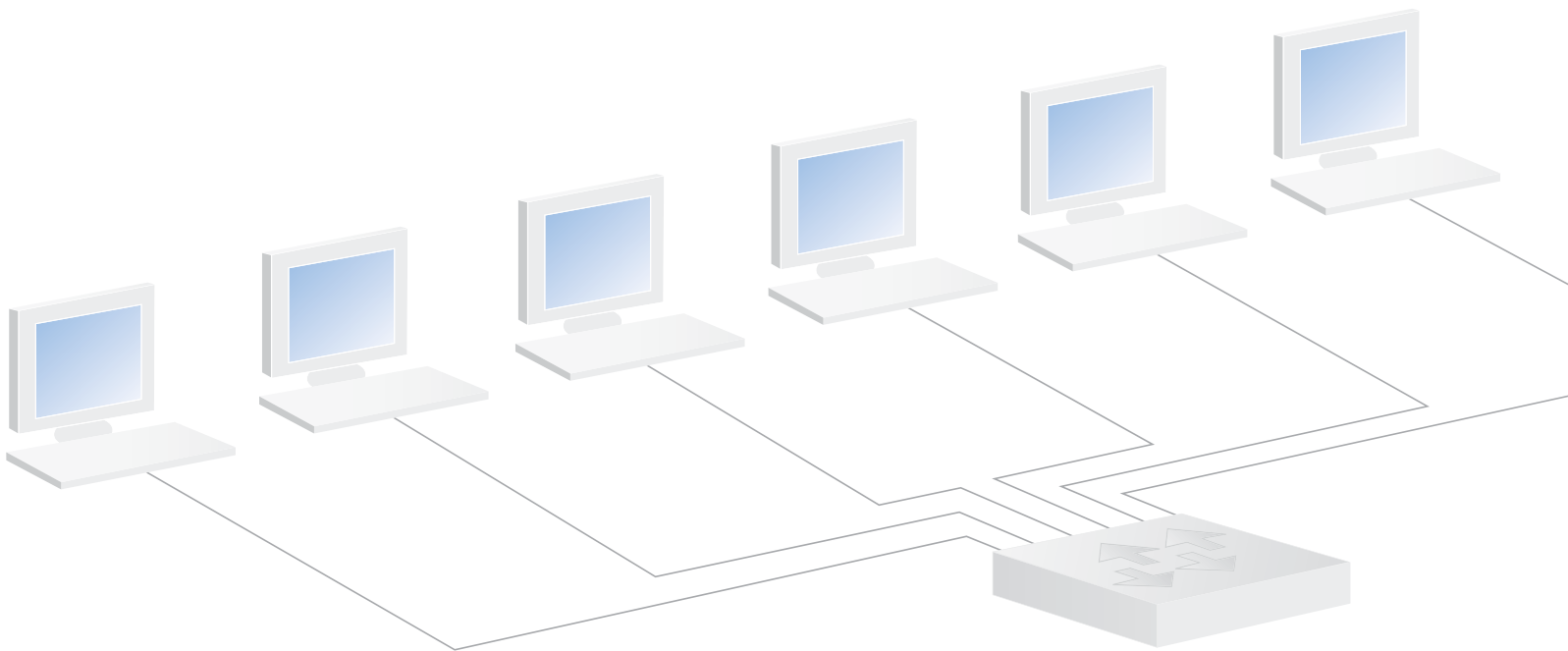


Network Security Forensics

As hacking and security threats grow in complexity and organizations face stringent requirements to document access to private data on the network, organizations require a new level of network visibility and surveillance. Network security forensics, a new method of capturing and storing every packet traversing the network, has emerged to address this need.



Summary

The world of network security has become an “arms race”. As organizations tighten their external defenses and install improved security tools, threats and attacks emerge to circumvent these security measures. Increasingly, this arms race is taking place in a regulated environment, where government rules such as HIPAA, Sarbanes-Oxley, and the EU Data Protection Directive require organizations to control access to private data and document security breaches.

The constant risk of circumvention and the need to have a record for investigation and compliance purposes is driving demand for a new type of network security monitoring solution known as network security forensics. A network security forensics device passively monitors the network, capturing and saving every packet, transaction, and communication for later analysis. This is the best method for identifying and understanding what occurred during a specific event.

