

Forum:[Hack Forums](#)

Thread: [A sneak peek at my Python pentesting tool](#)

xMoD - September 19, 2014, 2:21 pm

Note: I have updated it a bit, but I just got the below data from my previous post on another forum. I would hate to re-type it all.

I am creating a python script that can be imported, to do a quick port scan, banner grab, thing of that kind.

Heres what you can do with my package:

PHP Code

<?php

```
from fastpscan import Scan, getBanner
```

```
ports = {'ftp':[21], 'web':[80,443], 'smtp':[25], 'telnet':[23]}
```

```
#i.e if portOpen in ports['web'] = true then its probably a web service
```

```
myRouterOpenPorts = Scan('192.168.1.1',0,100)
```

```
print "Open Ports: "+str(myRouterOpenPorts)
```

```
for port in myRouterOpenPorts:
```

```
    if port in ports['web']:
```

```
        print "The machine has an open port, possibly dedicated to a web service | port: "+str(port)
```

And heres the output :D

And for those who cant read, thats a small 100 ports in 2.325 seconds.

This isnt too close to being done, but Im trying to push it out fast.

Of course I still have yet to add more security features but thats also coming.

My next possible feature could be checking against open ports and seeing if they are related to any software that could be vulnerable.

Which by the way I might need help compiling a list.

Then with an okay from the user, launch an nmap scan on the target to check for OS & version to see if indeed its possible for an attack, after that its probably up to the user to conduct the attack.

Also, the banner grabber does send a message to the port it connects to:

"I'm running a port scan on your server for penetration testing"

This is because this is intended to be a whitehat tool, but you may change it in the source if you wish to use a tad more discretely._____

Made simple ftp Dictionary attack option.

Moved all imports to imports.py, which is then imported with "from imports import **"

So far:

Spoiler ([Click to View](#))

fastpscan, which needs a new name in the future, contains functions used to port scan a target, and

check for open ports, with a specified starting and ending port.
Also contains a banner grabber.

imports - File that can be imported also, that contains all modules that need to be imported.

ftp . py - Contains methods that can : connect to, login to, and attempt a dictionary attack on an ftp server.

- Note: I made this module to mostly attempt attacks on an ftp server, and doesnt have any functions to put or get files or really do any other interaction with the server.

time_exec.py - I also made this with a class and two functions/methods to roughly calculate how long it takes a function or code block to execute.

Use:

PHP Code

```
<?php
```

```
t = time_exec.time()
```

```
t.start()
```

```
#... Execute code here ...
```

```
elapsed_time = t.stop()
```

```
print elapsed_time
```

pscan - Just the main files that uses all the above modules.

Dict-Attack example:

PHP Code

```
<?php
```

```
filez = '127.0.0.1'
```

```
localFTPServer_Login = ftp . brute_force(filez, 21, 'users.txt','passwd.txt')
```

```
print localFTPServer_Login
```

Next idea, which will be added to my current tool is an attack modules.

Which contains different attacks for a network.

- FTP Dictionary attack (already added in the tool, but Ill move to the new module) ++Assuming theres no autoban which would be annoying.
- SSH Server default cred guess/dict attack.
- ETC

WZDY - September 20, 2014, 1:54 am

Looks pretty cool & useful! Keep us updated when it's finished.

muz3 - September 21, 2014, 2:25 am

You should banner grab the port and by that output determine which service it's. Not depending on the default port, but you have a good start.

The Sly - September 21, 2014, 2:29 am

Looks amazing man! Keep us updated!

xMoD - September 21, 2014, 11:53 am

(Sep 21, 2014 02:25 AM)muz3 Wrote: [CITE](#) You should banner grab the port and by that output determine which service it's. Not depending on the default port, but you have a good start.

I know, but I figured by default whos really gonna run like a web service on port 23, am i right?
But I see your point, I could update it, or just write another function to do this.

I also am writing, a module to work with mobile devices with python.

It can scan the network, and attempts to search for iPhones and sees if port 22 is open (ssh).

(Usually opened by jail breaking)

Then try default creds; root:alpine or mobile:alpine.

Im writing it for my schools network.

My only issue is I didnt want to scan the entire network, and then try and rut thru all the windows machines, or just have to scan for port 22.

So I looked into DNS-SD, ZeroConf, and Bonjour type python implementations, but I cant seem to find anything suitable that would find apple/unix machines.

Note: If anyone could help with that part, or knows the best/fastest way to get all devices on network and could perhaps provide some example code, Id be grateful.

Edit:

Anyone know if I could get nmap on my rooted tablet?