Raspberry Pi Hacking Device

Jason Nguyen, Joshua Gilbert, Gary Choi, Mitch Wommack

ABSTRACT

Technology is always improving generation by generation; both being used in professional and personal areas. The idea of data safety has become especially important to today's generation. In an age where all your personal information is digital, losing secure control over it can have profoundly serious personal, professional, financial, psychological, or even physical consequences. The chances of situations like these, when the security of digital devices is not taken seriously, are surprisingly high. Anybody could easily gather your information, and they would just need to know how to use an internet search engine and not much more money than it takes to fill up the fuel tank of a large truck.

The worst part is that the average person does not even know that some of the best ways of protecting personal information are so simple and easy that anyone can do it:

- Create more complex passwords that contain a mixture of special characters/numbers/letters
- Changing the default password on any new devices
- Limit the personal information you put online that could be used as a password
- Keep your software up to date
- Use anti-malware software

The main purpose of our Raspberry Pi Hacker is to have people realize that they could defend against most hacking attacks if they took those extra steps towards security. Thanks to the low cost, portability, and minimum needs of the Raspberry Pi, anyone could become a hacker and cause problems for those

around them. The software that comes pre-installed in the Raspberry Pi Hacker's operating system (Kali Linux) has the ability to run a wide range of attacks against other devices. This project serves the purpose of showcasing real-world cybersecurity vulnerabilities for those who aren't familiar with them in a way that is more tangible than them just hearing about another hacking incident in the news. This will, in theory, make them more responsive to our suggestions for improving the security of their own devices. But for those that are more familiar with this field, the Raspberry Pi Hacker will be able to go beyond simple attacks and can be used for more complex penetration operations.

What's Important

We are making a device that, at a minimum, should be able to disrupt other people's devices, and ideally, gain access to their devices. This allows the average person to realize that these kinds of attacks can happen with minimum effort and cost from someone with ill intent. Professionals can easily spend a lot of money on various technologies to disrupt and hack into other systems. But we are trying to prove that anyone could achieve this with just a little bit of knowledge and just a little bit of money involved. Our end goal is for more people to take their cybersecurity more seriously and to better protect themselves and their devices. If more people take just a few extra steps on upgrading the security for their devices, hackers will have a lower chance of being successful. And that is what we want to prove throughout this project. In terms of the Raspberry Pi Hacker, our measure of success is the disruption of and/or unauthorized access to our target systems, which are set at default values. And if it succeeds at those default values but fails after the extra step on security has been implemented. Then that will be proof that the extra steps have done their job.

What is the difference between this and other projects?

As a whole group, we have talked about this project being as simple as possible. When we think of everyday people's perspectives, we know that many find that talking about, none the less understanding, technology as an overwhelming thing. So, we try to simplify everything involved so that understanding the process of how hacking/protecting our provided devices works more digestible and something that they can relate to. As mentioned above, we aim to gather materials that are not awfully expensive because we want to prove that we only cheap resources in order to invade people's privacy. And that to summarize why people should take those few and easy extra steps into their security protocols. Also, the main product of this project, the Raspberry Pi 4 8GB model, could be bought separately according to its parts so the price would be cheaper if finding the right prices on the market.

What are the expected results?

We plan to have the Raspberry Pi Hacker contain a remote interface so the attacker can discretely use it while the device is hidden, in say their bag, to attack their targets around them. As for targets, we are going to set up multiple devices that are different from each other such as routers, laptops, phones, etc. From this, we could prove the functionality of the Raspberry Pi Hacker's performance at its best. There are two ways we would want the audience to look at this project:

1. The Raspberry Pi hacking into various devices that have:

    a. Generic and default settings

    b. Poor choice of username and passwords

    c. A laptop with/without a firewall

    d. Poor security from different makes and models of mobile phones

    e. Poor router security

f. And other everyday devices and pitfalls

2. Then the Raspberry Pi attacking devices with:

a. Complex passwords

b. Better security software on the same devices

In this way, we could compare the two outcomes to see which option had better results in the scenario. If proven correct, the Raspberry Pi Hacker should have a more difficult time trying to access information in the second scenario than it did in the first. A good example would be the processing time being slowed down due to the extra security measures. Ultimately, we want to prove the fact if people have the motivation to implement a few extra measures tighten their security, there would be less successful attacks from people who have ill intent towards them. And to do so in a way that is relatable to people who are otherwise put-off by trying to understand how the technology all around them can be harmful to them.