

HkZ Audit



Rapport de pentest

I. Introduction

Un test d'intrusion sur serveur, également connu sous le nom de pentest, est un processus qui vise à identifier les vulnérabilités dans un système informatique ou un réseau cible. Il est réalisé par des experts en sécurité informatique pour simuler une attaque réelle et évaluer la capacité du système à résister aux menaces. Le but final est de fournir une analyse complète et détaillée des risques et des vulnérabilités identifiées, ainsi que des recommandations pour les corriger.

Il est important de noter que les résultats de ce test sont valides uniquement à la date indiquée sur la couverture et peuvent ne pas refléter les menaces et vulnérabilités actuelles.

Un test d'intrusion a été réalisé sur un serveur de l'Université Nice Côte d'Azur en respectant le contrat signé entre le prestataire de ce test et l'Université en date du 18 janvier 2023. L'objectif de ce test était d'évaluer le niveau de sécurité mis en place sur un serveur et de découvrir les vulnérabilités potentielles. Les menaces et les risques présents ont également été identifiés. Les résultats et les recommandations présentés dans ce rapport devraient aider l'Université Nice Côte d'Azur à améliorer la sécurité de son serveur.

II. Méthodologie du pentest

Le test d'intrusion a été mené à Sophia-Antipolis sur un serveur de l'IUT Nice Côte d'Azur dont l'adresse IP est 134.59.139.251. Nous avons collecté des informations publiques sur le serveur, grâce à des logiciels et aux résultats de recherche "Google Dorks", et avons utilisé des outils de scan tels que Nmap, Hydra et Burp Suite pour évaluer les vulnérabilités présentes. Les résultats de ces analyses sont présentés dans la section suivante, ainsi que les recommandations techniques pour corriger les faiblesses identifiées.

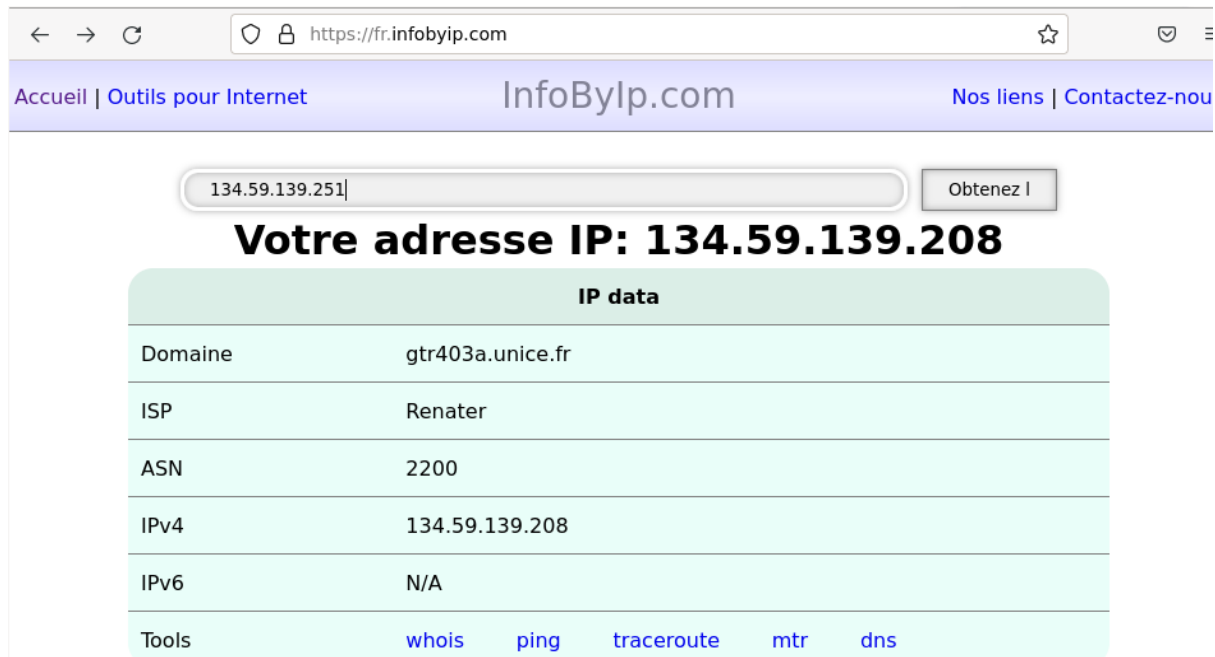
1) Collecte d'informations accessible en public

La collecte d'informations publiques est un élément clé de tout test d'intrusion (pentest). Cette phase consiste à recueillir des informations sur la cible avant de commencer l'attaque réelle. Cela peut inclure des informations sur les systèmes utilisés, les protocoles réseau, les utilisateurs et les groupes, les configurations de sécurité, les vulnérabilités connues et bien plus encore. Ces informations peuvent être obtenues à partir de sources publiques telles que les sites Web, les réseaux sociaux, les annuaires d'entreprises, les bases de données et les

registres de domaine. Google Dorks sont des méthodes pour utiliser les fonctionnalités avancées de recherche de Google pour trouver des informations sensibles qui sont exposées publiquement sur internet. La collecte d'informations publiques est cruciale pour planifier et cibler efficacement l'attaque, car elle permet aux pentesters de comprendre les forces et les faiblesses de la cible, ce qui leur permet de maximiser leur impact.

