GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Network Forensics Analysis Tools:
An Overview of an Emerging Technology

Rommel Sira
GSEC, Version 1.4

Security administrators need to actively monitor their networks in order to be proactive in their security posture. Network Forensic Analysis Tools (NFATs) help administrators monitor their environment for anomalous traffic, perform forensic analysis and get a clear picture of their environment. To gain a better definition of the tool, it examines three NFATs: SilentRunner, NetIntercept and NetDetector. The paper reviews the functions of each NFAT, their focus and their limitations including a brief discussion on recommendations to counter the limitations. Although not widely implemented, there is a growing interest with the technology due to the need of administrators to actively monitor their traffic and an increasing number of security threats.

Consider a standard security structure for a medium-sized company: a firewall guarding the perimeter, an antivirus solution protecting the workstations, a secure e-mail gateway, a web content manager, a network intrusion detection system and even a virtual private network to cover even home users logging into the network. The structure can also include ingress and egress filtering at the router level, a syslog server for monitoring logs at the server level, and even a Linux machine running Nessus for vulnerability assessment at the enterprise level. With all this in place, a security administrator would still not know everything going on in his / her network without active monitoring. Worse yet, it may have made any effective monitoring a much more difficult task due to the extra traffic and information being generated by the security tools. Yet a lot of networks have the same troubles and most administrators still do not know exactly what is happening in the network.

Current industry problems require security administrators to be more diligent about watching packets going in and out of their networks. Distributed Denial of Service attacks where many hosts are attacking the environment with the intent of bringing down services are unpredictable. The problem is that administrators are unaware of the attack until it is too late. The other problem is that because the attacks are originating from multiple hosts, the administrator left with very little information in order to track down the offending hosts. Internal threats are also a huge problem for the security administrator since they are within the trusted domain (behind the firewall and their external defenses). That is, "'[a]n external attacker is not motivated to do much damage, doesn't know what to look for and is more likely to stumble into an intrusion detection system…the attacks that hurt are from a disgruntled employee who is motivated to come after you'" (Robb, www.esecurity.com/trends/article/0,,10751_1405031,00.html).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Blended threats, like Nimda, which take on multiple characteristics and spread quickly, are on the rise as well. Because blended threats spread using virus and worm techniques in conjunction with exploiting known vulnerabilities, administrators have the burden of being proactive in their approach to securing their networks. That is, they need to know where they are vulnerable and be able to make sound decisions in order to protect their networks. When attacks occur, companies want all the evidence of an attack, all damage committed by the attack and if possible, who perpetrated an attack. Companies also need to have all the evidence necessary about employees who violate their Internet use policies. Several vendors offer a tool that allows administrators to monitor their networks, gather all information about anomalous traffic, and provide help with network forensics. These tools, although not an exactly new technology, are called Network Forensic Analysis Tools or NFATs. Three companies, which were reviewed in a February 2002 article in Information Security magazine, that offer NFATs are Raytheon (SilentRunner), Sandstorm Enterprises (NetIntercept) and Niksun (NetDetector). Security administrators need to have multiple layers of defense to be effective in protecting their networks (http://securityresponse.symantec.com/avcenter/refa.html). Network Forensic Analysis Tools support this notion of defense in depth. Their ability to analyze network traffic and correlate data from other security tools is important for administrators who need to have a clear picture of what they are protecting.

In the February 2002 article from Information Security magazine, the focus was on Network Forensic Analysis Tools and three NFATs were studied to better understand the technology in general. Being a new tool, there are no clear-cut definitions. However, there are two basic types of NFATs: "Catch-it-as-you-can systems" which capture network traffic, has the ability to store large amounts of data and is able to analyze that data in batch mode; and "stop, look and listen systems" which analyze each packet but without the storage capacity of the other (http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci859579,00.html, October 2002). Vendors also provide summaries of their products' basic functions. This adds up to a general picture of these tools. Although not a silver bullet for the security administrator, an NFAT can save time and money and help the administrator watch everything in the network. Basically, NFATs capture network traffic and send data to an engine, which analyzes that data and shows results to the NFAT administrator. From the February 2002 article from Information Security magazine, "NFAT products capture and retain all network traffic and provide the tools for forensics analysis … an NFAT user can replay, isolate and analyze an attack or suspicious behavior, then bolster network defenses accordingly" (King & Weiss, February 2002). An NFAT is a tool that stores all network traffic, analyzes that traffic and notifies security administrators of anomalous activity. Also included in the article are some of the functions of an NFAT (King & Weiss, February 2002):

