# The Importance of Knowing Your Own Security Posture

It is a typical day. Michael starts at 10:00 p.m. He grabs a bottle of highly caffeinated soda, turns on the Dub-step playlist, and sits down at his computer. Next, Michael launches his Tor client to ensure anonymity and begins to fingerprint, scan, and enumerate his target. After a few hours, Michael has a good idea of the company's network infrastructure as well as a list of servers—both Internet-facing and those sitting on the intranet. Michael also knows which systems have which vulnerabilities. Michael shuts down for the day and begins to plan his attack. The company that he targeted and mapped contains a database with thousands of credit cards that are worth thousands of dollars on the black market.

Even though Michael has all of the information that he needs to launch an attack, he also knows the time and realizes that the network operations team and the security response team for the company are beginning to start their normal workday. Launching an attack now might be detected by active eyes monitoring the system. After all, a hacker's goal is to not be caught. Michael will wait until the upcoming weekend to steal the credit card data, when it is least likely that he will be detected.

The problem is that the company Michael just "cased" is your company. This is no longer a random third party; you have a vested interest in the success of the company, and because you are a lead security analyst, you also want to protect the company's data. As you start your day, you notice that a couple of network pings, sweeps, and port maps took place from the Internet, but in reality, this is nothing new.

You are curious about the activity from overnight and conduct some preliminary investigations about the source of this activity. You see that it originates from a Tor network, so tracing the real origination source will be challenging, if not impossible. Therefore, it is not worth your time and resources. After all, you have a task that is far more important to complete.

You have been looking at the security posture of the company network resources for the past month. You have conducted scans, vulnerability assessments, and some penetration tests. It is time to finalize your report and deliver it to management and the operations teams.

After the meeting, everyone was impressed with your analysis, and they realize that the current systems need some changes. Your recommendations include the following:

- Configuration changes (from default to security settings)
- Changing of easy-to-guess passwords
- Patching of systems and firewalls

All of these are easy tasks, and the operations teams agree to accomplish them throughout the upcoming week.

Friday morning, you get word that most of the easy tasks have been tested and implemented. You conduct one more quick vulnerability assessment scan before you leave for the weekend and are pleased with the results. You feel good about the risk assessment that you conducted but even better that the organization took you seriously and implemented the changes. It's time for a fun, relaxing weekend!

Meanwhile, it's late Saturday, and Michael sits back down at his computer, turns up the stereo, and gets ready to make some money. He plans to break into the company he targeted the past weekend and steal those credit cards to sell them for quite a profit. He launches his Tor client, does a quick ping scan to make sure the targets are still there, and after confirmation, he launches his first attack…

Failure!

The buffer overflow exploit that he has used many times in the past did not work. He tries a second attack against a second machine, and again: failure. Confused, he completes the same scan activities that he performed last week, and the entire attack surface that he previously mapped has changed. Michael begins to wonder what happened and what he detected. Will he be caught and prosecuted?

Michael stops his activity for the time being to catch his breath, and he decides the target he's after is no longer a quick "smash-and-grab" situation. He moves on to his next target instead.

## Moral of the Story

Hackers attack sites every day for various reasons. They assess the security posture of an organization. They assess the value of the data or resources held in that organization. If the value is worth the risk and reward, they attack the system and organization.

Security professionals need to know and understand that they too can utilize the exact same tools and techniques that hackers use to assess the security posture of their organization. The difference is that with the knowledge of the existing vulnerabilities, you can take the information, make a positive change, and correct the issues. Hackers take the knowledge and exploit the situation.

A risk assessment can show the potential weaknesses in the organization's security posture, giving the organization the knowledge to effect change and secure the systems, stopping hackers and changing their risk–reward formula.