

Anti-Bot

Briana Jakell



Home network



Scanning network



telnet>_

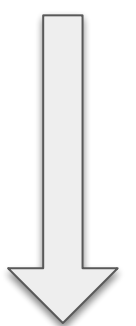
>_SSH ✓

Found open Telnet/SSH port



The Security Setup

Brute force combinations of default usernames and passwords



If found

~~PASSWORD~~

Password successfully changed

Project Overview:

The purpose of this project is to expose default credentials on open Telnet and SSH ports. If discovered, prompt the user to change default password. The hope is to prevent future botnets from being created.

```
[*] Running initial scan on local network....
[*] Scanning individual host: 192.168.1.1
[*] Scanning individual host: 192.168.1.5
[*] Scanning individual host: 192.168.1.9
[*] Scanning individual host: 192.168.1.10
[*] Scanning individual host: 192.168.1.14
[*] Scanning individual host: 192.168.1.18
[*] Scanning individual host: 192.168.1.19
[*] Scanning individual host: 192.168.1.22
[*] Found open telnet port on: 192.168.1.22
    [*] Brute forcing default username and password...
    [*] Valid credentials found.
        Username: pi
        Password: raspberry
    [*] Changing default credentials...
        (current) UNIX password: raspberry
        Enter new UNIX password: themonkeyisrunningfast
        Retype new UNIX password: themonkeyisrunningfast
        passwd: password updated successfully
    [*] Found open ssh port on: 192.168.1.22
    [*] Brute forcing default username and password...
        [*] No default username/password combination found.
[*] Scanning individual host: 192.168.1.11
[*] Scan complete.
```