Nous allons commencer notre pentest en effectuant une collecte d'informations publiques, en utilisant des outils tels que des sites spécialisés dans la recherche d'informations uniquement grâce à une adresse IP ou les "google dorks" pour recueillir des données sur la cible avant de passer à l'analyse plus approfondie de la sécurité.

J'ai utilisé le site <https://fr.infobyip.com/> pour avoir des premières informations générales sur la cible. On trouve ici le nom de domaine associé à l'adresse : « gtr403a.unice.fr », son ISP (fournisseur d'accès à Internet) : « Renater », une adresse ip « 134.59.139.208 ».

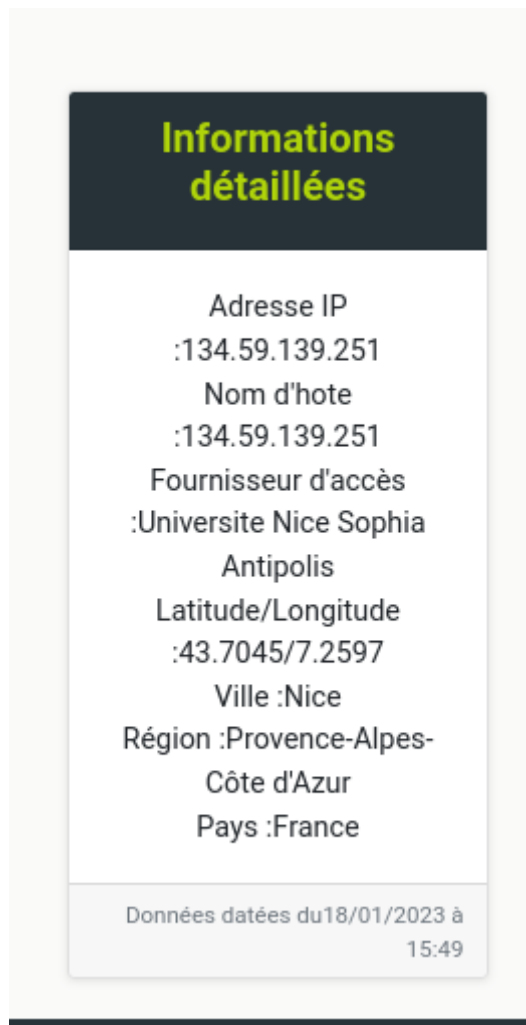


The screenshot shows the InfoByIp.com website interface. At the top, there's a navigation bar with 'Accueil | Outils pour Internet' on the left, 'InfoByIp.com' in the center, and 'Nos liens | Contactez-nous' on the right. Below the navigation bar, there's a search input field containing '134.59.139.251' and a button labeled 'Obtenez l'. Below the search field, the text 'Votre adresse IP: 134.59.139.208' is displayed in large, bold letters. Underneath, there's a table titled 'IP data' with the following information:

IP data	
Domaine	gtr403a.unice.fr
ISP	Renater
ASN	2200
IPv4	134.59.139.208
IPv6	N/A
Tools	whois ping traceroute mtr dns

On va utiliser un autre site, <https://www.monippublique.com/infossurip.html> pour confirmer ces informations et en avoir d'autres :

On trouve comme fournisseur d'accès internet une université « Université Nice Sophia-Antipolis », une université qui me dit vaguement quelque chose (😊). Son emplacement exact est précisé avec ses données gps et sa région « Provence Alpes Côte d'Azur »



Connaître le lieu exact de la cible permet de mieux comprendre les potentielles menaces et vulnérabilités liées à l'environnement physique dans lequel se trouve la cible, ainsi que les règles et réglementations en vigueur dans cette région qui pourraient avoir un impact sur les tests d'intrusion. Cela permet également de mieux cibler les méthodes et outils utilisés pour effectuer le pentest et de mieux comprendre les données collectées.

2) Analyse du réseau

Dans le cadre d'un pentest, l'analyse d'un réseau permet de déterminer les différents éléments qui composent le système cible, tels que les ordinateurs, les serveurs, les routeurs, les commutateurs, les périphériques réseau, etc. Cela permet également de déterminer les relations de confiance entre ces éléments et de comprendre comment ils communiquent entre eux. Cela permet de comprendre comment les utilisateurs se connectent au réseau et

comment les données sont transférées. Enfin, cela permet d'identifier les vulnérabilités et les points d'entrée potentiels pour une attaque

Nous allons donc maintenant procéder à l'analyse du réseau pour identifier les vulnérabilités et les risques.

Nous allons utiliser Nmap dans le cadre de notre pentest car cet outil permet de cartographier les ports et les services d'un système cible, ce qui nous permet de déterminer les points d'entrée potentiels pour une intrusion et de repérer les systèmes vulnérables. En d'autres termes, Nmap nous aide à identifier les faiblesses de notre serveur et à cibler les zones à tester pour maximiser l'efficacité de notre test d'intrusion.

