Recourse Technologies, Inc.™

ManHunt

TRACK INTRUDERS AND PREVENT ATTACKS

ManHunt™ is a covert security infrastructure product that identifies attacks against your network and aggressively responds by containing the attacks and tracking them back to the source. ManHunt takes a holistic approach to network protection through the use of distributed sensors, behavioral anomaly detection, and high-speed statistical correlation analysis. These advanced techniques enable a rapid and aggressive response to keep the attacker away from protected systems and discover his identity and methods. Whether the attack is an intrusion attempt or a denial of service (DoS) attack, ManHunt provides the highest level of information about, and response to, the attack and the attacker.

Identify Common and Novel Attacks

ManHunt employs advanced technologies for recognizing attacks, whether previously known or not. On-the-fly anomaly detection routines catch anything outside of normal or expected protocols, not just known signatures. Also, statistical correlation analysis evaluates aggregated events for positive identification and prioritization of potential attacks, minimizing false alarms. With 100 percent data capture at volumes exceeding 1 Gbps, ManHunt can identify threats in the most demanding enterprise and service provider environments.

Protect Critical Systems and Data

ManHunt rapidly responds to intrusion attempts and DoS attacks to minimize business interruptions and damage to customer confidence. ManHunt protects e-business infrastructures and provides recourse against hacking by:

- Stopping attacks and disconnecting the offending connection,
- Diverting attacks to a decoy environment, such as ManTrap™, and
- Tracking the attack back to its source, locally and across the Internet.

Track the Attack Across the Internet

Unique track back functionality automatically locates the source of the attack, whether internal or external to the monitored network. ManHunt identifies the attack path and its entry point to the protected network, even for distributed, reflected or spoofed attacks. ManHunt provides the information necessary to protect networks from attack, identify the culprit, and prosecute if desired.

ManHunt – A Higher Level of Security

ManHunt hosts are deployed strategically within networks, forming a networked layer of security that draws its strength from its ability to provide distributed network coverage and to dynamically reallocate resources between network segments, both within the administrative domain and across the Internet. While a multi-layered approach to security is important, the highest level must be a comprehensive security solution built on the same principles of interconnectedness and fault-tolerance as the networks they protect. A network of ManHunts fulfills this requirement.

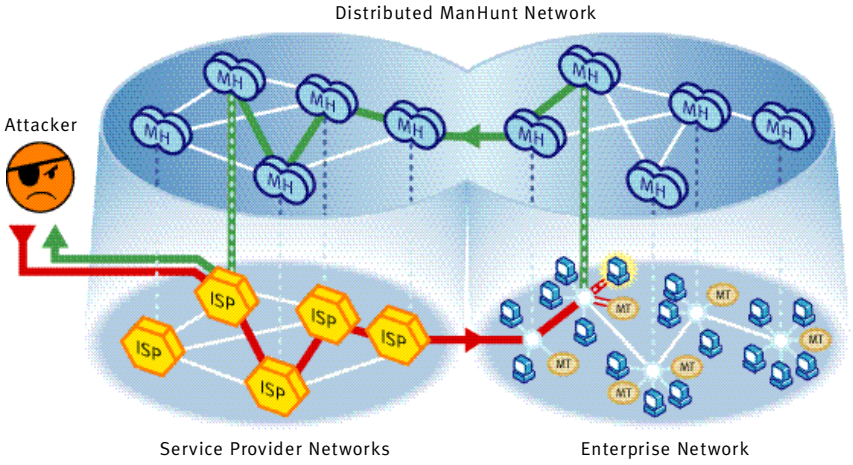
ManHunt networks are implemented at the highest level of the layered security solution. They are implemented within existing network infrastructures, leveraging existing assets to provide comprehensive and efficient protection from both internal and external attacks. Individual ManHunt nodes use broadly distributed dynamic sensors that may be redirected by other ManHunt nodes to gather additional information. The ManHunt network responds by mobilizing resources to find the entry point of the malicious hacker. At the administrative boundary the tracking process is handed off seamlessly to the next domain, where the process continues until the attack source is found and shut down.

Sample Scenarios

ManHunt addresses both intrusion attempts and DoS attacks, responding immediately and automating the track-back process.

In an intrusion attempt in which the attacker is attempting to use a spoofed IP address, ManHunt's anomaly detection recognizes the violation in state protocol and identifies the transaction as a potential attack. This event is aggregated with related events to determine the severity of the attack. The session is automatically hijacked into ManTrap, a deception host, where it is safely observed away from protected systems.

In another case, ManHunt detects a denial of service (DoS) attack and begins the track-back process. ManHunt tracks the attack to its point of entry into the network, requesting support from other ManHunt hosts as necessary. ManHunt also passes information to an upstream provider's ManHunt, which continues the process until the attack is isolated and shut down.



Cooperation Between ManHunt and ManTrap

Recourse Technologies provides a suite of products that work together to provide a complete security infrastructure. Network security is enhanced through gaining knowledge of an attacker's identity and methods. When a malicious attack is identified by ManHunt, it may be automatically disconnected, stopping the attack, although nothing is learned of the attacker's intentions.

A better solution is to hijack the session to ManTrap, a fully operational deception host, in which the attacker can continue the attack without risk to protected servers. Meanwhile, ManHunt continues to track the attack back to its source to locate and identify the attacker. The information gathered from the attacker's session in ManTrap can assist in improving the security of the network and protect against similar attacks in the future.

Additionally, if someone attempts to connect to ManTrap without violating any protocol, ManTrap will notify ManHunt to begin tracking the session back to its source.

System Requirements

Dedicated ManHunt Host

SPARC™ or Intel® platform

128MB RAM per CPU

Multiple CPUs recommended.

Sun® Solaris™ 8

1 Network Interface for each monitored device

1 Network Interface for general communication

ManHunt Administration Console

Java™ 2 Runtime Environment v1.2.2

Microsoft® Windows® 95/98/NT®/2000

Solaris 2.6/7/8

Network Devices

Monitored switches must support SMON and have a free port

Recourse Technologies, Inc.™

We Give You Recourse Against Hacking

1.877.786.9633

info@recourse.com

www.recourse.com