COMP 5370 – HW7a  
John Carroll | jcc0044/902521946

In computer terminology, a honeypot is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. Generally, a honeypot consists of data (for example, in a network site) that appears to be a legitimate part of the site but is actually isolated and monitored, and that seems to contain information or a resource of value to attackers, which are then blocked. This is similar to the police baiting a criminal and then conducting undercover surveillance, and finally punishing the criminal.

Two or more honeypots on a network form a honeynet. Typically, a honeynet is used for monitoring a larger and/or more diverse network in which one honeypot may not be sufficient. Honeynets and honeypots are usually implemented as parts of larger network intrusion detection systems. A honeyfarm is a centralized collection of honeypots and analysis tools.

The concept of the honeynet first began in 1999 when Lance Spitzner, founder of the Honeynet Project, published the paper "To Build a Honeypot": A honeynet is a network of high interaction honeypots that simulates a production network and configured such that all activity is monitored, recorded and in a degree, discreetly regulated.

A honeywall is a gateway computer that separates the honeypots on a honeynet from the network that the honeynet is deployed on. The Honeywall CDROM is a Linux installation CD that contains all of the tools necessary to install, configure, and manage a honeywall computer.

High-interaction honeypots imitate the activities of the production systems that host a variety of services and, therefore, an attacker may be allowed a lot of services to waste his time. By employing virtual machines, multiple honeypots can be hosted on a single physical machine. Therefore, even if the honeypot is compromised, it can be restored more quickly. In general, high-interaction honeypots provide more security by being difficult to detect, but they are expensive to maintain. If virtual machines are not available, one physical computer must be maintained for each honeypot, which can be exorbitantly expensive. High-interaction is complex to deploy, has greater risk, and captures extensive information. Examples of it include ManTrap and Honeynets.

Low-interaction honeypots simulate only the services frequently requested by attackers. Since they consume relatively few resources, multiple virtual machines can easily be hosted on one physical system, the virtual systems have a short response time, and less code is required, reducing the complexity of the virtual system's security. Low-interaction emulates services and operating systems, is easy to deploy, has minimal risk, and captures limited information. Some examples of it include Specter, KFSensor, and Honeyd.

Malware honeypots are used to detect malware by exploiting the known replication and attack vectors of malware. Replication vectors such as USB flash drives can easily be verified for evidence of modifications, either through manual means or utilizing special-purpose honeypots that emulate drives. Malware increasingly is used to search for and steal cryptocurrencies, which provides opportunities for services such as Bitcoin Vigil to create and monitor honeypots by using small amount of money to provide early warning alerts of malware infection.

An email address that is not used for any other purpose than to receive spam can also be considered a spam honeypot. Compared with the term "spamtrap", the term "honeypot" might be more suitable for systems and techniques that are used to detect or counterattacks and probes. With a spamtrap, spam arrives at its destination "legitimately"—exactly as non-spam email would arrive.

Databases often get attacked by intruders using SQL Injection. As such activities are not recognized by basic firewalls, companies often use database firewalls for protection. Some of the available SQL database firewalls provide/support honeypot architectures so that the intruder runs against a trap database while the web application remains functional.

Just as honeypots are weapons against spammers, honeypot detection systems are spammer-employed counter-weapons. As detection systems would likely use unique characteristics of specific honeypots to identify them, a great deal of honeypots in use makes the set of unique characteristics larger and more daunting to those seeking to detect and thereby identify them. This is an unusual circumstance in software: a situation in which "versionitis" (a large number of versions of the same software, all differing slightly from each other) can be beneficial. There's also an advantage in having some easy-to-detect honeypots deployed. Fred Cohen, the inventor of the Deception Toolkit, even argues that every system running his honeypot should have a deception port that adversaries can use to detect the honeypot. Cohen believes that this might deter adversaries.

In many cases, honeypot use cannot be labelled as being unethical because of its apparent advantages. The article, 'Combat Viruses' by Kurt Kleiner, proves that in some systems, honeypots have been known to contain and fight computer viruses. In another article, 'Using honeypots to fake out an attacker', Mark Edmead lists the most common advantages of using honeypots in security systems. Honeynet.org is an organization committed to raising awareness of the vulnerabilities that exist on the Internet today and putting the advantages of honeypots into use.

Litmus is an alternative to honeypots.