Un simple Nmap sur notre adresse nous donne déjà beaucoup d'information :

Un scan Nmap avec les options -v, -sS et -A sur l'adresse IP 134.59.139.251 va nous donner des informations utiles telles que :

- **Les ports ouverts** (80/tcp → http, port 21/tcp → **FTP**)
- Les services en cours d'exécution sur le serveur cible
- Les informations de version du système d'exploitation et de l'application
- Les mécanismes de sécurité actifs (pare-feu, filtrage d'adresses IP, etc.) et des informations sur les vulnérabilités potentielles.

Ces informations peuvent nous aider à identifier les points d'entrée pour les attaques et à planifier les étapes suivantes de leur test d'intrusion.

On va pouvoir réutiliser ces informations afin d'y trouver une faille. Une simple recherche en source ouvert nous donne des potentiels failles possible sur un serveur possédant le **port FTP** ouvert : cela peut présenter des risques de sécurité si les configurations et les méthodes d'authentification ne sont pas correctement mises en place. Il est possible que des personnes malveillantes puissent accéder à des fichiers sensibles ou télécharger des programmes malveillants sur le serveur si les informations d'identification sont faibles ou non protégées. On **présentera et on attaquera** le serveur à l'aide de cette faille (cf partie suivante).

Avoir le port **http ouvert** n'est pas forcément une faille cependant, il est important de s'assurer que les applications web sur ce port sont sécurisées et ne présentent pas de vulnérabilités connues, car elles peuvent être exploitées par des attaquants pour accéder à des informations sensibles ou prendre le contrôle du serveur. Il est donc important de surveiller régulièrement et de mettre à jour les applications web en place. On a donc essayé d'exploiter cette potentielle faille **sans succès**.

```

(root@kali)=[~]
# nmap -v -sS -A 134.59.139.251
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-18 09:51 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 09:51
Completed NSE at 09:51, 0.00s elapsed
Initiating NSE at 09:51
Completed NSE at 09:51, 0.00s elapsed
Initiating NSE at 09:51
Completed NSE at 09:51, 0.00s elapsed
Initiating Ping Scan at 09:51
Scanning 134.59.139.251 [4 ports]
Completed Ping Scan at 09:51, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:51
Completed Parallel DNS resolution of 1 host. at 09:51, 0.01s elapsed
Initiating SYN Stealth Scan at 09:51
Scanning 134.59.139.251 [1000 ports]
Discovered open port 80/tcp on 134.59.139.251
Discovered open port 21/tcp on 134.59.139.251
Completed SYN Stealth Scan at 09:51, 4.51s elapsed (1000 total ports)
Initiating Service scan at 09:51
Scanning 2 services on 134.59.139.251
Completed Service scan at 09:51, 5.01s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 134.59.139.251
Retrying OS detection (try #2) against 134.59.139.251
Initiating Traceroute at 09:51
Completed Traceroute at 09:51, 0.01s elapsed
Initiating Parallel DNS resolution of 1 host. at 09:51
Completed Parallel DNS resolution of 1 host. at 09:51, 0.00s elapsed
NSE: Script scanning 134.59.139.251.
Initiating NSE at 09:51
Completed NSE at 09:51, 16.10s elapsed
Initiating NSE at 09:51
Completed NSE at 09:51, 0.02s elapsed
Initiating NSE at 09:51
Completed NSE at 09:51, 0.00s elapsed
Nmap scan report for 134.59.139.251
Host is up (0.00032s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  tcpwrapped
22/tcp    closed ssh

```

On liste les appareils actifs sur le réseau :

Lister les appareils actifs sur le réseau est important car cela permet de connaître les différents éléments qui composent le réseau et de les identifier. Cela aide à comprendre la topologie du réseau et à identifier les points d'entrée potentiels. En outre, cela permet également de détecter les appareils qui ne devraient pas être présents sur le réseau, tels que les appareils malveillants ou les appareils qui ne sont pas gérés par l'entreprise. Cela aide à évaluer les risques pour la sécurité du réseau et à prendre les mesures de sécurité appropriées.

Dans notre cas rien de particulier n'a été détectés.

```
└─# nmap -sn 134.59.139.251/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-18 10:06 EST
Nmap scan report for 134.59.139.0
Host is up (0.00051s latency).
Nmap scan report for 134.59.139.1
Host is up (0.00019s latency).
Nmap scan report for gtr201a.unice.fr (134.59.139.2)
Host is up (0.00044s latency).
Nmap scan report for 134.59.139.3
Host is up (0.00040s latency).
Nmap scan report for gtr400a.unice.fr (134.59.139.4)
Host is up (0.00070s latency).
Nmap scan report for 134.59.139.5
Host is up (0.00064s latency).
Nmap scan report for gtr406a.unice.fr (134.59.139.6)
Host is up (0.00059s latency).
Nmap scan report for 134.59.139.7
Host is up (0.00037s latency).
Nmap scan report for gtr506b.unice.fr (134.59.139.8)
Host is up (0.00069s latency).
Nmap scan report for 134.59.139.9
Host is up (0.00071s latency).
Nmap scan report for 134.59.139.10
Host is up (0.00063s latency).
Nmap scan report for 134.59.139.11
Host is up (0.00056s latency).
Nmap scan report for gtr302b.unice.fr (134.59.139.12)
Host is up (0.00049s latency).
Nmap scan report for 134.59.139.13
Host is up (0.00042s latency).
Nmap scan report for 134.59.139.14
Host is up (0.00053s latency).
Nmap scan report for gtr302e.unice.fr (134.59.139.15)
Host is up (0.00066s latency).
Nmap scan report for 134.59.139.16
Host is up (0.00045s latency).
Nmap scan report for gtr302g.unice.fr (134.59.139.17)
Host is up (0.00044s latency).
Nmap scan report for 134.59.139.18
Host is up (0.00039s latency).
Nmap scan report for gtr302i.unice.fr (134.59.139.19)
Host is up (0.00035s latency).
```