This paper will:

- Identify the need for a network security camera to capture and save all network transactions and activities
- Illustrate how network security forensic appliances provide new visibility and evidence for security and compliance investigations
- Highlight real-world examples from clients demonstrating the role network security forensics plays in identifying security and compliance violations
- Provide the key components to look for in any network security forensics solution

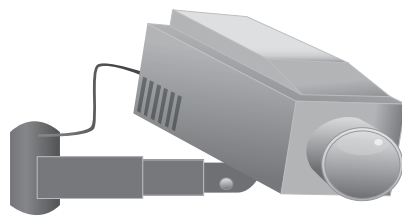


The Need for Visibility

Network engineers face a variety of changing threats in ensuring their organization is secure. These threats can range from hackers looking to exploit unpatched systems to employees attempting to steal company financial records. Although many organizations have taken significant measures to reduce their exposure to outside attacks, potential threats from trusted employees or contractors looking to exploit their knowledge of internal systems still remain. In addition, due to the evolving nature of security threats, existing security measures may be circumvented.

A need for greater network visibility resulted from these potential security breaches and new regulations that restrict access to customer information and corporate financials. For example, the Health Insurance Portability and Accountability Act (HIPAA) requires that a healthcare organization be able to appropriately document any breach involving compromised data and demonstrate that action has been taken to prevent the issue from occurring in the future. Organizations require a new level of network visibility, including data capture and analysis capabilities, to effectively ensure compliance and resolve security issues.

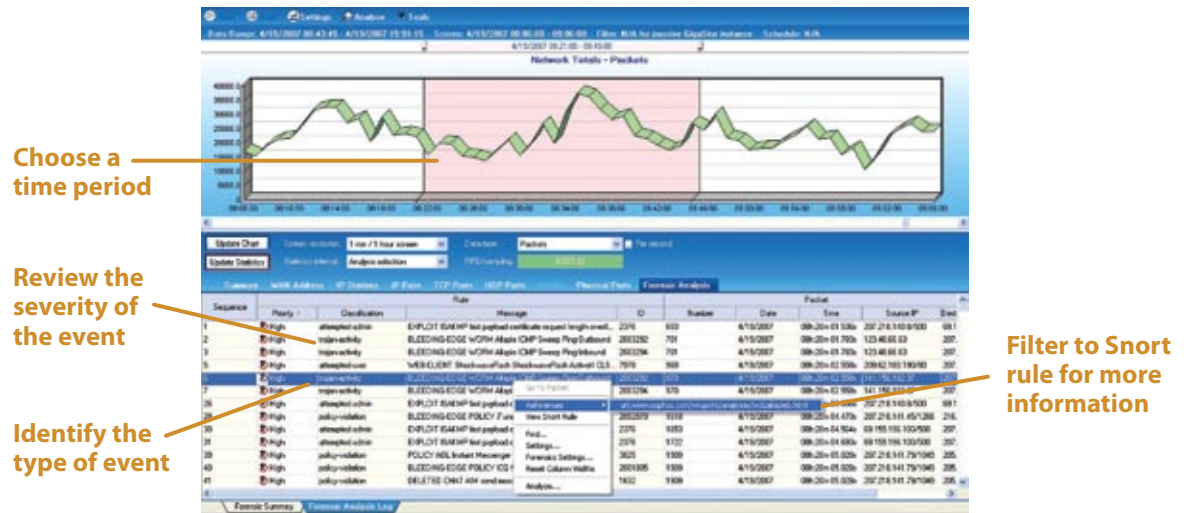
The need for surveillance and recording of business activities can be seen in environments outside networking. Although banks are secured with guards and alarms to prevent robbery, they rely on security cameras to record all activities should a break-in occur. The recording can then be used for further investigation, and to identify ways to prevent future robberies. In the network world, there is a need to capture and store every packet, transaction, and communication traversing the network for later investigation and future attack prevention.



