Have you ever left the light, radio or TV on when you left home? The idea is usually that would-be burglars would see the lights or hear the noise, assume someone was there and move on to less dangerous targets. Over the ages, we humans have become very well versed at feeding our foes false stimuli, using trickery and deceit as a defensive technique. In the information age, little has changed, other than the medium. This remains a highly effective tool for adding to the security of an organization.

Using honeypot techniques in the corporate IT world has some challenges, but done properly, the capabilities are simply amazing. Honeypots have been around in the IT world for quite some time.

The Honeynet Project, probably the most significant work in the field, was founded in 1999. While their work is primarily focused on high interaction, academic study of attacker techniques by offering target systems and network environments up for exploitation, their implementations likely require more than most corporate organizations can manage in time, effort, forensic analysis and capability.

However, by simplifying honeypot technologies away from a systemic approach to emulation of specific services we can begin to pare down the requirements to a more manageable level.

Further, by refining the idea of what data the honeypot should gather from the deeply academic to the more focused “get what a corporate IT person needs” we can easily extend the idea of a “low interaction” honeypot into the corporate IT environment.

The underlying principle is easy to understand. If something is fake, then there is essentially no reason why anyone should interact with it. If we emulate a fake web server, for example, no legitimate users of the network should ever use it, since it holds no real data or significance for them.

Thus, any interaction with a fake service (hereafter referred to as a pseudo-service) is suspicious at best and malicious at worst. That means that from a detective standpoint, if you treat all connections to a pseudo-service as suspicious and investigate them as a potential security incident, they are actually helping you be more secure, even though they are "fake".

Pseudo-services, and other low interaction honeypot technologies, can provide you with visibility into the security posture of your environment. They are very effective at capturing the details of attackers who might be performing reconnaissance against your systems.

They have proven to be capable of detecting human attackers probing for vulnerabilities and malware seeking to spread from system to system inside a network. Pseudo-services simply wait for interaction, after which they capture the essentials that are important to the corporate IT security team, such as source IP addresses and the frequency of the connections. Additionally, since they are able to log all commands and transactions, they often offer deeper insights into the intent and capability of the attacker or malware infection, allowing the security team the flexibility to take different actions as the result of specific threats. For example, they may create automated tools to shutdown the network switch ports for hosts that are clearly infected with a simple worm, while they might activate their full incident response team to handle a more focused, knowledgeable and clearly human attacker.

With a small amount of analysis of the honeypot detection patterns and the observed events, it quickly becomes clear what type of threat is underway.

Pseudo-services, and other low interaction honeypot technologies, can provide you with visibility into the security posture of your environment.

Deployment of pseudo-services is often the first step in an organization's leveraging of honeypot technologies. Usually, this begins by the security team deploying a few services on a dedicated laptop or desktop device and moving this "decoy host" from network to network. This approach is usually referred to as "scatter sensing", since the idea is that you scatter these mobile sensors around the environment.

Once the security team becomes more familiar and comfortable with the honeypot tools, they typically move on to deploying additional decoy hosts on each network segment, or they begin to deploy pseudo-services on their existing production servers, workstations and devices.

Once the honeypot sensors are fully deployed, most organizations find that they are essentially low noise, high signal tools for detecting potential security issues. Most corporate environments with even a basic security program, identify between four and ten security events using the pseudo-service approach each month. Since any and all interactions with a pseudo-service are suspicious, they investigate each occurrence and do not suffer any false positive alerts. The best part of this technique is that the deployments are essentially "deploy and forget". Little ongoing management and maintenance is required since there are no signatures to update or tune!

In my experience, once they get their feet wet in the honeypot world, organizations then typically begin to grow their capabilities beyond pseudo-services. Some begin to create specialized Trojan horse documents and executables to track unauthorized access to files or the movement of files around the world. Many create specialized PDF and HTML documents with embedded links to track who is reading their information in detail.

With some imagination, they create honeypot accounts in their Windows AD infrastructure that alert the security team if and/or when they are accessed. They might begin to use tools to send "fake" credentials across the wire, hoping to direct those attackers using sniffers toward their pseudo-services.

Their experiences vary depending on the effectiveness of the rest of their security program, but many organizations have reported much success with these techniques. Obviously, they have caught infected machines scanning their environments, worms attempting to spread to emulated pseudo-services and employees dabbling in off-the-shelf attack tools. Some have identified 0-day exploits that eluded both network defenses and anti-virus installations.

Others have found that their deployed pseudo-services have been connected to from the public Internet, exposing misconfigurations in perimeter firewalls, routers and port forwarding configurations. In many cases, internal employees and contractors have been identified that were simply "looking around the network" where they should not have been. Corporate honeypots, in my opinion, represent a vastly misunderstood and underutilized resource. Presenting the concepts to upper management may return anything from acceptance to dismay, and from curiosity to "it might make attackers mad". The key to being successful is careful, concise communication of the value. Progressing the idea that these "fake" services can be deployed once, then depended on for ongoing security with little or no day-to-day effort has shown to be a powerful idea in the boardroom.

Starting small, with dedicated workstations and the scatter sensing approach is usually easy to do and requires the smallest of security investments. It also lends itself well to finding that first malware infected host that most security teams leverage to shed light on the proof of concept to their management.

Presenting the concepts to upper management may return anything from acceptance to dismay, and from curiosity to "it might make attackers mad". The key to being successful is careful, concise communication of the value.

Products and services are widely available in the honeypot space. A variety of solutions, both open source and commercial are easily found with a simple Google search. Several consulting firms offer services around designing and implementing honeypot technologies and employing them effectively to help secure your informational assets.

Whether you choose to pursue them on your own or with the guidance of an expert, I believe that your organization will find great value and capability in corporate honeypots. My experiences have shown that they are effective, easy to manage and capable security tools. Give them a try, and please, share your findings with others.

Brent Huston is the CEO and Security Evangelist at MicroSolved (www.microsolved.com). Brent is an accomplished computer and information security speaker and has published numerous white papers on security-related topics. Follow Brent on Twitter at @lbhuston.

Open Disclosure: I am the author of a commercial honeypot suite of products and techniques known as HoneyPoint Security Server. My opinions, do not represent any corporation or other entity. Your paranoia and milage may vary...