Avec Nmap on peut avoir des informations sur l'OS comme sa version :

Ici on peut voir qu'aucun os n'est associé à cette adresse IP.


```

# nmap -O 134.59.139.251
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-18 09:59 EST
Nmap scan report for 134.59.139.251
Host is up (0.00084s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    closed ssh
80/tcp    open  http
3306/tcp  closed mysql
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
No OS matches for host

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.56 seconds

```

Un ping permet de vérifier la disponibilité d'un serveur en envoyant des paquets ICMP (Internet Control Message Protocol) à l'adresse IP cible. Cela permet de savoir si le serveur est connecté et répond aux requêtes réseau. Dans le cadre de notre pentest, cela permet de déterminer si le serveur cible est actif et accessible sur le réseau, ce qui est important pour planifier les étapes suivantes de l'audit de sécurité. Ici on remarque que le serveur est accessible.

```

# ping 134.59.139.251
PING 134.59.139.251 (134.59.139.251) 56(84) bytes of data.
64 bytes from 134.59.139.251: icmp_seq=1 ttl=63 time=0.922 ms
64 bytes from 134.59.139.251: icmp_seq=2 ttl=63 time=1.63 ms
64 bytes from 134.59.139.251: icmp_seq=3 ttl=63 time=1.47 ms
64 bytes from 134.59.139.251: icmp_seq=4 ttl=63 time=1.50 ms
^C
— 134.59.139.251 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.922/1.379/1.631/0.271 ms

```

Cette commande Whois nous donne beaucoup d'information sur l'adresse IP (nom de domaine, des numéros de tels, des noms de personnes, des adresses précises). Cependant toutes ces informations ne vont nous être utiles dans le cadre de ce pentest.

La commande whois nous permet de récupérer des informations sur l'adresse IP de notre serveur. On peut voir qu'il inclut des informations sur l'enregistrement du domaine, les dates d'expiration, les coordonnées de contact, et d'autres détails pertinents. Dans le cadre de notre pentest, cela peut aider à identifier des informations sur la propriété et la gestion d'un serveur ou d'un réseau cible, ce qui peut être utile pour établir un contexte et cibler les attaques.


```
# whois 134.59.139.251
```

```
#  
# ARIN WHOIS data and services are subject to the Terms of Use  
# available at: https://www.arin.net/resources/registry/whois/tou/  
#  
# If you see inaccuracies in the results, please report at  
# https://www.arin.net/resources/registry/whois/inaccuracy\_reporting/  
#  
# Copyright 1997-2023, American Registry for Internet Numbers, Ltd.  
#
```

```
NetRange:      134.58.0.0 - 134.61.255.255  
CIDR:          134.58.0.0/15, 134.60.0.0/15  
NetName:       RIPE-ERX-134-58-0-0  
NetHandle:     NET-134-58-0-0-1  
Parent:        NET134 (NET-134-0-0-0-0)  
NetType:       Early Registrations, Transferred to RIPE NCC  
OriginAS:        
Organization:  RIPE Network Coordination Centre (RIPE)  
RegDate:       2003-11-26  
Updated:       2003-11-26  
Comment:       These addresses have been further assigned to users in  
Comment:       the RIPE NCC region. Contact information can be found in  
Comment:       the RIPE database at http://www.ripe.net/whois  
Ref:           https://rdap.arin.net/registry/ip/134.58.0.0
```

```
ResourceLink:  https://apps.db.ripe.net/search/query.html  
ResourceLink:  whois.ripe.net
```

```
OrgName:       RIPE Network Coordination Centre  
OrgId:         RIPE  
Address:       P.O. Box 10096  
City:          Amsterdam  
StateProv:       
PostalCode:    1001EB  
Country:       NL  
RegDate:         
Updated:       2013-07-29  
Ref:           https://rdap.arin.net/registry/entity/RIPE
```

```
created:      2016-09-06T08:41:59Z
last-modified: 2022-12-01T17:31:54Z
source:      RIPE # Filtered

person:      Nicolas BONICCO
address:     Universite Nice Sophia Antipolis
address:     28 avenue Valrose
address:     BP 2135 06103 Nice
phone:       +33 4 92 07 67 67
nic-hdl:     NB6946-RIPE
mnt-by:      RENATER-MNT
remarks:     changed:      rensvp@renater.fr 20160906
remarks:     changed:      rensvp@renater.fr 20181011
created:     2016-09-06T08:38:03Z
last-modified: 2018-10-11T13:46:23Z
source:      RIPE # Filtered

person:      Richard MANAS
address:     Universite Nice Sophia Antipolis
address:     28 avenue Valrose
address:     BP 2135 06103 Nice
phone:       +33 4 92 07 67 67
fax-no:      +33 4 92 07 67 00
nic-hdl:     RM18504-RIPE
mnt-by:      RENATER-MNT
remarks:     changed:      rensvp@renater.fr 20160906
created:     2016-09-06T08:38:03Z
last-modified: 2016-09-06T08:38:03Z
source:      RIPE # Filtered

person:      Stephane MAUREL
address:     Universite Nice Sophia Antipolis
address:     28 avenue Valrose
address:     BP 2135 06103 Nice
phone:       +33 4 92 07 67 67
fax-no:      +33 4 92 07 67 00
nic-hdl:     SM30964-RIPE
mnt-by:      RENATER-MNT
remarks:     changed:      rensvp@renater.fr 20160906
created:     2016-09-06T08:38:03Z
last-modified: 2016-09-06T08:38:03Z
source:      RIPE # Filtered
```

