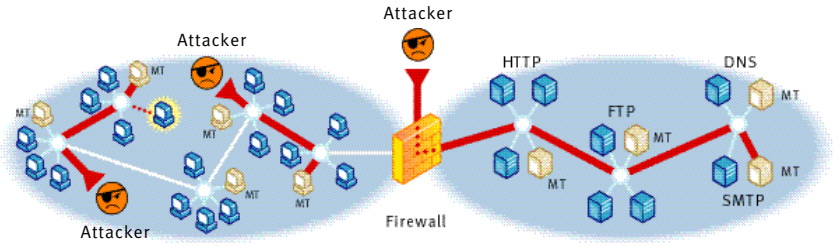
Recourse Technologies, Inc.™

ManTrap

TRAP INTRUDERS AND CONTROL ATTACKS

ManTrap™ protects networked resources by providing deception hosts that contain attackers before they attack valued systems. This allows organizations to contain, control and respond to intruders, whether the source of the attack is internal or external. Wherever ManTrap hosts are located on the network, they lessen the risk of business interruption and information loss, providing data critical to making response decisions and giving system administrators the time needed to respond to an attack. The attacker may think his attack has succeeded, when in reality he is being monitored, thus providing the information necessary to profile the attacker and the attack.



Recourse Against Internal Attacks

A large number of attacks against organizations come from attackers who have access to the internal network. To combat attackers who have access to the network from inside, ManTrap hosts can be placed in strategic locations throughout the network. ManTrap cages can be configured to resemble hosts that currently exist within a network by having similar hostnames, mirrored file systems, sequential IPs, and similar services of servers within the network. A ManTrap cage might closely mimic another system or it may be configured to look slightly more vulnerable than the other systems in the network. Since attackers often look for the path of least resistance, configuring ManTrap cages to look slightly more vulnerable than the surrounding servers can be an effective way to lure attackers.

Real System

ManTrap presents a real system to the attacker, complete with customized data. Unlike an emulated environment that might be easily identified by experienced attackers, ManTrap is built upon a real server operating system complete with expected behavior, applications and company information.

The decoy environment is called the ManTrap "cage." During installation, ManTrap automatically populates the cage with data that is unique to each ManTrap installation. Company information, such as full employee names, user names and other business information, can be easily integrated into the automatically generated content of the ManTrap cage. In addition, ManTrap continues to add data to the cage in real time to make the system appear active. This reduces the time necessary to create a system that appears authentic and valuable to attackers.

ManTrap also enables creation of custom data for the cage. Any application that can run on the host's operating system can be installed and run in the cage because the host's operating environment is replicated within the cage. For example, services or applications such as Apache, Oracle®, IBM® DB2™ or NFS can be installed inside the cage, and then populated with the appropriate data.

Recourse Against External Attacks

ManTrap can also be an integral security component against external attackers. In this configuration, ManTrap hosts might reside in a multitude of ways within a DMZ (demilitarized zone). As with internal attacks, a ManTrap cage can be configured to resemble another host, like a public FTP, mail or web server. Having a ManTrap cage that mirrors a corporate web site mitigates the risk of defacement to the site.

Intruder Profiling - Who is Attacking Me?

ManTrap maintains an audit trail of the attacker's activities, saves log files and records keystrokes—unbeknownst to the intruder. The attacker's every move is monitored and logged. With this information, a profile of the intruder can be developed that indicates their skill level and the likely intention of an attack. An accurate profile of the intruder enables informed resource allocation decisions when responding to an attack.

The ManTrap log files also record new attack signatures. Attackers are always adding to their bag of tricks and the ManTrap log files will give the system administrator a complete footprint of the attack allowing the system administrators to harden other networked resources against another such attack.

Alerting

ManTrap's alerting system can be configured to send alert messages based on specific classes of events. When an intruder accesses the ManTrap cage, a list of system administrators is immediately alerted, putting them in control and allowing them to quickly determine how to respond. ManTrap also uses SNMP alerting which works seamlessly with existing network management software. The ManTrap software has an extremely low rate of false-positives since any traffic directed at the ManTrap cage should be considered suspicious.

Reporting

ManTrap logs relevant activity in the cage, such as keystrokes, process invocation, and file accesses. The ManTrap log files can be stored locally on the ManTrap host and can be spooled via syslog to a remote host. Storing the log files remotely protects the integrity of the log files during a catastrophic event on the ManTrap host. ManTrap also includes a graphical event analysis tool that presents a prioritized view of events, significantly reducing the administrative overhead required to parse and interpret the log files.

In order to guarantee the integrity of the log files, ManTrap digitally signs its log files using a secure hardware token. Using cryptographic algorithms, the log files are hashed and signed making it computationally infeasible to compromise the integrity of log messages.

ManTrap Administration

ManTrap is easily administered using a Java™-based user interface, allowing administration from any Java2-enabled client. The ManTrap administrative interface allows configuration and control of an entire network of ManTrap hosts from a single client, reducing administrative overhead. The administrative interface connects to the ManTrap hosts using a covert and secure protocol to further conceal the existence of Mantrap and minimize the risk of unauthorized access to the ManTrap host. ManTrap also automatically archives the log files it generates, making it a truly self-maintaining security solution.

SYSTEM REQUIREMENTS

ManTrap Host

SPARC™ or Intel® platform

128MB RAM plus 32MB RAM per ManTrap cage

2GB disk space per ManTrap cage

1 network interface per ManTrap Cage

Sun® Solaris™ v.2.6

Sun Solaris 7

Sun Solaris 8

ManTrap Administration Console

Java™ 2 Runtime Environment v1.2.2

Microsoft® Windows® 95/98/NT®/2000

Solaris 2.6/7/8

Recourse Technologies, Inc.™

We Give You Recourse Against Hacking

1.877.786.9633

info@recourse.com

www.recourse.com