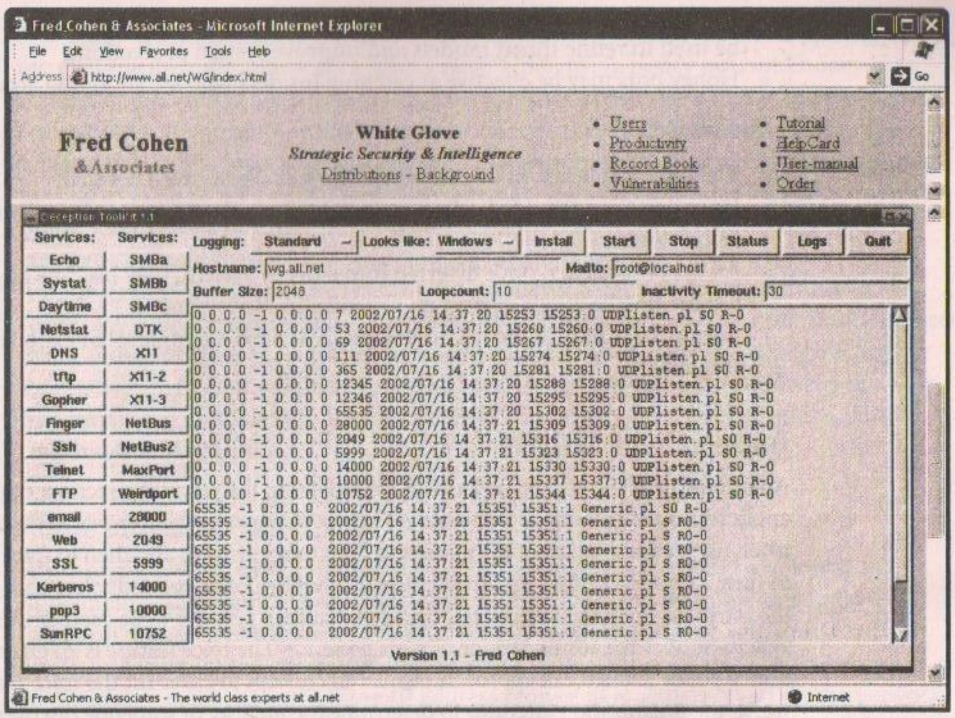
HONEY POTS, HONEY NETS, AND PADDED CELL SYSTEM

A class of powerful security tools that go beyond routine intrusion detection is known variously as honey pots, honey nets, or padded cell systems. To realize why these tools are not yet widely used, you must understand how these products differ from a traditional IDS. Honey pots are decoy systems designed to lure potential attackers away from critical systems and encourage attacks against the themselves. Indeed, these systems are created for the sole purpose of deceiving potential attackers. In the industry, they are also known as decoys, lures, and fly-traps. When a collection of honey pots connects several honey pot systems on a subnet, it may be called a honey net. A honey pot system (or in the case of a honey net, an entire sub network) contains pseudo-services that emulate well-known services but is configured in ways that make it look vulnerable-that is, easily subject to attacks. This combination of attractants (i.e., attractive features such as the presence of both well-known services and vulnerabilities) is meant to lure potential attackers into committing an attack, and thereby revealing their existence-the idea being that once organizations have detected these attackers, they can better defend their networks against future attacks against real assets. In sum, honey pots are designed to:

- Divert an attacker from accessing critical systems
- Collect information about the attacker's activity
- Encourage the attacker to stay on the system long enough for administrators to document the event and, perhaps, respond

Honey pot systems are filled with information that is designed to appear valuable (hence the name honey pots), but this information is fabricated and would not even be useful to a legitimate user of the system. Thus, any time a honey pot is accessed, this constitutes suspicious activity. Honey pots are instrumented with sensitive monitors and event loggers that detect these attempts to access the system and collect information about the potential attacker's activities. A screenshot from a simple IDS that specializes in honey pot techniques, called Deception Toolkit, is shown in Figure 7-8. This screenshot shows the configuration of the honey pot as it is waiting for an attack.