% Information related to '134.59.0.0/16AS2200'

On test d'autres commande nmap qui ne donne rien de spécial.

```
(root@kali)-[~]
# nmap -sL 134.59.139.251
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-18 10:21 EST
Nmap scan report for 134.59.139.251
Nmap done: 1 IP address (0 hosts up) scanned in 0.02 seconds

(root@kali)-[~]
# nmap -sP 134.59.139.251
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-18 10:21 EST
Nmap scan report for 134.59.139.251
Host is up (0.00026s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds

(root@kali)-[~]
```

On va maintenant test

III. Identification/Exploitation des vulnérabilités

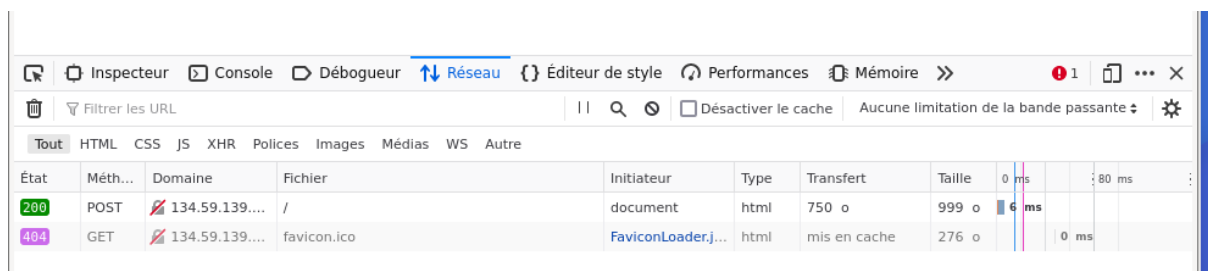
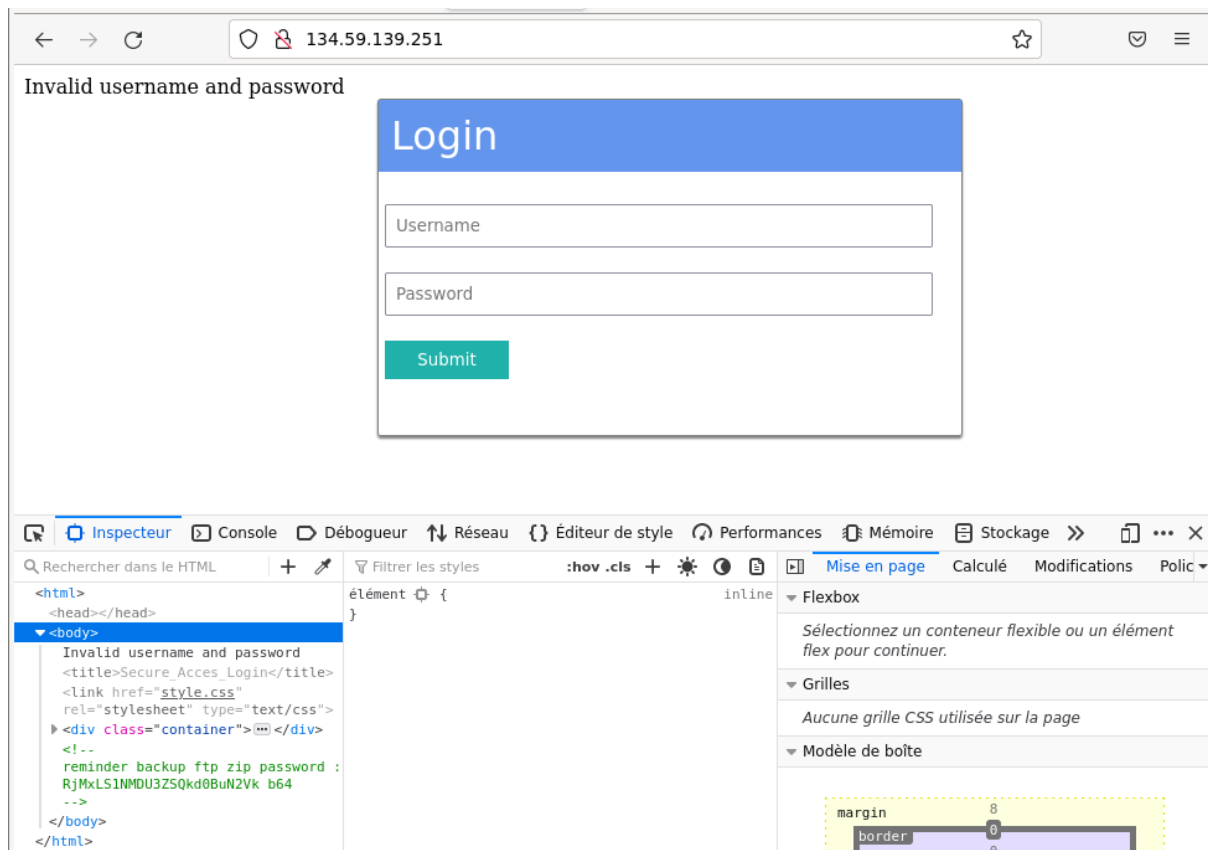
Nous allons utiliser les vulnérabilités identifiées pour accéder aux systèmes et aux données de la cible.

