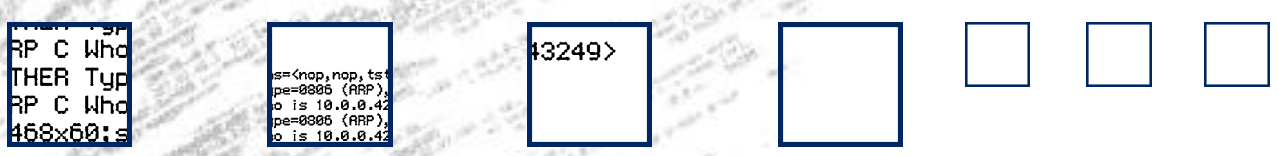
Recourse Technologies™

Securing Your Network Infrastructure with Threat Management Solutions



Abstract

ManHunt expands the expectations of intrusion detection systems into attack detection, analysis and response. This evolution reflects the market demands for a security solution that offers higher performance and is simpler to manage. ManHunt provides more sophisticated detection capabilities, context-based analysis, and response mechanisms that aggressively protect network assets and provide an unprecedented level of information about network attacks. Its architecture promotes seamless communication and cooperation among resources distributed across network segments and organizations to enhance both threat detection and response. ManHunt can monitor traffic volumes up to 1 gigabit per second from either multiple Fast Ethernet segments or a single Gigabit Ethernet segment. This raw monitoring capability is augmented by the use of steerable sensors, which can be dynamically shifted across network segments as the need dictates. ManHunt is also the first product capable of effectively combating denial of service (DoS) attacks by automatically performing an attack tracing process (TrackBack) to find the source of the attack.

Introduction

The nature of attacks on the Internet has changed radically since the design and implementation of traditional Intrusion Detection Systems (IDS). When these IDSes were developed, virtually all attacks across the network were *intrusions*, or break-ins. Conventional intrusions have relied on "stealthiness" to hide the malicious activity, as well as the identity of the intruder, until the damage has been done. The problem has always been to keep up with the latest attack methods in order to recognize that an attack is taking place; and the rate of new and modified attacks is ever increasing. More recently, denial of service (DoS) attacks have become prominent. Since a DoS attack does not require a TCP connection to be made to the target system or network, there is no connection to terminate, even if it is recognized. In these cases, the only effective countermeasure is to quickly locate the source of the attack, so that the data stream can be cut off without disrupting the legitimate business that must take place on the victim's network.

In the case of intrusion attempts and DoS attacks, the attackers have traditionally held the advantage because they have been able to maintain anonymity throughout the attack process. Even if the attack is detected and terminated, a savvy attacker rarely needs to worry about his identity or methods being exposed, because very little information about the attack is captured. Clearly, if network administrators are to regain control of their networks and claim that they have an advantage over their attackers, a new approach to security is required – one that not only has a better chance of discovering attacks as they happen, but can actively protect network resources and provide information about the attacker's identity, location and methods. With rapid attack recognition and response, and increased information about the attack, administrators would be available to significantly improve security standards and force attackers to be on the defensive, for a change.

