Know Your Enemy: Honeynets. HoneyNet Project
Review by Frank Fetters

This paper discusses a data collection technique which involves creating a network of honeypots to lure malicious users into trying to compromise them. The goal is to study and learn from these attacks in order to create stronger protection for actual networks. The paper goes over the three architectural requirements, Data Control, Data Capture, and Data Collection. To sum up, you have to first make sure that the machines you set up to be compromised aren’t used to cause damage outside of your fake network. You also have to come up with a way to record the attacks made on the network without giving up the fact that it is a fake network and without being vulnerable to being disabled by the attacker. And thirdly you must come up with a way to collect and combine all the data collected from multiple machines and networks into a usable report.

The part of this paper that stuck out to me was the amount of discussion on risks. I have read many other articles which skim over this extremely critical part of honeypots and honeynets. In my opinion this is a very dangerous activity. Basically you are setting up a challenge to any malicious person who sees your easy target on the network. I see this as very similar to when the police do a sting operation. The main difference is that the police keep a constant vigilance over their bait and jump in the instant anything illegal goes down or if there man on the inside gets in danger. First of all, honeynets aren’t watched by humans 24/7, but instead rely on automated diction which can definitely be overcome. The paper does advise that human monitoring be implemented, but to my understanding of the current honeypots that are setup this is not the case. Instead humans wait for a notice to be sent to them that a user has been detected. Secondly, honeynets don’t jump in and stop when an unauthorized user comes in. They invite the illegal activity to go on so it can be learned from. Obviously there is a lot that could wrong and I feel this paper did an outstanding job of listing all the possible threats.

The most interesting risk was the risk of detection. If your honeynet is flagged by crackers and listed such, its value decreases. However, this introduces some neat ideas. The paper suggests that a bad-guy might start to watch your honeynet traffic and try to analyze its behaviors in order to take it over. They might try simple easy to detect attacks to see how your honeynet will respond. This creates a “who is watching who” scenario to me. I wonder if there are security professionals watching over the shoulders of crackers who are watching the honeynets which are trying to watch them. I feel this is the epitome of the actual situation on the internet today. We have security professionals creating tools to detect for weaknesses so they can patch them, and then malicious users using these tools intended for security to find weaknesses to exploit.

Overall this was a great article about a very interesting subject.