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Intellectual property protection
- Detection of employee misuse/abuse of company networks and/or computing resources
- Risk assessments
- Network forensics and security investigations
- Exploit (break-in) attempt detection
- Data aggregation from multiple sources, including firewalls, IDSs and sniffers
- Incident recovery
- Prediction of future attack targets
- Anomaly detection
- Network traffic recording and analysis
- Network performance
- Determination of hardware and network protocols in use

NFATs are not new. Sniffers were around and a necessity for administrators when computers were placed in a network. Administrators had the ability to monitor changes and receive alerts from servers without extra overhead. Freeware is available to help administrators perform vulnerability testing for their environment. Other types of network forensics tools are also available to administrators who need to monitor and understand their networks. One such tool is The Coroner's Toolkit. It is a forensics tool used for UNIX systems after a break-in has occurred. Its main function is to do most of the investigative work for the security administrator but it does have a drawback – "the technical analysis of this output can easily take hours or days" (www.cert.org/security-improvement/implementations/i046.02.html, May 2001). Another useful forensics tool is Ethereal, which can be used for both UNIX and Windows systems. Ethereal captures packets and helps the administrator study the information from those packets. These tools perform some basic forensic work for the security administrator but the advantage of NFATs is that they are able to capture packets from multiple sources, conduct forensic analysis, and be able to paint a picture of the network in near real time. It is able to gather all the data in the network, analyze it and help the administrator make better decisions about the network. Administrators can get a better baseline picture of their network and know where more security is needed. They can better protect their network if they know where the holes are and what patterns are developing. A short discussion on forensics can show the benefits of an NFAT.

When a virus or malicious code has entered a system, an administrator needs to perform several steps in order to rectify the damage caused by the infection. The first step is to understand the vulnerabilities of an environment. The security administrator must be proactive by preventing those vulnerabilities from being exploited by a malicious user. The administrator needs to determine what is

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

normal versus anomalous traffic attributed to an attack. If and when a breach does occur, the next step needs to be gathering evidence of this attack. Several tools are available that allow an administrator to gather information about the attack. After gathering all the evidence, the administrator will need to analyze that data. If free tools such as fport.exe and netstat.exe used to gather information about the event, administrators will have a large amount of data to go over and analyze. However, administrators can write their own scripts to correlate all the captured data and have a better understanding of the actual event. Once the investigation has ended and the administrator has been able to determine what has occurred and what has been damaged, the final step is to remove the malicious code. If an Administrator- or system-level breach has occurred, an administrator will need to consider re-installation of the operating system due to the uncertainty of what actually has been affected by the infection. With the help of NFATs, a security administrator would be able to decrease the amount of time spent on investigation. Although there are no real shortcuts to this first step (because this includes following best practice guidelines of setting up systems), NFATs can decrease the time of studying the normal activity of a network. NFATs can paint a general picture of all the events happening on the network. NFATs are designed to gather evidence on the network with its ability to capture packets. Along with their analysis ability, NFATs are able to decrease the time sent on evidence gathering and data analysis. Once data has been analyzed, an administrator can find all other instances of the breach within the network by having the ability to drill down to the packet level from the NFAT console. This way, re-installation of a production server may no longer be the only alternative since administrators can be aware of all the effects of the infection. Security administrators can use simple tools to do incident response and forensic work on a small scale. However, if enterprise-wide breach (for example, Nimda) or an Administrator- or System-level compromise has occurred, a security administrator will need to be able to automate most of the tasks of forensic work so that the damage can be rectified and the production system can return to its normal behavior.

"Computer forensics involves the preservation, identification, extraction, documentation and interpretation of computer data."(Kruse and Heiser, p.2) According to this book, the basic methodology is "acquiring the evidence without altering or damaging the original, Authenticate that your recovered evidence is the same as the originally seized data, and analyze the data without modifying it". What NFATs perform adhere to these methodologies. They can gather evidence since they are listening on the network. They do not alter data because their premise is to be non-intrusive. They have replay features giving administrators the evidence they need to show an attack or a breach in policy has occurred without altering or damaging the actual evidence on a machine. A separate engine, in the case of SilentRunner, does analysis for the administrator. Traditional forensics is done by gathering evidence at the hard drive / physical

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

level. Since analysis and evidence gathering is done by the NFAT, it saves the administrator time rather than going to each victim machine. Evidence is authenticated by the NFAT because other tools like IDSs and firewalls would also the same logs that the NFAT has seen. That is, NFATs validate the logs from other systems. Along with its monitoring, alerting and analysis capabilities, NFATs also provides administrators a way to have "point & click administration".