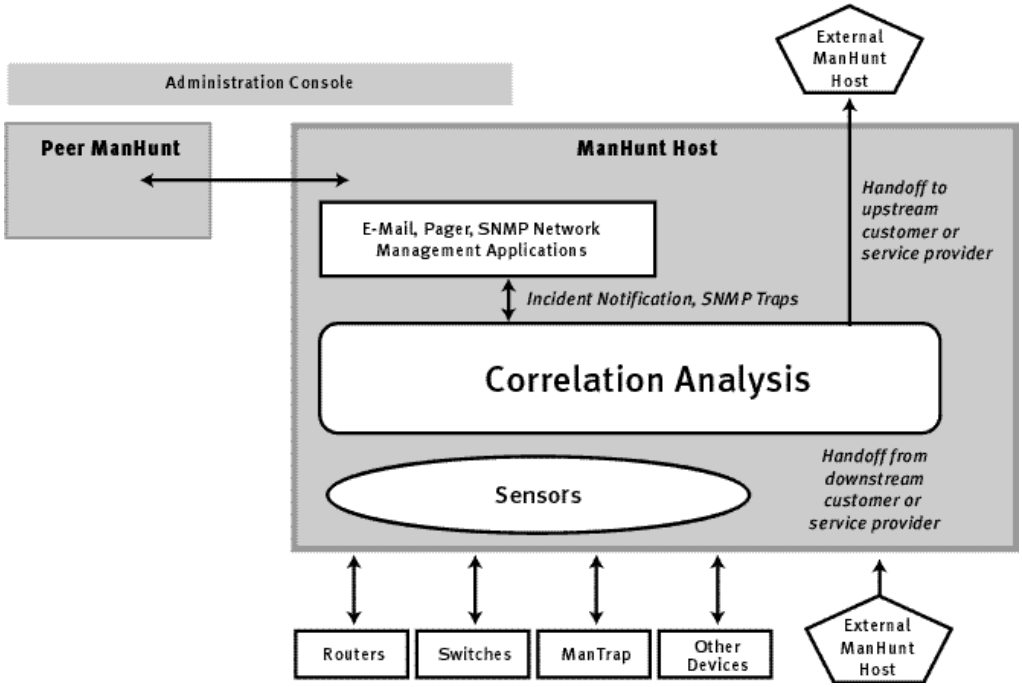
ManHunt provides this new "time and information" approach. In the sections below are the details of a product that was built from the ground up to address many of the failings and inadequacies of the traditional approach to intrusion detection, and that goes even further by adding a set of tools to actively respond to the attacks that are detected. First, we will discuss the architecture and introduce the primary components that make up the ManHunt host software. This will include the architecture that enables multiple ManHunt hosts to share resources and communicate effectively within distributed networks and across administrative boundaries. The following sections will detail the technology that comprises the Detection, Analysis and Response functions.

Architecture

Discussion of the solution indicated above must begin with a discussion of product architecture, because the traditional approach to intrusion detection contains inherent impediments to performance, detection, intelligent evaluation of collected data, and the ability to respond effectively to network threats. These will be discussed in detail in the relevant sections of this paper.

ManHunt is a software product that is deployed on a dedicated server, residing in the same location as the switches and other network devices that are carrying the traffic to be monitored, ideally in the same racks. It has a primary interface used for administrative communication, as well as communication with other ManHunt hosts. Additional network interface cards (NICs) installed in the host machine are connected directly to the switches to be monitored. The number of additional interfaces depends on the number of devices to be monitored, and is limited only by the processing power of the ManHunt host hardware. These interfaces are set to promiscuous mode, monitoring full duplex communications, and are not network addressable.

The main components of the ManHunt software are the Sensors, Correlation Analysis Framework, Knowledge Base, and Administrative Graphical User Interface (GUI). All but the Administrative GUI reside on the ManHunt host, while the GUI, used to configure and monitor ManHunt, may be operated remotely on any Java-enabled system with network access to ManHunt hosts. Sensors take information from each of the monitored switches and classify events as either legitimate or "suspicious". Only suspicious events are passed up to the Analysis Framework, where related events are grouped as incidents and evaluated "in context" to determine their severity. The Analysis Framework references the Knowledge Base in the process of evaluating incidents to determine what action should be taken. The Knowledge Base is a collection of databases, containing security "intelligence", including dynamic statistical measures, current incident tracking, network topology, and user-definable policies and configurations. The Knowledge Base is also where all logs are stored. The Administrative GUI communicates directly with the Knowledge Base to perform many functions, including configuring ManHunt hosts and monitoring current and past incidents.



ManHunt Architecture

When multiple ManHunt hosts are in operation under a single organization, their configuration and monitoring may take place from a single GUI. Multiple ManHunt hosts may be required if multiple physical locations are to be monitored, or more than ten network segments need to be monitored concurrently in the same location. In either case, multiple ManHunts controlled within one organization are referred to as a ManHunt Cluster. All ManHunts within a cluster will automatically communicate with each other and share information and resources as necessary to gather additional information about an attack or perform a track back across the network to locate the entry point of an attack into the protected network. This trusted communication takes place through a protocol service that uses triple-DES encryption and a configurable port number.

