Global Information Assurance Certification Paper

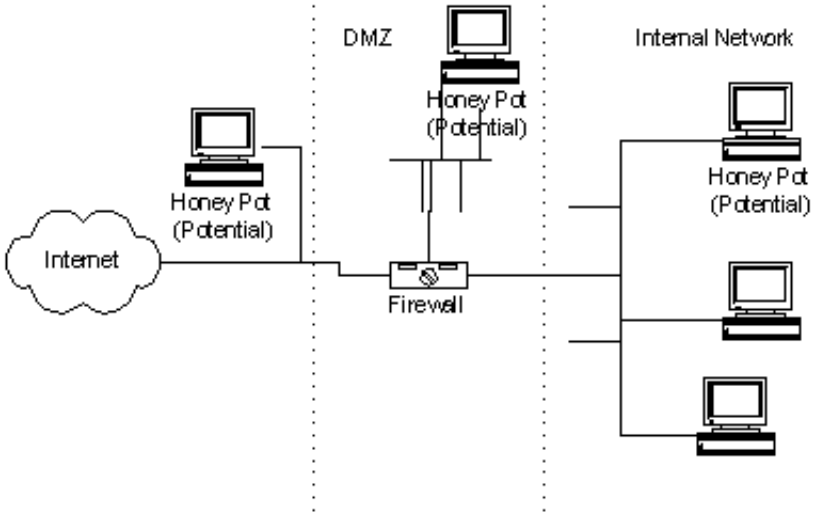
Honey Pot Systems Explained
Loras R. Even
July 12, 2000

Overview

Honey Pot Systems are decoy servers or systems setup to gather information regarding an attacker or intruder into your system. It is important to remember that Honey Pots do not replace other traditional Internet security systems; they are an additional level or system.

Honey Pots can be setup inside, outside or in the DMZ of a firewall design or even in all of the locations although they are most often deployed inside of a firewall for control purposes. In a sense, they are variants of standard Intruder Detection Systems (IDS) but with more of a focus on information gathering and deception.

An example of a Honey Pot systems installed in a traditional Internet security design:



A Honey Pot system is setup to be easier prey for intruders than true production systems but with minor system modifications so that their activity can be logged of traced. The general thought is that once an intruder breaks into a system, they will come back for subsequent visits. During these subsequent visits, additional information can be gathered and additional attempts at file, security and system access on the Honey can be monitored and saved.

Generally, there are two popular reasons or goals behind setting up a Honey Pot:

1. Learn how intruders probe and attempt to gain access to your systems. The general idea is that since a record of the intruder's activities is kept, you can gain insight into attack methodologies to better protect your real production systems.
2. Gather forensic information required to aid in the apprehension or prosecution of intruders. This is the sort of information often needed to provide law enforcement officials with the details needed to prosecute.

The common line of thought in setting up Honey Pot systems is that it is acceptable to use lies or deception when dealing with intruders. What this means to you when setting up a Honey Pot is that certain goals have to be considered.

Those goals are:

1. The Honey Pot system should appear as generic as possible. If you are deploying a Microsoft NT based system, it should appear to the potential intruder that the system has not been modified

or they may disconnect before much information is collected.
2. You need to be careful in what traffic you allow the intruder to send back out to the Internet for you don't want to become a launch point for attacks against other entities on the Internet. (One of the reasons for installing a Honey Pot inside of the firewall!)
3. You will want to make your Honey Pot an interesting site by placing "Dummy" information or make it appear as though the intruder has found an "Intranet" server, etc. Expect to spend some time making your Honey Pot appear legitimate so that intruders will spend enough time investigating and perusing the system so that you are able to gather as much forensic information as possible.

Some caveats exist that should be considered when implementing a Honey pot system. Some of the more important are:

The first caveat is the consideration that if the information gathered from a Honey Pot system is used for prosecution purposes, it may or may not be deemed admissible in court. While information regarding this issue is difficult to come by, having been hired as an expert witness for forensic data recovery purposes, I have serious reservations regarding whether or not all courts will accept this as evidence or if non-technical juries are able to understand the legitimacy of it as evidence.

The second main caveat for consideration is whether hacking organizations will rally against an organization that has set "traps" and make them a public target for other hackers. Examples of this sort of activity can be found easily on any of the popular hacker's sites or their publications.

Levels or Layers of Tracking

The information provided on an intruder depends on the levels of tracking that you've enabled on your Honey Pot. Common tracking levels include the firewall, system logs on the Honey Pot and sniffer-based tools.

