Global Knowledge®

Expert Reference Series of White Papers

Network Forensics for Attack Mitigation

Network Forensics for Attack Mitigation

Kerry Doyle, MA, ZDNet/CNet.com Associate Editor

Introduction

For many organizations, network traffic has increased to the point where supporting speeds of 10G or more is commonplace. They're finding that traditional Security Information and Event Management (SIEM) network analysis is simply inadequate. As a result, these companies are relying on a combination of vendor-based security solutions or custom algorithms, forensics specialists, and their own approaches to identify and mitigate threats.

Network forensics can best be defined as the monitoring, recording, and analysis of network traffic and events. Technicians perform network forensics to discover the source of security incidents, attacks, or other potential problems.

Choosing the right forensics tool enhances defense capabilities by providing security warnings, detection, and response. It can also be used to collect and retain raw network data for restructuring, playback, and information retrieval. While not foolproof, employing a solution along with the right approach to network forensics can help reassure C-level executives and the entire workforce that an effective defense is in place.

Frequently, network forensics are employed for things other than security. These include low-performance network segment analysis, analyzing VoIP quality, and checking network transactions. In this white paper, we explore the importance of network forensics for system monitoring and attack mitigation. We also examine other possible use cases and the general effectiveness of network forensics in these areas.

Today's Data Center: Faster Networks, More Data, and Advanced Threats

As 40G and 100G deployments soon become the norm, network forensics will play an increasingly critical role for gaining visibility into a range of problems. Some of the factors which contribute to the growing amount of data that networks routinely handle include online communications (video, VOIP, etc.), mobility, and IoE connections.

Since its inception in the 1990s, network forensics has gradually increased in sophistication. In addition to firewalls and intrusion detection systems (IDS), it offers a formidable set of tools to mitigate attacks. Such tools enable companies to be more versatile when responding to intrusions, and to conduct more effective investigations once an attack has occurred.

Choosing not to employ these tools when data theft occurs can be compared to ignoring security camera footage taken at the scene of a crime. In fact, more and more companies are using network forensics to resolve other related issues.

Copyright ©2015 Global Knowledge Training LLC. All rights reserved.

Network forensics can also be used to:

- Verify/troubleshoot questionable transactions
- Analyze overall network performance
- Identify low-performing segments
- Verify VOIP or video traffic problems
- Validate compliance

In general, specific solutions have been developed to collect and retain raw data or to record all transactions for later playback and evaluation. Tools also exist to help identify specific types of security attacks or information leakage. In addition to enhancing preexisting defense capabilities (firewalls, etc.), forensics can provide security warnings and real-time analysis.

Once a network forensics system is in place, an IT professional can work with security experts to analyze traffic and quickly determine the cause of a network event based on hard evidence.

In many cases, simply looking at data logs around the time an attack occurred is unlikely to uncover the source. Knowing what to look for and using the data queries developed by a specialist can help to focus a search. However, it's not just investigating residual data on the storage media from a system or a device, but an ability to analyze transient communications that continue to occur. In the end, successfully mitigating and investigating an attack often depends on a number of components, and having a good forensics solution in place is key.

Network Forensics: Basic Approaches

Post-incident response investigations rely on effective command-and-control and data extraction channels. Whether an administrator or engineer can accomplish a genuine forensic investigation depends on taking certain steps: effectively capturing data, a thorough review across a network for signs of compromise, and performing a forensic post-capture analysis.

After an incident, one approach might consist of retrieving a list of key security datasources, including logs and IDS/IPS systems. These sources contain the forensic evidence that will be important later on when establishing the particular methods used for a network intrusion.

In addition, creating a thorough list of when abnormal network behavior first occurred and linking similar events to form a pattern is key. External events that could be related include the departure of a disgruntled employee, lost or stolen hardware, or repeated attempts to retrieve passwords.

However, one can waste precious time simply searching through logs to pinpoint an intrusion based on the general time when abnormalities first occurred. On the other hand, the sampled traffic and high-level statistics which characterize some forensic solutions can be inadequate when compared to more in-depth, granular investigations.

Engaging a security specialist to assist in sorting through the issues can make all the difference. A trained specialist translates technical possibilities to actionable queries that help focus the search for clues within data files. Forensic technicians also make it possible to leverage existing infrastructure devices that contain months or years of useful evidence as well as advise how to place new collection platforms while an event is already underway.

In order to determine whether a network has been compromised and how the incursion took place, a variety of tools are available. Some organizations will have in place network monitors in the form of firewalls and flow connectors. Engineers can examine NetFlow records and firewall logs, and perform low-level pcap exploration. The tcpdump, captured from a mirrored port, enables packet capture and analysis.

Packet capture provides a variety of health information for a network segment. Statistical traffic info from "normal" traffic will also help to establish a baseline that will speed future investigations for both security and network incidents.

Forensics Tools: Network Analysis and Response

The use of specific security solutions and application technology in computer crime investigations, threat assessment, and analysis is well established. In addition to the protection offered by firewalls and network intrusion detection, these tools support current defenses and can provide critical security warnings.

They consist of canned forensics products for SMBs and mid-level organizations, and professional-grade tools that offer custom algorithms for incident detection for large enterprises. Professional tools monitor traffic 24/7 and provide statistical information about node usage and protocols. They offer analyses of connections into and out of a system.

