Global Information Assurance Certification Paper

Centralized Network Security Management: Combining Defense In Depth with Manageable Security

By
Scott Rasmussen
GSEC – Version 1.3
Administrivia version 2.0

Abstract

Centralized network security management is the practice of funneling the vast amount of security-related data from the various sources in the network through a centralized process and personnel. This effort ensures a comprehensive view of the network security status. It promotes good communication and redundancy in analysis. Centralized network security management also provides the capability to have a comprehensive and real time awareness of network security by integrating all of the tools and knowledge base from the implementation of defense in depth practices. With a few careful considerations for data redundancy and archival, centralized network security management can take advantage of the full power and potential for defense in depth and a hardened security posture.

Centralized Network Security Management:
Combining Defense In Depth with Manageable Security

As defense in depth becomes the standard practice for the implementation of effective security practices, the manageability of the information gathered and its associated analysis becomes a more challenging and diversified effort. With so many different solutions on so many different platforms reporting the data in so many different formats, accountability becomes more of an issue than comprehensive network security practices in the corporate structure. The signs of a distributed attack or incident may go completely unrecognized without the analysis of the aggregate data from all of the network security and monitoring devices through a centralized, comprehensive methodology. Without diligence and coordination, the implementation of defense in depth can become "security through obscurity," when parallel elements become individualized responsible entities as opposed to a central information data collection, normalization and analysis center. For defense in depth to work effectively, information must be correlated before being analyzed and aggregated in order to provide a complete network-wide view of the security posture. Although the unification of data formats is progressing, the need for centralized network security management becomes almost a necessity to establish a credible security posture, near real time or even real time awareness of network security status and effective enforcement of policy.

The Principles

Defense in depth promotes the idea that a layered approach to network security makes for a formidable challenge for attackers to circumvent and/or compromise networks and their systems (see Figure 1). The general principle is to have several layers of defense, sometimes overlapping, to provide the broadest and most complete coverage of the network. This would be accomplished utilizing diverse methods and technologies that integrate into a comprehensive representation of the network. Defense in depth follows the premise that there is no single solution to network security that makes a network completely secure. Instead, there is the more practical and effective practice of establishing several layers of security so that an intruder would have to navigate and compromise several layers of devices and policies in order to actually and fully compromise a network without being noticed. Also, the intruder would find fewer opportunities and vantage points to successfully attack the network because of the distributed approach of defense in depth. Defense in depth attempts to unify many approaches to security under an integrated umbrella of protection and awareness. The more layers, to a degree, the stronger the security and the more diversity the more comprehensive the protection.

An example to illustrate the defense in depth approach might be to establish a border router with access lists in order to enforce ingress and egress policy, also known as perimeter defense. To compliment this, a firewall might be put in place to provide network address translation, proxy filtering and more finite ingress/egress policy. From here, there may be a network intrusion detection system with one or more sensors monitoring traffic internally and looking for anomalies. Adding to this, host intrusion detection systems may be in place on critical servers

and workstations in order to maintain and validate their integrity. Virus detection compliments this by adding protection against malicious payload that gets carried in via email, possibly avoiding policy and initial intrusion detection. A syslog server could be established to provide centralized or redundant alerting of infrastructure devices as well as historical data that is easily backed up. Finally, a network management station can provide traffic analysis and network stability reporting for preventative actions as well as analysis of the events and trends that led up to a previous incident. This robust approach to network security offers a full spectrum of coverage and awareness to security issues and anomalous network activity. It provides near real-time awareness to potential or active problems and security breaches while being meshed within the total infrastructure. Weaknesses and faults in the network devices can be recognized and addressed to prevent future compromise. The result is a very wide range in the types of protection, which are layered around each other to provide a broad depth of protection, prevention and awareness.