Firewall Logs

Firewalls are useful as part of the overall Honey Pot design for many reasons. Most firewalls provide activity-logging capabilities which can be used to identify how an intruder is attempting to get into a Honey Pot. I liken firewall logs to router logs; they can both be set to trap and save packets of a pre-determined type. Remember that when setting up the firewall, you would normally want to log ALL packets going to the Honey Pot system, as there should be no legitimate reason for traffic going to or from the Honey Pot.

Reviewing the order, sequence, time stamps and type of packets used by an intruder to gain access to you Honey Pot will help you identify the tools, methodology being used by the intruder and their intentions (vandalism, data theft, remote launch point search, etc.). Depending on the detail capabilities of logging on your firewall you may or not be able to gain considerable information from these logs.

Another useful function of many firewalls is their notification capabilities. Most firewalls can be configured to send alerts by email or pager to notify you of traffic going to or from your Honey Pot. This can be extremely useful in letting you review intruder activity WHILE it's happening.

System Logs

Unix and Microsoft NT seem to have the lion share of the Internet server markets. Luckily, both operating systems have logging capabilities built into their operating systems, which help identify what changes or attempts have been made. It should be noted that out-of-the box, Unix offers superior logging capabilities as compared to Microsoft NT.

Some of their out-of-the box logging capabilities include:

1. Microsoft NT
    a. Security – Available from Event Viewer
    b. User Management – Needs to be enabled through User Manager

    c. Running Services – Netsvc.exe needs to be manually run and compared to baseline.
2. Unix
    a. User activity logs – utmp, wtmp, btmp, lastlog, messages
    b. Syslogd – An important option is that it can log to a remote server! The range of facilities and priorities available through syslogd is very good.

There are also several tools available that greatly increase the information that can be gathered. Many of the Unix tools are public domain, while many of the Microsoft NT tools are not.

Sniffer Tools

Sniffer tools provide the capability of seeing all of the information or packets going between the firewall and the Honey Pot system. Most of the sniffers available are capable of decoding common tcp packets such as Telnet, HTTP and SMTP. Using a sniffer tool allows you to interrogate packets in more detail to determine which methods the intruder is trying to use in much more detail than firewall or system logging alone.

An additional benefit to sniffer tools is that they can also create and store log files. The log files can then be stored and used for forensic purposes.

Honey Pot Solutions

Implementation of a Honey Pot solution as part of a security system first involves the decision of whether to purchase a commercial solution or decide to develop your own.

Building a Honey Pot

There is a variety of public domain tools and software available that can be useful to help you setup a Honey Pot as well as many sites dedicated to helping guide you through the process. Most tools seem to have originated on the Unix platform, while many have been ported to Microsoft NT.

What you will need to create or develop your own Honey Pot system are a minimum of the following components and considerable configuration time:

1. A Workstation or PC. It appears as though an Intel-based workstation is fine.
2. An operating system. I prefer BSD Unix or RedHat as there are more tools available for the Unix platform than NT.
3. Sniffer package.

Commercial Honey Pot Systems

There are a variety of commercial Honey Pot systems available. The operating systems most widely supported are Microsoft NT and Unix. As many of the commercial product have been released in the past 12 – 18 months, some of them are still in relatively early versions. I tried to find information regarding market share but wasn't able to find any published statistics.

Some of the commercial Honey Pot systems available are:

1. Network Associates, Cybercop Sting
2. Tripwire, Tripwire
3. Fred Cohen and Associates, Deception Toolkit
4. Recourse Technologies, ManTrap

Schwartau, Winn. "Lying to hackers is okay by me: Part 9 of 9" 7 July 1999. URL: http://www.nwfusion.com/newsletters/sec/0705sec2.html?nf 21 June 2000

Young, Kevin. "A Fly-strip Security Scheme." 15 Nov. 1999. URL: http://www.zdnet.com/computershopper/stories/reviews/0,7171,2392030,00.html 21 June 2000

Ranum, Marcus. "Intrusion Detection: Challenges and Myths." URL: http://www.nfr.net/forum/publications/id-myths.html 21 June 2000

Duvall, Mel. "New Decoy Technology Designed to Sting Hackers." 1 June 1998. URL: http://www4.zdnet.com/intweek/daily/980601k.html 21 June 2000

Spitzner, Lance. "To Build a Honeypot." 7 June 2000 7 June 2000. URL: http://www.enteract.com/~lspitz/honeypot.html 22 June 2000