- Port http (80) ouvert :

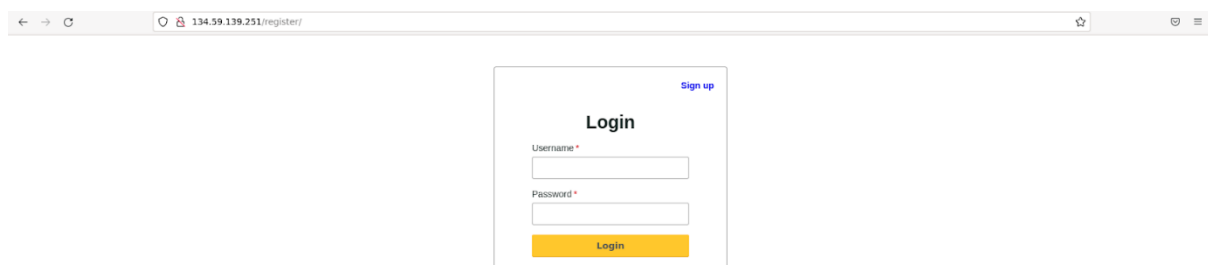
Après avoir taper l'adresse ip dans un navigateur web (Firefox de préférence pour son inspecteur de page) on à accès à un formulaire de connexion :

On test les principaux mdp potentiellement utilisé : admin/admin, admin/admin123 Mais rien qui ne fonctionne.

Après des tests **d'injections SQL** rien ne marche non plus, le formulaire semble sécurisé.



Après une recherche sur le code de la page du formulaire de connexion du serveur on a pu voir une potentielle page d'inscription. Après quelques recherches sur internet, on a pu trouver la page « register » du serveur :



Après une inscription on a donc accès au serveur à l'aide d'un identifiant.

[Login](#)

Registration

Username *

Email *

Password *

Confirm Password *

Sign up

[Sign up](#)

Login

Username *

Password *

Login

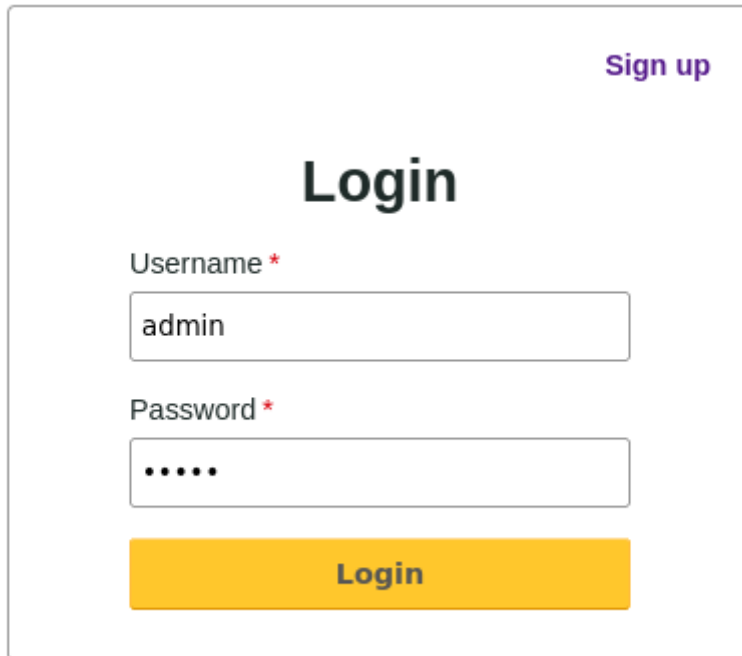
[Logout](#)

Welcome cahcalot

« Welcome cachalot » nous sommes donc bien sur le serveur.

