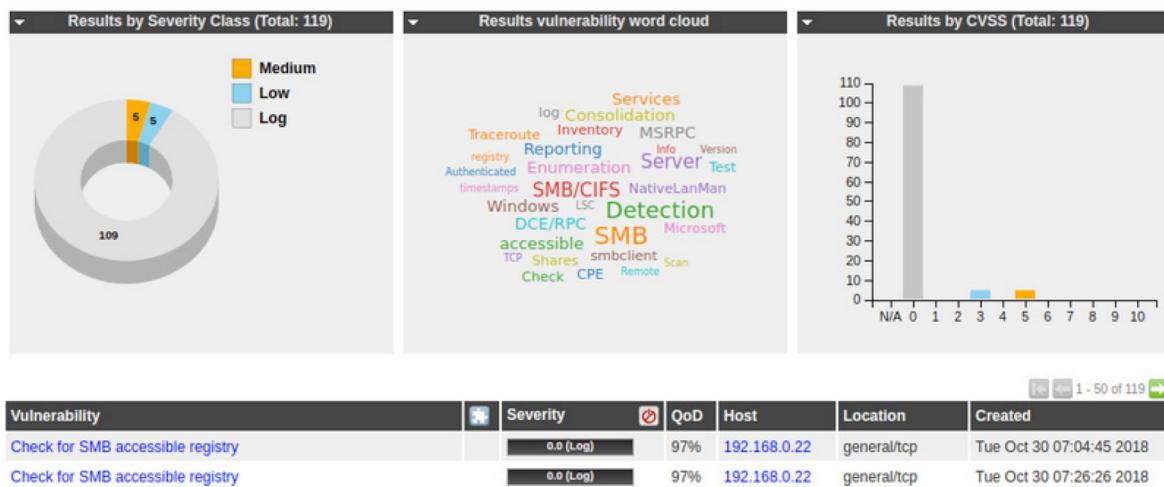


```
root@kali:~/gocode/bin# ./gobuster -u google.com -w /usr/share/wordlists/dnsmap.txt  
Gobuster v1.4.1          OJ Reeves (@TheColonial)  
=====  
[+] Mode      : dir  
[+] Url/Domain : http://google.com/  
[+] Threads   : 10  
[+] Wordlist  : /usr/share/wordlists/dnsmap.txt  
[+] Status codes: 204,301,302,307,200  
=====  
/ads (Status: 301)  
/adx (Status: 200)
```