Where network security forensics is needed:

- Monitoring internal threats
- Documenting evidence for investigations
- Solving the “Whodunnit” mystery
- Complying with government regulations such as HIPAA, SOX, and the EU Data Protection Directive
- Complying with corporate HR and network-use policies

Network security forensic tools have emerged to address this need. The appliances are unique in their ability to capture and save terabytes of packet-level data to disk or SAN. Users then select a specific time period of captured network activity, and the appliance sifts through the historical traffic to identify any anomalous traffic or potential security breach. In analyzing and identifying security events such as an attack, these devices commonly rely upon intrusion detection rules such as Snort, or other signature-identification systems. In addition to identifying security breaches, forensic tools should have the ability to reconstruct captured packet data into its original format, whether it be an e-mail, IM, web page, VoIP call, or other form of communication.



New Layer of Visibility

A network security camera complements an organization's existing security infrastructure. For example, when an intrusion detection or prevention system alerts the engineer to an attack, the security forensics appliance can be used to verify the attack. Although an IDS can be configured to begin a packet capture upon matching a signature, this can be a tremendous strain on IDS sensor resources. Cisco, for example, recommends strictly limiting the number of signatures that employ IP logging as an event action to eliminate the chance of an IDS slowdown.

Secondly, the IDS is not presenting a full view of the attack. With a network security forensics device, the engineer can confirm the attack and view everything that occurred on the network before, during, and after. Rather than simply learning from the IDS that an attack or hacking script was identified on the network, the network security forensics appliance provides more in-depth information, such as identifying the infected laptop that connected to the network minutes before the attack. Security forensics solutions can also help in identifying network infrastructure that may have been compromised during the attack.

In the case of unauthorized access or data theft, the security forensics device provides a paper trail of all network communications and access attempts between the user's computer and key network resources. Through data stream reconstruction, any confidential documents sent out of the organization over e-mail, web-mail accounts, FTP, or IM could be reconstructed as proof of an infraction.

Just as it documents access violations, a security forensics devices can ensure compliance with internal and government regulation compliance. When any security tool has identified a compliance violation, the network security forensics appliance provides an unaltered record of network activities, which can be used to document the event. Also, many security forensic solutions offer the ability to perform keyword searches to locate specific types of data, including specific names and social security and account numbers. Once identified, communications containing the keyword can be rebuilt and viewed in their original format.

Security forensic appliances provide the following benefits:

- Complement IDS/IPS tools by recording and investigating network traffic
- Offer a complete view of the attack and other network activities
- Provide complete documentation and evidence for forensic investigations
- Assist with corporate and federal compliance practices

“the network security forensics appliance provides an unaltered record of network activities, which can be used to document the event”

Security Forensic Scenarios

The following examples show how security forensic devices can play a key role in investigating and resolving compliance and security issues.

Security Scenario

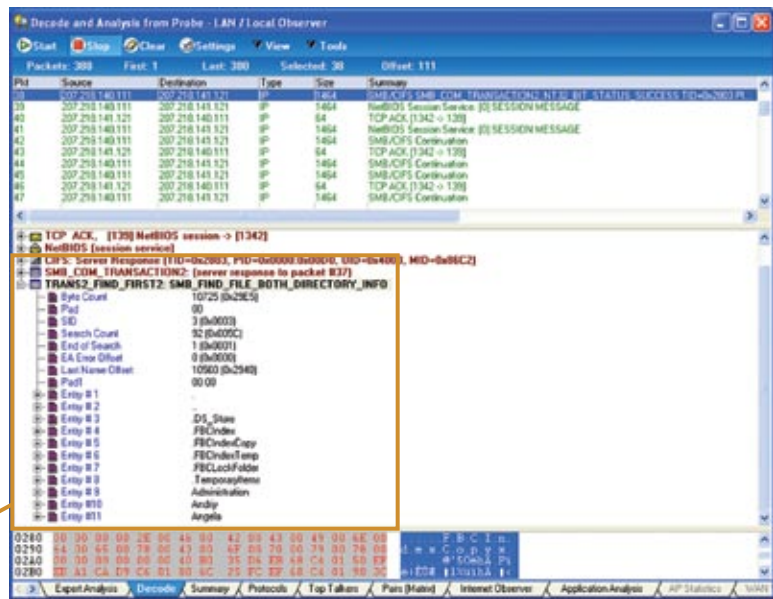
Over the weekend, seemingly random security anomalies began to appear in the organization's DMZ. The intrusion prevention system (IPS) was able to detect and successfully repel the attacks. During the same time and without detection by the IPS, a brute force attack occurred and successfully compromised the default "Admin" account on the company's VPN concentrator.

