

Forum:[Hack Forums](#)

Thread: [\[Sui Generis\] Discover and attack Raspberry Pi's on your network.](#)

Wake - July 16, 2019, 2:25 pm

Discover and attack Raspberry Pi's on your network.

Written by [Wake](#)

Disclaimer

This thread is for informational and educational purpose only. I will not be responsible for any action performed by any reader.

Introduction

In this thread i will be covering the problems with default credentials and how we can use default credentials to effortlessly login and control a Raspberry Pi on our network remotely.

What Will I Need For This?

[+] A machine running a linux distro or a Virtual machine.

[+] BusesCanFly RPI-Hunter script found [here](#) (i will go over how to install this later on)

[+] A Raspberry Pi on your network that you have permission to test on with default credentials and ssh enabled.

What is RPI-Hunter

RPI-Hunter is a script from the Github user [BusesCanFly](#) that allows us to automate sending payloads or commands to our Raspberry Pi. RPI-Hunter is useful when we have multiple Raspberry Pi's on our network with known or default credentials. RPI-Hunter can be especially useful when you have more than one Raspberry Pi on your network making it easy to modify each device individually or access all your Raspberry Pi's as a group

Why are default credentials a huge problem

Devices using default credentials are a huge problem and a risk when connecting them to a network. Some IoT devices wont even allow you to change your devices details because they have hardcoded credentials. These types of devices are a target for hackers who want to take advantage of your device. If you know the default password a device is using it is extremely easy to login and perform multiple actions.

How to discover and attack Raspberry Pi's on your network

The first thing we are going to need to do is make sure we have SSH enabled on our Raspberry Pi we can do this by clicking start going to Preferences and Raspberry Pi configuration.

Once we are in the Raspberry Pi configuration menu click on the Interfaces tab and enable SSH and press Ok.

Spoiler ([Click to View](#))

Now what we are going to need to do is to download BusesCanFly RPI-Hunter script

We can do this by typing this one line variant into Terminal.

```
[+] sudo pip install -U argparse termcolor && sudo apt -y install arp-scan tshark sshpass && git clone https://github.com/BusesCanFly/rpi-hunter && cd ./rpi-hunter && chmod +x rpi-hunter.py
```

Once you have typed that command into terminal it will install the script and leave you in the directory to execute it.

Spoiler ([Click to View](#))

Next we can execute this command to see what options we have. We can do this by typing this command into Terminal.

```
[+] sudo python ./rpi-hunter.py --help
```

We are greeted with a list of arguments and what they do.

Spoiler ([Click to View](#))

We are going to use the argument -r to scan our ip range for Raspberry Pi's by typing in this command

```
[+] sudo python ./rpi-hunter.py -r 192.168.0.0/24
```

This will scan our whole network for Raspberry Pi's.

Spoiler ([Click to View](#))

Now we have located our Raspberry Pi we can either chose to change our address to that of the Raspberry Pi or keep it as it is. (if you have more than one Raspberry Pi on your network keep the address the same as it will target all your Raspberry Pi's and not just a single one)

Now we know the address of our Raspberry Pi we can see what options we have to target it. Type this into Terminal to see what Payloads we can forward to our Raspberry Pi.

```
[+] sudo python ./rpi-hunter.py --list
```

Here we can see a list of payloads we can execute.

Spoiler ([Click to View](#))

For this example we are going to be using the payload "warning" this will send the Raspberry Pi owner a friendly reminder that there Raspberry Pi is vulnerable and they should change there password.

But before i do that i am going to SSH into my Raspberry Pi to show you this is a device i own and there was no message previously put there.

As you can see when we SSH into our Raspberry Pi it even warns us about using default credentials and tells us to change the password for the user 'pi'

Spoiler ([Click to View](#))

If this wasn't warning enough we will now go ahead and send the payload giving the target more of a hint that they should change there default password.

We can customize this message to say what ever we would like it isn't really to hard to change but for this example i am just going to leave it as it is and show you how it is done.

To forward the payload you can type into Terminal

```
[+] sudo python ./rpi-hunter.py --payload warning ( or what ever payload you want to forward ) and press enter
```

Now we can see our payload has been sent. We are now going to send our own payload to reboot the Raspberry Pi so these changes take affect. We can type

```
[+] sudo python ./rpi-hunter.py --payload 'sudo reboot'
```

Once that command has been entered our Raspberry Pi will reboot and once we SSH in again or open a Terminal window within the Raspberry Pi we will be left with a friendly reminder letting us know to reset our password.

Spoiler ([Click to View](#))

Now if we go to SSH into our Raspberry Pi or open a Terminal window on the Raspberry Pi we will be greeted with a message reminding us to change our password.

SSH

Spoiler ([Click to View](#))

Terminal on the Raspberry Pi

Spoiler ([Click to View](#))

If you are struggling with this or have any questions post below or send me a private message.

The above tool is for own use or educational testing purpose only.

Thank you for taking the time to read this thread.

Haseo™ - July 16, 2019, 2:39 pm

This is a nice tutorial wake, nicely done. Well written and displayed.

Mr. Robot - July 16, 2019, 2:40 pm

Nice basic tut although you could just attack it with a dict over ssh. Also odds of coming across rogue pis is slim.

It'd be fun to see some on dvp

<http://raspwn.org/>

This entire thread could have been 3 sentences

Wake - July 18, 2019, 1:20 am

(Jul 16, 2019 02:39 PM)Haseo™ Wrote: [\[CITE\]](#) This is a nice tutorial wake, nicely done. Well written and displayed.

Thank you. Thanks for reading.