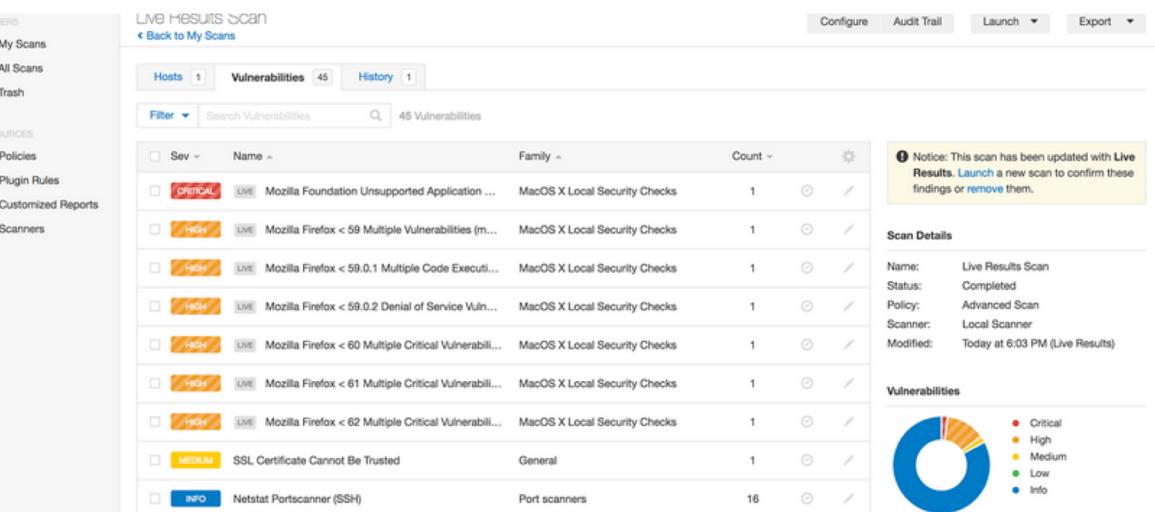
Les outils pour les tests d'intrusion

Reconnaissance Active

Nessus / OpenVAS, bien que très verbeux et facilement detectable, il est parfois intéressant d'utiliser ce type de solution pour avoir une vision sur un périmètre vaste.



OpenVAS



Nessus

Les outils pour les tests d'intrusion

Reconnaissance Active - Exploitation

ExploitDB, est un site regroupant un grand nombre de description d'exploitation et de code d'exploitation.

Date	D	A	V	Title	Type	Platform
2021-01-22	↓		×	Atlassian Confluence Widget Connector Macro - SSTI	WebApps	Multiple
2021-01-22	↓		×	ERPNext 12.14.0 - SQL Injection (Authenticated)	WebApps	Multiple
2021-01-22	↓		×	CASAP Automated Enrollment System 1.0 - Authentication Bypass	WebApps	PHP
2021-01-22	↓		×	Library System 1.0 - Authentication Bypass Via SQL Injection	WebApps	PHP
2021-01-22	↓		×	Oracle WebLogic Server 14.1.1.0 - RCE (Authenticated)	WebApps	Java

Searchsploit, est un outil en ligne de commande permettant de rechercher dans ExploitDB et de récupérer les différents codes d'exploitation.

```
kali㉿kali:~$ searchsploit wordpress mail list
[+] Exploit Title | Path
[+] WordPress Plugin Mailing List - Arbitrary File Download | php/webapps/18276.txt
[+] WordPress Plugin Mailing List 1.3.2 - Remote File Inclusion | php/webapps/17866.txt
[+] WordPress Plugin WP-phpList 2.10.2 - 'unsubscribe@mail' Cross-Site Scripting | php/webapps/33365.txt
```

Les outils pour les tests d'intrusion

Reconnaissance Active - Exploitation

BurpSuite, est un outil permettant d'inspecter et de modifier les requêtes réalisées entre un client et un serveur.

The screenshot shows the BurpSuite interface with the following components:

- Left Panel:** Shows a list of captured HTTP requests. The 6th request, which is highlighted in orange, is from "https://cloud.poneyquitousse.fun" and has a status of "GET /".
- Request pane:** Displays the details of the selected request. It includes fields for Host, Method, URL, and Params. The URL is "/".
- Response pane:** Displays the response received from the server. The status line shows "HTTP/1.1 502 Bad Gateway". The response body contains HTML code indicating a 502 Bad Gateway error, with the text "502 Bad Gateway" repeated multiple times.

#	Host	Method	URL	Params
1	https://www.google.com	GET	/complete/search?client=firefox&q=co	✓
2	https://www.google.com	GET	/complete/search?client=firefox&q=co	✓
3	https://www.google.com	GET	/complete/search?client=firefox&q=cl	✓
4	https://www.google.com	GET	/complete/search?client=firefox&q=clo	✓
5	https://www.google.com	GET	/complete/search?client=firefox&q=cl...	✓
6	https://cloud.poneyquitousse.fun	GET	/	
7	https://cloud.poneyquitousse.fun	GET	/favicon.ico	

Les outils pour les tests d'intrusion

Exploitation

Patator, est un outil permettant de réaliser du bruteforce sur plusieurs types de services, allant d'HTTP à SSH en passant par FTP.

