



Université Abdelmalek Essaâdi

Faculté Polydisciplinaire

- Larache -

Master : Devops & Cloud Computing

Mini-Projet du module Cybersécurité

---

# Password Attacks

---

Réalisé par :

- Fatima Aflous
- Hajar Wafiq
- Salma Hafiani

Encadré par:

- Mm.Chaymae Taib

Année Universitaire : 2023-2024

**Security is not a product ,  
but a process.**

- Bruce Schneier

# PLAN:

Résumé :	6
Abstract :	7
<b>I. Introduction général:</b>	<b>8</b>
1. Contexte et Problématique :	8
2. Organisation du rapport :	9
<b>II. Généralités sur la cybersécurité :</b>	<b>10</b>
1. Introduction :	10
2. Sécurité informatique :	10
3. Problèmes liées à la sécurité :	10
4. Objectifs de la sécurité :	11
5. Conclusion :	11
<b>III. Contexte Général du Projet :</b>	<b>12</b>
1. Introduction :	12
2. Présentation général du sujet :	12
3. Exploration de l'attaque par mot de passe	14
a. Définition :	14
b. Objectifs :	14
4. Les types d'attaques par mots de passe :	15
a. Attaque par force brute :	15
b. Attaque par dictionnaire	15
c. Attaque par Rainbow Tables	16
d. Attaque par Rejeu	16
e. Attaque par Keylogger	16
f. Attaque par Credential Stuffing	17
5. Conclusion :	17
<b>IV. Techniques et outils pour les attaques par mot de passe</b>	<b>17</b>
1. Introduction :	17
2. Framework Metasploit :	17
a. Définition :	17
b. Fonctionnalités :	18
c. Architecture du Metasploit :	18
3. Outils de Simulation des Attaques par Mot de passe :	20
❖ Hydra :	20
❖ Hashcat :	20

❖ John The Ripper: .....	21
❖ Medusa : .....	21
❖ Ncrack : .....	21
4. Conclusion : .....	21
<b>V. Stratégies de Prévention et Défense</b> .....	22
1. Introduction : .....	22
2. Méthodes de Défense : .....	22
a. Création de mots passe plus forts : .....	22
b. Utilisation de l'Authentification Multi facteurs(MFA):.....	23
❖ Authentification biométrique : .....	24
❖ Jetons matériels : .....	24
❖ Authentification mobile : .....	24
❖ Authentification hors bande : .....	24
c. Utilisation d'outils de détection des attaques : .....	25
d. Surveillance des journaux : .....	25
e. Authentification sans mot de passe : .....	25
3. Conclusion : .....	25
VI. Analyse de cas : Simulation d'une attaque par Force Brute avec DVWA, Burp Suite, Openbullet2, Wazuh et Fail2ban.....	26
A. Initiation de l'Attaque: .....	26
B. Détection de l'attaque:.....	37
C. Prévention de L'attaque : .....	40
D. Conclusion .....	42
Conclusion Général: .....	43
Références : .....	44

## Liste des Figures :

Figure 1:cyber security challenges .....	10
Figure 2:CIA Triad .....	11
Figure 3:Password Breach Statistics .....	12
Figure 4:U.S. DATA BREACHES & EXPOSED RECORDS OVER TIME .....	13
Figure 5:Metasploit .....	17
Figure 6:Metasploit Framework architecture .....	20
Figure 7:Hydra.....	20
Figure 8:Hashcat.....	20

Figure 9:John The Ripper .....	21
Figure 10:Medusa .....	21
Figure 11:Ncrack .....	21
Figure 12:Interface de 1Password .....	23
Figure 13:Facteurs d'authentification .....	24
Figure 14:installation de la suite burpsuite.....	26
Figure 15:Mise en place de BurpSuite .....	26
Figure 16:Interface BurpSuite .....	27
Figure 17:Installation de Metasploitable.....	27
Figure 18:Machine Metasploitable.....	28
Figure 19:Adresse IP du machine Metasploitable .....	28
Figure 20:Acces au Metasploitable par Kali Linux.....	28
Figure 21:Page de Connexion de DVWA.....	29
Figure 22:Interface DVWA.....	29
Figure 23:Page Brute Force.....	30
Figure 24:Brute Force login Page.....	30
<b>Figure 25:Proxy BurpSuite .....</b>	<b>31</b>
<b>Figure 26:Proxy Navigateur .....</b>	<b>31</b>
Figure 27:Lancer l'interception.....	32
Figure 28:Test connexion .....	32
Figure 29:Résultat Intruder .....	33
Figure 30:Interface Intruder.....	34
Figure 31:Preparer l'attaque .....	34
Figure 32:payload username.....	35
Figure 33:payload password.....	35
Figure 34:Resultat d'attaque .....	36
Figure 35:configuration 1 du fail2ban.....	40
Figure 36:configuration 2 fail2ban .....	41
Figure 37:résultat Fail2ban.....	42

## Résumé :

A l'ère numérique, les mots de passe jouent un rôle crucial dans la protection de nos données et de nos identités en ligne. Cependant, face à l'évolution constante des cybermenaces, il est essentiel de comprendre les différentes formes d'attaques par mot de passe, les outils utilisés par les pirates et les méthodes efficaces pour se prémunir contre ces intrusions. Ce rapport débute par un exposé historique approfondi ainsi qu'une introduction détaillée sur les attaques par mots de passe. Il analyse ensuite en détail les différentes techniques employées par les pirates, telles que les attaques par force brute, par dictionnaire, les keyloggers, les attaques par rejeu, entre autres. De plus, le rapport explore l'arsenal des pirates informatiques, comprenant les logiciels et outils spécialisés utilisés pour automatiser les attaques par mot de passe, craquer les hachages et exploiter les vulnérabilités des systèmes. Pour tester les connaissances, ce rapport propose des simulations d'attaques par mot de passe réelles, permettant ainsi de comprendre les tactiques des pirates et de renforcer les défenses. La section finale est consacrée à la prévention et à la défense contre les attaques par mot de passe, où sont présentées des pratiques exemplaires, des mesures préventives et des stratégies de défense pour protéger les comptes contre les attaques les plus récentes.

**Mots clés :** cybermenaces , attaque force brute , attaque par dictionnaire , attaque par keyloggers , attaque par rejeu.

## Abstract :

In the digital age, passwords play a crucial role in protecting our data and online identities. However, given the constant evolution of cyber threats, it is essential to understand the various forms of password attacks, the tools used by hackers, and effective methods to defend against these intrusions. This report begins with a comprehensive historical overview and a detailed introduction to password attacks. It then thoroughly analyzes the different techniques employed by hackers, such as brute force attacks, dictionary attacks, keyloggers, replay attacks, among others. Additionally, the report explores the arsenal of hackers, including specialized software and tools used to automate password attacks, crack hashes, and exploit system vulnerabilities. To assess knowledge, the report offers real password attack simulations, providing insight into hackers' tactics and strengthening defenses. The final section focuses on prevention and defense against password attacks, presenting best practices, preventive measures, and defense strategies to safeguard accounts against the latest threats.

**KeyWords :** cyber threats , brute force attacks , dictionary attacks , keyloggers , replay attacks.

## I. Introduction général:

### 1. Contexte et Problématique :

Depuis les premiers jours de l'informatique, notamment à MIT en 1961, le concept d'authentification des utilisateurs a émergé, donnant naissance aux mots de passe comme moyen de vérifier l'identité des utilisateurs. À cette époque, le paysage de la sécurité était encore en développement, avec des violations relativement bénignes et des pirates plus intéressés par l'exploration que par des activités criminelles.

À la fin des années 1970, de véritables pirates ont commencé à émerger, créant des défis nouveaux pour la sécurité des systèmes informatiques. Pour répondre à ces préoccupations, le National Bureau of Standards a introduit le Data Encryption Standard (DES) en 1979, établissant ainsi une norme pour le cryptage des données pendant deux décennies.

Les années 1980 ont été marquées par la prolifération des ordinateurs de bureau et l'apparition d'incidents notables tels que le ver Morris de 1988, qui a infecté des milliers d'ordinateurs en réseau. Parallèlement, les jetons d'authentification multi-facteurs (MFA) ont commencé à émerger, en particulier pour les VPN à accès distant.

En 1997, l'Advanced Encryption Standard (AES) a été introduit, offrant un niveau de cryptage plus puissant. Vers la même époque, CAPTCHA a été développé pour distinguer les humains des robots, évoluant au fil du temps vers des formes plus sophistiquées comme le CAPTCHA invisible.

Malgré ces avancées, les mots de passe restent vulnérables face aux attaques, notamment avec l'expansion des appareils mobiles, de l'IoT et des médias sociaux. Cette situation a conduit à une demande croissante d'expériences numériques fluides, incitant à explorer des alternatives aux mots de passe traditionnels. Des organisations telles que The FIDO Alliance et le World Wide Web Consortium (W3C) travaillent activement à cette transition, visant à renforcer la sécurité et l'expérience utilisateur à l'ère numérique.



## 2. Organisation du rapport :

Dans le contexte actuel, notre objectif principal est de présenter plusieurs types d'attaques par mots de passe, d'explorer les différents outils utilisés pour mener ces attaques, ainsi que les environnements associés tels que Metasploit, qui facilite et offre des fonctionnalités supplémentaires pour des attaques plus ciblées. Pour ce faire, notre rapport sera structuré en trois chapitres suivis d'une conclusion générale.

- **Le premier chapitre :** généralités sur la cybersécurité .
- **Le deuxième chapitre :** fournira un contexte général sur le sujet, accompagné de quelques statistiques pertinentes.
- **Le troisième chapitre :** comprendra des simulations d'attaques, ainsi que des explications sur leur fonctionnement.
- **Le quatrième chapitre :** traitera des mesures de prévention et de défense pour se prémunir contre les attaques par mots de passe.
- **Le cinquième chapitre :** Analyse de cas d'attaque par force brute et mesures de détection et de prévention.

En conclusion, nous synthétiserons les principaux points abordés dans notre travail et mettrons en évidence les recommandations clés pour renforcer la sécurité des mots de passe.

## II. Généralités sur la cybersécurité :

### 1. Introduction :

Dans ce premier chapitre, nous entamerons notre exploration de la cybersécurité en introduisant ses concepts fondamentaux, en identifiant les défis majeurs de la sécurité informatique et en définissant ses objectifs primordiaux.

### 2. Sécurité informatique :

Les systèmes informatiques devenus plus en plus vulnérables, chaque jour le nombre des cyberattaques reporté augmente, Cependant, les cybercriminels sont les plus préoccupants pour les organisations et les entreprises. Aujourd'hui, un attaquant n'a besoin que d'une machine et une connexion internet pour effectuer une action malveillante grâce la mise à disposition d'outils et logiciels en ligne.

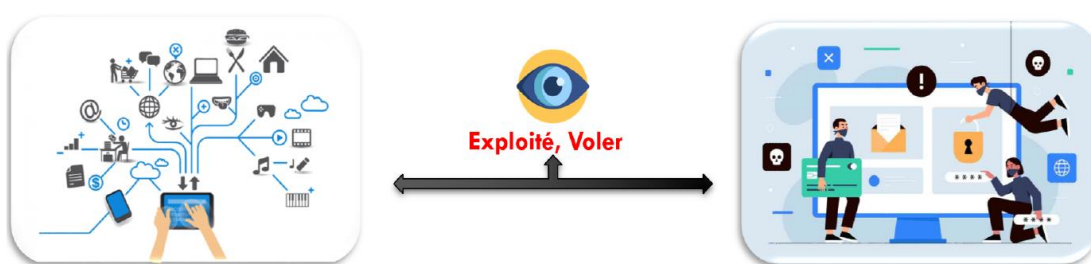


Figure 1:cyber security challenges

La cybercriminalité est devenue un véritable trouble tant pour les individus que pour la société dans son sens large, plus les mesures de sécurité se développent, plus la criminalité augmente.

### 3. Problèmes liées à la sécurité :

La sécurité informatique est un ensemble des outils mis en place, des mesures technologiques de sécurité pour assurer une bonne approche et une meilleure pratique afin de garantir une sécurité et protection fiables des systèmes d'information contre toute utilisation et accès non autorisés. les actifs de l'organisation et de l'utilisateur comprennent les dispositifs informatiques connectés, le personnel, l'infrastructure, les applications, les services, les systèmes de télécommunications, et la totalité des informations transmises et/ou stockées dans le cyber environnement.

#### 4. Objectifs de la sécurité :

L'objectif principal de la sécurité informatique est d'assurer la disponibilité, l'intégrité et la confidentialité des systèmes d'informations. La figure 2 suivante représentent les trois objectifs de base de la sécurité ou bien ce qu'on appelle le CIA triangle :



Figure 2:CIA Triad

D'où on distingue :

- **La disponibilité** : est un objectif de sécurité signifie un accès et une utilisation rapide et fiable des informations pour les personnes autorisées.
- **L'intégrité** : est un objectif de sécurité permettant de lier à son tour au concept d'intégrité éthique, défini comme étant la prévention de la modification ou de la destruction inappropriée d'informations et qui inclut spécifiquement l'authenticité et la non répudiation des informations.
- **Confidentialité** : est un objectif de sécurité permettant de protéger les données confidentielles lors de son échange contre tout accès non autorisé, elle permet d'assurer que les données personnelles transmises sont accessibles uniquement aux personnes autorisées.

#### 5. Conclusion :

En résumé, ce premier chapitre nous a initiés à la cybersécurité en explorant ses concepts, ses défis et ses objectifs principaux. Nous avons mis en avant l'importance de garantir la disponibilité, l'intégrité et la confidentialité des données pour assurer la sécurité des systèmes informatiques. Les chapitres suivants se concentreront spécifiquement sur les attaques par mots de passe et leur impact sur la sécurité en ligne

### III. Contexte Général du Projet :

#### 1. Introduction :

Dans ce chapitre, nous nous attarderons sur le contexte général du sujet, en commençant par quelques statistiques pour nous immerger dans le domaine. Ensuite, nous procéderons à la définition d'une attaque par mots de passe, en mettant en lumière son impact et ses conséquences. Nous explorerons également les différents types d'attaques par mots de passe afin de mieux comprendre les diverses stratégies utilisées par les attaquants.

#### 2. Présentation général du sujet :

Depuis les débuts de l'informatique, les mots de passe ont été indispensables pour sécuriser les données sensibles et limiter l'accès aux systèmes. Aujourd'hui, quasiment toutes les plateformes numériques exigent une authentification par mot de passe pour permettre l'accès[1]. Pourtant, malgré leur utilisation répandue, les mots de passe sont de plus en plus vulnérables. En 2020, 81 % des violations de données dans les entreprises étaient liées à l'exploitation de mots de passe, en faisant ainsi la méthode d'attaque la plus courante, comme montre dans la figure 3.