Avoir réussi à se connecter sur le serveur à l'aide d'un compte peut nous aider à accéder aux systèmes et aux données de manière privilégiée, ce qui nous permet d'avoir une vue plus complète et détaillée des vulnérabilités présentes et de pouvoir les exploiter de manière plus efficace. Cela peut également nous permettre de déplacer des privilèges et de continuer à naviguer dans le système pour obtenir un accès à des informations sensibles.

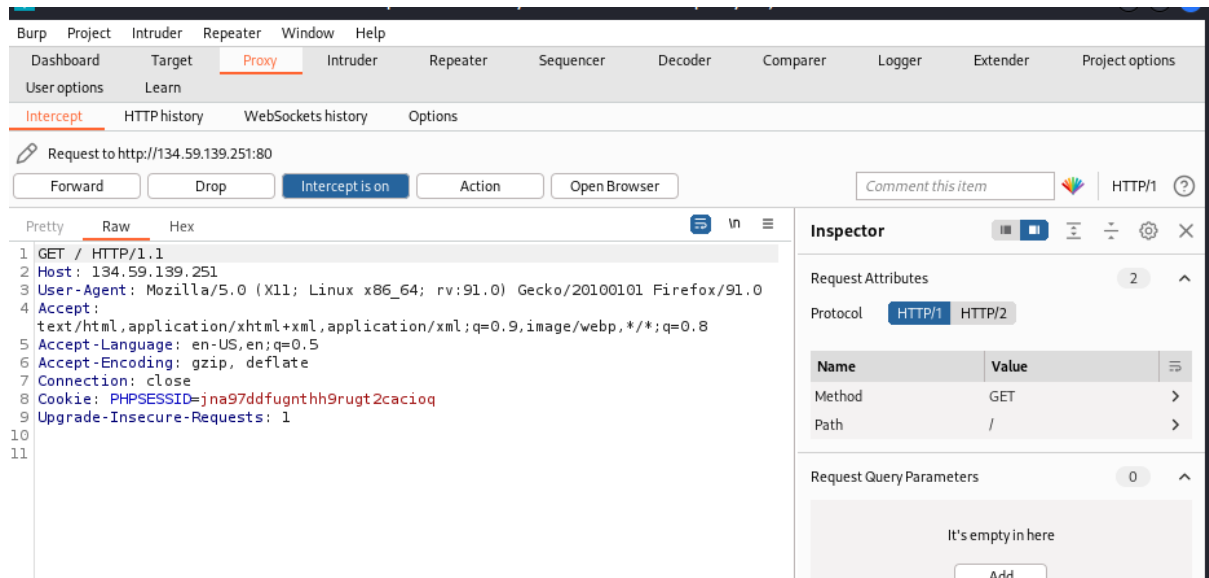
Sur ce formulaire les identifiants admin/admin ont marché mais c'était probablement un compte créer par un autre utilisateur. Car il était impossible en partant de ce compte d'avoir d'autres droits plus importants.

A screenshot of a web application login form. The form is enclosed in a light gray border. In the top right corner, there is a purple link labeled "Sign up". The title "Login" is centered in a large, bold, black font. Below the title, there are two input fields. The first is labeled "Username *" in a small, gray font, and it contains the text "admin". The second is labeled "Password *" in a small, gray font, and it contains five black dots. Below these fields is a large, yellow button with the word "Login" in a bold, black font.

Utilisation du logiciel Burp Suite sur kali linux qui est un outil de sécurité informatique utilisé pour effectuer des tests d'intrusion et des audits de sécurité. Il permet de scanner les applications web pour identifier les vulnérabilités, de capturer et d'intercepter les requêtes

et les réponses HTTP/HTTPS, de manipuler les données de ces requêtes et de les réinjecter, de lancer des attaques automatisées, de générer des rapports et bien plus encore. Il est souvent utilisé par les pentesters et les professionnels de la sécurité pour évaluer la sécurité des applications web et des systèmes d'informations.

Ici l'utilisation du **proxy** n'a rien donné de particulier, ni **l'attaque de mot de passe par force**.



- Port FTP (21) ouvert :

```
# nmap -T4 -F 134.59.139.251
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-18 12:12 EST
Nmap scan report for 134.59.139.251
Host is up (0.00066s latency).
Not shown: 95 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    closed ssh
80/tcp    open  http
3306/tcp  closed mysql
8008/tcp  open  http

Nmap done: 1 IP address (1 host up) scanned in 1.77 seconds
```

Connexion au serveur FTP :


```

# ftp 134.59.139.251
Connected to 134.59.139.251.
220 (vsFTPd 3.0.3)
Name (134.59.139.251:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>

```

On peut voir que la connexion au serveur FTP a été un succès.

