11.3.2 Honeypot Facts

Honeypots are a unique type of IDS. Although a honeypot can act as a form of IDS, that is only a fraction of its functionality. Honeypots are set up to capture attacker behavior and techniques without compromising real network operations.

This lesson covers the following topics:

- Honeypot overview
- Honeypot interaction levels
- Honeypot tools

Honeypot Overview

The purpose of a honeypot is to look so much like a legitimate network resource that an attacker finds it indistinguishable from the real thing. The honeypot is set up in a secure containment, separate from an organization's network.

Keep in mind the following facts regarding honeypots:

- A honeypot is designed to look and function like a real resource in order attract attackers.
- A honeypot can appear to be a server, a single host, a service on a host, a network device, a virtual entity, or even a single file.
- Two or more system honeypot entities is called a honeynet.
- An attack on a honeypot allows an ethical hacker to monitor the malicious activity to gain knowledge of how attacks are being carried out.
- The logging capability of a honeypot is far greater than other network security tools. The honeypot captures raw, packet-level data, including the keystrokes and mistakes made by attackers.
- Honeypots can be physical or virtual.
  - Physical honeypots are actual devices with an IP address that are placed on the network. Physical honeypots usually provide the highest level of interaction.
  - Virtual honeypots are simulated on a physical device. However, they usually attract less attention because attackers more easily detect them as decoys.

Honeypots are not a substitution for an IDS or firewall and do not protect a system from a compromise.

Honeypot Interactions Levels

There are different levels of honeypot interactions that can be implemented based on the network security needs. The following table describes honeypot interaction levels.

Level	Description
Low	A low-level interaction honeypot simulates only a limited number of services and applications of a target system or network. It relies on the emulation of services and programs that would be found on a vulnerable system. Low-level honeypots are generally created to collect information about network probes and worm activities.
Medium	A medium-level interaction honeypot simulates a real OS, applications, and services. It provides a better façade of an OS than low-interaction honeypots.
High	A high-level interaction honeypot simulates all services and applications. It can be completely compromised by attackers, allowing an attacker full access to the system in a controlled area. High-level interaction honeypots can capture complete information about an attack vector, such as techniques, tools, and the attacks intent.

Honeypot Tools

The following table describes honeypot tools.

Tool	Description
KFSensor	KFSensor is a Windows host-based intrusion detection system. It acts as a vulnerable server, including open fake ports, to attract hackers. It records the activities of the hacker.
HoneyBOT	HoneyBOT is a decoy robot designed as a fully functional factory machine to attract hackers. It can simulate ICMP echo, FTP, Telnet, SMTP, HTTP, POP3, and Radmin protocols, as well as a range of malware such as Devil, Mydoom, Blaster, and Netbus.
HoneyDrive	HoneyDrive is a Linux-based honeypot that provides pre-installed and pre-configured honeypot software. It includes many useful pre-configured scripts and utilities for malware analysis, forensics, and network monitoring.