Exemple : patator **ssh_login** host=127.0.0.1 user=admin password=FILE0 0=/path/vers/dictionnaire.txt

Le type de service visé

Définition de la variable pour PASSWORD

Définition de la variable FILE0

```
patator http_fuzz url="http://127.0.0.1/mywiki/index.php?id=start&do=login" method=POST  
body='do=login&u=FILE0&p=FILE1' 0=user.txt 1=password.txt
```

```
root@kali:~/patator# ./patator.py ssh_login host=192.168.157.131 user=root password=FILE0 0=/root/newpass.txt  
10:10:45 patator INFO - Starting Patator v0.7 (https://github.com/lanjelot/patator) at 2017-12-19 10:10 EST  
10:10:45 patator INFO -  
10:10:45 patator INFO - code size time | candidate | num | msg  
10:10:45 patator INFO - 1 22 0.034 | | 9 | Authentication failed.  
10:10:45 patator INFO - 0 31 0.068 | root | 8 | SSH-2.0-OpenSSH_7.5p1 Debian-10  
10:10:47 patator INFO - 1 22 1.943 | 12345678 | 1 | Authentication failed.  
10:10:47 patator INFO - 1 22 1.942 | 1234567 | 2 | Authentication failed.  
10:10:47 patator INFO - 1 22 1.945 | 11111111 | 3 | Authentication failed.  
10:10:47 patator INFO - 1 22 1.943 | 111111111 | 4 | Authentication failed.  
10:10:47 patator INFO - 1 22 1.941 | 22222222 | 5 | Authentication failed.  
10:10:47 patator INFO - 1 22 1.975 | 44444444 | 6 | Authentication failed.  
10:10:47 patator INFO - 1 22 1.942 | 55555555 | 7 | Authentication failed.  
10:10:47 patator INFO - 1 22 1.942 | toor | 10 | Authentication failed.  
10:10:47 patator INFO - Hits/Done/Skip/Fail/Size: 10/10/0/0/10, Avg: 3 r/s, Time: 0h 0m 2s
```

Les outils pour les tests d'intrusion

Exploitation

Metasploit, est un framework d'exploitation permettant de simplifier grandement les attaques. Son but est d'être le plus accessible possible pour que chaque personne puisse mener ses propres tests d'intrusion, et d'améliorer sa sécurité.

```
# cowsay++  
< metasploit >  
-----  
 \  'oo'  
  (____)\\ *  
 ||--||  
  
Love leveraging credentials? Check out bruteforcing  
in Metasploit Pro -- learn more on http://rapid7.com/metasploit  
=[ metasploit v4.14.0-dev ]  
+ --=[ 1627 exploits - 927 auxiliary - 282 post ]  
+ --=[ 472 payloads - 39 encoders - 9 nops ]  
+ --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

Basic options:				
Name	Current Setting	Required	Description	
SRVHOST	0.0.0.0	yes	The local host to listen on. This must be an address on the local machine or 0.0.0.0	
SRVPORT	8080	yes	The local port to listen on.	
SSL	false	no	Negotiate SSL for incoming connections	
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)	
URIPATH		no	The URI to use for this exploit (default is random)	

Les outils pour les tests d'intrusion

Exploitation

Nikto, est un scanner de vulnérabilité pour les sites web. Il est très accessible d'utilisation mais est très bruyant, donc facilement détectable.

Exemple : nikto -host 127.0.0.1

```
root@kali:~# nikto -host 192.168.80.129 -output /root/Desktop/results -Format HTM
- Nikto v2.1.6
-----
+ Target IP:          192.168.80.129
+ Target Hostname:    192.168.80.129
+ Target Port:        80
+ Start Time:         2016-12-23 10:38:32 (GMT -5)
-----
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to
protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to rend
er the content of the site in a different fashion to the MIME type
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.6
5 (final release) and 2.2.29 are also current.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily b
route force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The followi
ng alternatives for 'index' were found: index.php
```

Les outils pour les tests d'intrusion

Exploitation - Post Exploitation

Hashcat, permet notamment de bruteforcer des hash pour trouver des mots de passes. Un autre outil est utile en complément, **hash-identifier** qui permet d'identifier quel type de hash est utilisé.