After entering the perimeter through a created VPN account, the hacker installed trojan applications such as remote control utilities and keystroke loggers. Subsequent malicious activity was then perpetrated against key internal systems using these utilities. All packet-level data and network activities were recorded by the security forensics solution.

To identify the attacks, the network engineer first isolated the timeframe, beginning when the perimeter attacks began, and tracked internal activities over the weekend period. Using the latest intrusion signatures, the selected time frame was analyzed for possible exploits, internal DOS attacks, and any key-logging scripts.

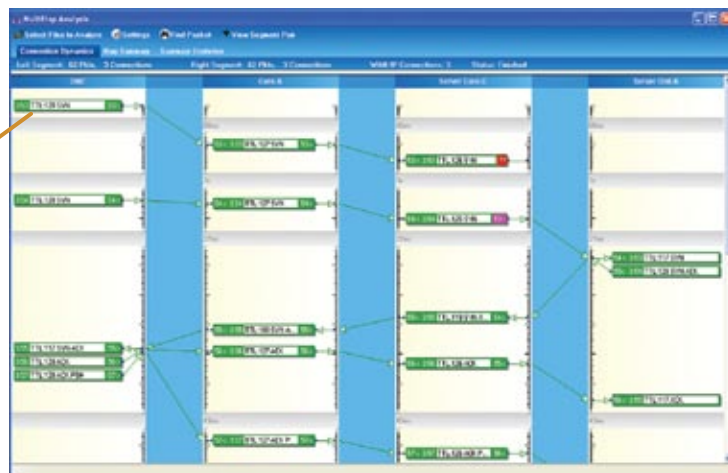
Once the exploit had been identified, the appliance drilled down into the individual frame to isolate any suspicious activities, such as data transfer under false pretenses. In this case, a trojan was used to access a critical file server.

Trojan used to access Windows file system



In addition to documenting specific cases of data theft, the security forensic appliance also identified the intruder's path across the network, allowing the security staff to identify potentially compromised infrastructure.

Follow the hacker's route over the network.