Logging: Standard
Looks like: Windows
Hostname: wg.all.net
Mailto: root@localhost
Buffer Size: 2048
Loopcount: 10
Inactivity Timeout: 30

```
0.0.0.0 -1 0.0.0.0 7 2002/07/16 14:37:20 15253 15253:0 UDPlisten.pl S0 R-0
0.0.0.0 -1 0.0.0.0 53 2002/07/16 14:37:20 15260 15260:0 UDPlisten.pl S0 R-0
0.0.0.0 -1 0.0.0.0 69 2002/07/16 14:37:20 15267 15267:0 UDPlisten.pl S0 R-0
0.0.0.0 -1 0.0.0.0 111 2002/07/16 14:37:20 15274 15274:0 UDPlisten.pl S0 R-0
0.0.0.0 -1 0.0.0.0 365 2002/07/16 14:37:20 15281 15281:0 UDPlisten.pl S0 R-0
0.0.0.0 -1 0.0.0.0 12345 2002/07/16 14:37:20 15288 15288:0 UDPlisten.pl S0 R-0
0.0.0.0 -1 0.0.0.0 12346 2002/07/16 14:37:20 15295 15295:0 UDPlisten.pl S0 R-0
0.0.0.0 -1 0.0.0.0 65535 2002/07/16 14:37:20 15302 15302:0 UDPlisten.pl S0 R-0
0.0.0.0 -1 0.0.0.0 28000 2002/07/16 14:37:21 15309 15309:0 UDPlisten.pl S0 R-0
0.0.0.0 -1 0.0.0.0 2049 2002/07/16 14:37:21 15316 15316:0 UDPlisten.pl S0 R-0
0.0.0.0 -1 0.0.0.0 5999 2002/07/16 14:37:21 15323 15323:0 UDPlisten.pl S0 R-0
0.0.0.0 -1 0.0.0.0 14000 2002/07/16 14:37:21 15330 15330:0 UDPlisten.pl S0 R-0
0.0.0.0 -1 0.0.0.0 10000 2002/07/16 14:37:21 15337 15337:0 UDPlisten.pl S0 R-0
0.0.0.0 -1 0.0.0.0 10752 2002/07/16 14:37:21 15344 15344:0 UDPlisten.pl S0 R-0
65535 -1 0.0.0.0  2002/07/16 14:37:21 15351 15351:1 Generic.pl S0 R-0
65535 -1 0.0.0.0  2002/07/16 14:37:21 15351 15351:1 Generic.pl S R0-0
65535 -1 0.0.0.0  2002/07/16 14:37:21 15351 15351:1 Generic.pl S R0-0
65535 -1 0.0.0.0  2002/07/16 14:37:21 15351 15351:1 Generic.pl S R0-0
65535 -1 0.0.0.0  2002/07/16 14:37:21 15351 15351:1 Generic.pl S R0-0
65535 -1 0.0.0.0  2002/07/16 14:37:21 15351 15351:1 Generic.pl S R0-0
65535 -1 0.0.0.0  2002/07/16 14:37:21 15351 15351:1 Generic.pl S R0-0
65535 -1 0.0.0.0  2002/07/16 14:37:21 15351 15351:1 Generic.pl S R0-0
65535 -1 0.0.0.0  2002/07/16 14:37:21 15351 15351:1 Generic.pl S R0-0
65535 -1 0.0.0.0  2002/07/16 14:37:21 15351 15351:1 Generic.pl S R0-0
```

FIGURE 7-8 Deception Toolkit

Padded cells take a different approach. A **padded cell** is a honey pot that has been

Padded cells take a different approach. A **padded cell** is a honey poi that has been protected so that that it cannot be easily compromised. In other words, a padded cell is a hardened honey pot. In addition to attracting attackers with tempting data, a padded cell operates in tandem with a traditional IDS. when the IDS detects attackers, it seamlessly transfers them to a special simulated environment where they can cause no harm-the nature of this host environment is what gives the approach its name, padded cell. As in honey pots, this environment (an be filled with interesting data, some of which can be designed to convince an attacker that the attack is going according to plan. Like honey

pots, padded cells are well-instrumented and offer unique opportunities for a would-be victim organization to monitor the actions of an attacker.

IDS researchers have used padded cell and honey pot systems since the late 1980s, but until recently no commercial versions of these products were available. It is important to seek guidance from legal counsel before deciding to use either of these systems in your operational environment, since using an attractant and then launching a back-hack or counterstrike might be construed as an illegal action and make the organization subject to a lawsuit or a criminal complaint.

The advantages and disadvantages of using the honey pot or padded cell approach are summarized below:

Advantages:

- Attackers can be diverted to targets that they cannot damage.
- Administrators have time to decide how to respond to an attacker.
- Attackers actions can be easily and more extensively monitored and the records can be used to refine threat models and improve system protections.
- Honey pots may be effective at catching insiders who are snooping around a network.

Disadvantages:

- The legal implications of using such devices are not well defined.
- Honey pots and padded cells have not yet been shown to be generally useful security technologies.
- An expert attacker, once diverted into a decoy system, may become angry and launch a

more hostile attack against an organization's systems.

- Administrators and security managers will need a high level of expertise to use these systems.

Source : http://elearningatria.files.wordpress.com/2013/10/ise-viii-information-and-network-security-06is835-notes.pdf