Introduction

Systems and networks are constantly being probed by attackers to find vulnerabilities. These vulnerabilities are usually some kind of secret door where attackers are able to enter the system to change system settings, view private data, and even take control and launch attacks on other systems. Two established practices to understand and learn about these vulnerabilities are through honeypots and Honeynets.

A honeypot can be defined as: an information system resource whose value lies in unauthorized or illicit use of that resource.\textsuperscript{1} Based on this definition, honeypots are of no use if there are no attackers. Honeypots are not actually production systems, and thus one would not expect much activity unless it was under some kind of malicious attack. There are a few major advantages of having honeypots:
- consists of a simple architecture
- collects high valued data
- requires minimal resources.

A simple architecture is an advantage because it means that there is little time spent on maintenance, supervision, or developing complex algorithms. In this case, simple is better because one does not have to worry about mistakes made, software bugs, or configuration problems. By far the main advantage of honeypots is that data collected is of high value. During the normal course of a day, a system may encounter numerous attacks or attempted attacks but it would also have lot of regular activity from customers and/or internal traffic. Network administrators must sift through all the transactions, and service requests to identify which were malicious. This takes computing time and human resource time and thus, can become very costly. Honeypots only collect malicious data, data that is more valuable to security. The Honeypot requires minimal resources, one machine can emulate a number of others or even a network, and since there is only traffic from malicious attacks, capacity is not a problem.

Honeypots are mainly used in two different categories, production and research. In production, organizations use honeypots to detect attackers, track them, and understand how they commit malicious attacks or denial of service attacks (DOS). Having a way to detect and be deceptive to an attacker is a huge advantage to organizations because they can prepare themselves, fix vulnerabilities, and anticipate attacks. Understanding the enemy and being one step ahead is crucial.

Honeynet
There are two main differences between a Honeynet and honeypot. The first difference is that a Honeynet is a network of systems, and not a single system. The network is behind a firewall so that data entering and exiting is recorded, and controlled. The data is analyzed as in the case of honeypots. The Honeynet network can be customized to contain a number of different systems, different operating systems, databases, different types of encryption, etc. Once the attacker enters the Honeynet, his actions can be monitored, tactics, strategies and tools can be studied to take preventative measures on a real network. The network can be configured such that it can simulate networks of different organizations that require different security requirements. The second difference in a Honeynet is that the systems used in the Honeynet are standard production systems instead of emulations. Therefore, interaction with a Honeynet is as real as any other organization's system and the discoveries that it makes can be very applicable to security flaws in systems used for production.

The value of a Honeynet is the same value as a honeypot. To be able to learn about the enemy before an attack and then inform affected parties or targets of these attackers can save a lot of system down time and potential damage to data integrity. One such example was when a group of attacker conversations were monitored in an IRC (internet relay chat) by using Honeynets and then they were monitored during the attacks as well directed against systems all of one countryii. The Honeynet was able to capture all this information and warn other systems of the victimized country their method of attack so that they had more time to react and defend against the threat. Every packet and keystroke sent to a system in the Honeynet is monitored, so trying to analyse an attack or trying to detect a system being compromised is easier because all the data is complete and known to be malicious. The main security areas that Honeynets have improved are logging, intrusion detection systems (IDS), forensics, network traffic analysis, kernel modules, system hardening, as well as a variety of others.

In setting up the Honeynets, the systems are installed with default installations. For example, Windows NT server would be installed on a system without any added security measures. Many organizations perform security hardening measures to their systems to prevent compromises or breaches but the vast majority of systems connected to the internet only have default installations of operating systems with no added security measures. By creating Honeynets with default installations, data collected will be useful to many networks connected to the internet. Honeynets can also be customized to be similar to a particular network as mentioned above, and that configuration would be able to assist any particular network.

The two main requirements of a Honeynet is data control and data capture. Data control involves controlling the actions of the attacker such that the attacker cannot use any of the systems to launch an attack on another. Data capture is exactly what it implies, logging data that the attacker types in and the actions that are performed. One of the difficulties in satisfying these requirements is that the Honeynet must hide these requirements from the attacker. Attackers can become suspicious if attempts made to launch an attack do not perform as expected. Attackers may also find processes running that indicate monitoring of his/her actions. One way to prevent attackers from launching
an attack (usually denial of service attack) is the snort-line method. This method allows
the attacker to send an attack out but the attack packets are disabled when the Honeynet
detects that an outbound attack is being sent, making the attacker wonder what went
wrong but not being able to figure out why. Capturing data can be difficult at times
especially when the attacker uses personal scripts and encryption. SSH encryption
protocol is used by many students at McMaster to log onto the McMaster network but
attackers also use this to encrypt what they are typing when accessing the system after the
system has been compromised. Even systems that do not have SSH installed find that the
attacker installs SSH first before continuing with their intentions. One way to monitor all
this is to have an especially developed kernel module that has been developed to decipher
all the encrypted data. Once data is collected it must be stored remotely or risk the
chance of the attacker finding it and deleting it or realizing that the network is a Honeynet.
Figure 1.0 depicts an example of a Honeynet. The firewall is used to control the inbound
and outbound data.

Figure 1.0 A picture a network where systems connected to the switch are part of the
Honeynet.

In addition, Honeynets and honeypots are not advertised nor is there anything they
do to attract attackers. However, resourceful attackers do eventually find them and the
Honeynets and honeypots are then able to collect useful information. There is a non-
profit organization called The Honeynet Project that is dedicated to security and raising
awareness. The organization creates Honeynets to conduct research to learn more about
security issues and then provides this information to the public.

Conclusion

Unfortunately, the existence of a network or system connected to the internet is
enough to attract attackers. This means that our networks and computers are always at
risk and we must do what we can to protect our systems from these malicious attacks.
There is often no motive for these attacks other than a cheap thrill at the cost of someone
else. A few recommendations to avoid known windows of opportunity for attack are to
always download latest security patches, install anti-virus software and keep virus
definitions updated, and avoid sharing files with strangers. Preventative action is the purpose of the honeypots and Honeynets, this preventative action is one way to stay one step ahead of the enemy in the ongoing cyber security war.


iv The Honeynet Project, 17, March, 2003 www.honeyet.org