ManHunt may also communicate with ManHunts outside of the administrative domain, using another protocol designed specifically for communication across administrative boundaries. This would take place when ManHunt has performed a TrackBack within its network to discover the entry point of an attack. At this point, ManHunt may send information upstream about the attack in order for the upstream provider or peer to continue the TrackBack through their network. This level of automation is invaluable in the effort to quickly get as close as possible to the source of the attack to cut it off without adversely affecting legitimate business operations. The information may be sent by an authenticated e-mail to the appropriate person at the service provider, such that the data stream may be tracked manually through the provider's network. However, if that provider has ManHunt in place, the entire process is automated and takes place in a small fraction of the time – minutes, rather than hours or days.

Detection

The first step in any network intrusion detection product is to monitor some portion of the network with intent to detect malicious activity. There are three factors that impact the effectiveness of this step: performance, location and detection technique.

HIGH PERFORMANCE:

A single ManHunt host is capable of monitoring up to 1 gigabit per second (Gbps), distributed over ten or more network segments or a single Gigabit Ethernet segment. When conventional Intrusion Detection Systems (IDSes) are operating at 100 Mbps or less, often with high packet drop rates, how does ManHunt achieve such high rates?

First, ManHunt uses a unique anomaly detection technique that does not rely solely on a signature database to identify network threats (see Anomaly Detection). The signature lookup tables used by conventional IDSes have the advantage of allowing easier customization by the end user. However, the process of comparing every network event on the wire to a separate signature database, and the latencies involved in those communications, severely limit the volume of traffic that can be monitored. Second, ManHunt has implemented custom kernel modules that allow ManHunt's sensors to communicate directly with the network interface cards, eliminating the time cost of doing business through the machine's operating system.

STEERABLE SENSORS:

In any enterprise or service provider network, decisions must be made as to where to apply intrusion detection resources. The traditional approach requires that a dedicated sensor host reside in a static position on a single network port. With limited resources, this means that there will inevitably be areas of the network that are never monitored. ManHunt provides a very flexible option to this dilemma with *steerable* sensors.

ManHunt gathers its primary detection data directly from switches through copy ports. On supported switches, ManHunt can dynamically reassign the ports that are copied to the sensors, giving the ability to monitor *all* ports over a period of time. This is called "roaming", which is very different from "sampling". Sampling is a term used to define the behavior of an IDS when it is unable to keep up with the stream of traffic and packets are dropped. Dropped packets are not available for any kind of analysis, whether it is anomaly-based or signature-based.

Roaming is a method where 100 percent of traffic on a port may be monitored for a period of time, generally providing at least enough time to evaluate the full state machine of all communications on that port. If there is nothing of interest taking place on that port, ManHunt will select another port to monitor. The selection of the subsequent port is based on a combination of random numbers and the user-configured priority of the port. By selecting a higher or lower priority for

a port, in relation to other ports, resources are focused exactly where they are needed. For example, a switch may be connected to a sensitive server and also to several users' desktop systems. Setting a high priority on the server port and lower priorities on the others, means that most of the time will be spent watching the server communications, and occasionally, the desktop systems would be monitored. Roaming is a powerful option that gives ManHunt users tremendous flexibility in how resources are distributed for maximum security coverage with minimal resources.

Roaming port monitoring may be used in combination with static port monitoring, and in whatever quantity is supported by the monitored switch. If it is desirable to watch an entire segment or VLAN, simply copy the up-link. This can also be done in combination with individual port monitoring, which may be valuable since malicious port-to-port traffic would not be detected on the up-link. Also note that ManHunt is not limited to a single segment or subnet. Sensors on a single host may be connected into the DMZ, and multiple internal administrative groups simultaneously if desired.

PROTOCOL ANOMALY DETECTION:

In order for intrusion detection to serve any purpose at all, it must be able to detect threats. Traditionally, an intrusion detection system's ability to do so has been measured by the number of attack signatures that the product has in its database. We discussed the performance limitations of this approach. Another limitation of this "virus approach" to intrusion detection is the need to always have the latest signatures updated on the system, or the network is completely vulnerable to the newest attacks. This means that there is a significant security risk on top of the resource overhead required to check for and perform frequent updates to the system. Realize that new attacks are most heavily deployed during the first week or so of their availability, during which the new signatures are typically still being developed.