NFATs help administrators do forensic work. They can look at the logs and use the replay feature to see what exactly happened in a certain event. Companies that need NFATs would be those that get attacked frequently or those under regulation to protect its assets like healthcare and e-commerce. Although free tools are available that do the same things as NFATs, the benefit with the commercial products is their reporting ability. NFATs like SilentRunner, for example, have the ability to show the trends of network traffic. Usually companies use outside companies to do vulnerability assessments for them. These companies also use penetration tests against the security structure of the enterprise. With NFATs, companies have these resources in house and save time and money. They also help out the security administrators since they are able to have a better picture of the environment that they are protecting. Administrators can start focusing on prevention by understanding where they are most vulnerable. They can spend more time in expanding user education. NFATs can test the IDSs to ensure that they are seeing the signatures they are supposed to be detecting. This way, they can also focus on improving the tools already in place in the environment so that all the security tools are working together for one purpose. Security and network administrators can use the information from the NFATs to know how well the network is performing. They can detect slow downs that may be a warning of a pending DOS attack. They can see rogue servers. And have a better tool to prevent internal attacks. They can better monitor internal threats by seeing all the events in the network. Emails can be read and administrators can be warned if certain thresholds are crossed. If certain confidential information is going out of the company, this can be detected. Activities that violate Internet and email use policies can also be detected. The great part of this is that administrators have a better way to record all the events. Evidence gathering is not as difficult as it once was.

Three examples of Network Forensic Analysis Tools are Raytheon's SilentRunner, Sandstorm Enterprises' NetIntercept and Niksun's NetDetector. SilentRunner is the big player in the NFAT market. SilentRunner gives the administrator a 3-dimensional view of their network. Its focus is on network monitoring and analysis so if abnormal traffic is detected, SilentRunner alerts the appropriate personnel. It allows the administrator to literally monitor all the packets passing through the network. It allows administrators to examine the packet layer and know what is exactly happening where on the network. The tool also has the ability to replay events as they occur. Combining the ability to

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

visually know what is going on in the network and replay events, SilentRunner gives administrators a lot of help as they look to protect their company's assets. By being able to literally see everything, and understand how things are shaping, administrators can make better decisions about the security in the enterprise. SilentRunner's main focus; however is on internal threats. It detects anomalous traffic and follows all the patterns of that traffic while alerting the appropriate personnel. With its powerful analysis engine aiding the administrator in acquiring evidence about a certain event, SilentRunner is able to cut down the time to perform investigative work. Tools are available now that allow an administrator to be notified of changes in the network. For example, if an Intrusion Detection System is set up in the environment, an administrator can be alerted about known attacks being perpetrated against their network. However, traffic not known by the IDS or log files that become too much for one or a few people to look at can become wearisome and a security hole. Most security professionals want to automate their duties as much as possible. IDS monitoring and log file keeping, although somewhat automated, is still a manual task. Administrators, especially with a small security team, do not always know (or have the time) when something should be ignored or should be investigated more thoroughly. With an actual picture of the network status, administrators can make better judgments as they survey everything on the network with one tool. However, it must be noted that NFATs, like all other security tools, are not a replacement for security structure. They are an addition to the security in an environment. They enhance the features of other security tools already in place.