```
hashcat (v6.0.0) starting...
CUDA API (CUDA 10.2)
=====
* Device #1: GeForce GTX 1080, 7982/8112 MB, 20MCU

Minimum password length supported by kernel: 4
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Applicable optimizers:
* Single-Hash
* Single-Salt
* Brute-Force
* Slow-Hash-SIMD-LOOP

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1725 MB

$bitlocker$1$16$30383234343937323731353330333732$10...09e60e:20200615

Session.....: hashcat (Brain Session/Attack:0xdd79fcf8/0xc2bc45aa)
Status.....: Cracked
```

```
HASH: 52e88f267c3eb581024320e377aa1933
Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))
Least Possible Hashs:
[+] RAdmin v2.x
|480 x 325|
```



Les outils pour les tests d'intrusion

Post Exploitation

LinPEAS et WinPEAS, sont des scripts qui permettent de trouver facilement des axes de post exploitation sur les systèmes déjà compromis.

Ils sont à utiliser avec précaution car verbeux et demandeur en ressources.

```
[+] Me
[!] https://book.hacktricks.xyz/linux-unix/privilege-escalation#groups
uid=1000(user) gid=1000(user) groups=1000(user),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev)

[+] Testing 'sudo -l' without password & /etc/sudoers
[!] https://book.hacktricks.xyz/linux-unix/privilege-escalation#commands-with-sudo-and-suid-commands
Matching Defaults entries for user on this host:
    env_reset, env_keep+=LD_PRELOAD