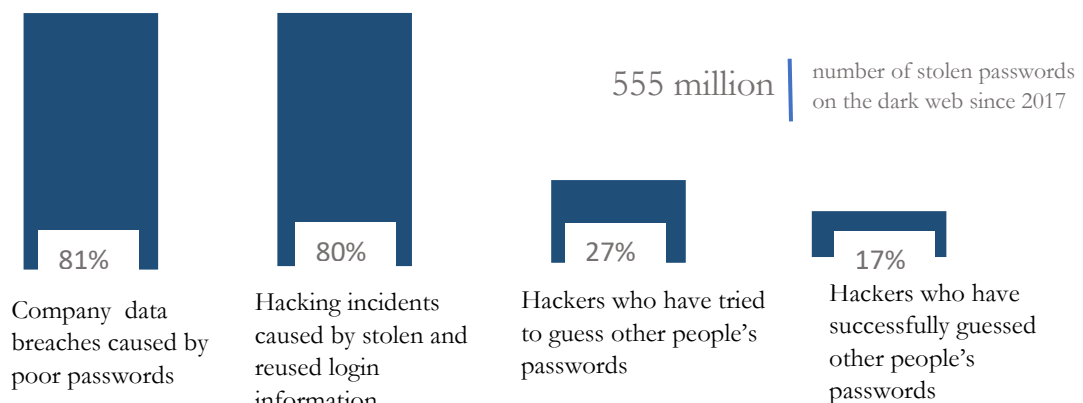


Figure 3: Password Breach Statistics

1

<sup>1</sup> Source : CENT , Google , Verizon , TraceSecurity

Depuis 2013, un nombre alarmant d'enregistrements ont été continuellement exposés par des pirates informatiques, avec des milliers d'enregistrements tombant quotidiennement entre les mains de personnes non autorisées. Cela se traduit par un taux ahurissant de 158 727 enregistrements par heure comme montré dans la figure 2 et 2 645 enregistrements par minute et jusqu'à 44 enregistrements exposés chaque seconde. Cette tendance continue des violations de données souligne le besoin urgent de mesures de cybersécurité robustes pour protéger les informations sensibles.

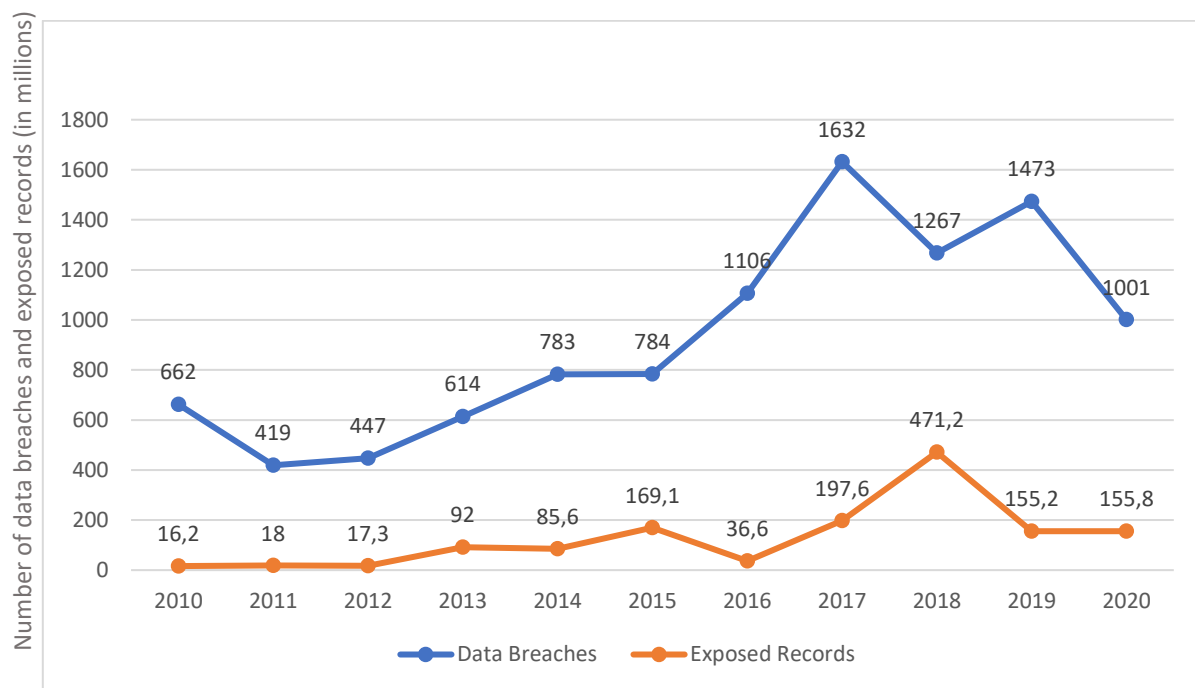


Figure 4:U.S. DATA BREACHES & EXPOSED RECORDS OVER TIME

2

En examinant ces graphiques, il devient manifeste que la vulnérabilité des mots de passe est en augmentation .

<sup>2</sup> Source : The Identity Theft Resource Center (ITRC)

### 3. Exploration de l'attaque par mot de passe

#### a. Définition :

Une attaque par mot de passe est une tentative malveillante d'obtenir l'accès non autorisé à un système informatique, à un compte en ligne ou à une ressource protégée par un mot de passe. Les pirates informatiques emploient diverses techniques pour voler ou deviner les mots de passe des utilisateurs, dans le but de réaliser des actions malveillantes telles que :

- Vol de données: Dérober des informations sensibles, telles que des données personnelles, des informations financières ou des secrets commerciaux.
- Usurpation d'identité: Se faire passer pour l'utilisateur légitime afin d'effectuer des transactions frauduleuses ou accéder à des informations confidentielles.
- Propagation de malwares: Installer des logiciels malveillants sur l'appareil de l'utilisateur pour prendre le contrôle de son système, voler ses données ou diffuser d'autres logiciels malveillants.
- Interruption de services: Démêler les services en ligne ou les systèmes informatiques en surchargeant les serveurs ou en empêchant les utilisateurs légitimes d'y accéder.

#### b. Objectifs :

Les motivations derrière les attaques par mot de passe varient selon les pirates informatiques et leurs intentions. Les objectifs les plus courants incluent :

- Gain financier: Voler des informations financières, telles que des numéros de carte de crédit ou des comptes bancaires, pour réaliser des transactions frauduleuses ou revendre ces informations sur le marché noir.
- Espionnage: Obtenir des informations confidentielles ou des secrets commerciaux pour les exploiter à des fins personnelles ou les revendre à des concurrents.
- Cybercriminalité: Commettre des actes de cybercriminalité tels que le vol d'identité, la fraude fiscale ou le blanchiment d'argent.
- Vandalisation: Démêler les systèmes informatiques ou les services en ligne par simple malice ou pour causer des dommages.
- Cyberterrorisme: Mener des attaques informatiques à des fins politiques ou pour semer la peur et la discorde.

#### 4. Les types d'attaques par mots de passe :

Les systèmes informatiques ont longtemps utilisé l'authentification par nom d'utilisateur et mot de passe, offrant aux acteurs malveillants le temps et l'expérience nécessaires pour cibler les vulnérabilités courantes. Certaines attaques sont simples, comme deviner les mots de passe, tandis que d'autres sont complexes et impliquent des outils automatisés. Voici quelques-unes des attaques par mot de passe les plus courantes et dangereuses :

##### a. Attaque par force brute :

Une attaque par force brute est une méthode de piratage qui utilise l'essai et l'erreur pour craquer les mots de passe, les identifiants de connexion et les clés de chiffrement. Les pirates expérimentent avec différents noms d'utilisateur et mots de passe jusqu'à ce qu'ils trouvent les informations de connexion correctes[2]. Ils utilisent généralement un ordinateur pour tester un grand nombre de combinaisons. En fait, un pirate informatique peut essayer 2,18 billions de combinaisons de mots de passe/noms d'utilisateur en 22 secondes. Souvent, les attaques par force brute sont facilitées par des outils numériques, permettant aux attaquants d'essayer potentiellement des trillions de combinaisons en peu de temps. [3]

##### b. Attaque par dictionnaire

Les attaques par dictionnaire exploitent la tendance à choisir des mots courants comme mots de passe. Les pirates utilisent des listes de mots courants, y compris des mots personnels comme lieux de naissance ou noms d'animaux, pour essayer de deviner les mots de passe. Contrairement aux attaques par force brute, les attaques par dictionnaire sont plus rapides car elles ciblent les mots les plus courants. Cependant, elles ont leurs limites, car elles ne peuvent pas craquer les mots de passe imprévisibles.[4]

#### c. Attaque par Rainbow Tables

Une attaque par table arc-en-ciel est une méthode sophistiquée pour craquer des mots de passe chiffrés. Contrairement à une attaque par force brute qui tente de deviner directement les mots de passe, une attaque par table arc-en-ciel utilise des tables précalculées contenant des correspondances entre les valeurs de hachage et les mots de passe. Ces tables, appelées "tables arc-en-ciel", sont générées à l'avance en appliquant des algorithmes de hachage à une liste de mots de passe possibles. Lorsqu'une attaque est lancée, elle compare les hachages de la base de données cible aux entrées de la table arc-en-ciel pour trouver des correspondances, permettant ainsi de récupérer les mots de passe associés aux hachages. Bien que cette méthode soit efficace pour craquer des mots de passe rapidement, elle est limitée aux mots de passe contenus dans la table arc-en-ciel, ce qui rend les mots de passe plus longs et plus complexes moins susceptibles d'être découverts.[5]

#### d. Attaque par Rejeu

Une attaque par rejeu est une forme d'attaque réseau dans laquelle une transmission de données valide est malicieusement ou frauduleusement répétée ou retardée. L'objectif principal est de tromper le système en acceptant la retransmission des données comme légitime. De plus, les attaques par rejeu sont dangereuses car il est difficile de les détecter. De surcroît, elles peuvent réussir même si la transmission d'origine était chiffrée.[6]

#### e. Attaque par Keylogger

Un keylogger est une technique de vol de données qui consiste à enregistrer la frappe au clavier sur un ordinateur. En enregistrant quand les informations sont saisies, les intrus peuvent les récupérer et les voler. Les keyloggers sont un type de logiciel malveillant conçu pour suivre chaque frappe au clavier et la transmettre à un pirate informatique. Généralement, un utilisateur télécharge le logiciel en croyant qu'il est légitime, mais il installe en fait un keylogger sans préavis.[7]



## f. Attaque par Credential Stuffing

Le credential stuffing, ou bourrage d'identifiants, est une forme d'attaque informatique qui implique généralement des tentatives répétées de connexion à des comptes en ligne en utilisant des identifiants et des mots de passe volés à partir d'autres services en ligne[8]. Il exploite la tendance naturelle des utilisateurs à réutiliser les mots de passe pour faire face au nombre croissant de comptes en ligne à gérer. Les attaquants savent que le nom d'utilisateur et le mot de passe utilisés sur un site Web peuvent également être utilisés sur une demi-douzaine d'autres sites.

### 5. Conclusion :

En conclusion, ce chapitre d'introduction a dressé le cadre général du sujet en détaillant l'attaque par mots de passe, ses objectifs et les différentes méthodes utilisées.

## IV. Techniques et outils pour les attaques par mot de passe

### 1. Introduction :

Dans ce chapitre, nous plongerons dans le vif du sujet en explorant les techniques et les outils utilisés dans les attaques par mots de passe. Nous procéderons à des simulations de différentes attaques pour mieux comprendre leur fonctionnement. De plus, nous

examinerons les divers outils employés ainsi que les environnements dans lesquels ces attaques sont déployées.

### 2. Framework Metasploit :

#### a. Définition :

Metasploit Framework est un cadre de test d'intrusion open-source largement utilisé pour identifier, exploiter et tester les vulnérabilités des systèmes informatiques. Il offre un environnement complet pour les pentesters et les développeurs de sécurité, leur permettant d'effectuer des tests de pénétration complets et d'analyser la posture de sécurité de leurs réseaux et systèmes.



Figure 5:Metasploit

b. Fonctionnalités :

Les fonctionnalités principales de Metasploit Framework sont :

- Identification des vulnérabilités: Scanne les réseaux et les systèmes pour identifier les vulnérabilités connues, en utilisant des exploits, des scanners et des outils d'analyse automatisés.
- Exploitation des vulnérabilités: Exécute des exploits pour exploiter les vulnérabilités identifiées, permettant l'accès non autorisé aux systèmes cibles.
- Exécution de payloads: Exécute des payloads sur les systèmes compromis, permettant l'installation de logiciels malveillants, la collecte de données sensibles ou la prise de contrôle du système.
- Post-exploitation: Offre des outils pour maintenir l'accès aux systèmes compromis, explorer l'environnement réseau et effectuer des analyses plus approfondies.
- Développement d'exploits: Fournit un environnement pour le développement d'exploits personnalisés, permettant aux utilisateurs de tester et d'exploiter des vulnérabilités nouvellement découvertes.

c. Architecture du Metasploit :

L'architecture modulaire du Framework Metasploit lui confère une flexibilité et une extensibilité significatives pour répondre aux besoins variés des professionnels de la sécurité. Voici un aperçu des principaux composants et de leurs interactions dans l'architecture de Metasploit :

➤ **Bibliothèques :**

Metasploit utilise diverses bibliothèques pour gérer différents aspects de son fonctionnement interne :

- Bibliothèques de manipulation de données : Pour gérer les données utilisées par les modules et les outils de Metasploit.
- Bibliothèques réseau : Pour la communication avec les machines cibles et la gestion des protocoles réseau.
- Bibliothèques de chiffrement : Pour assurer la confidentialité et l'intégrité des communications entre Metasploit et les machines cibles.

### ➤ Outils :

Metasploit comprend une gamme d'outils pour faciliter le développement, le test et l'exploitation des vulnérabilités :

- Outils de génération de payloads : Pour créer des charges utiles à exécuter sur les machines cibles.
- Outils de recherche de vulnérabilités : Pour identifier les failles de sécurité dans les systèmes cibles.
- Outils de capture de trafic réseau : Pour surveiller et analyser le trafic réseau pendant les opérations de test.

### ➤ Modules :

Les modules constituent les éléments de base de Metasploit, fournissant les exploits, les payloads et d'autres fonctionnalités essentielles :

- Exploits : Modules utilisés pour exploiter des vulnérabilités spécifiques dans les logiciels ou les systèmes cibles.
- Payloads : Charges utiles exécutées sur les machines cibles après exploitation avec succès.
- Modules auxiliaires : Modules offrant diverses fonctionnalités d'appui, telles que la découverte de réseaux ou la collecte d'informations.
- Modules post-exploitation : Modules utilisés après l'exploitation réussie d'une machine cible pour effectuer des activités supplémentaires, telles que l'exploration du système ou la collecte d'informations.

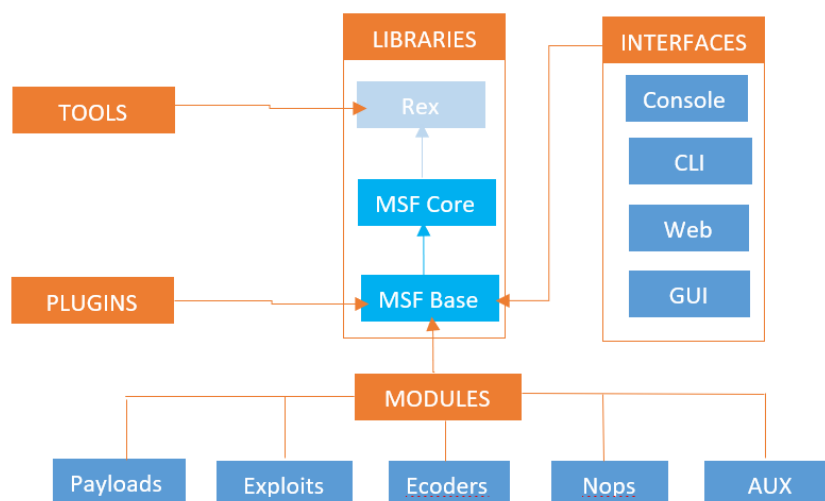


Figure 6:Metasploit Framework architecture

### 3. Outils de Simulation des Attaques par Mot de passe :

#### ❖ Hydra :

Hydra est un outil de craquage de mot de passe open-source puissant et parallélisé qui prend en charge de nombreux protocoles réseau pour les tests de mots de passe. Cet outil est principalement utilisé par les chercheurs en sécurité et les consultants en sécurité pour démontrer la facilité d'accès à distance non autorisé en raison de mots de passe faibles. De plus, les professionnels de la sécurité et les administrateurs réseau utilisent Hydra pour évaluer la force des mots de passe au sein de leurs systèmes, identifier les vulnérabilités potentielles et améliorer la posture de sécurité globale.



