From nothing to root

P0wned

Stapler: 1 on vulnhub.com

Where to start

$ nmap IP -p1-65535

Ex: nmap 127.0.0.1 -p1-65535

```
PORT      STATE  SERVICE
20/tcp    closed ftp-data
21/tcp    open   ftp
22/tcp    open   ssh
80/tcp    open   http
443/tcp    open   https
12380/tcp open   unknown
```

$ 1 port = 1 service

Knock knock

$ Visit the service found

- $ manually to avoid detection
  - $ robots.txt, /admin/, /login/...
- $ automatically (nikto, dirbuster...)

```
$ nikto -h http://192.168.56.102:80
$ nikto -h http://192.168.56.102:12380
...
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
...
```

$ Be careful

Wordpress, lucky me !

$ Makes bloggins easier

$ Plugins usually not updated

$ Interesting files and directory :

/wp-content/, /wp-admin/

wp-config.php <--- database password in clear

$ Tools

$ wpscan, searchsploit

Get yourself a shell !

$ Basic information gathering

```
$ id
    uid=1026(zoe) gid=1026(zoe) groups=1026(zoe)
$ who
    zoe      pts/0        2017-09-24 20:25 (192.168.56.101)
$ cat /etc/*-release
$ uname -a
    Linux red.initech 4.4.0-21-generic...
$ cat /etc/passwd
```

Get r00t !

$ Cron

$ Kernel exploit

$ SSH keys

$ Looking for credentials

$ Web server config files

$ Setuid files

$ Localhost services

$ Stupid users (files, history etc.)&

Now what ?

$ Openclassroom : TCP/IP

$ Bosser sérieusement ses TP de bash

$ http://overthewire.org/

$ CTF la semaine prochaine :D

Questions ? No ? Good.

Ressources

https://www.exploit-db.com/exploits/

https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation

Training:

https://www.vulnhub.com

https://www.owasp.org/index.php/Category:OWASP WebGoat Project

https://www.root-me.org