User user may run the following commands on this host:
    (root) NOPASSWD: /usr/sbin/iftop
```

Les outils pour les tests d'intrusion

Post Exploitation

Il existe un nombre important de vérifications à réaliser une fois qu'on a réussi à compromettre une machine.

Quelques pistes :

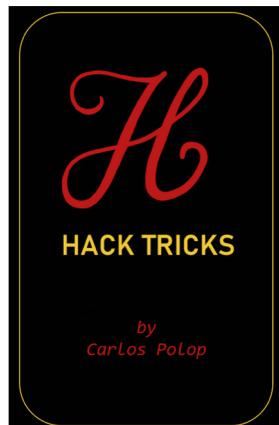
- SUID
- Clefs SSH non protégées
- Vérifier les fichiers cachés
- Vérifier les droits des fichiers
- Vérifier les évènements
- Vérifier le bash history
- Les droits sudo

Les outils pour les tests d'intrusion

Exploitation - Post Exploitation

Une liste de ressources supplémentaires :

- <https://github.com/swisskyrepo/PayloadsAllTheThings> (payload)
- <https://github.com/danielmiessler/SecLists> (bruteforce)
- <https://book.hacktricks.xyz/> (techniques)
- <https://github.com/tennc/webshell> (webshell)



Ressources complémentaires

Plateforme de hacking



App - Script  22 épreuves Cette série d'épreuve vous confronte aux vulnérabilités liées à des faiblesses d'environnement, de configuration ou encore à des (...)	App - Système  75 épreuves Cette série d'épreuve vous confronte aux vulnérabilités applicatives principalement liées aux erreurs de programmation (...)
Cracking  38 épreuves Ces challenges permettent de comprendre le sens du terme « langage compilé ». Ce sont des fichiers binaires à décrypter (...)	Cryptanalyse  50 épreuves Retrouvez les secrets protégés par des systèmes de chiffrement plus ou moins solides en réalisant des attaques (...)
Forensic  25 épreuves Mettez à l'épreuve vos techniques d'investigations numériques en analysant des traces mémoire, des fichiers de journalisation, (...)	Programmation  17 épreuves Automatisez des tâches de plus en plus complexes pour valider ces challenges en moins de quelques (...)
Réaliste  36 épreuves Vous allez vous retrouver dans des environnements complets sur des thèmes divers et variés. À vous d'en comprendre le (...)	Réseau  21 épreuves Apprenez à analyser et à manipuler les différents protocoles et services les plus courants pour les tourner à votre (...)

Ressources complémentaires



Résultats	Nom	Validations	Nombre de points	Difficulté
✓	Command & Control - niveau 2	8%	14610	15
✓	Analyse de logs - attaque web	3%	5456	25
✓	Command & Control - niveau 5	0%	9529	25

15 Points

Analyse mémoire

Auteur

Thanat0s, 16 février 2013

Niveau



Validations

14610 Challengeurs

8%

Note

★★★★★ 1146 votes

J'aime

Je n'aime pas

Énoncé

Berthier, grâce à vous la machine a été identifiée, vous avez demandé un dump de la mémoire vive de la machine et vous aimerez bien jeter un coup d'œil aux logs de l'antivirus. Malheureusement, vous n'avez pas pensé à noter le nom de cette machine. Heureusement ce n'est pas un problème, vous disposez du dump de memoire.

Le mot de passe de validation est le nom de la machine.

Le hash md5 du dump mémoire décompressé est e3a902d4d44e0f7bd9cb29865e0a15de

[Démarrer le challenge](#)

2 ressource(s) associée(s)