ManHunt's Protocol Anomaly Detection technology addresses these limitations by analyzing network traffic using a combination of techniques that relies primarily on its ability to recognize activity that is unusual, unexpected, or in violation of legitimate communication behavior. Rather than trying to specifically identify each variation of malicious activity and list it in a table, as in the traditional approach, ManHunt sensors model appropriate behavior and consider deviation from that model to be suspicious. ManHunt uses protocol and state machine models that are custom designed to perform in a security role. This means that there is an acknowledgement that legitimate business communication often deviates slightly from the strict protocol models. It also recognizes that legal and legitimate traffic can actually be an attack. An example of this is a SYN flood. Un-ACKed SYNs occur regularly in most environments, but an unusual quantity of them may suggest malicious behavior.

By understanding how legitimate communications typically take place over all major protocols, ManHunt sensors identify not only known attacks, but also most new and novel attacks that signature-based systems will miss. A common method of IDS evasion is to take a known attack and change it slightly, often just by changing a bit that has no significance to the attack itself.

ManHunt will still recognize the attack because it is insensitive to the specifics of how the data has been manipulated, only that it is not what it should be. And because all of these "suspicious" events are passed up to the Analysis Framework, where they are evaluated in context before any action is taken, ManHunt can provide a high level of security while minimizing both false positives and false negatives.

While ManHunt's Protocol Anomaly technology identifies the vast majority of attacks, there is still a small set of attacks where the signature approach makes sense. There are some attacks that are simpler to model by signature than to catch in the anomaly umbrella. These are the cases where signatures have been added to the sensor models, but there is no desire for this list to grow – there are many more advantages to this list being very small.

ManHunt sensors also incorporate a statistical, or rate counter, component to very quickly identify DoS or flood attacks. This element is designed to be self-tuning, recognizing that different environments, and even different organizations within a company, experience vastly different types of traffic. Legitimate volumes of a certain type of event in one location would have to be considered a flood attack in another location.

Of course ManHunt sensors operate on defragmented packets and perform reconstruction from layer 3 to layer 7. Regardless of the detection method, effectiveness drops radically if these steps are not taken.

Analysis

It is important to understand that all anomalous or signatured events are not malicious, and some attacks are more significant than others. ManHunt goes beyond the binary approach to intrusion detection, where individual events are identified as either good or bad, and provides added value to the raw data that otherwise requires significant time and resources to evaluate manually. Network security is not black and white. This is why ManHunt is designed with an analysis layer, operating above the sensor array, which adds intelligence to the raw sensor data and presents a more complete picture of security-related activities on the network. Additional benefits of this added component include the ability to create phased responses, and to minimize false positives.

ManHunt's analysis layer, on top of the detection function, helps to make sense of the events taking place on the network, and evaluate them in context. This dramatically reduces the effort traditionally required by administrators who must pour over reams of data in an attempt to decide if something bad has really happened. A lot of "bad" events take place on the network that are not threatening at all, and definitely do not warrant a wake up call at 3:00 in the morning. Conversely, too many "good" events can destroy an entire network. False positives have been identified as one of the most aggravating characteristics of traditional IDS products, and false negatives can be a very costly imperfection in the system as well. ManHunt addresses these, and other issues in the Analysis Framework, or the "brains" of ManHunt.

Built into the multiple layer analysis architecture described above is an additional security measure, called Weighted Fair Queuing, that provides a filter for data entering the Analysis Framework from the sensor arrays. This is important to be able to efficiently process potentially huge amounts of data, and to insure the integrity of the system itself by protecting it from flood attacks and standard IDS evasion techniques.

Finally, the Analysis Framework makes ManHunt a true distributed security solution, leveraging resources from across the protected network. The ability to dynamically interact with other ManHunt hosts, and existing network devices, drastically improves the efficiency and effectiveness of all of ManHunt's activities, including detection, analysis, response, and centralized security Management.