Figure 7:Hydra

#### ❖ Hashcat :

Hashcat est un outil de craquage de mots de passe de haute performance qui prend en charge une large gamme d'algorithmes de hachage. Il est conçu pour utiliser la puissance de traitement des processeurs graphiques (GPU) pour accélérer le processus de craquage des mots de passe. Hashcat est largement utilisé par les professionnels de la sécurité informatique et les chercheurs en sécurité pour tester la force des mots de passe et les vulnérabilités des systèmes. Son interface flexible et sa capacité à gérer efficacement différents types de hachages en font un outil précieux dans le domaine de la sécurité des informations.



Figure 8:Hashcat

### ❖ **John The Ripper:**

John the Ripper est un outil conçu pour aider les administrateurs système à trouver des mots de passe faibles (faciles à deviner ou à craquer par force brute) et même à envoyer automatiquement des avertissements aux utilisateurs à ce sujet, si nécessaire. C'est un outil de craquage de mots de passe largement connu et vérifié, disponible pour Windows, DOS, BeOS et OpenVMS ainsi que pour de nombreuses variantes de Linux. Il utilise des listes de mots/dictionnaires pour craquer de nombreux types de hachages, y compris MD5, SHA, etc. Il est gratuit et Open Source, son objectif principal est de détecter les mots de passe Unix faibles.



Figure 9: John The Ripper

### ❖ **Medusa :**

Medusa est un outil de craquage de mots de passe modulaire, rapide et parallèle. Il est utilisé pour forcer l'accès à des comptes en essayant différentes combinaisons de mots de passe sur une variété de protocoles réseau. Medusa est conçu pour être puissant et efficace, avec la capacité de gérer de nombreux protocoles différents, ce qui en fait un choix populaire parmi les professionnels de la sécurité informatique pour évaluer la robustesse des mots de passe et renforcer la sécurité des systèmes.



Figure 10: Medusa

### ❖ **Ncrack :**

Ncrack est un outil puissant d'authentification réseau intégré à Kali Linux. Il évalue rapidement la solidité des mots de passe protégeant l'accès au réseau, permettant aux professionnels de la sécurité de détecter les vulnérabilités potentielles. Une fois les vulnérabilités identifiées, Ncrack peut tenter de les exploiter afin de gagner un accès non autorisé à un système. Il dispose d'une bibliothèque de modules d'exploit intégrés et peut également en charger d'autres développés par la communauté. De plus, Ncrack peut effectuer des analyses et des tentatives d'exploitation simultanément sur plusieurs systèmes cibles, ce qui accélère considérablement le processus de test d'intrusion.



Figure 11: Ncrack

## 4. Conclusion :

En somme, ce chapitre a présenté un ensemble d'attaques possibles dans le cadre des attaques par mots de passe, ainsi qu'un ensemble d'outils pour y parvenir.

## V. Stratégies de Prévention et Défense

### 1. Introduction :

Dans ce chapitre, nous examinerons un ensemble de techniques de prévention et de conseils à suivre pour protéger nos mots de passe et renforcer notre résistance contre les attaques.

### 2. Méthodes de Défense :

#### a. Création de mots passe plus forts :

Créer un mot de passe fort et sécurisé peut réduire le risque que les cybercriminels devinent votre mot de passe et accèdent à des données sensibles. Les mots de passe compromis ont causé 80 % de toutes les violations de données en 2019, entraînant des pertes financières tant pour les entreprises que pour les consommateurs. La peur d'oublier des mots de passe complexes, surtout lorsqu'il y en a plusieurs à retenir, est une préoccupation courante lors de leur création. Un mot de passe fort rend le temps nécessaire pour le deviner exponentiellement plus long, surtout si vous utilisez un mot de passe aléatoire de 20 caractères avec des lettres majuscules/minuscules, des chiffres et des symboles. Il faudrait à un ordinateur 3 sextillions d'années pour le craquer. Voici donc un ensemble de bonnes pratiques à suivre pour créer un mot de passe assez fort :

- Ne réutilisez pas les mots de passe.
- Utilisez un mot de passe unique et fort pour chaque site web, application et système.
- Utilisez un mélange de symboles, de chiffres et de lettres majuscules et minuscules.
- N'utilisez pas d'informations personnellement identifiables (PII) telles que votre date de naissance ou le nom de votre chien.
- Utilisez un générateur de mots de passe.

L'utilisation d'un générateur de mots de passe est une pratique de sécurité essentielle. Ces outils sont extrêmement puissants car ils sont capables de créer des mots de passe forts, complexes et difficiles à craquer. En évitant d'avoir à se souvenir d'innombrables mots de passe, les générateurs de mots de passe simplifient grandement la gestion des identifiants. Les mots de passe générés sont automatiquement enregistrés et synchronisés, permettant un accès facile et sécurisé à vos comptes où que vous soyez. Parmi les gestionnaires de mots de passe disponibles sur le marché, 1Password se distingue comme l'un des meilleurs.

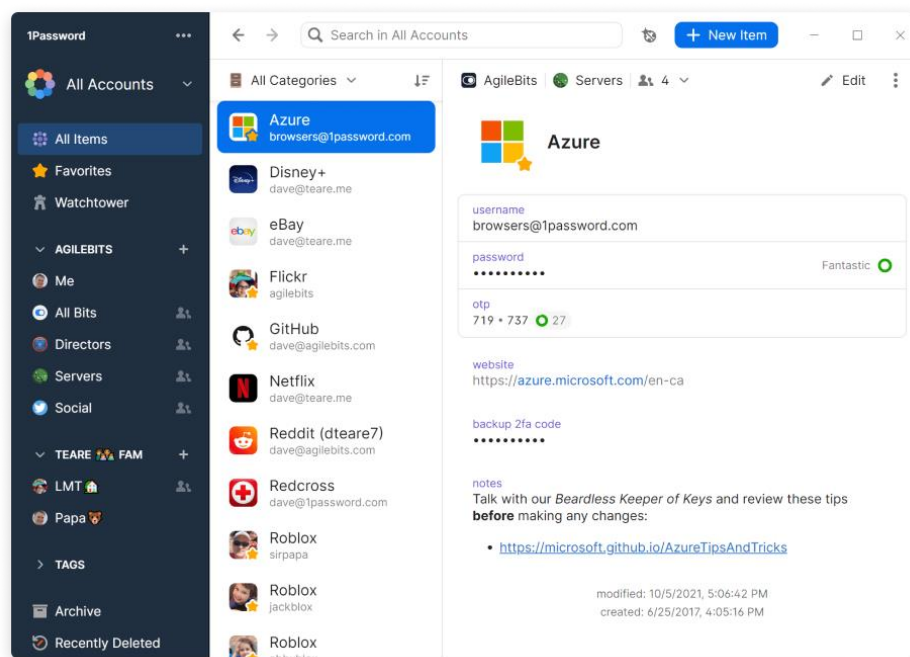


Figure 12:Interface de 1Password

b. Utilisation de l'Authentification Multi facteurs(MFA):

L'authentification multi facteur (MFA) est une méthode de vérification d'identité qui nécessite que l'utilisateur fournisse au moins deux types de preuves pour accéder à une ressource, telle qu'une application, un compte en ligne ou un VPN. La MFA est un élément crucial de toute stratégie de gestion des accès et des identités (IAM) visant à renforcer la sécurité. Plutôt que de se limiter à un nom d'utilisateur et à un mot de passe, la MFA exige la présentation de plusieurs types de preuves, ce qui diminue considérablement le risque de réussite d'une cyberattaque.

Voici une variété de technologies MFA fréquemment utilisées :

❖ **Authentification biométrique :**

Les technologies biométriques permettent une authentification précise et sécurisée des utilisateurs à l'aide de leurs appareils mobiles. Les méthodes biométriques courantes incluent la numérisation des empreintes digitales et la reconnaissance faciale. De plus, la biométrie comportementale, qui analyse les interactions uniques de l'utilisateur avec son appareil, comme la frappe au clavier ou les mouvements de la souris, offre une couche de sécurité supplémentaire.

❖ **Jetons matériels :**

Ces petits dispositifs portables permettent d'autoriser l'accès à un service réseau. Ils fournissent un facteur de possession pour l'authentification multifactorielle en générant des codes d'accès à usage unique (OTP), ce qui renforce la sécurité des applications bancaires et autres.

❖ **Authentification mobile :**

Cette méthode vérifie les utilisateurs via leurs appareils Android ou iOS, offrant une connexion sécurisée à distance à des sites et ressources.

❖ **Authentification hors bande :**

Ce type d'authentification requiert une méthode de vérification secondaire via un canal de communication distinct, tel que la connexion Internet de l'utilisateur ou un réseau sans fil. Parmi les exemples figurent les codes Cronto et les notifications push qui délivrent des codes d'authentification ou des mots de passe à usage unique sur les appareils mobiles. De plus, les messages texte SMS ou vocaux peuvent être utilisés pour transmettre ces codes. Les jetons logiciels, quant à eux, génèrent des codes PIN uniques sur les smartphones, offrant ainsi une autre couche de sécurité pour l'authentification multifactorielle.

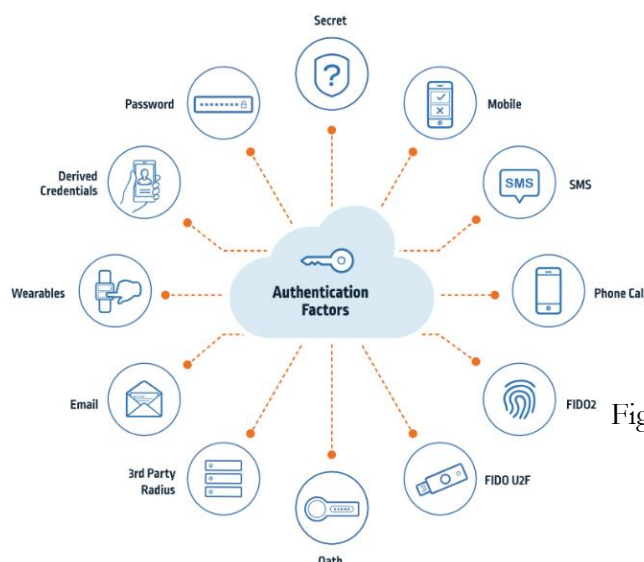


Figure 13:Facteurs d'authentification



c. Utilisation d'outils de détection des attaques :

Les outils de détection des attaques par mot de passe sont des logiciels conçus pour surveiller l'activité sur un réseau ou un système informatique et détecter les tentatives d'intrusion ou d'attaques par force brute visant à compromettre les mots de passe des utilisateurs. Ces outils analysent les schémas de trafic, les modèles de connexion et d'autres indicateurs pour identifier les comportements suspects, tels que les tentatives répétées de connexion avec des mots de passe incorrects ou les tentatives massives de connexion depuis une même adresse IP. Une fois une attaque détectée, ces outils peuvent déclencher des alertes pour informer les administrateurs système afin qu'ils puissent prendre des mesures correctives immédiates, comme le blocage de l'adresse IP source de l'attaque ou la réinitialisation des mots de passe compromis.

d. Surveillance des journaux :

La surveillance des journaux consiste à examiner régulièrement les fichiers journaux générés par les systèmes informatiques, les applications et les appareils réseau pour repérer les activités suspectes ou anormales. Ces fichiers journaux enregistrent toutes les interactions et les événements qui se produisent sur le système, y compris les tentatives de connexion réussies ou infructueuses, les changements de configuration, les erreurs système, etc. En surveillant activement ces journaux, les administrateurs peuvent détecter les tentatives d'attaques par mot de passe, telles que les tentatives de connexion avec des identifiants incorrects ou les activités de brute force, et prendre des mesures préventives pour renforcer la sécurité, telles que le verrouillage des comptes ou le renforcement des politiques de mot de passe.

e. Authentification sans mot de passe :

L'authentification sans mot de passe est une méthode d'authentification qui permet aux utilisateurs de se connecter à des systèmes ou des services sans avoir à saisir de mot de passe traditionnel. Au lieu de cela, cette méthode repose généralement sur d'autres facteurs d'authentification plus sécurisés, tels que des clés publiques/privées, des tokens, des appareils biométriques (empreintes digitales, reconnaissance faciale, etc.), des applications mobiles ou des e-mails/SMS.

3. Conclusion :

En résumé, ce chapitre a présenté divers outils et stratégies de prévention contre les attaques par mots de passe, soulignant ainsi l'importance de renforcer la sécurité des identifiants d'accès dans les environnements informatiques actuels.

## VI. Analyse de cas : Simulation d'une attaque par Force Brute avec DVWA, Burp Suite, Openbullet2, Wazuh et Fail2ban

### A. Initiation de l'Attaque:

Pour mener à bien notre attaque, nous avons tout d'abord commencé par l'installation de la suite Burp Suite via le lien suivant : <https://portswigger.net/burp/communitydownload>

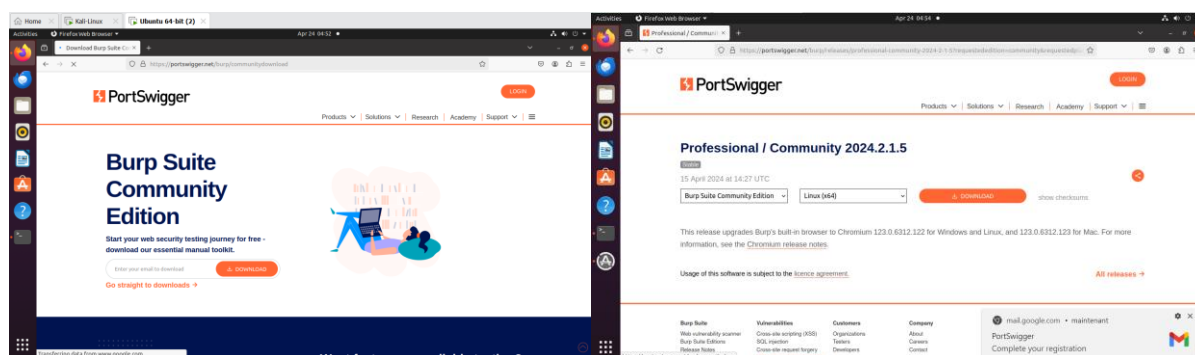


Figure 14: installation de la suite burpsuite

Et pour la mise en place, nous devons lancer le script d'installation après avoir téléchargé le fichier, tout en lui accordant les permissions d'exécution.

