# Humanity Has Never Been More Programmable

In the world of computer security, there’s a term known as pentesting (short for penetration testing). Pentesting is the process of testing a computer system or network (or a building) for weaknesses that can be exploited.

!http://screwthezoo.wpenginepowered.com/wp-content/uploads/hacked-binary.jpg

Companies will hire a hacker or a team of hackers to attempt to break into their physical and/or digital properties preemptively. Talk about fascinating! Considering how many massive computer security breaches we’ve seen in the last few years, perhaps a few more companies should be investing in pentests.

When a hacker conducts a penetration test, they typically start with the most common weaknesses: people, default passwords on servers and software, easy to guess user passwords, well known and unpatched vulnerabilities, etc. They start with the low hanging fruit, and in far too many cases, that’s sufficient to break into a system. As Einstein said, \*“Two things are infinite, the Universe, and human stupidity.”\*

>

>

>

> \*“A lot of hacking is playing with other people, you know, getting them to do strange things.” – Steve Wozniak\*

>

The thing is, the human brain isn’t all that different from a computer when it comes to [exploitable weaknesses](https://en.wikipedia.org/wiki/Social\_engineering\_%28security%29). Virtually all people suffer from the same set of psychological vulnerabilities, and if you make an effort to learn what these vulnerabilities are, you can use them to your advantage.

What, you ask, are these weaknesses? Psychologists call them Cognitive Biases. Here are just a few of the more common ones, courtesy of Wikipedia:

- \*\*Bandwagon Effect –\*\* The tendency to do (or believe) things because many other people do (or believe) the same.

- \*\*Confirmation Bias –\*\* The tendency to search for, interpret, focus on, and remember information in a way that confirms one’s preconceptions.

- \*\*Frequency Illusion –\*\* The illusion in which a word, a name, or other thing that has recently come to one’s attention suddenly seems to appear with improbable frequency shortly afterwards.

- \*\*Gambler’s Fallacy –\*\* The tendency to think that future probabilities are altered by past events, when in reality they are unchanged.

- \*\*Hindsight Bias –\*\* The tendency to see past events as being predictable at the time those events happened, even though they were nothing of the sort.

- \*\*Loss Aversion –\*\* The disutility of giving up an object is greater than the utility associated with acquiring it. (In other words, you’ll fight harder to keep something than you will to acquire it in the first place.)

- \*\*Survivorship Bias –\*\* Concentrating on the people or things that “survived” some process, and inadvertently overlooking those that didn’t because of their lack of visibility.

This is \*\*far\*\* from a complete list, as there are literally hundreds of cognitive biases. Seriously, go to Google and search \*\*[List of Cognitive Biases](https://en.wikipedia.org/wiki/List\_of\_cognitive\_biases)\*\*, and read through the Wikipedia page. Your. Mind. Will. Be. Blown.

In fact, there’s a great book that came out recently called \*[The Art of Thinking Clearly\*, by Rolf Dobelli](http://www.amazon.com/The-Thinking-Clearly-Rolf-Dobelli/dp/0062219685/), that explores many cognitive biases in more detail.

Of course, different people experience these cognitive biases to greater or lesser degrees, but you’ll find their existence to be fairly universal. And, once you know what to look for, and how to leverage them, you’ll be amazed at what you can accomplish.

When a skilled hacker is preparing to break into a network, the first thing they do is research. They observe, poke around, and try to get a feel for their target. Hacking people is no different.

Because we’re all human, we’re all subject to these same biases. So, before you go trying to hack someone else, first you need to pentest yourself, and shore up your own weaknesses.

Like many of the skills in this book, this one starts with introspection. I recommend the following steps:

\*\*1 –\*\* Go to Wikipedia and carefully read through [the list of cognitive biases](https://en.wikipedia.org/wiki/List\_of\_cognitive\_biases). As you do so, make a note of the cognitive biases that you feel most strongly apply to you.

If you’ve gone through the self-awareness exercises from [earlier in the book](http://www.amazon.com/Screw-Zoo-Escape-From-World/dp/0996154906), you’ll have an advantage at this point. If you haven’t, I recommend you go back and work on the tasks from that section before you do this.

\*\*2 –\*\* Once you have your list of cognitive biases that you feel apply most strongly to you, I want you to start carrying this list around with you.

Then, whenever you find yourself making a judgment, or preparing to make an important decision, I want you to go through your personal list and ask yourself, “Are any of these affecting me right now?”

\*\*3 –\*\* If you find that your judgments or decisions are being impacted by cognitive biases, do your best to re-examine things with that in mind, and to make a more informed judgment or decision.

\*\*4 –\*\* Rinse and repeat. The more you work through this process, the more aware you will become of when your mind is being clouded by cognitive biases. At the same time, your ability to spot biased thinking in others will improve dramatically.

Before you proceed any further, I want you to go through the above process. Why? Because a wise hacker secures their own system before they go poking around in someone else’s. I’d also recommend that you read \*[The Art of Deception\* by Kevin Mitnick](http://www.amazon.com/The-Art-Deception-Controlling-Security/dp/0471237124/). It’s an excellent primer on human hacking.

Beyond that, before you go hacking anyone or anything, you should always stop to consider the consequences; not just the potential consequences to yourself, but the potential consequences to others.