MULTI-SOURCE EVENT ANALYSIS:

Most corporations have a multitude of sources of security information, each with their own console and reporting application. Even if the application can perform analysis on these data, it is still not correlated with other sources of security information and a potentially rich source of data is unavailable.

ManHunt collects data not only from it's sophisticated sensors, but can also perform event aggregation, correlation and analysis on events from Cisco® IDS appliance and blade products as well as from the Recourse ManTrap® deception host. ManHunt performs the same analysis for events from third-party sources as it does for local events. This allows security administrators to centralize monitoring of security incidents and relate incidents from disparate locations and devices. Because events are aggregated using the same user interface, the user can easily understand and create response policies (see below) for events regardless of their source.

WEIGHTED FAIR QUEUING:

One of the tactics used in attacks to reduce the chance of detection is to hide the real attack within a flood of packets, such as a Denial-of-Service attack. This creates two potential points of failure for traditional IDSes. First, its sensor may drop enough of the packets from the real attack that its engine cannot identify the attack. The tactic is especially effective against engines designed under the assumption of 100% packet capture. Second, the flood of packets can provide enough separation between the packets in the real attack that the normal pruning of data performed by the engine will prevent it from recognizing the attack.

ManHunt counters this scheme by using a technique known as Weighted Fair Queuing. This creates particular resistance to detecting DoS attacks and similar packet floods while maintaining sensitivity to single packet exploits that may accompany the flooding attacks.

EVENT AGGREGATION (INCIDENTS):

ManHunt makes the assumption that the first step to better intrusion detection is better information and a better understanding of what activities are taking place on the network.

ManHunt does not presume that an individual network event is either bad or good by an isolated evaluation. In order to evaluate an event "in context", the Analysis Framework groups related events into Incidents. Events are deemed to be related if they share some common characteristics, such as type, source or destination.

When an event is received from the sensors, the Analysis Framework considers its characteristics to decide if it is part of an existing incident. If it is, it is added to that incident – if not, a new incident is created. All further analysis is based upon the current incidents and not on the individual events. If no new events are added to an incident for a predetermined period of time, the incident expires and is moved to the historical incident list. Subsequent events that might otherwise have been associated with an expired incident will be aggregated in a separate incident. The expiration time for an incident is configurable.

Incidents are extremely valuable in the determination of malicious activities because individual events may or may not be important by themselves, until other related events take place and build a profile of activity. For example, a port scan is not an important enough event to send a notification at 3:00 in the morning. But, rather than throwing away that information, an incident will hang on to it to see if more activities follow. An invalid login on an open port also is not necessarily a significant event. Incidents allow these activities to be associated such that the priority may be increased. After a certain number of invalid logins, the priority for the incident may be high enough to take action. This allows for a much more granular approach to attack response, so that no one is bothered when the threat severity is low, but resources can be allocated rapidly when necessary.

CORRELATION ANALYSIS:

The most effective network security solution consists of the ability to take a holistic view of the network being protected. This means looking across the entire network at the same time. It means considering the possibility that something taking place in one area of the network may be related to something in an entirely different area. It means understanding the difference between legitimate business behavior and malicious behavior. It means understanding the methods and tools used in malicious activities and what might be going on in the mind of the attacker. Evaluating network events from a security standpoint is significantly more complex than performing protocol or performance analysis. Correlation Analysis involves integrating multiple and disparate raw data sources with a knowledge base that can help to make sense of it all. It also involves bringing all of that data together in a single user interface for management, configuration and monitoring, regardless of network size or distribution.

ManHunt is the first Network security product that is capable of seamlessly sharing resources across broadly distributed networks to gather the data necessary to evaluate the current generation of security threats, such as distributed denial of service attacks and complex reflected attacks. One ManHunt host, in the process of evaluating a potential threat in one part of the network, can directly control sensor resources and share knowledge base information from another ManHunt.

Statistical data is also collected and shared to expand the scope of threats that can be addressed, and is likely different for each area of the network. These elements all make up ManHunts ability to respond intelligently to the widest range of network security threats, from the simplest script kiddies to behavioral and statistical anomalies to distributed denial of service attacks.