SilentRunner is made up of three major parts: Collector, Analyzer, and Visualizer. Similar to an IDS system which has a sniffer and a reporter, SilentRunner uses the Collector to capture packets and the Analyzer to correlate and organize the data into meaningful information. However, unlike most IDSs, the packet collector is not an appliance. It is installed on a Windows 2000/XP machine using a SilentRunner-modified Network Driver Interface Specification packet driver. The Collector captures packets without interrupting network performance and reassembles the sessions based on HTTP, POP, IMAP, SMTP, Telnet and NNTP content. An inference engine makes conclusions about network events, separating what is actually happening in the network and what has been concluded by the Collector. It supports many different types of networks, from 10/100 MB Ethernet connections to others like frame relay, T1, T3, etc. The Analyzer is the main reporter and the component that pulls the collector data together. After pulling data from the collector, the Analyzer uses n-gram analysis (method of breaking up large documents into smaller pieces, finding similarities among the smaller pieces, in order to find relationships among the large documents) to define patterns for the administrator. The Analyzer is also able to analyze firewall logs and IDS data so that it is much more than just a sniffer or IDS. Working with the Visualizer component, they are able to create a 3-dimensional picture of the entire network.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

On the other side of the NFAT scale is Sandstorm Enterprises' NetIntercept. It is a hardware appliance (FreeBSD) focused on capturing network traffic and forensics but lacks the same visual capability of SilentRunner. Its advantage is on capturing traffic and analyzing actual traffic. It is an example of a "Catch-it-as-you-can system" because it analyzes traffic in batches and has the ability to store a large amount of data. An organization can store up to 650 GB worth of data in tcpdump-format and in addition to this space, can offload information using NetIntercept's built-in CD-RW. It has the ability to do replays so that administrators can do investigative work when an attack has been detected. NetIntercept has three functions: to capture network traffic, analyze network traffic and perform data discovery. NetIntercept continually captures traffic but does not save the traffic. That is, older data is replaced by new data unless it is saved by the administrator. Analysis is started by an administrator who chooses a certain time interval to study. That batch of traffic is reassembled into meaningful information so that analysis can be performed by the analysis engine. The analysis engine attempts to understand the content of the data stream rather than report on packet information. Finally, with data discovery, an administrator is able to perform trend analysis because prior records are archived into NetIntercept. Administrators can also generate different types of reports based on network traffic (bandwidth usage), content (trend analysis on Internet traffic), user behavior and breaches (helping administrators increase network security where it is needed). NetIntercept's analysis is not as powerful or as detailed as SilentRunner's, "but it does it in a way that it is actually looking at the traffic rather than making conclusions based on header information or protocols (Sandstorm 2002)." However, a noteworthy advantage of NetIntercept over SilentRunner is its ability to decrypt SSH-2 sessions. Additionally, NetIntercept only accepts secure remote administration into the appliance. This is a huge difference to SilentRunner which does not provide remote administration of the collectors. NetInterecpt also allows for its own log files to be exported and analyzed by different tools like tcpdump. Network Forensic Analysis Tools may not represent the silver bullet everyone is looking for, but they do alleviate some of the laborious functions of investigation and analysis work for data security.

The other NFAT studied in the Information Security magazine article is Niksun's NetDetector. Like the other two NFATs, NetDetector is a passive network analysis tool that captures, analyzes and reports on network traffic. Like NetIntercept but not SilentRunner, it is an appliance. Unlike the other two, its advantage is in its alerting mechanism (varies from GUI pop-ups, email, pager, etc) (Niksun 2002). Its other advantage is that when coupled with an Intrusion Detection System (Niksun integrates with Cisco IDS), it is able to run a complete forensic investigation for the security administrator. It supports many common network interfaces (10/100/1000 Ethernet, T1, FDDI) and protocols (TCP/IP,

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

frame relay). The appliance also has a large storage supply and supports exporting of data if it is required but that is limited to HTTP, FTP and SCP.

Like any security tool, Network Forensics Analysis Tools have limitations. Depending on the environment, these limitations may hinder a company from considering the use of these tools. One of the major drawbacks for an NFAT is the overall cost for the system. For example, the SilentRunner standard edition is priced at $65,000 ($8,000 for each additional collector module), Niksuns' NetDetector ranges from $20,000 to $80,000 and Sandstorm Enterprises' NetIntercept costs $15,000. This cost does not include the training costs that are needed to understand the product. There is also a very high cost in terms of learning how the product works. NFAT administrators need to know how the product works, what to look for and understand the output of the product. Another drawback to NFATs is the fact that freeware tools are available that can perform similar forensic analysis for an environment. Although some freeware tools do not have the same analysis and visual (SilentRunner) capabilities of NFATs, their price tag is attractive for many companies. New technology with such a high price tag is a hard sell.