Cette connexion au serveur FTP permet de tester la sécurité de celui-ci en essayant d'accéder à des fichiers et des répertoires qui pourraient être protégés par des mots de passe ou des autorisations d'accès insuffisantes. Cela permet également de vérifier si des fichiers sensibles ou des informations confidentielles sont stockés sur le serveur et si elles sont protégées adéquatement. En cas d'accès réussi, il permet de récupérer des informations sensibles.

```

msf6 > use auxiliary/scanner/ftp/anonymous
msf6 auxiliary(scanner/ftp/anonymous) > set rhosts 134.59.139.251
rhosts => 134.59.139.251
msf6 auxiliary(scanner/ftp/anonymous) > exploit

[+] 134.59.139.251:21 - 134.59.139.251:21 - Anonymous READ (220 (vsFTPd 3.0.3))
[*] 134.59.139.251:21 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ftp/anonymous) >

```

```

# nmap -p 21 134.59.139.251 --script ftp-anon
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-18 12:14 EST
Nmap scan report for 134.59.139.251
Host is up (0.00036s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT

Nmap done: 1 IP address (1 host up) scanned in 30.30 seconds

```

```

# nmap -p 21 134.59.139.251 --script ftp-anon
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-18 12:14 EST
Nmap scan report for 134.59.139.251
Host is up (0.00036s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT

Nmap done: 1 IP address (1 host up) scanned in 30.30 seconds

```

Il y a plusieurs façons d'attaquer un serveur FTP après une connexion, nous avons utilisé deux des méthodes les plus courantes :

1. Brute force : en utilisant des outils automatisés pour tester de nombreux mots de passe différents, l'attaque par force brute peut permettre à un pirate de découvrir les informations d'identification valides pour un compte utilisateur sur le serveur FTP.
2. Injection de commande : en utilisant des techniques d'injection de commande, un pirate peut envoyer des commandes malveillantes au serveur FTP, qui les exécutera et pourrait permettre à l'attaquant de prendre le contrôle du serveur ou d'accéder à des informations sensibles.

Mais aucune n'a réellement fonctionner.

IV. Recommandations

- **Menace sur le port http :**

Les risques sur un port http sont multiples, ils incluent les attaques de type injection de code, de dénégaration de service (DoS) et de vol de données sensibles. Les menaces peuvent être des pirates informatiques, des logiciels malveillants ou des utilisateurs malveillants qui cherchent à accéder ou à compromettre les systèmes et les données.

Solutions adaptées :

Parmi les solutions pour protéger contre les risques liés au port HTTP, il y a l'utilisation d'un **pare-feu**, la mise en place **d'un système de détection d'intrusion**, la **mise à jour régulière des logiciels** et des systèmes d'exploitation, l'utilisation d'un certificat SSL pour protéger les communications sensibles, et la mise en place **de politiques de sécurité strictes** pour limiter l'accès aux serveurs et aux données sensibles. Il est également important de sensibiliser les employés à la sécurité et de les former sur les meilleures pratiques pour éviter les erreurs qui pourraient causer des vulnérabilités.

- **Menaces sur le port FTP (21) :**

Les risques et menaces sur le port FTP incluent les attaques de force brute pour deviner les identifiants d'utilisateur et les mots de passe, ainsi que les vulnérabilités de logiciels FTP qui peuvent permettre à un attaquant d'exécuter du code malveillant sur le serveur.

Solutions adaptées :

Pour protéger contre ces risques, il est important de mettre en place des **politiques de sécurité fortes pour les mots de passe** et de maintenir les logiciels FTP à jour avec les dernières mises à jour de sécurité. Il est également recommandé de **limiter les utilisateurs qui ont accès au service FTP** à uniquement ceux qui en ont absolument besoin et de configurer des règles de pare-feu pour limiter les connexions entrantes uniquement aux adresses IP autorisées. Il est également possible d'utiliser des protocoles de transfert de fichiers plus sécurisés, tels que **SFTP ou FTPS**.

- **Menaces sur l'authentification :**

Les menaces liées à l'authentification d'un serveur incluent les attaques de force brute, où un pirate tente de deviner les mots de passe en utilisant une liste de mots de passe couramment utilisés, ainsi que les attaques d'ingénierie sociale, où un pirate se fait passer pour un utilisateur légitime pour obtenir des informations d'identification.

Solutions adaptées :

Les menaces sur l'authentification d'un serveur incluent les attaques par force brute, les fuites de mots de passe, les comptes par défaut non modifiés et les faiblesses de l'authentification multi facteur. Pour contrer ces menaces, les solutions adaptées incluent l'utilisation de mots de passe forts et uniques, l'application de politiques de mot de passe efficaces, la mise en place de l'authentification multi facteur et la surveillance régulière des journaux d'authentification pour détecter les tentatives d'intrusion. Il est également important de maintenir les systèmes d'authentification à jour avec les derniers correctifs de sécurité.

Récapitulatif des vulnérabilités trouvées :

Risques	Sévérité
Port http ouvert	Haute
Port FTP ouvert	Critique

V. Conclusion

En conclusion, notre analyse de pentest a permis de découvrir des vulnérabilités sur le serveur ciblé, notamment sur les ports HTTP et FTP. Nous avons identifié des risques potentiels tels que des attaques de phishing, de dénéiation de service ou encore des accès non autorisés. Pour remédier à ces vulnérabilités, il est recommandé de mettre en place des solutions de sécurité adaptées telles que l'utilisation de certificats SSL pour le port HTTP, l'utilisation de protocoles de chiffrement pour les échanges FTP et l'utilisation de mécanismes d'authentification forts pour l'accès au serveur. Il est également important de continuer à surveiller régulièrement le système pour détecter tout nouveau risque émergent.