Response

The ideal security product would keep network assets secure and keep attackers away without any demands on the administrator. The reality today is that administrators are involved in the security process a lot more than they would like to be. Checking on false positives is a time-consuming task, but even when the system is working properly, a notification of malicious activity means that someone must intervene and take action to keep the attacks away from networks and systems. ManHunt goes a step beyond simple notification by providing automated responses to protect systems and buy time and peace of mind for the administrator.

For this discussion, it is important to understand that there are two distinct classes of attacks: Intrusion Attempts and Denial of Service (DoS) Attacks. There are two differences worth noting between these classes of attacks. Specifically, for an intrusion, there must be a TCP session open and the volume of data involved in the attack will be relatively low. A DoS attack does not require a connection to be made and the attack consists of very large volumes of data. For these reasons, an intrusion attempt is a much simpler attack to deal with, once it has been identified, because there is a connection that can be terminated. However, in combination with a DoS attack, traditional IDS products may be unable to identify the intrusion attack or send notification of the attack because the network segments are flooded.

The following responses are automated and the rules for applying them are established in the policy configuration of the ManHunt host. Multiple responses may also be configured for the same incident, in combination with each other and in the desired sequence. Policies can be configured for any type of attack or combination of attacks, related to any particular segment. This provides administrators the capability of alerting on some attacks that may be commonplace on some segments but not on others. For example, a port scan may not be of high interest on an external segment, however it would be of great interest on an internal segment.

NOTIFICATION:

Notification is a standard component of IDS products, because that is how an administrator knows what is going on when not seated in front of the IDS console. Many IDS products use the same interface for detection and notification, thus rendering the notification feature useless during a flood attack. ManHunt uses a completely separate interface for notification, often located on a secure administrative domain. This makes it more likely that the notification will be sent successfully, and there is less chance of deliberate compromise. Note that with numerous automated responses designed to protect threatened systems and gather information about the attack, notification may be the third or fourth activity that takes place. ManHunt may send a

notification that the threat has already been addressed.

SESSION TERMINATION:

Session Termination is a response option for ManHunt when the attack is an intrusion attempt. This is often considered an advanced feature for the products that offer it because it is the most active thing that they do to protect the network. A session termination is typically accomplished by sending a TCP Reset command, which kills the malicious connection.

TRACKBACK:

When it is desirable to locate the source of an attack, most often with a spoofed address, the traditional approach is to manually interrogate routers, hunting for the relevant stream of data. This is a grueling exercise that can take many hours to many days, even for a skilled network engineer. Consequently, it is not something that takes place very often. In the case where the source address is not spoofed, this process can be simpler, but the simplicity and popularity of spoofed attacks is so high today that it is advantageous to start with this as an assumption. It is worth noting here that there are a few "trace route" products that appear to automate this process, but only have value in the simplest, non-spoofed attacks. There just are not very many of these simple types of attacks, and they are generally not the attacks to be worried about.

The ManHunt TrackBack function is designed to automatically track a data stream to the entry point into the administered network. It does this by using special sensors designed to search the network, systematically looking for the data stream with matching characteristics. It does this through communications with switches, routers, and other ManHunt hosts within the cluster. ManHunt uses its knowledge of the network topology to make intelligent choices as to which devices to interrogate about the attack stream; and rather than eliminating possible paths, it simply prioritizes them. This way, minimal resources are used in the process and there is minimal impact on the processing of normal network traffic. It also allows ManHunt to deal very effectively with Distributed Denial of Service (DDoS) attacks in which data streams are coming from multiple locations by initiating multiple TrackBack processes, tracking multiple flows back through the network simultaneously.

During this process, one ManHunt node may cooperatively employ sensor resources from another ManHunt node, leveraging the distributed nature of the ManHunt Cluster. In order to continue the TrackBack process beyond the administrative boundary, communication to the upstream peer network is required. The default format for this information is an authenticated e-mail message, containing all the information that a network administrator would need to manually track the data through his network. If the upstream peer has ManHunt installed, the tracking information may be received automatically, at which time that ManHunt would initiate its own TrackBack process to find the entry point into its network. This automated process will be discussed more in the next section.