By performing analysis on all networks using collection, filtering, and comparison, these tools enable security professionals to quickly investigate and trace problems back to the source. While some commercial solutions provide full packet capture (i.e., copy all packets that cross the network), others offer unique formulas for Meta data capture.

Most appropriate for larger companies, these solutions provide a combination of advanced formulas, canned analytics, and visualization dashboards to help security analysts and engineers improve their efficacy and efficiency.

Ultimately, purpose-built tools can often be more effective at certain mitigation tasks. In addition to the previously mentioned Netflow or Argus analysis/aggregation tools, foundational elements of any personal toolkit would include packet analyzers WireShark and tcpdump.

Another indispensable tool is grep along with Perl- or Ruby-based scripts, which offers the ability to perform detailed text log analysis. Such shell scripts allow one to enter a series of commands or write complex programs in terms of an edited text file. Commands are then executed by the shell to greatly simplify searches.

As network speeds increase to handle the growing amounts of data, and large-scale attacks become more frequent, forensics tools are tasked with determining the exact cause of a network event. Often, false positives occur, requiring engineers to distinguish between a real attack and a false alarm.

In the case of a real attack, peer mapping can be essential. Having identified the IP address of a machine responsible for an attack, a peer map illustrates key patterns. It shows all network activity between a suspect IP address and any other IT assets.

Such information includes which protocols were used and how much data was exchanged. Peer mapping can be essential for classifying false positives, and basic forensics tools will enable an IT professional to methodically sort through data, allowing content playback and analysis.

Key Approaches to Network Forensics

Prevention, detection, and response are key aspects of security in general, and they're also important components of network forensics. On a very basic level, IT professionals along with security experts are tasked with understanding what is happening with a network, finding the problem, and fixing it.

Copyright ©2015 Global Knowledge Training LLC. All rights reserved.

Of course, firewalls are primarily responsible for prevention—they block illicit agents from entering. In tandem with firewall logs that show traffic features, Intrusion Detection Systems (IDS) classify traffic based on patterns observed in malicious activity.

IDS validates alerts and detects violations in applications that weren't initially blocked by a firewall. Combining IDS with wide-scale packet captures, or pcaps, can be a powerful means of investigation. This combination can help validate alerts and determine the response to an attack. A security specialist or IT professional can also learn all manner of health information about a network segment from pcaps.

A range of tools and technologies can be employed to integrate intrusion evidence into an investigation, however certain procedures are essential. These include:

- Effective Data Capture: With increased network speeds, current solutions must capture packets reliably at a minimum of 20Gbps and never drop packets, even when networks are operating at peak demand.

- Comprehensive Data Recording: The size of a company's storage capacity can play an important part in data recording. It should be sufficient to store days or weeks of packet-based network data. Frequently, this can add up quickly to terabytes of information. Effective data recording makes it possible to identify the causes of a problem, show proof of incursions, and initiate other types of forensics investigations.

- Search and Inspection: Combing through archived network traffic for forensic clues can be an ineffective way to conduct a forensic investigation. On the other hand, powerful software applications exist that automatically analyze, identify, and isolate problems. An effective forensics solution should enable search and inspections as well as the export of data for further analysis.

- Event Reporting: Actionable reports enable security specialists and IT professionals to document the results of investigations. An effective post-mortem analysis can show network vulnerabilities. Well-documented reports can also be crucial for identifying the source of an attack, and for reinforcing existing safeguards.

Organizations need better awareness of the data traversing their networks. Deploying a forensics solution represents one of the main ways that companies are gaining 24/7 visibility into those network operations. Ultimately, such solutions, along with methodical forensics approaches, are helping to make analysis of network performance and IT risks substantially reliable.

Conclusion

Since increasing numbers of attacks are circumventing traditional SIEM analysis, network forensics represents the key to intrusion investigations and resolution. As IT professionals grapple with how best to cope with faster networks, greater amounts of data to analyze, and an increase in the number of malware threats, they're incorporating network forensics solutions into those investigations.

They're also using tested methods of analysis to answer questions, such as: What did the attackers do? How did they do it? and, Are we still compromised? They're using a combination of forensics tools and established approaches that include effective data capture and recording, methodical search and inspection, and event reporting to defend against these attacks.

According to recent research by ESG, the network forensics market is set to dramatically expand as increasing numbers of organizations become the victims of malware attacks. Limiting the damage from these incursions, and avoiding potentially crippling losses, are key motivators for businesses of any size. And network forensics offers a powerful set of tools to help companies achieve those goals.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge through training.

CCFP Certification Prep Course

Systems Forensics, Investigation, and Response

Network Traffic Analysis (NT100)

Visit **www.globalknowledge.com** or call **1-800-COURSES (1-800-268-7737)** to speak with a Global Knowledge training advisor.

About the Author

Kerry Doyle writes for a diverse group of companies based in technology, business, and higher education. As an educator and former editor at PC/Computing, reporter for PCWeek magazine, and associate editor at www.ZDNet.com, he has written extensively on high-tech issues for over 15 years. He specializes in computing trends vital to SMBs and enterprises alike—from virtualization and cloud computing to disaster recovery and network storage.

Copyright ©2015 Global Knowledge Training LLC. All rights reserved.