# Chapter 3.31
# Deploying Honeynets

**Ronald C. Dodge, Jr.**
*United States Military Academy, USA*

**Daniel Ragsdale**
*United States Military Academy, USA*

## ABSTRACT

*When competent computer network system administrators are faced with malicious activity on their networks, they think of the problem in terms of four distinct but related activities: detection, prevention, mitigation, and response. The greatest challenge of these four phases is detection. Typically, detection comes in the form of* intrusion detection system *(IDS) alerts and automated application and log monitors. These however are fraught with mischaracterized alerts that leave administrators looking for a needle in a haystack. One of the most promising emerging security tools is the honeynet Honeynets are designed to divert the malicious user or attacker to non-production systems that are carefully monitored and configured to allow detailed analysis of the attackers' actions and also protection of other network resources. Honeynets can be configured in many different ways and implemented from a full DMZ to a carefully placed file that is monitored for access.*

## SYSTEM ADMINISTRATOR VS. ATTACKER

*"All warfare is based on deception."*
*Sun Tzu*

System administrators often consult an intrusion detection system or will manually review the event log on servers, firewalls, or hosts computers when investigating malicious activity. Unfortunately, this response to suspected malicious behavior often causes system administrators to draw erroneous conclusions. These faulty conclusions fall into two categories: mischaracterizing good traffic as malicious (known as a "false positive" or "false alarm") and failing to detect an attack (sometimes called a "false negative" or "miss"). Clearly, both types of faulty conclusions can have very serious negative consequences. Making the problem even worse is the exponentially increasing volume of legitimate traffic and system activity that IDSs must evaluate to identify malicious activity. In the present day, if an administrator were to rely solely on conventional IDSs and manual log analysis to identify malicious behavior system, it is a foregone conclusion that he or she will suffer from one or both types of errors.

Competent hackers are, of course, concerned with obscuring their malicious activity. Unfortunately for present day system administrators, hackers have developed a wide array of sophisticated tools and techniques that support their malicious intentions while minimizing the likelihood of detection. From the first stages of an attack to the final steps, skilled hackers typically work to achieve their malicious end without ever being noticed. During the reconnaissance phase, for example, skillful hackers use techniques that are specifically designed not to raise flags on conventional intrusion-detection systems while collecting as much useful information as possible about targeted systems and networks. Once a host has been compromised, hackers often retrieve powerful tools and utilities from a previously compromised computer acting as a file repository that enables them to install root kits and backdoors and conduct further stealthy penetration of the target network. They do this to allow for future access to the compromised host, while masking their activity.

Honeynets are an extremely useful security tool that can supplement conventional intrusion-detection systems and thwart hackers' attempts to avoid detection and remain anonymous. A honeynet introduces deception into the system administrators' arsenal. When implemented, a honeynet can turn a system administrator's job from finding a needle in a haystack to having a pile of needles. They do this by providing a target for hackers to attack that is designed to monitor, record, and track all of their activity while mitigating the risk exposure to the rest of the targeted network. Honeynets provide three primary functions: intrusion detection, attack understanding, and attacker attribution.

## NETWORK DECEPTION

While network deception is not a new concept, deception is an emerging model in network operations. A common example of deception is the Allies effort to hide from Germany the nature of Operation Overlord, the invasion of France, offering false thrusts and fake equipment. A classic military definition of deception is (DOD, 2004):

> *Actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.*

We define computer security deception as being those actions taken to deliberately mislead computer attackers and to cause them to take specific actions. The application of honeynets as part of a deception plan for network security is supported by this definition. Our general deception goal is to mislead an attacker into a predictable course of action that can be exploited (Dewar, 1989). Honeynets can be deployed in many ways—each employment should be designed to support a specific goal in the overall network deception plan. As an example, a honeynet could be deployed within the DMZ subnet of an organization providing external Web services or deployed on the inside of a network behind most firewall and intrusion detection devices. Additionally, the type of honeynet can vary from a robust network of systems designed to look like a small domain or a single record placed in a sensitive database. We will define these honeynet architectures in detail later in the chapter.