Another major drawback is that technology itself and what it can monitor is limited to traffic that can be monitored. That is, encrypted traffic such as SSL and SSH are undetectable by most NFATs. The problem here is that SSL-enabled web servers are vulnerable to similar exploits. If an SSL-enabled web server is placed in a production environment but is not patched, a malicious user can launch attacks undetected from the monitoring tool. Yet another limitation for Network Forensic Analysis Tools is that they are "mostly reactive, rather than proactive" (Garfinkel, December 2002). The technology is designed to watch the network and alert the appropriate personnel of any anomalous behavior. The technology does not interfere with network traffic because it is designed to be passive. Although the tool is geared to help administrators find a baseline of normal network traffic, automating the process is still not a reality. However, despite these shortcomings, the technology is gaining interest because organizations do need to find a way to monitor their networks and automate the analysis of traffic. Moreover, there are methods where other tools can come into play and respond to these shortcomings.

Several recommendations exist that can help alleviate some of the limitations facing Network Forensic Analysis Tools and other monitoring tools like Intrusion Detection Systems. These recommendations may or may not fit well with the overall security structure of an enterprise. Since SSL encrypted traffic is undetectable by a monitoring tool like an NFAT, one such recommendation is to use SSL via a proxy server. With this recommendation, clear-text requests on port 80 are received from the SSL proxy, which then sends encrypted data to the SSL-enabled server. Using this method, the NFAT can be pointed to monitor the

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

SSL-proxy instead of the actual SSL-enabled web server thereby accounting for the encrypted traffic. Several SSL proxy applications are available such as sslproxy.c (http://www.obdev.at/products/ssl-proxy/index.html) and stunnel (http://www.stunnel.org/). Another recommendation is to incorporate a tool that forwards the SSL negotiation to another machine rather than having the web server perform the negotiation itself (Prosise and Shah, August 2000). With this recommendation, the performance of the web server is increased since it is no longer responsible for the SSL connection. (http://www.innovapp.com/intel_ecomm_accel.cfm)
To help administrators deal with the problem of false positives, NFATs like NetDetector work well with Intrusion Detection Systems. By using both tools, the IDS detecting the anomaly and the NFAT confirming the traffic, administrators have a better way to measure their security structure. That is, administrators can be certain of an actual breach and they can bolster their defenses accordingly.

The Network Forensic Analysis Tool is still a developing technology. Like any security tool and new technology, companies need to weigh the pros and cons of this new technology. For most enterprises, this technology, with its limitations, cannot be considered to be implemented. However, with the visual capabilities of such tools as SilentRunner and the ability for NetIntercept to monitor encrypted data, NFATs may become more widely implemented as they are developed. If not, they are, at least, a move in the right direction of helping security administrators confidently monitor and protect their networks.

References

Robb, Drew. "Internal Security Breaches More Damaging." July 15, 2002.
URL: http://www.esecurityplanet.com/trends/article/0,,10751_1405031,00.html

Symantec Corporation. "Glossary: Blended Threat." URL:
http://securityresponse.symantec.com/avcenter/refa.html

"searchSecurity.com Definitions: network forensics." October 28, 2002
URL: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci859579,00.html

King, Nate and Weiss, Errol. "Analyze This! Network forensics analysis tools (NFATs) reveal insecurities, turn sysadmins into systems detectives." February 2002.
URL: http://www.infosecuritymag.com/2002/feb/cover.shtml

"Using The Coroner's Toolkit: Harvesting information with grave-robber." May 22, 2001.
URL: http://www.cert.org/security-improvement/implementations/i046.02.html

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Kruse II, Warren G. and Heiser, Jay G. Computer Forensics: Incident Response Essentials. Toronto, Canada. Addison-Wesley, August 2002: 2.

Sandstorm Enterprises, Inc. 2002. URL: http://www.sandstorm.net/downloads/netintercept/ni-1-1-datasheet.pdf

Niksun, Inc. 2002. URL: http://www.niksun.com/documents/NetDetector_Datasheet.pdf

Garfinkel, Simson. "Next Year's Hot Security Tools: Today's pain points are tomorrow's vendor opportunities." December, 2002. URL: http://www.csoonline.com/read/120902/machine.html

Prosise, Chris and Shah, Saumil Udayah. "SSL: A False Sense of Security." August 9, 2000. URL: http://webbuilder.netscape.com/webbuilding/pages/Servers/SecurityIssues/080900/

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.