Patience is Key Element of Success

Network Security // 1580 points

Description

ShoppingBaba's IT admin is frugal and forgetful, and refuses to admit that his setup was exploitable by the attackers. He abides by the aphorism "security through obscurity". Prove him wrong by finding out his secret port and secret file!

P.S. Since he's forgetful, he left himself a clue in 167.99.28.65:2000-2100 P.S. A 1bps broadband plan was used to deter l33t hackers.

P.S.S. Rules: 1. Do not add, delete or modify any files on the server. 2. Be patient!

Solution

Since we can assume that this challenge wants us to port-knock to find a responding tcp port using netcat. However, this process is too tedious by hand and takes too long waiting due to the slow speed.

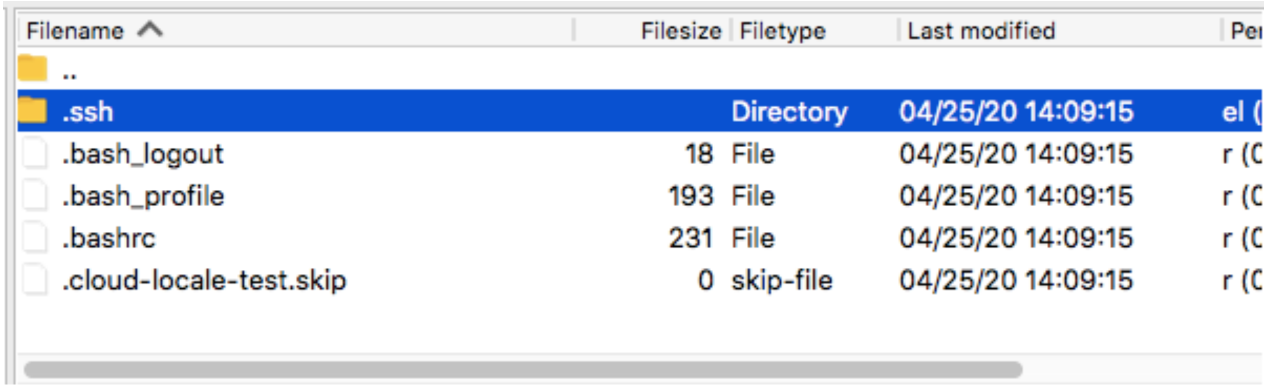
So instead, we write a nodeJS script to automatically do this for us.

```
const net = require('net');
const IP = "<server ip>";

for (let i=2000; i<=2100; i++) {
  const client = new net.Socket();
  client.connect(i, IP, () => {
    console.log('Port found!', i);
  });
  client.on('data',(data) => {
    console.log(data.toString(), i);
  });
}

console.log('All open!');
```

Upon running this script, we find that the "secret port" is actually port 2042, and the output leads us to another port 4242.

By connecting to the port 4242, we realise that it is a FTP server from the welcome message. We then connect to the server and slowly wait for the files to show up (1bps is really slow!)

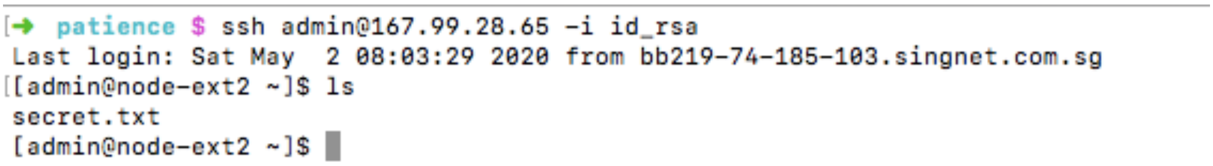
After probing around the folders, we notice a suspicious `.ssh` folder which contains credentials for SSH.



Filename	Filesize	Filetype	Last modified	Per
..				
.ssh		Directory	04/25/20 14:09:15	el (
.bash_logout	18	File	04/25/20 14:09:15	r (C
.bash_profile	193	File	04/25/20 14:09:15	r (C
.bashrc	231	File	04/25/20 14:09:15	r (C
.cloud-locale-test.skip	0	skip-file	04/25/20 14:09:15	r (C

We now download the keypair used for the connection and after that connect to the SSH server.

Inside we get a shell, and simply running the command `ls` tells us what exactly we need to find.



```
[➜  patience $ ssh admin@167.99.28.65 -i id_rsa
 Last login: Sat May  2 08:03:29 2020 from bb219-74-185-103.singnet.com.sg
[[admin@node-ext2 ~]$ ls
 secret.txt
 [admin@node-ext2 ~]$ 
```

Takeaways

- Just because a challenge might take some time to respond, does not mean that it is not solvable and you only need to be patient.
- Some people might think FTP server does not work properly but actually it does, just really really slow.