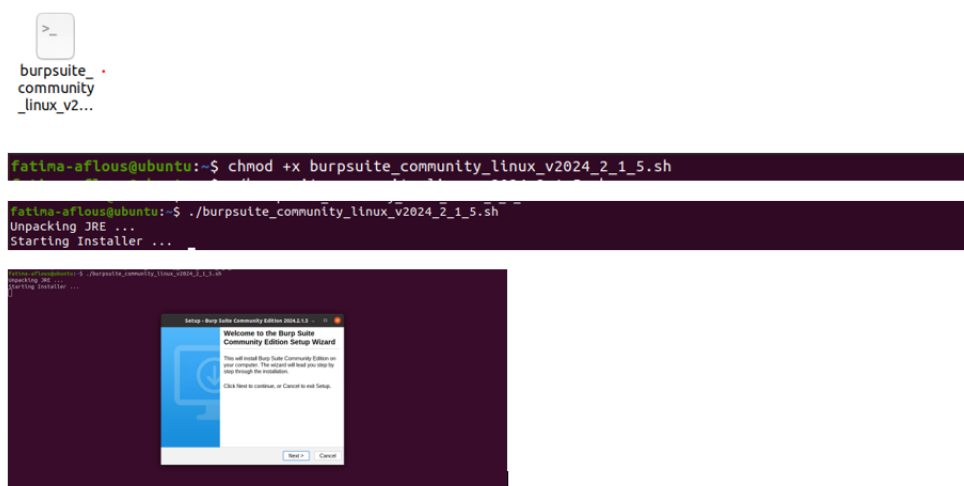


Figure 15: Mise en place de BurpSuite

Puis lancer la suite Burpsuite avec la commande **burpsuite** :

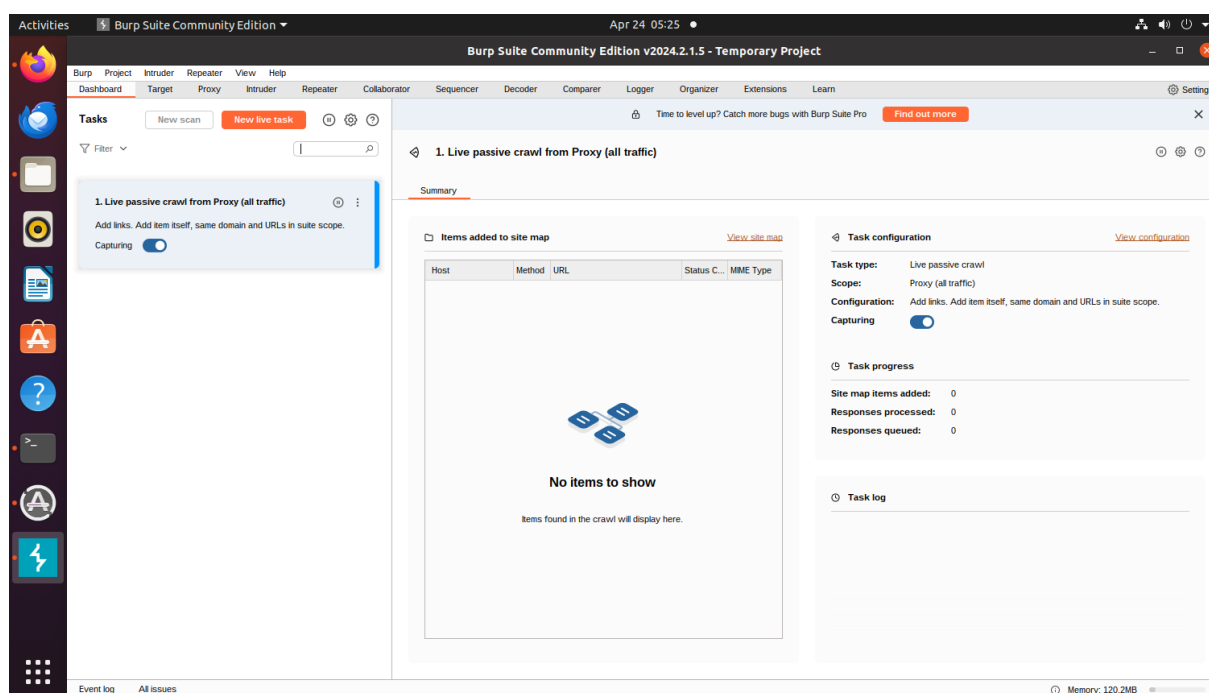


Figure 16:Interface BurpSuite

De l'autre côté, nous devons installer la machine Metasploitable qui nous permettra d'accéder à la machine DVWA sur laquelle nous mènerons l'attaque. Pour le téléchargement, voici le lien suivant : <https://sourceforge.net/projects/metasploitable2/>

#### Remarque :

**Metasploitable** est une machine virtuelle Linux intentionnellement vulnérable. Cette VM peut être utilisée pour dispenser des formations en sécurité, tester des outils de sécurité et pratiquer des techniques courantes de test de pénétration. Contrairement à d'autres machines virtuelles vulnérables, Metasploitable se concentre sur les vulnérabilités au niveau du système d'exploitation et des services réseau plutôt que sur des applications personnalisées et vulnérables.


 Metasploitable2-Linux	24/04/2024 15:08	Dossier de fichiers	
 metasploitable-linux-2.0.0.zip	24/04/2024 15:05	Archive WinRAR ZIP	852 653 Ko

Figure 17:Installation de Metasploitable

Ensuite, nous utilisons "msfadmin" / "msfadmin" comme nom d'utilisateur et mot de passe pour accéder à la machine :

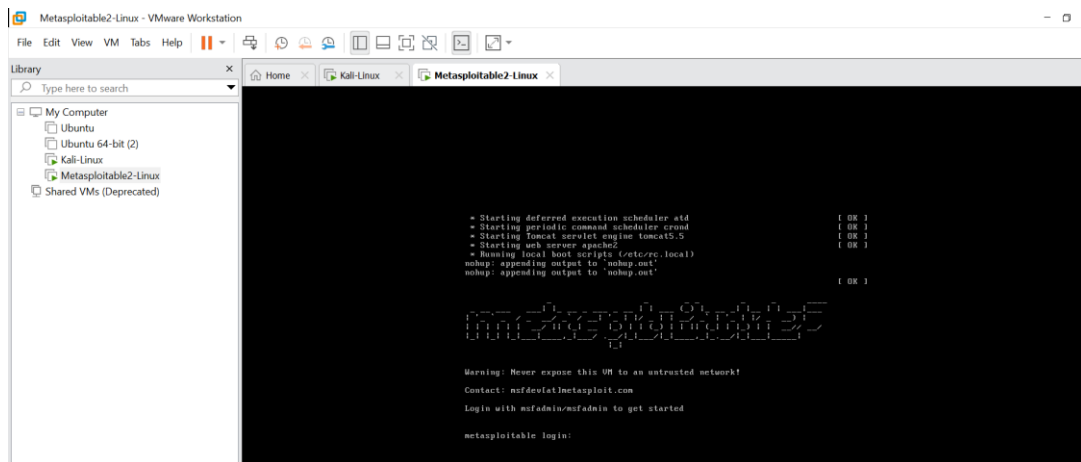


Figure 18:Machine Metasploitable

Puis, nous recherchons l'adresse IP de la machine qui nous aidera par la suite à y accéder à partir d'autres machines virtuelles.

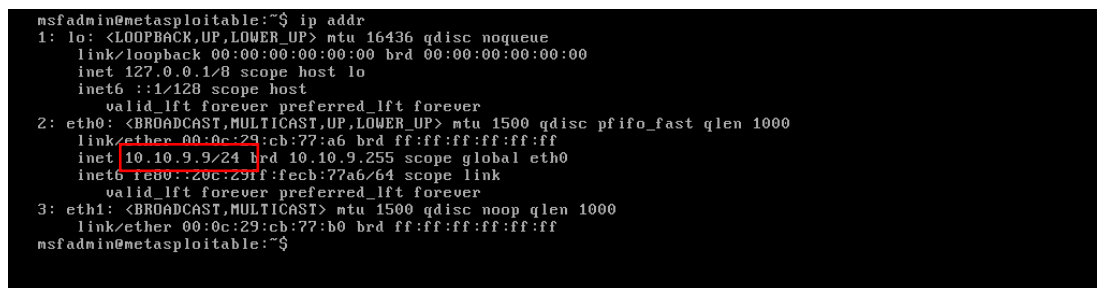


Figure 19:Adresse IP du machine Metasploitable

Donc, comme le montre la figure ci-dessus, l'adresse IP est la suivante : 10.10.9.9. Nous utiliserons cette adresse pour accéder aux services de cette machine à partir d'une autre machine Kali que nous utiliserons ensuite pour lancer l'attaque :

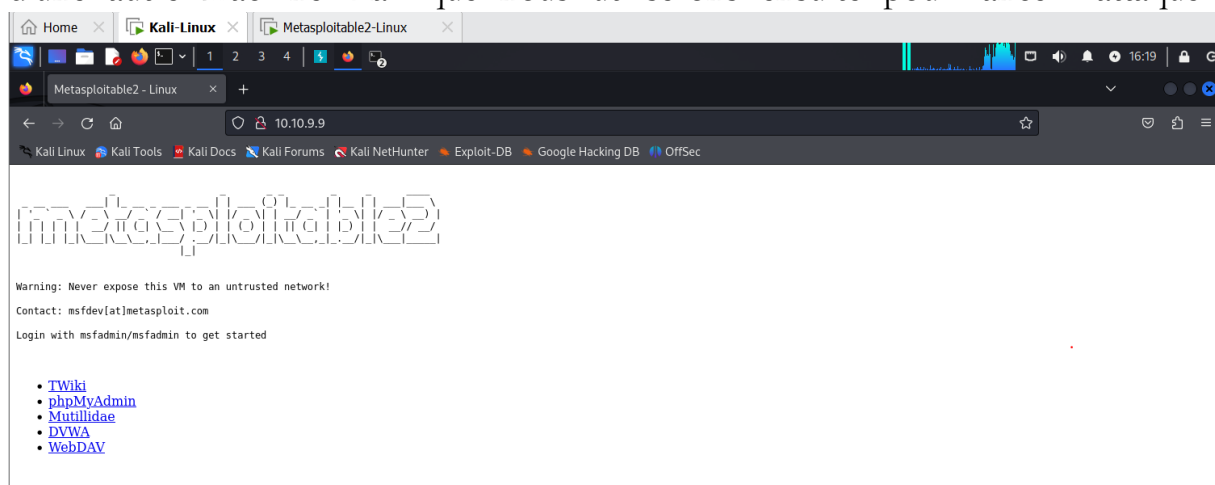


Figure 20:Acces au Metasploitable par Kali Linux

Cette machine nous offre plusieurs environnements de test. Pour notre cas, nous allons choisir DVWA, qui est une application web PHP/MySQL. Son objectif principal est de permettre aux professionnels de la sécurité de tester leurs compétences et leurs outils dans un environnement légal. DVWA, abréviation de "Damn Vulnerable Web Application", simule une application web vulnérable avec différentes failles de sécurité telles que l'injection SQL, la cross-site scripting (XSS), et la falsification de requête intersite (CSRF), permettant ainsi aux utilisateurs de pratiquer la détection et l'exploitation de ces vulnérabilités dans un environnement contrôlé et sécurisé et nous allons admin/password pour se connecter :

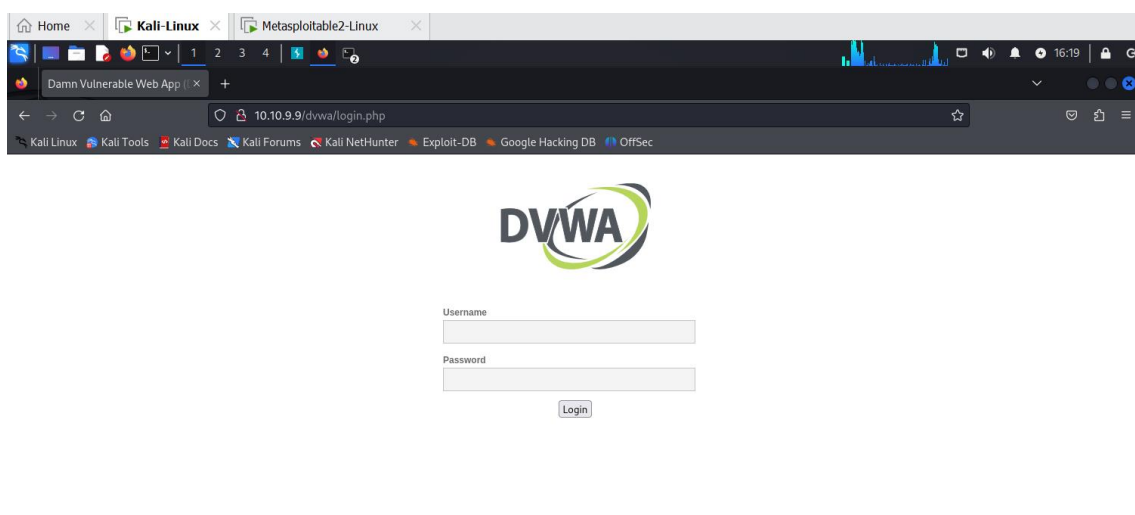


Figure 21:Page de Connexion de DVWA

Après une connexion réussie, cette interface s'affiche :

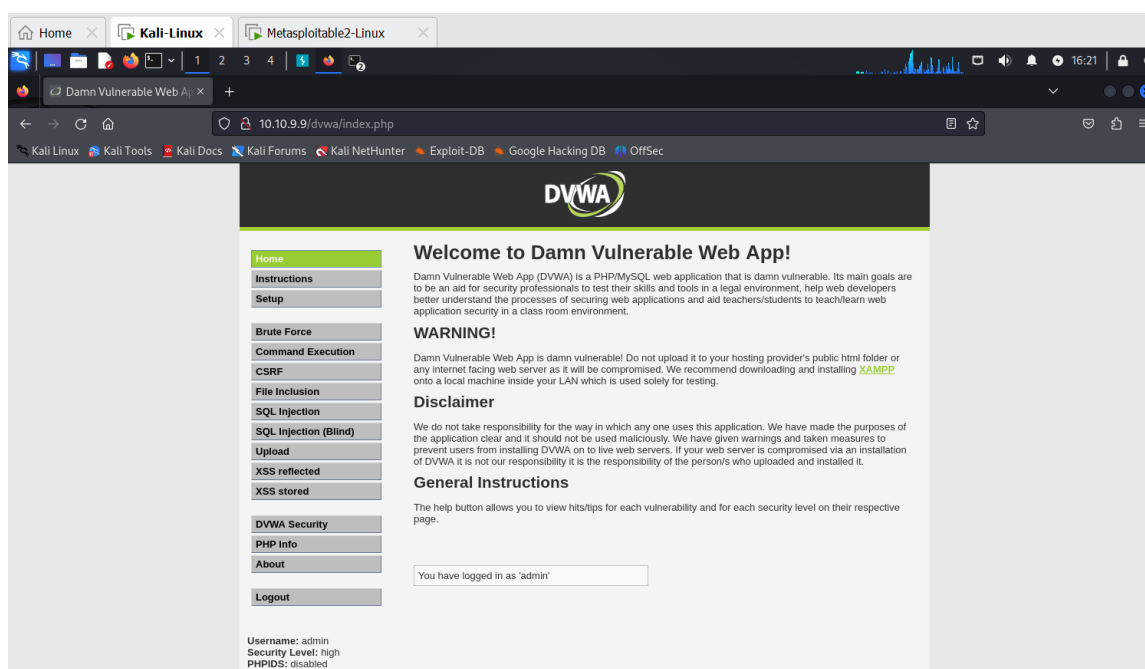


Figure 22:Interface DVWA

Nous allons choisir Brute force et cela va nous conduire vers cette page :