When interrogating devices in the process of a TrackBack, ManHunt interacts with both switches and routers. ManHunt will typically be connected directly to switch ports, and can dynamically reconfigure copy ports as necessary. ManHunt communicates with routers, depending on the manufacturer and the preferences of the network engineers using a telnet connection with a password or TACACS authentication. ManHunt sets appropriate "allow" filters for a short period of time on routers to look for the flow in question. This method is both safe and non-intrusive as the filter uses virtually no resources on the router and does not affect the router's operation even if communication between the ManHunt host and the router is disrupted.

In the event of a Denial of Service attack, TrackBack is absolutely essential to network protection. A DoS attack cannot be handled within the company under attack unless that company is willing to pull their plug to the Internet. Of course, very few companies are willing to do this because of the legitimate business that must take place across those wires. Being able to quickly identify a DoS attack is a valuable first step, but this information is of very little value unless there is TrackBack functionality that can get to the source of the attack. In some cases, it is possible to reconfigure the local firewall or router to block or rate limit the DoS packets, but an IDS must identify which packets to block quickly, or else the DoS flood becomes effective.

HANDOFF:

As mentioned above, a DoS attack cannot effectively be dealt with solely by the company under attack. The traffic that would need to be blocked to protect internal systems from the DoS attack would generally include legitimate business traffic as well. The only truly effective location to block traffic or break a network connection is at the location where the attack is entering the Internet. In order to accomplish this, efforts must be coordinated across the Internet and must involve the relevant service providers. One of the primary reasons ManHunt was developed was to address this exact problem.

ManHunt is designed to both send and receive tracking information across administrative boundaries, if policies have been configured to do so. The information is sent directly to the upstream ManHunt in a secure authenticated message that contains only the information required to continue tracking the data stream within the upstream network; no privileged information needs to be sent. The upstream ManHunt then generates an incident for this attack and initiates its own TrackBack process through its network. Policy would likely dictate that, if the attack stream were coming from another service provider, the incident would get handed off to this upstream peer. However, if the source identified turned out to be a client, the source location can be considered found. At this point, the service provider may choose to physically pull their network connection, apply ingress filters on the appropriate router or firewall, or contact the authorities for additional follow-up.

The protocol for Handoff communication has been designed in such a way that it would be very difficult to be used for the purposes of breaking into the system or for inflicting a DoS attack on a ManHunt host. First, all communication between ManHunt hosts is authenticated by a physical

secure token attached to the ManHunt host hardware. Also ManHunt hosts may register with each other when it is desired that they be able to communicate. ManHunt will only respond to a message from a registered and authenticated ManHunt. Furthermore, the length of time it takes for ManHunt to generate a valid message, is two orders of magnitude greater than the time it takes to decode and read the message. This virtually eliminates the possibility of a compromised ManHunt to attack other ManHunts.

Summary

ManHunt™ is a threat management system 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, protocol 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.

ManHunt employs advanced technologies for recognizing attacks, whether previously known or not. On-the-fly protocol 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 very high data capture at volumes up to 1 Gbps, ManHunt can identify threats in the most demanding enterprise and service provider environments.

Underlying ManHunt's ability to detect, protect, contain, and track, is an architecture that enables and promotes efficient communication and cooperation across the network. This unprecedented level of resource sharing and information aggregation makes ManHunt very powerful and, at the same time, very simple to manage from a single location.

System Requirements

MANHUNT HOST:

- SPARC™ or Intel, platform
- 512 MB RAM per CPU
- 64-bit Sun, Solaris™ 8
- Multiple CPUs recommended for maximum performance
- 1 Network interface for general communication and administration
- 1 Network interface for each monitored device (100Mbps or Gigabit Ethernet)

ADMINISTRATION CONSOLE:

- Java™ 2 Runtime Environment v 1.3
- Microsoft, Windows, 98/NT,/2000
- Solaris 2.6/7/8

NETWORK DEVICES:

- Dynamic port configuration requires supported switches.
- Static port monitoring may be performed on any switch or hub.

For More Information

For more information, please contact Recourse Technologies, Inc. at:
www.recourse.com
sales@recourse.com
1-877-RUOWNED (1-877-786-9633)

We Give You Recourse Against Hacking

1.877.786.9633

info@recourse.com

www.recourse.com