- (volatility (Forensic))
- (Volatility cheatsheet v2.4 (Forensic))

Ressources complémentaires



 Potr Genaoueg 

Mes informations

- Statut : Visiteur
- Nombre de posts : 0
- ChatBox : 0

Validations



24% 97/393

 1647
Place

 3160
Points

 97
Challenges

 0
Compromissions

Classement

Place	Avatar	Utilisateur 	Langue	Rang 	Score
# 1642		plean		newbie	3165
# 1642		dyroxyd		newbie	3165
# 1647		Potr Genaoueg		newbie	3160
# 1651		H4rmony		newbie	3155
# 1651		PsycoR		newbie	3155

Ressources complémentaires



Invite Challenge
Hi! Feel free to hack your way in :)

Hack this page to get your invite code!

Hack your code and enter it here...

Sign Up

If you are already a member click [here](#) to login.

Need a hint?
Click Here!

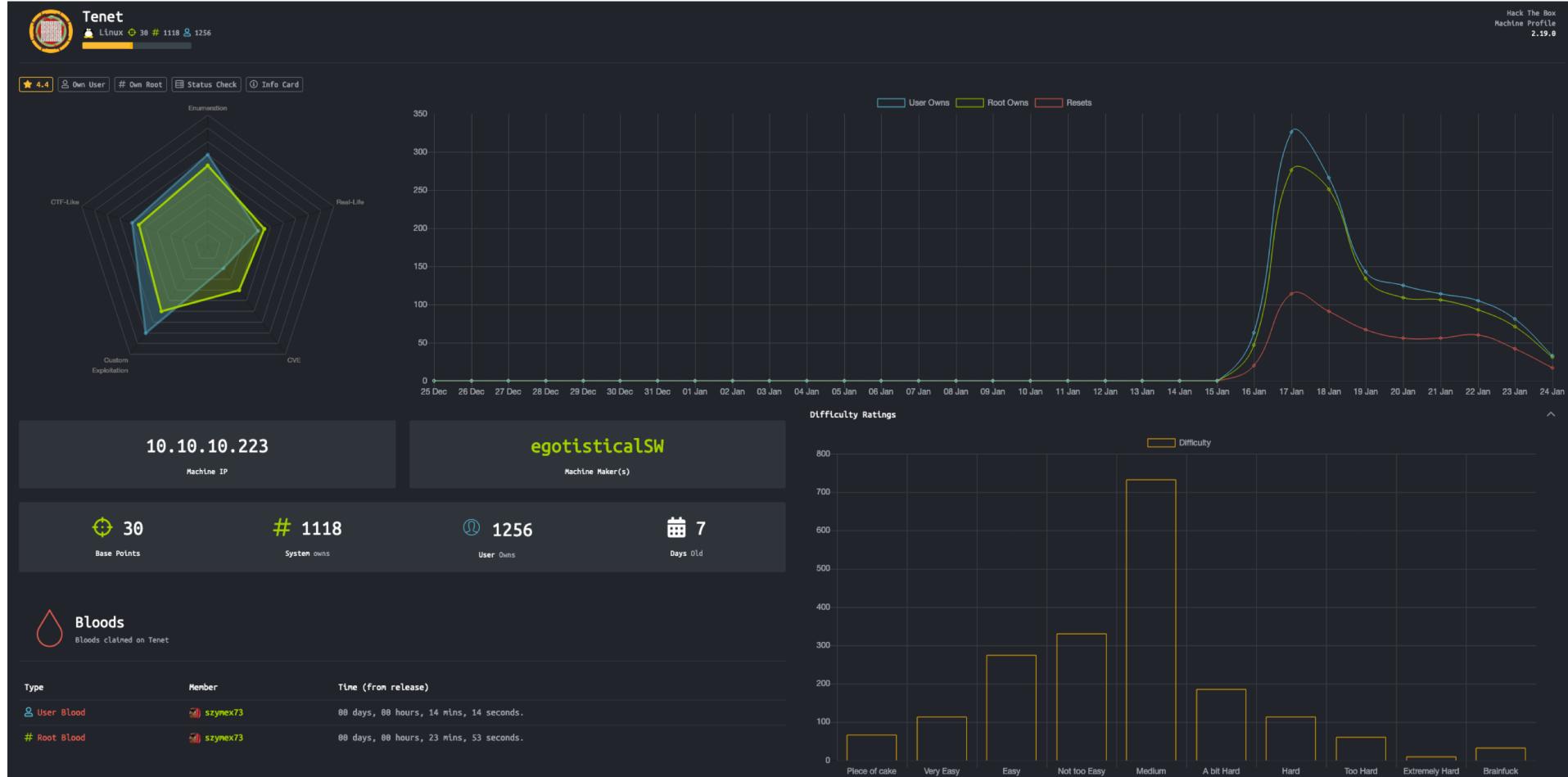
You could check the console...

Almost there but not quite?
Check out the cyber security courses at HTB Academy and start sharpening your skills. The hacking challenge will be waiting!

Go To Academy

Name	Difficulty	Rating	Owns
Tentacle	Low	★ 0.0	4 🚧 0 #
Attended	Medium	★ 4.7	81 🚧 32 #
Cereal	Medium	★ 4.9	178 🚧 148 #
APT	High	★ 3.4	432 🚧 302 #
Sharp	High	★ 4.8	382 🚧 351 #

Ressources complémentaires



Ressources complémentaires

S'entraîner sur des sites conçus pour le pentest ou participer à des **compétitions CTF** :



Possibilité également de participer à des **programmes de bug-bounty rémunérés/récompensés** :

YES WE H~~A~~C^K

hackerone

bugcrowd

Et bien sûr, possibilité de faire carrière dans l'un des nombreux métiers de la sécurité informatique !



Les métiers de la sécurité informatique



Managérial

- Analyste de la menace (*Threat Intelligence*)
- Chef de projet sécurité
- Consultant sécurité «organisationnel»
- Correspondant sécurité
- Délégué à la Protection des Données
- Juriste spécialisé en cybersécurité
- Responsable de la Sécurité des Systèmes d'Information
- Responsable du plan de continuité d'activité
- Spécialiste en gestion de crise cyber



Technique

- Administrateur sécurité
- Analyste SOC
- Architecte sécurité
- Consultant sécurité «technique»
- Cryptologue
- Développeur sécurité
- Auditeurs et évaluateurs sécurité
- Expert réponse à incident
- Intégrateur de sécurité
- Technicien sécurité

TP03-1 – Attaque sur infrastructure

Vous êtes chargés de réaliser un test d'intrusion sur un serveur, vous avez eu quelques informations lors de vos phases de reconnaissance, le serveur héberge un site de l'entreprise « Ceban Corp », l'administrateur supposé s'appellerait Alice.

Monter l'OVA « TP03-1 » dans VirtualBox ou VMWare.

Si besoin, changer l'adaptateur réseau pour qu'il soit connecté à votre KaliLinux.

Deux flags sont à récupérer, en tant qu'utilisateur et l'autre en root.

Pour trouver l'IP de la machine à attaquer : nmap X.X.X.X/24

Have Fun & Hack Smart.

TP03-2 – Attaque sur infrastructure

Vous êtes chargés de réaliser un test d'intrusion sur un second serveur, aucune information probante n'est en votre possession. Vous allez devoir commencer de zéro.