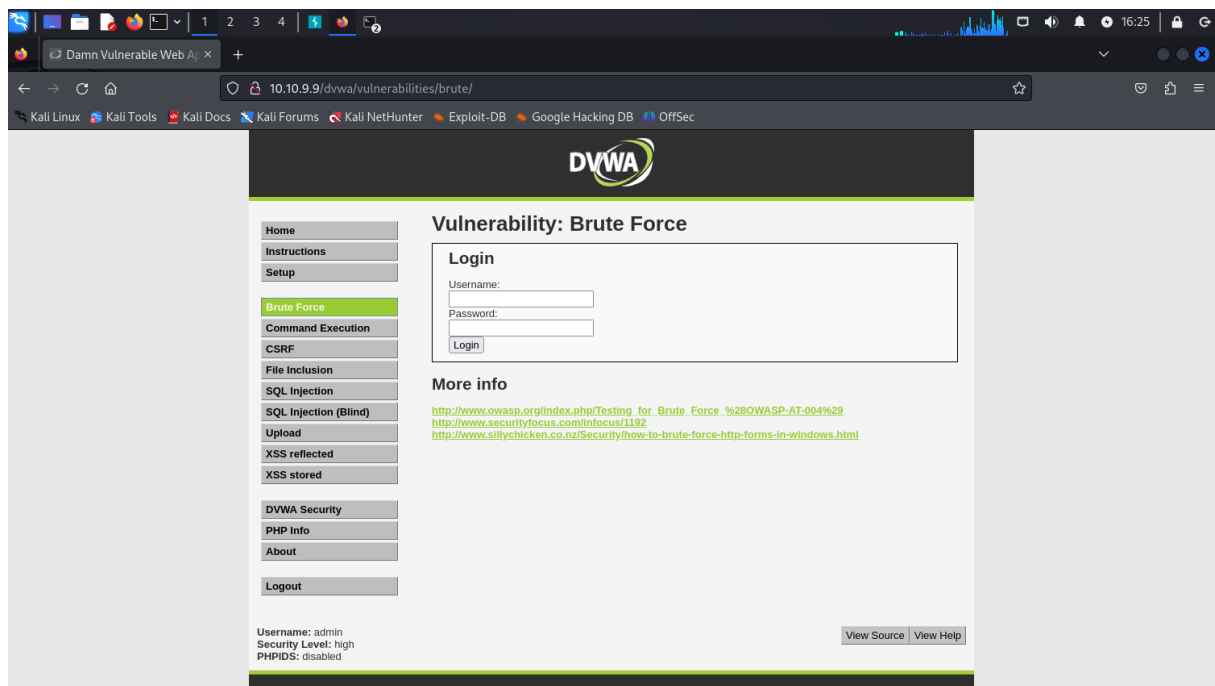


Figure 23:Page Brute Force

Nous allons utiliser "admin/password" comme nom d'utilisateur et mot de passe pour nous connecter :

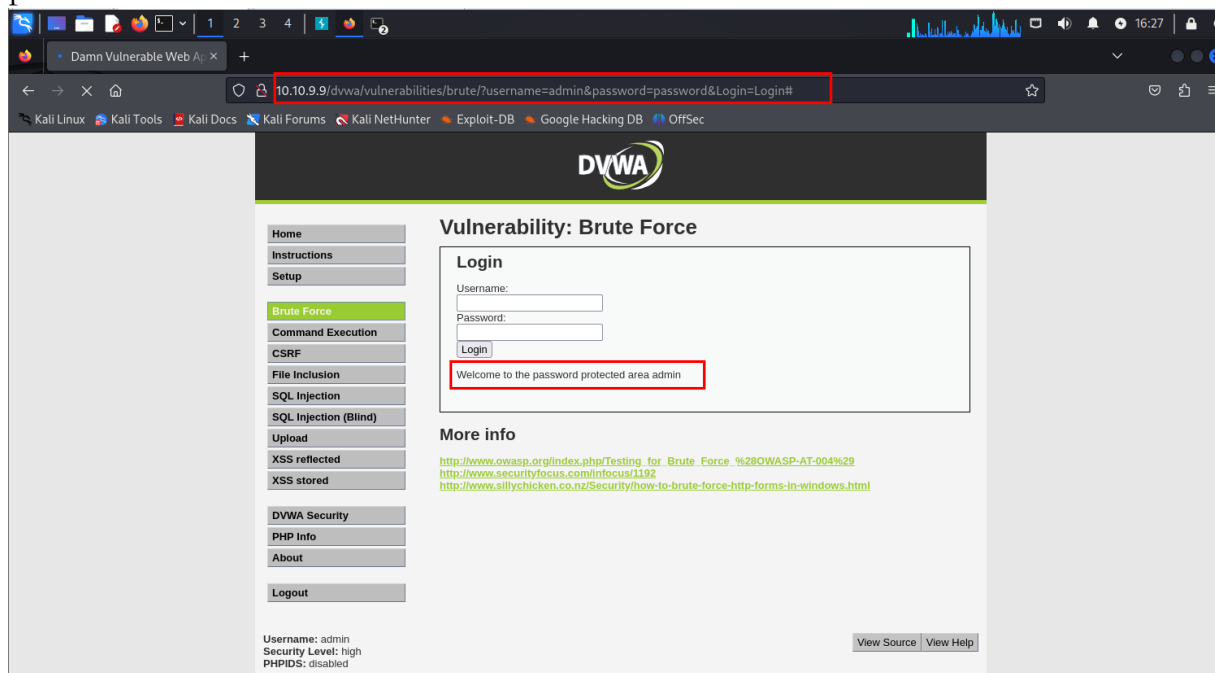


Figure 24:Brute Force login Page

Puis nous lançons burpsuit et nous accédons au proxy :

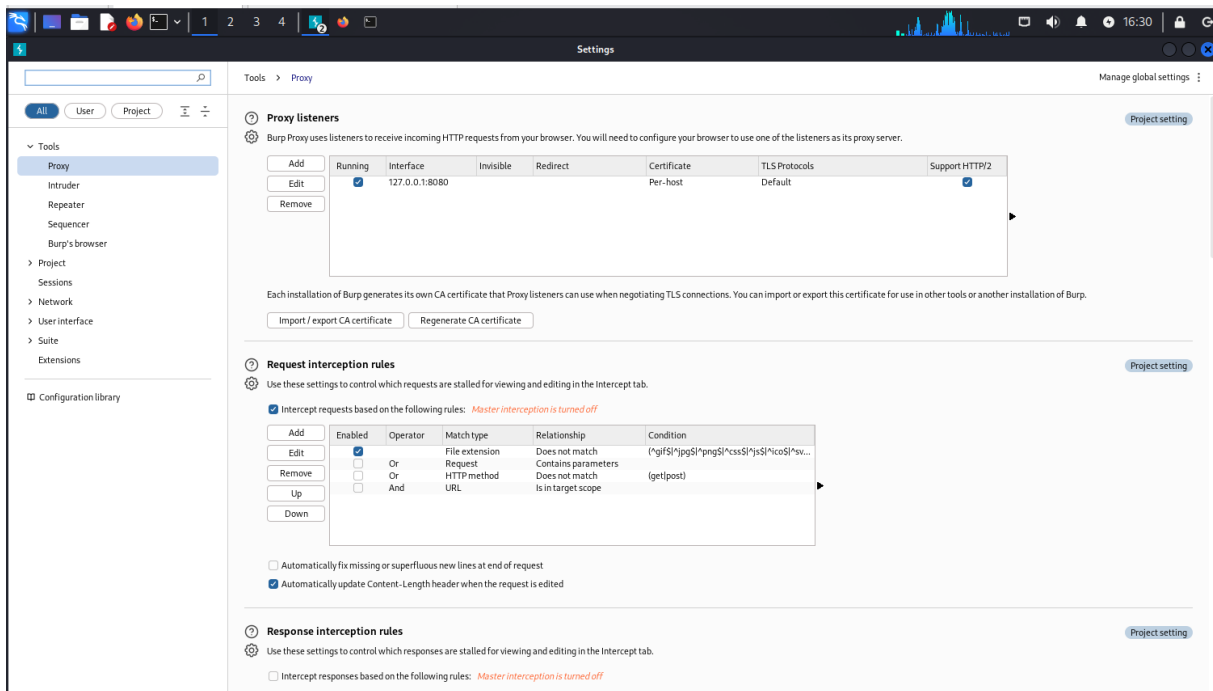


Figure 25:Proxy BurpSuite

Par la suite nous configurons le proxy du browser en se basant sur le proxy de burpsuite :

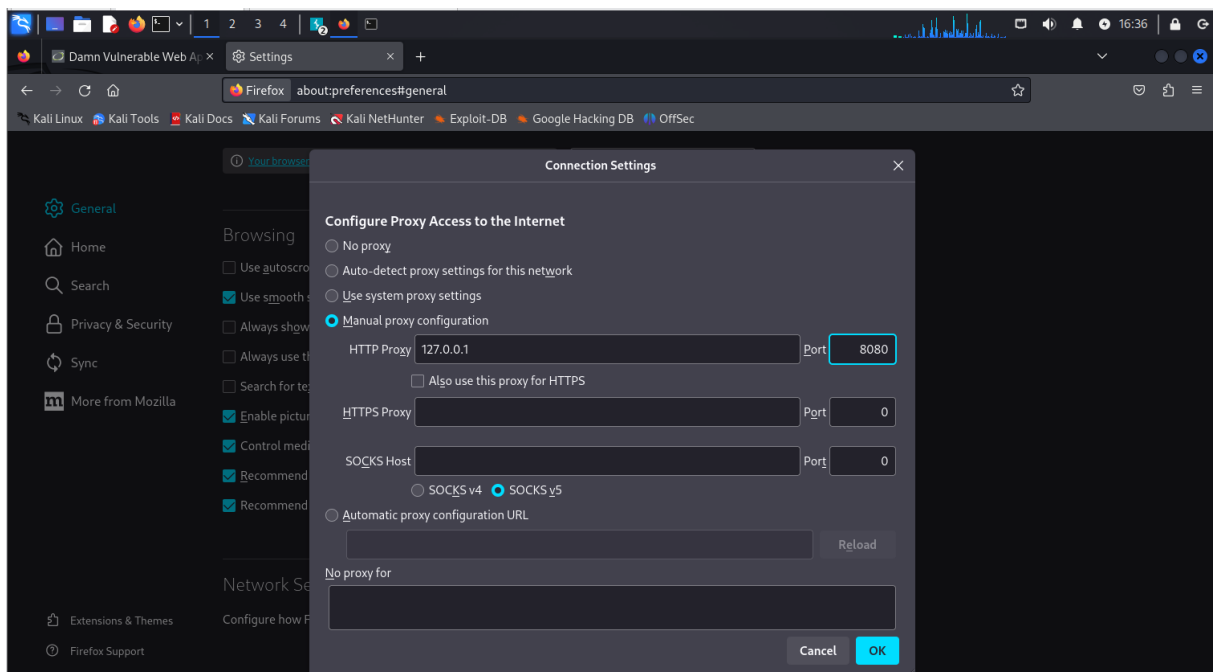


Figure 26:Proxy Navigateur

Après cela, nous activons l'interception dans le proxy de Burp. L'objectif de l'interception est de permettre à l'outil de sécurité (dans ce cas, Burp) de capturer et d'analyser le trafic entre le navigateur et le serveur web. Cela nous permet de manipuler les requêtes et les réponses HTTP, ce qui est utile pour identifier les vulnérabilités et tester la sécurité de l'application web.

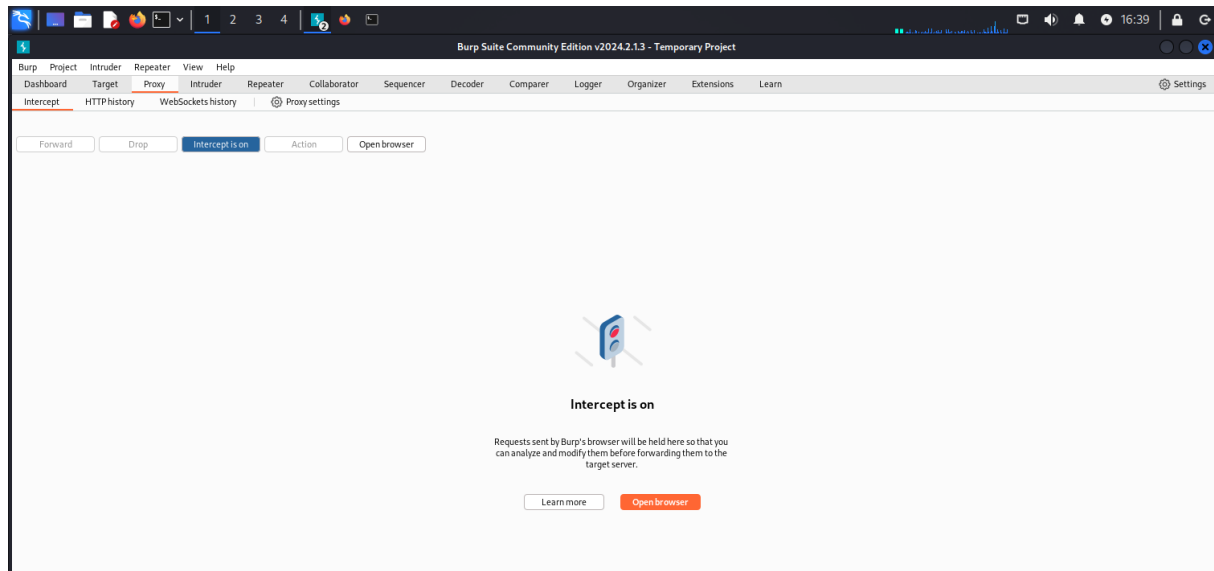


Figure 27:Lancer l'interception

Pour tester cela, nous utilisons des données incorrectes pour nous connecter une nouvelle fois. L'objectif est de capturer et d'analyser le trafic entre le navigateur et le serveur web afin de comprendre comment les données sont échangées et traitées lors des tentatives de connexion.