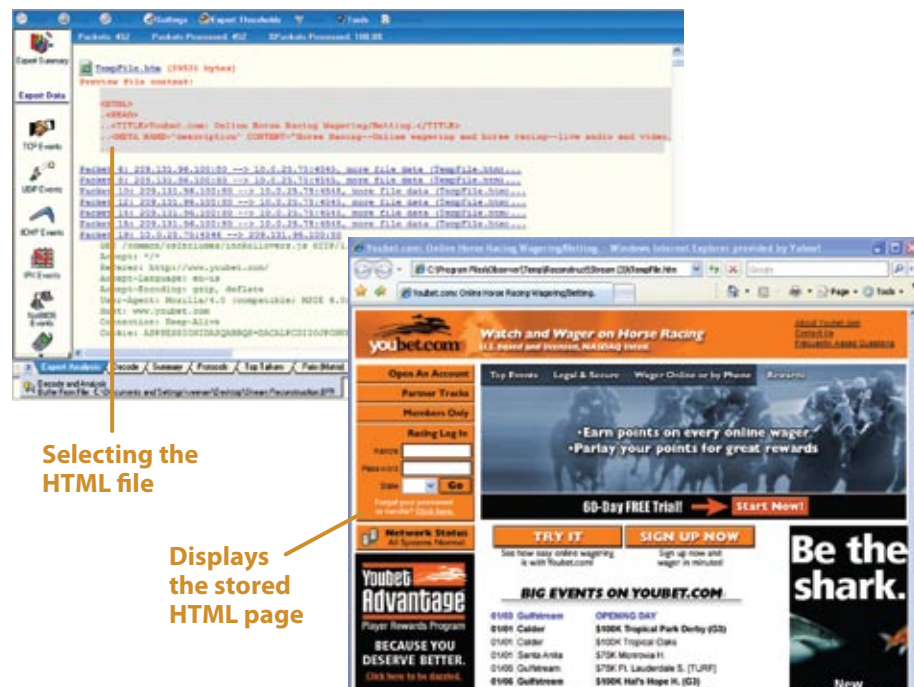


Compliance Scenario

Security forensics can help document and ensure enforcement of internal HR policies as well as government regulations. At a large financial organization, an employee was being reviewed for possible termination by human resources. Among the offenses, the employee was accused of browsing prohibited web sites on company equipment.

The network team was tasked with researching possible offences. In order to terminate the employee, HR needed conclusive proof of the infraction; providing only domain names and web addresses was not acceptable. The network team needed to document the incidents in a way that would reflect the activity the employee perpetrated and eliminate the chance of a wrongful termination lawsuit.

In this scenario, the network team tracked the user and his traffic patterns using the security forensics appliance, which allowed them to identify periods of excessive activity. In addition, visits to offensive web sites caught by the organization's web filter could be corroborated and documented. In this case all web sessions were captured and saved by the security forensics device. The specific HTML session was isolated and reconstructed to present the web site including images, exactly as it was when viewed by the user.



This was the proof the financial company needed to dismiss the employee without incurring any legal exposure.

Conclusion

New security tools will continue to emerge to combat constantly evolving security threats. There will never be a single "set it and forget it" security solution for stopping breaches on the network. To effectively address and prevent security breaches requires constant monitoring and adjusting of infrastructure and policy. If a successful attack is perpetrated against an organization, the monitoring solution becomes even more critical to ensure the attack is accurately identified and appropriate steps are taken to prevent future attacks. Network security forensic devices are uniquely positioned to provide a full view of all activities before, during, and after the event. These tools also have the ability to isolate the breach, identify software, scripts and exploits used; and locate potentially compromised infrastructure.

The ability to capture all packet-level data is also critical to compliance enforcement and the documentation of potential violations. The ability to accurately diagnose the breach or policy violation through reports and reconstructing communications or web sessions provides evidence necessary for proving compliance.

Security Forensics Checklist

The following is a checklist of key components that you should look for in a security forensics solution:

Network Security Forensics System Requirements	
Minimum storage capacity	4TB
Minimum capture-to-disk rate	250 MBps (2000Mbps)
Write-to-SAN capability	Yes
Data stream reconstruction	Reconstruct HTTP, IM, e-mail, VoIP, and documents
Security event and anomaly detection	Solution should support IDS rules, such as Snort rules
Ability to conduct time-based analysis	User should be able to select the time period for analysis
Handles multiple network topologies	Yes

About Network Instruments

Network Instruments provides in-depth network intelligence and continuous network availability through innovative analysis solutions. Enterprise network professionals depend on Network Instruments' Observer product line for unparalleled network visibility to efficiently solve network problems and manage deployments. By combining a powerful management console with high-performance analysis appliances, Observer simplifies problem resolution and optimizes network and application performance. The company continues to lead the industry in ROI with its advanced Distributed Network Analysis (NI-DNA™) architecture, which successfully integrates comprehensive analysis functionality across heterogeneous networks through a single monitoring interface. Network Instruments is headquartered in Minneapolis with sales offices worldwide and distributors in over 50 countries. For more information about the company, products, technology, NI-DNA, becoming a partner, and NI University please visit www.networkinstruments.com.

Solution Bundles

Contact a Network Instruments representative or dealer to ask about product bundles that cover all of your network management needs.



Corporate Headquarters

Network Instruments, LLC • 10701 Red Circle Drive • Minnetonka, MN 55343 • USA
toll free (800) 526-7919 • telephone (952) 358-3800 • fax (952) 358-3801

www.networkinstruments.com

European Headquarters

Network Instruments • 7 Old Yard • Rectory Lane • Brasted, Westerham • Kent TN16 1JP • United Kingdom
telephone + 44 (0) 1959 569880 • fax + 44 (0) 1959 569881

www.networkinstruments.co.uk