**Honeypots (1):**
**Introduction**

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In recent weeks, we’ve been looking at managing vulnerability assessment systems and intrusion detection systems. Norwich University undergraduate student Bob Pelletier is doing some interesting research work on honeypots in the IS406C independent study program with me this term in which he is building a working honeypot system using virtual machines. He did some good background reading about honeypots in the IS340 Intro to Information Assurance and CJ341 Cyberlaw and Cybercrime courses; he has very kindly allowed me to publish his work here as part of the ongoing series. As usual, I’ve made some minor edits for the new context, but all of the following is Bob’s own writing.

* * *

With the growing use of computers in today’s society, the protection of information has become of key importance. Malicious hackers (*blackhats*) continuously try to breach security measures to gain access to protected information. Some blackhats attack computers for fun but others are truly criminals seeking personal gain. The security community is faced with the daunting task of fending off computer attackers and ensuring the confidentiality, integrity, availability, control, authenticity and utility of information. To help better understand the methods used by the blackhat community, a new tool has been developed: the *honeypot*. The use of honeypots has caused a heated debate within the security field. Many question the legality and ethics of such a system. This series of articles outlines the basic legal issues surrounding honeypots as well as some ethical issues to ponder.

A honeypot is any system designed for the sole purpose of being exploited. This is a broad definition that can be implemented in many ways. Some honeypot systems use software, some use actual production machines, and some even use virtual machines such as with VMware. Whichever honeypot design method is chosen, the underlying goal is to create a system that appears to be vulnerable.

What makes a honeypot different from other vulnerable computer systems is its extensive logging capability. The systems most often include at least four layers of logging to capture attacker activity. Every file accessed, every connection made, every keystroke an attacker makes on a honeypot is logged to a secure location. The advantage of logging attacker activity is the chance to get an inside view of the blackhat community’s methodology. Learning common methods and attack tools of attackers can aid security experts in designing new protection measures. Studying attack trends can also help predict future attacks. The *Honeynet Project* founded by Lance Spitzner demonstrates the usefulness of honeypots as a research tool.

Honeypots are not only used for research purposes, but also for production. Implementing a honeypot within a company can create a type of intrusion detection system (IDS). The design of a honeypot suggests that any connection attempts made with the system are unauthorized. This is because normal business functions do not use the honeypot; only an attacker would be
attempting to use the system. Therefore, activity on a honeypot can alert an organization that an attacker is present. From there a company can close the security hole used by the attacker, investigate the incident, and possibly press charges.

* * *

In the next articles in this series, Bob Pelletier (mailto:pelletib@norwich.edu) looks at some of the legal issues surrounding the use of honeypots.

* * *

For further reading:

Honeypots.net: Intrusion detection, honeypots & incident response (resources).  http://www.honeypots.net/


* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.norwich.edu/msia> for full details.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2003 Bob Pelletier & M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.