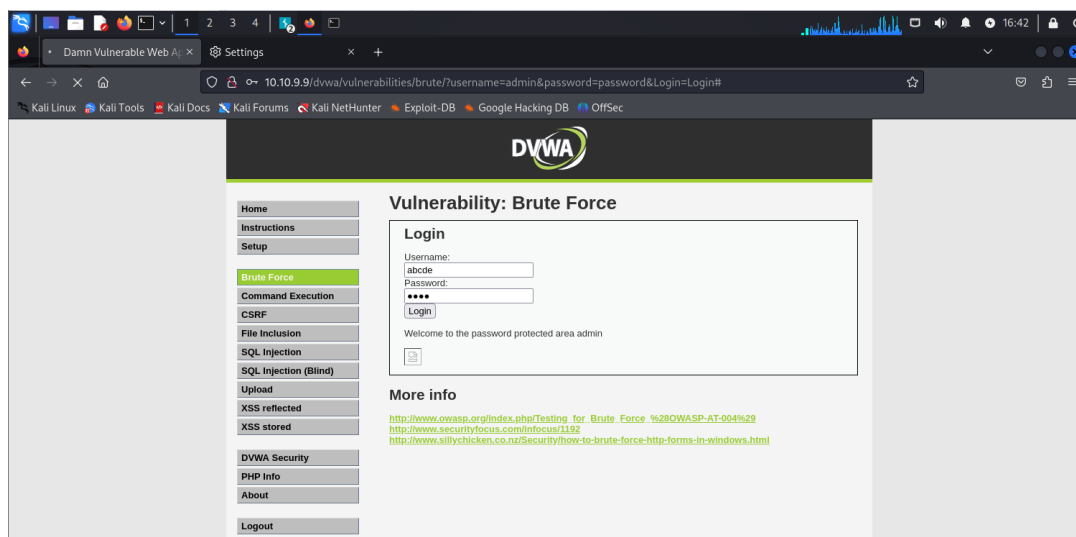


Figure 28:Test connexion



Cela va lancer burpsuite automatiquement qui intercepte et analyse les données échangées entre le navigateur et le serveur web. Il permet de visualiser en détail les requêtes HTTP, y compris la méthode utilisée, l'URL et ses paramètres, ainsi que les en-têtes HTTP et les cookies de session. En scrutant ces données, Burp Suite peut identifier des vulnérabilités potentielles telles que des paramètres de requête mal formés ou des en-têtes exposant des informations sensibles. Grâce à ses outils d'analyse, il offre une inspection approfondie pour détecter toute anomalie ou faiblesse de sécurité.

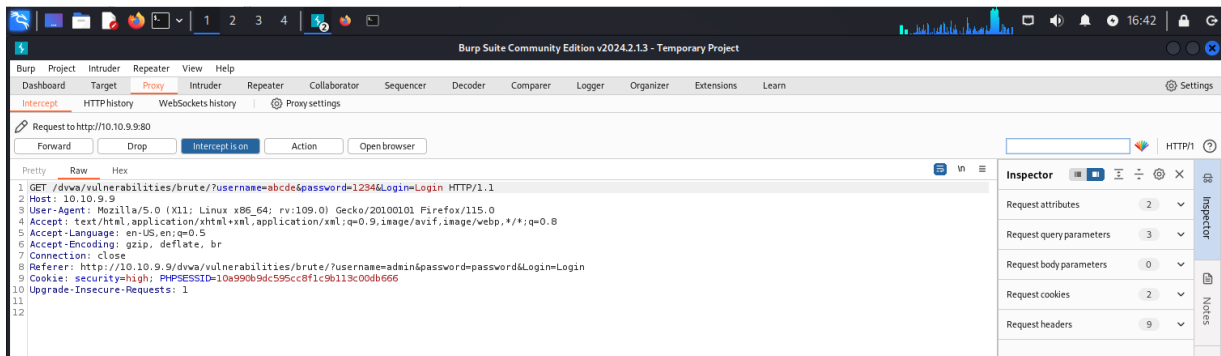
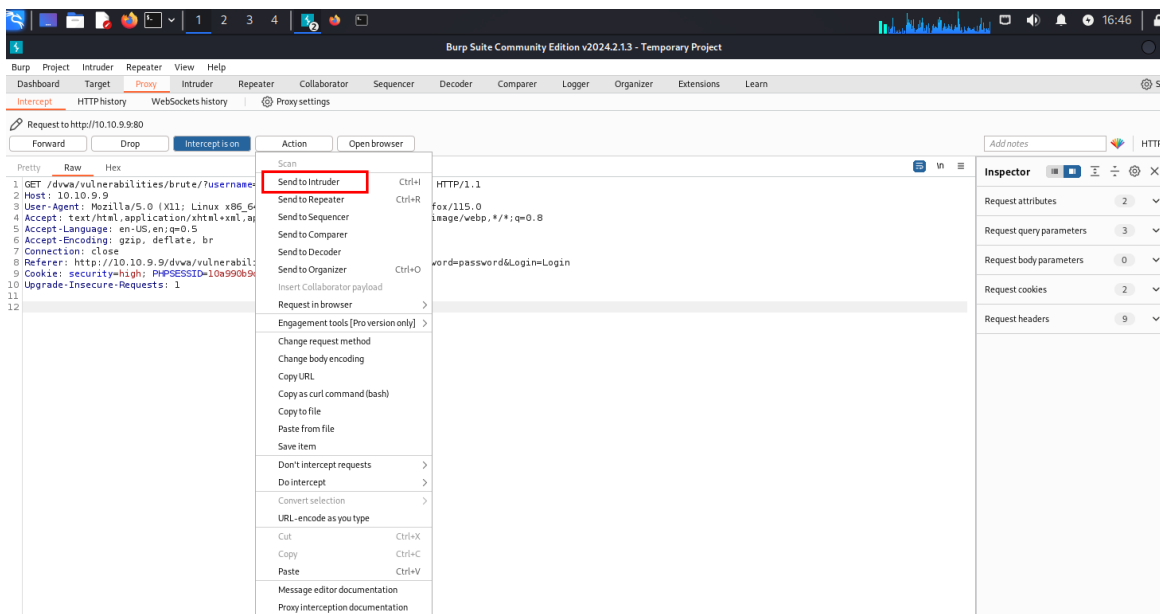


Figure 29:Résultat Intruder

Par la suite, nous utilisons le résultat obtenu et l'envoyons à l'outil Intruder de Burp Suite. Intruder est un outil utilisé dans les tests d'intrusion pour automatiser l'envoi de requêtes HTTP avec différentes données, ce qui permet de repérer les vulnérabilités potentielles. Son rôle principal est d'injecter des charges utiles dans les paramètres de la requête afin de tester la réactivité du serveur et d'identifier d'éventuelles failles de sécurité. En analysant les réponses du serveur à ces requêtes, Intruder nous aide à détecter des comportements anormaux ou des signes de vulnérabilités, ce qui contribue à renforcer la sécurité des applications web.



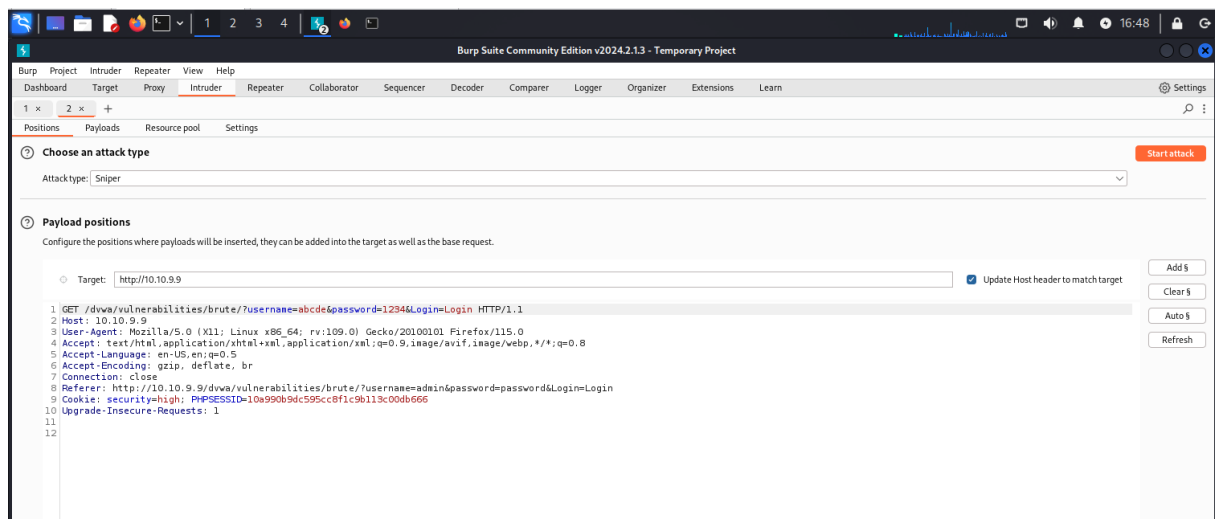


Figure 30:Interface Intruder

Pour lancer l'attaque, nous procédons par étapes. Tout d'abord, nous sélectionnons le type d'attaque, en l'occurrence "Cluster Bomb", ce qui détermine la méthode utilisée pour tester les vulnérabilités. Ensuite, nous utilisons l'option "Clear" pour effacer toutes les annotations existantes associées aux champs "username" et "password", assurant ainsi une base propre pour notre attaque. Enfin, nous ajoutons les champs "username" et "password" comme charges utiles à l'aide de l'option "Add", ce qui permet à l'outil d'Intruder d'envoyer des requêtes avec différentes combinaisons de données pour détecter d'éventuelles failles de sécurité.

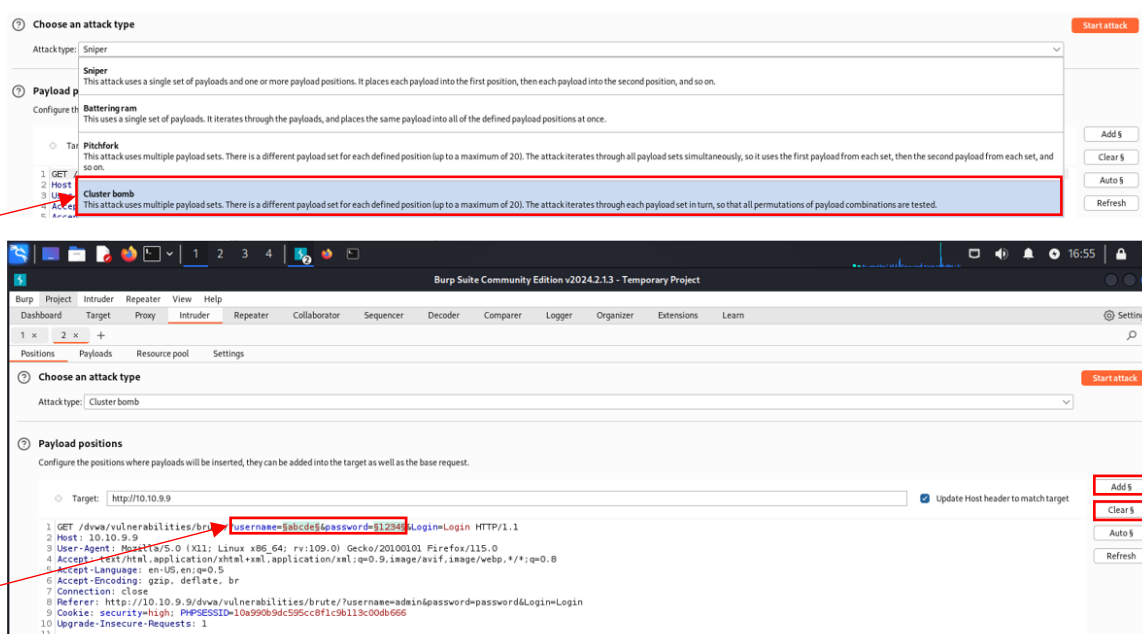


Figure 31:Preparer l'attaque

L'étape avant-dernière et la plus cruciale avant de lancer l'attaque consiste à fournir des charges utiles, c'est-à-dire une liste de mots de passe et de noms d'utilisateurs, qui seront ensuite utilisés par Burp Suite pour effectuer des tentatives d'authentification par force brute. Ces charges utiles sont essentielles car elles déterminent les données que Burp Suite utilisera pour tester la résistance du système aux attaques de force brute. En fournissant une variété de mots de passe et de noms d'utilisateurs, nous augmentons les chances de succès de l'attaque tout en permettant à Burp Suite d'explorer différentes combinaisons pour tenter de compromettre la sécurité du système ciblé.