Monter l'OVA « TP03-2 » dans VirtualBox ou VMWare.

Si besoin, changer l'adaptateur réseau pour qu'il soit connecté à votre KaliLinux.

Il n'y a qu'un seul flag en tant que root.

Pour trouver l'IP de la machine à attaquer : nmap X.X.X.X/24

Have Fun & Hack Smart.

TP Final – Attaque de l'infrastructure happycompany.hack

Vous souhaitez intégrer un groupe d'attaquant très connu dans le milieu. Ils sont connu pour faire passer des tests d'entrés assez sélectif.

Ils vous ont fourni des informations sur votre cible :

- Une connexion VPN à une partie de leur infrastructure
- Le site web.happycompany.hack (10.0.0.11)
- Le site wiki.happycompany.hack (10.0.0.12), il semblerait qu'il y ait des informations intéressante sur leurs infrastructure sur ce site...

Ils vous demande de mener une attaque complète sur l'ensemble des machines que vous trouverez et d'en compromettre un maximum.

Bien entendu, pour prouver que vous avez bien réaliser les hack, vous allez devoir leur rendre un rapport avec la démarche et les différents flags que vous trouverez sur les machines.

TP Final – Attaque de l'infrastructure happycompany.hack

Les règles de manière général :

- Ne pas supprimer / altérer des données
- Si vous pensez qu'il faut faire du bruteforce, il ne sert à rien d'utiliser des dictionnaires de 1000000000 mots de passes. S'ils sont faillibles, ils tomberont rapidement... (Pensez aux seclists, notamment le top darkweb...)
- Ne pas déconnecter / empêcher les autres personnes d'évoluer sur les machines (pas de DOS...)
- Ne pas laisser des preuves trop évidentes de votre passage pour éviter de donner la solution aux autres personnes sur la machines

Le TP sera noté et sera réalisé en groupe de 2 personnes. La date du rendu sera une semaine supplémentaire à la date de la réalisation de celui-ci.

Donc au plus tard le jeudi 24 à 23h59.

Ce qui est attendu dans le rapport :

- Une synthèse expliquant la suite logique de l'attaque sans rentrer dans la technique.
- L'ensemble des preuves, outils et techniques utilisées avec une explication brève de la faille exploitée.

TP Final – Attaque de l'infrastructure happycompany.hack

Pour se connecter à l'infrastructure :

- Installer openvpn s'il n'est pas installé sur votre KaliLinux (*sudo apt-get install -y openvpn network-manager-openvpn*)
- Récupérer le fichier « vpn.zip » et le décompresser.
- Utiliser la commande « openvpn prénom.ovpn », normalement aucune erreur ne devrait s'afficher et le terminal garde le service ouvert.
- Vous pouvez réaliser un ping de « 10.0.0.11 » pour valider le bon accès à la plateforme
- Il n'y a pas de DNS sur cette plateforme, si vous souhaitez utiliser les noms des machines que vous allez trouver, vous pouvez les renseigner localement dans /etc/hosts
- **Pensez bien à prendre des screenshot de vos attaques/tentatives d'attaques pour le rapport.**

Have fun & Hack Smart