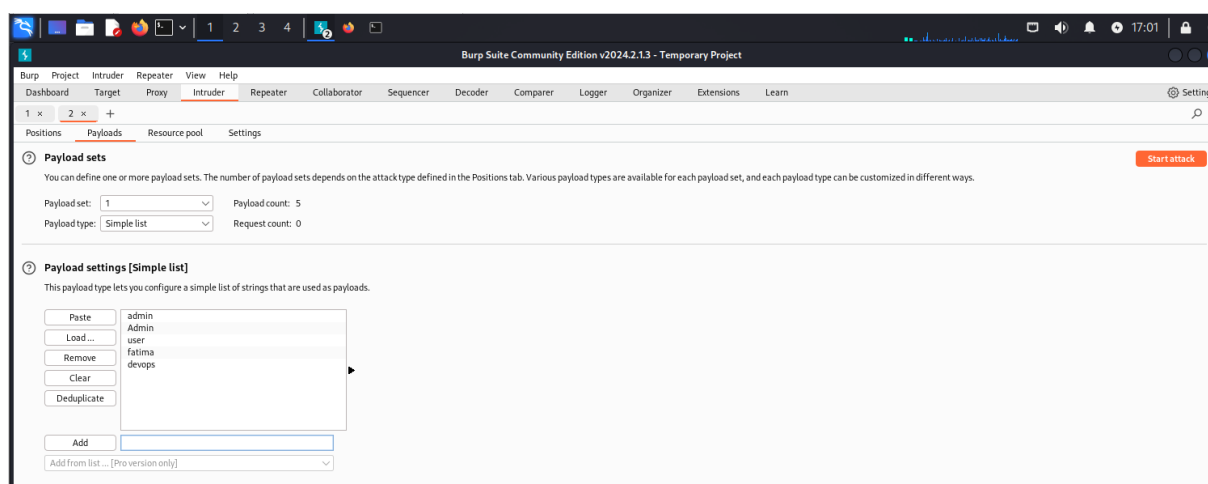


Figure 32:payload username

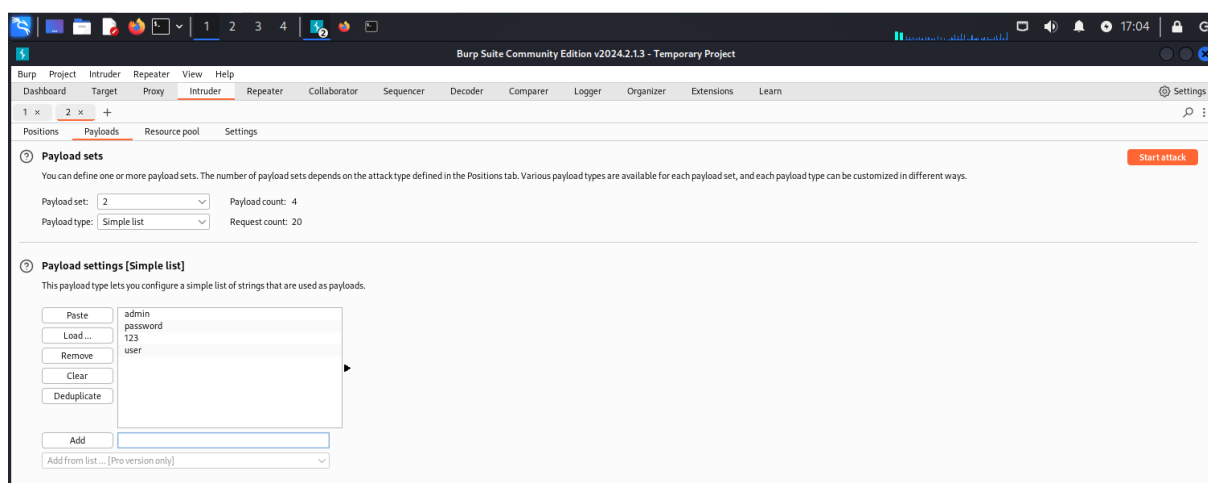
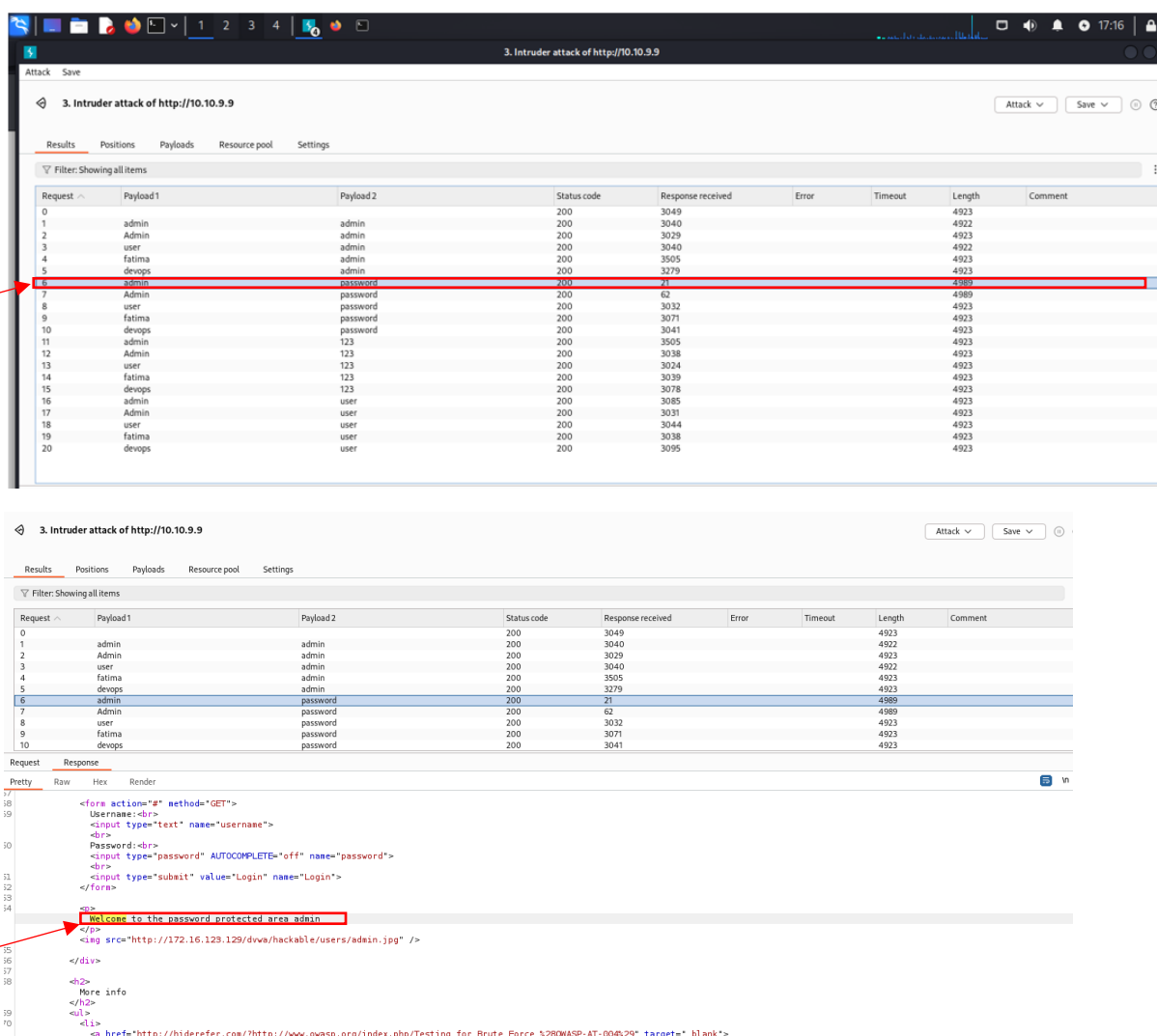


Figure 33:payload password

Enfin on lance l'attaque :

Start attack

Une fois que Burp Suite a exécuté l'attaque en utilisant les charges utiles fournies, il génère un ensemble de résultats révélant les tentatives d'authentification par force brute qui ont réussi. Ces résultats incluent une liste des combinaisons de noms d'utilisateur et de mots de passe qui ont été validées par le système cible. Burp Suite identifie ces combinaisons réussies en analysant les réponses du serveur. Pour déterminer la combinaison correcte, Burp Suite utilise deux critères : d'abord, il examine le code de statut de la réponse reçue, qui est 21 pour la combinaison correcte et environ 3000 pour les autres combinaisons. Ensuite, il recherche un message spécifique dans la réponse de la requête : "welcome to protected password area admin", qui n'apparaît que pour la combinaison correcte. Ces indices permettent de repérer les informations d'identification valides et de signaler les vulnérabilités de sécurité.



3. Intruder attack of http://10.10.9.9

Attack Save

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
0			200	3049			4923	
1	admin	admin	200	3040			4922	
2	Admin	admin	200	3029			4923	
3	user	admin	200	3040			4922	
4	fatima	admin	200	3505			4923	
5	devops	admin	200	3279			4923	
6	admin	password	200	21			4989	
7	Admin	password	200	62			4989	
8	user	password	200	3032			4923	
9	fatima	password	200	3071			4923	
10	devops	password	200	3041			4923	
11	admin	123	200	3505			4923	
12	Admin	123	200	3038			4923	
13	user	123	200	3038			4923	
14	fatima	123	200	3039			4923	
15	devops	123	200	3078			4923	
16	admin	user	200	3085			4923	
17	Admin	user	200	3031			4923	
18	user	user	200	3044			4923	
19	fatima	user	200	3038			4923	
20	devops	user	200	3095			4923	

3. Intruder attack of http://10.10.9.9

Attack Save

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
0			200	3049			4923	
1	admin	admin	200	3040			4922	
2	Admin	admin	200	3029			4923	
3	user	admin	200	3040			4922	
4	fatima	admin	200	3505			4923	
5	devops	admin	200	3279			4923	
6	admin	password	200	21			4989	
7	Admin	password	200	62			4989	
8	user	password	200	3032			4923	
9	fatima	password	200	3071			4923	
10	devops	password	200	3041			4923	

Request Response

Pretty Raw Hex Render

```

17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
217
```

## B. Détection de l'attaque:

Pour la phase de détection, nous allons utiliser l'outil Wazuh, une puissante plateforme de surveillance de sécurité open source. Pour commencer, nous allons installer d'abord l'Agent Wazuh en utilisant la commande suivante :

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7
```

Après l'installation, nous devons exécuter les commandes suivantes pour le lancer :

```
sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
```

Pour une configuration plus rapide, nous allons utiliser le fichier OVA du serveur Wazuh, pré-construit et pouvant être facilement importé dans des logiciels de virtualisation tels que VirtualBox ou VMware. Pour que l'agent Wazuh puisse communiquer avec le serveur, nous devons attribuer une adresse IP ou un nom de domaine complet (FQDN) à notre serveur gestionnaire Wazuh, accessible depuis le réseau où l'agent est installé.

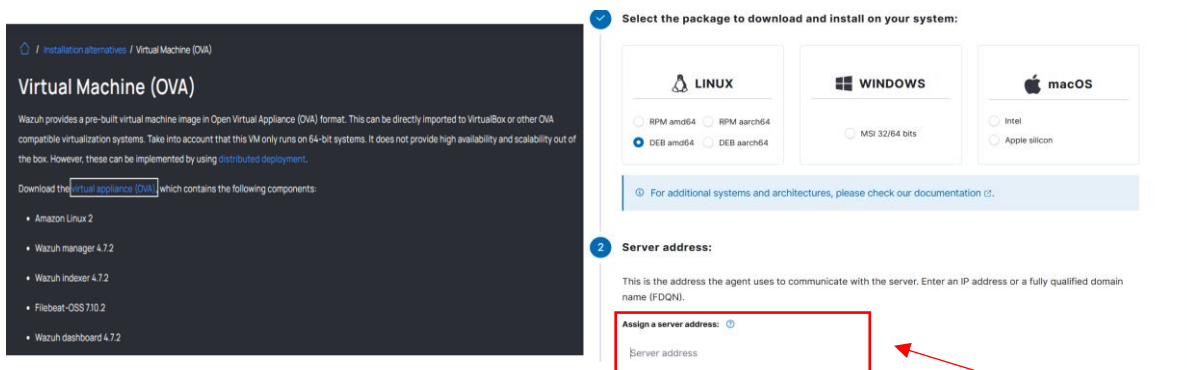


Figure 35:Installation de Wazuh

Pour lancer Wazuh nous utilisons la commande suivante :

```
sudo systemctl start wazuh-agent
```

Et nous obtenons l'interface suivante :

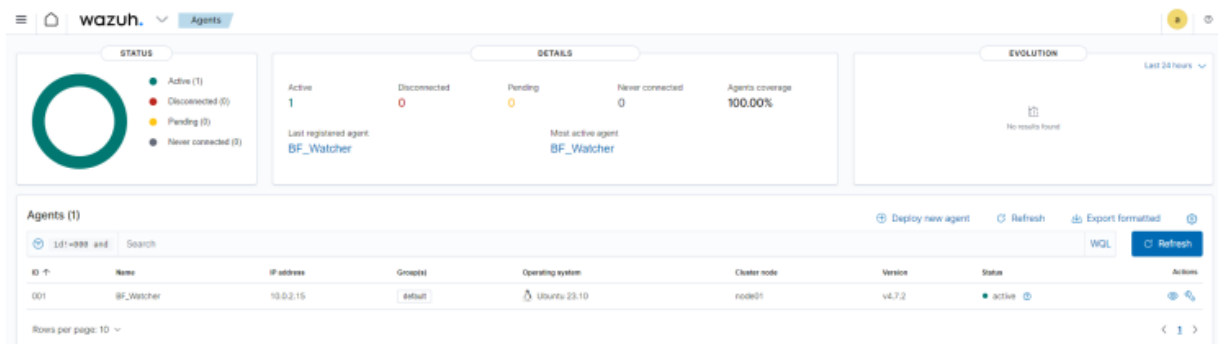


Figure 36:Activation du Wazuh

Maintenant, afin de tester la capacité de détection d'actions malveillantes par Wazuh, nous avons rapidement lancé une fois de plus une attaque par force brute, mais cette fois-ci avec l'outil OpenBullet 2 car il est plus rapide que DVWA et BurpSuite.

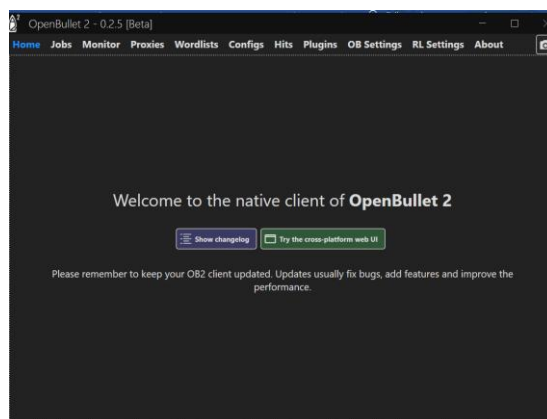


Figure 37:Interface du OpenBullet 2

Ainsi, pour la première fois, nous utilisons une adresse IP statique : 72.10.160.171 pour lancer l'attaque, comme le montre la figure 38 :

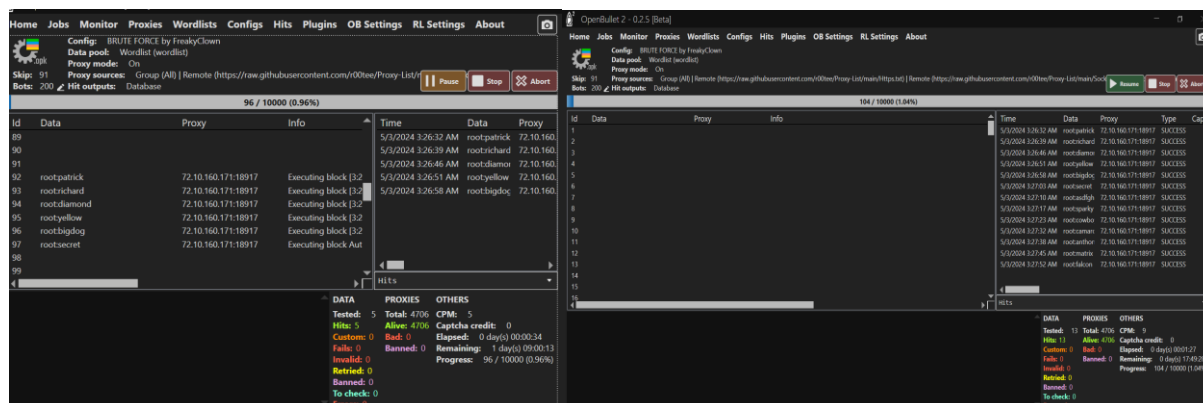


Figure 38:Résultat d'attaque

Cependant, Wazuh a réussi à détecter la tentative malveillante d'accès que nous étions en train de lancer.

>	May 3, 2024 @ 04:02:16.790	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: authentication failed.	5	5760
>	May 3, 2024 @ 04:02:08.782	T1110.001 T1021.004	Credential Access, Lateral Movement	sshd: authentication failed.	5	5760

Figure 39:Detection d'attaque

Due à ceci Wazuh a mis en évidence par un nombre élevé d'alertes générées, principalement dues à des échecs d'authentification. Cette activité, couplée à la nature des alertes, suggère fortement qu'une attaque par force brute a été tentée



Figure 40 : Analyse des événements de sécurité Wazuh

Cette fois-ci, nous allons relancer l'attaque mais en utilisant une adresse IP dynamique , ce qui signifie qu'elle pouvait varier au cours de l'attaque :

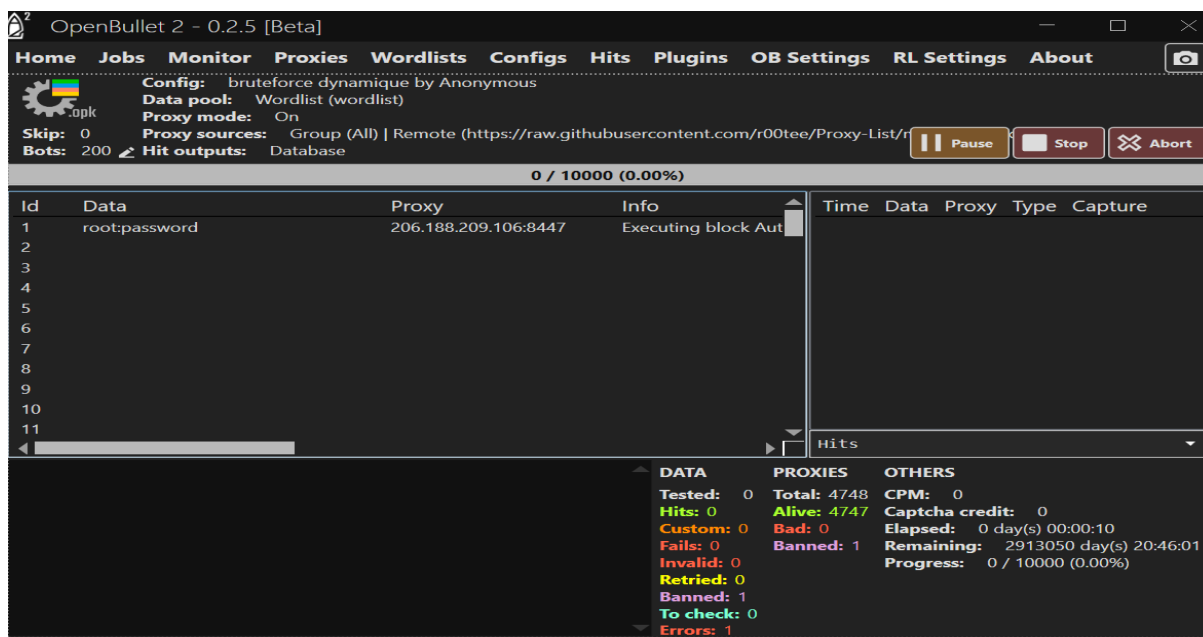


Figure 41 : lancement d'attaque avec une adresse IP dynamique

En utilisant encore une fois Wazhu pour analyser les journaux d'activité et les événements réseau, nous avons pu identifier les tentatives de connexion suspectes provenant de différentes adresses IP dynamiques. Suite à cette détection, des mesures immédiates ont été prises pour bloquer les adresses IP sources de l'attaque et renforcer la sécurité de nos systèmes. Des actions correctives ont également été envisagées pour améliorer la résilience de notre infrastructure contre de telles attaques à l'avenir :

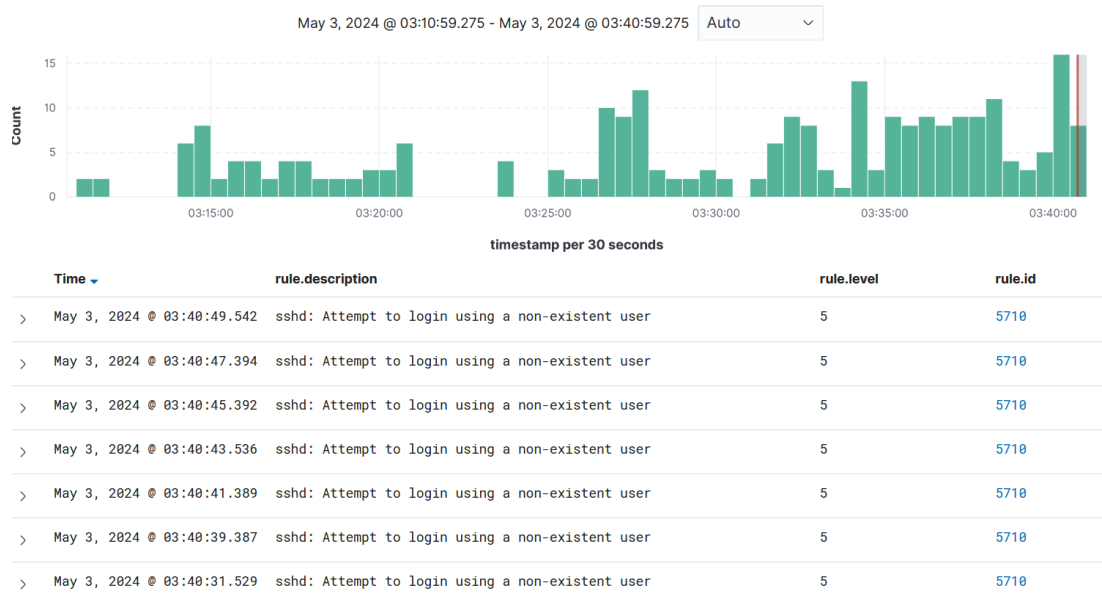


Figure 42 : Détection des attaques avec Wazuh

En intégrant des outils de détection avancée comme Wazuh dans notre infrastructure, nous renforçons notre capacité à protéger efficacement nos actifs numériques contre les attaques malveillantes.

C. Prévention de L'attaque :

La dernière phase est consacrée à la prévention, et pour ce faire, nous allons utiliser l'outil Fail2ban. Pour ce faire, nous allons tout d'abord commencer par l'installation de l'outil Fail2ban en utilisant la commande suivante :**sudo apt-get install fail2ban** , puis nous allons créer le fichier de configuration pour DVWA dans le répertoire /etc/fail2ban/filter.d/ en utilisant la commande suivante : **sudo nano /etc/fail2ban/filter.d/dvwa.conf**. Ensuite, nous allons ajouter les règles suivantes dans ce fichier :

```
[Definition]
failregex = ^<HOST> -.*)"POST /vulnerabilities/brute/\?username=.*HTTP/1\..1" 200 .*$
```

Figure 35:configuration 1 du fail2ban



Les règles établies dans le fichier de configuration, définissent un motif de recherche dans les journaux pour détecter les tentatives de connexion brute force. L'expression `^<HOST>` permet de capturer l'adresse IP de l'hôte effectuant la connexion, tandis que `-.*"POST /vulnerabilities/brute/\?username=.*HTTP/1\1"` recherche une requête POST vers une URL spécifique de DVWA avec un paramètre de nom d'utilisateur. La présence du code **200** vérifie que la réponse du serveur à cette requête était un code HTTP 200, indiquant le succès de la requête. En somme, ces règles spécifient les critères permettant d'identifier les tentatives de connexion brute force en recherchant des requêtes POST spécifiques dans les journaux, sans spécifier de motif à ignorer.

Puis nous passons pour configurer le jail DVWA dans Fail2Ban, nous ajoutons des règles spécifiques dans le fichier de configuration des jails. Un jail est une section de configuration dédiée à surveiller et à agir sur un service ou une application spécifique. En définissant ces règles, Fail2Ban peut détecter et répondre aux tentatives de connexion malveillantes sur DVWA. Cela se fait en utilisant cette commande

```
sudo nano /etc/fail2ban/jail.conf
```

```
[dvwa]
enabled = true
filter = dvwa
action = iptables-multiport[name=dvwa, port="http,https", protocol=tcp]
logpath = /var/log/apache2/access.log
maxretry = 3
findtime = 600
bantime = 3600
```

Figure 36:configuration 2 fail2ban

Ces règles permettent d'activer le jail DVWA (**enabled = true**), de spécifier le filtre à utiliser pour l'analyse des journaux (**filter = dvwa**), et de configurer une action pour bloquer les adresses IP attaquantes sur les ports HTTP et HTTPS en cas de détection d'une activité malveillante. Les journaux d'accès Apache sont surveillés à l'emplacement `/var/log/apache2/access.log`. De plus, le nombre maximal de tentatives infructueuses est limité à 3 avant de bloquer l'adresse IP pour une durée définie (**maxretry = 3, bantime = 3600**). En résumé, le jail DVWA est conçu pour bloquer les adresses IP tentant de se connecter de manière malveillante à DVWA, en limitant les tentatives infructueuses et en appliquant un blocage temporaire. Ces règles spécifiques aident à identifier les tentatives de connexion brute force en recherchant des requêtes POST dans les journaux et en vérifiant la réponse du serveur HTTP.

Enfin, pour tester la capacité de Fail2Ban à prévenir les actions malveillantes, nous avons relancé l'attaque avec DVWA et BurpSuite, comme expliqué précédemment dans la section "Initiation à l'attaque". Voici les résultats obtenus :

Attack Save Columns

4. Intruder attack of http://127.0.0.1

Attack Save Columns

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Requ...	Payload 1	Payload 2	Status code	Error	Redire...	Timeout	Length	incorr...	3207	Comment
0			200	<input type="checkbox"/>	1	<input type="checkbox"/>	4734	1	e='hidden' name='use...	
1	1234567		200	<input type="checkbox"/>	1	<input type="checkbox"/>	4734	1	e='hidden' name='use...	
2	12345678	e='hidden' name='user_toke...	200	<input type="checkbox"/>	1	<input type="checkbox"/>	4734	1	e='hidden' name='use...	
3	123abc	e='hidden' name='user_toke...	200	<input type="checkbox"/>	1	<input type="checkbox"/>	4734	1	e='hidden' name='use...	
4	Admin	e='hidden' name='user_toke...	200	<input type="checkbox"/>	1	<input type="checkbox"/>	4734	1	e='hidden' name='use...	
5	admin	e='hidden' name='user_toke...	200	<input type="checkbox"/>	1	<input type="checkbox"/>	4734	1	e='hidden' name='use...	
6	pass	e='hidden' name='user_toke...	200	<input type="checkbox"/>	1	<input type="checkbox"/>	4734	1	e='hidden' name='use...	
7	password	e='hidden' name='user_toke...	200	<input type="checkbox"/>	1	<input type="checkbox"/>	4734	1	e='hidden' name='use...	
8	P@ssword	e='hidden' name='user_toke...	200	<input type="checkbox"/>	1	<input type="checkbox"/>	4734	1	e='hidden' name='use...	
9	backup	e='hidden' name='user_toke...	200	<input type="checkbox"/>	1	<input type="checkbox"/>	4734	1	e='hidden' name='use...	
10	backupexec	e='hidden' name='user_toke...	200	<input type="checkbox"/>	1	<input type="checkbox"/>	4734	1	e='hidden' name='use...	
11	changeme	e='hidden' name='user_toke...	200	<input type="checkbox"/>	1	<input type="checkbox"/>	4734	1	e='hidden' name='use...	
12	cluster	e='hidden' name='user_toke...	200	<input type="checkbox"/>	1	<input type="checkbox"/>	4734	1	e='hidden' name='use...	
13	clustadm	e='hidden' name='user_toke...	200	<input type="checkbox"/>	1	<input type="checkbox"/>	4734	1	e='hidden' name='use...	
14	compaq	e='hidden' name='user_toke...	200	<input type="checkbox"/>	1	<input type="checkbox"/>	4734	1	e='hidden' name='use...	
15	default	e='hidden' name='user_toke...	200	<input type="checkbox"/>	1	<input type="checkbox"/>	4734	1	e='hidden' name='use...	
16	del1	e='hidden' name='user_toke...	200	<input type="checkbox"/>	1	<input type="checkbox"/>	4734	1	e='hidden' name='use...	
17	dmz	e='hidden' name='user_toke...	200	<input type="checkbox"/>	1	<input type="checkbox"/>	4734	1	e='hidden' name='use...	
18	domina	e='hidden' name='user_toke...	200	<input type="checkbox"/>	1	<input type="checkbox"/>	4734	1	e='hidden' name='use...	
19	exchange	e='hidden' name='user_toke...	200	<input type="checkbox"/>	1	<input type="checkbox"/>	4734	1	e='hidden' name='use...	
20	guest	e='hidden' name='user_toke...	200	<input type="checkbox"/>	1	<input type="checkbox"/>	4734	1	e='hidden' name='use...	
21	office	e='hidden' name='user_toke...	200	<input type="checkbox"/>	1	<input type="checkbox"/>	4734	1	e='hidden' name='use...	

Finished

Figure 37: resultat Fail2ban

On remarque que l'attaque a échoué, car elle n'a pas pu détecter le mot de passe, qui est "password". Ainsi, Fail2Ban a prouvé son efficacité dans la protection du DVWA contre les attaques par force brute grâce à la configuration préalablement fournie.

En incorporant des outils de prévention avancée tels que Fail2ban dans notre infrastructure, nous renforçons notre capacité à protéger de manière proactive nos actifs numériques contre les attaques malveillantes.

#### D. Conclusion

En résumé, notre expérience d'attaque brute force contre DVWA, utilisant BurpSuite pour l'attaque, Wazuh pour la détection et Fail2ban pour la prévention, souligne l'importance cruciale de ces outils dans la sécurisation de nos systèmes contre les menaces.

## Conclusion Général:

En guise de synthèse, ce rapport offre une vision holistique du paysage des attaques par mots de passe. En retraçant leur évolution historique et en examinant leurs origines, nous avons mis en lumière les défis auxquels les systèmes informatiques sont confrontés en matière de sécurité. À travers l'identification des types d'attaques les plus répandus et des outils utilisés par les attaquants, nous avons souligné l'importance d'une vigilance constante pour contrer ces menaces. De plus, en réalisant des simulations et des études de cas, nous avons illustré de manière concrète les conséquences potentielles de telles attaques sur les organisations et les individus.

Dans le but de renforcer la résilience des systèmes et de protéger les données sensibles, nous avons proposé un ensemble de précautions et de meilleures pratiques à suivre. Celles-ci vont de l'adoption de politiques de gestion des mots de passe robustes à la mise en place de solutions de gestion des identités et des accès. En intégrant ces mesures dans une approche globale de la sécurité informatique, il est possible de réduire les vulnérabilités et de garantir l'intégrité, la confidentialité et la disponibilité des informations cruciales.

## Références :

- [1] M. Raza, M. Iqbal, M. Sharif, et W. Haider, « A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication », 2012.
- [2] B. Al-Sharaa et S. Thuneibat, « Ethical hacking: real evaluation model of brute force attacks in password cracking », *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 33, p. 1653, mars 2024, doi: 10.11591/ijeecs.v33.i3.pp1653-1659.
- [3] « (PDF) Phishing and Countermeasures in Spanish Online Banking ». Consulté le: 13 avril 2024. [En ligne]. Disponible sur: [https://www.researchgate.net/publication/41043220\\_Phishing\\_and\\_Countermeasures\\_in\\_Spanish\\_Online\\_Banking](https://www.researchgate.net/publication/41043220_Phishing_and_Countermeasures_in_Spanish_Online_Banking)
- [4] P. Kapoor, P. Agrawal, et A. D, « ANALYZING PASSWORD DECRYPTION TECHNIQUES USING DICTIONARY ATTACK », *International Journal of Advanced Research*, vol. 9, p. 515-523, août 2021, doi: 10.21474/IJAR01/13299.
- [5] L. Zhang, C. Tan, et F. Yu, « An Improved Rainbow Table Attack for Long Passwords », *Procedia Computer Science*, vol. 107, p. 47-52, janv. 2017, doi: 10.1016/j.procs.2017.03.054.
- [6] A. K. Singh et A. K. Misra, « Analysis of Cryptographically Replay Attacks and Its Mitigation Mechanism », in *Proceedings of the International Conference on Information Systems Design and Intelligent Applications 2012 (INDIA 2012) held in Visakhapatnam, India, January 2012*, S. C. Satapathy, P. S. Avadhani, et A. Abraham, Éd., Berlin, Heidelberg: Springer, 2012, p. 787-794. doi: 10.1007/978-3-642-27443-5\_90.
- [7] Samsoni *et al.*, « Keylogger Threats in Computer Security Aspects », *International Journal of Integrative Sciences*, vol. 2, p. 867-872, juin 2023, doi: 10.55927/ijis.v2i6.4520.
- [8] « Bureau of Internet and Technology Business Guide f.pdf ». Consulté le: 14 avril 2024. [En ligne]. Disponible sur: <https://ag.ny.gov/sites/default/files/businessguidecredentialstuffingattacks.pdf>