The Tools of the Trade

There are several tools that are available and widely used to implement security solutions. Many times these tools are used in combination to provide a thorough implementation of network security through defense in depth, as mentioned previously. There are firewalls like Cisco Routers, Cisco Pix, Gauntlet, Raptor, CheckPoint-1, and Linux ipchains/iptables, among others. Some of the network intrusion detection tools include Snort, Shadow, ISS RealSecure, Prelude, SecureNet Pro, Cisco NetRanger and several others. Some of the host intrusion detection tools include Linux Intrusion Detection System (LIDS), BlackIce Defender, Zone Alarm and many more. For network management there are endless products as well including HP OpenView, CiscoWorks, OpenNMS and NTop. In short, there is a wealth of tools available that are both free and commercial for Windows and Unix platforms in varied levels of skill and scale. When these tools are integrated to form a homogeneous security solution, there are often gaps that are not covered or oversights that are not supported. When products from these families of security are combined together in a heterogeneous nature is when they reach their greatest power. Because of the different approaches to their function, the heterogeneous implementation can provide a much greater level of coverage as well as provide another technology to discover, understand and overcome. However, this also makes for a diverse and unique data structure for possibly each of the devices or products. This may establish a requirement for its own process and technical knowledge base for the network security staff to effectively operate and maintain. This can become a failing point in implementing effective defense in depth security measures, since there is no peripheral view of activities and the security staff will be required to have an in depth knowledge of the various technologies as well.

The Nature of the Enemy

Attackers have a wealth of tricks and methods to support their activities in compromising the security of a network. Some of the tools they use are developed by others and utilized by novices, often called “script kiddies,” while others are true innovators that develop their own

tools to fit their needs and ever-changing environments. However, they both pose a threat to security and have to be acknowledged as such. Their motivations are as diverse as their methods and practices. Most of the time, attackers are at least a half step ahead of the security industry in finding and exploiting vulnerabilities. This makes the ability to identify and react quickly paramount to the success of maintaining the integrity of network security.

Port scanning is one of the most common activities that attackers usually start with. It is the initial phase of reconnaissance that they can find potentially vulnerable targets with. Port scanning is an automated process where the computer will go and ask other computers if they offer particular services and gather other pertinent information such as the hostname and IP address. This information is then passed back to the attacker as a list of vulnerable systems with their associative potential vulnerabilities. Although this process can often be detected, it becomes more difficult to recognize when stealthier methods are used. One of the possible ways to stealth port scanning include the ability to time the scans so that there are only one or two connections here and there. Because of the fact that the sensor on the device is looking for several connections in rapid succession to signify a port scan, this probing may go undetected and provide no warning of the imminent attack. Furthermore, partial connections can be made as well as other bogus requests to determine the operating system of the computer and avoid port scan detection, based on the non-standard method of connection. Add to this the ability to use remote computers, called zombies, which have had malicious software installed on them, called Trojans, and the probing can be done by several different computers and pulled together for analysis. This would most probably not raise any alarms on any security sensors, as the communications would appear as legitimate or below the threshold of being classified as anomalous. Some of the port scanners that are in use today are VeteScan, Nmap and Distributed Port Scanner.

After the reconnaissance is completed, the target can then be attacked a number of ways, depending on the vulnerability. The important consideration to remember is that the same resources exist to compromise the vulnerable system, including the use of zombies. As an example, a distributed denial of service (DDoS) is a very effective tool to shut down a computer and its services, or even just to keep it busy long enough for another system to slip in amongst the confusion and bypass any security filters. Because of the mass volume of traffic from different sources, the illegitimate connections are hard to distinguish from the legitimate connections. If a single line of defense were in place, the whole network would be compromised at this point. However, if a layered approach were in place, this would only be the first of many methods and efforts the attacker would have to make in order to compromise the network. With a distributed approach of defense in depth, the attacker would have to have a great deal more knowledge and conviction to compromise the network, which may encourage them to move on to an easier target. On the other side of the fence, the network security personnel are faced with the same requirement to maintain currency on the diverse architecture as well as vigilance. Getting hold of the process and finding meaning in the results is the biggest obstacle.

The Process

The diverse data structure of the different devices and the method that they use to accomplish their tasks can often make event correlation a difficult and time-consuming job, particularly in a heterogeneous environment. Perimeter defenses such as routers often use simple network management protocol (SNMP) on transmission control protocol (TCP) and user datagram protocol (UDP) ports 161 and 162 to send events and alerts. These events and alerts are sent to monitoring stations or network management stations that parse and format the data for reporting. In contrast, the syslog service, as many Unix machines use, can send its logs and alerts to remote hosts via (UDP) port 514 and can incorporate other devices' SNMP alerts into its reporting. These alerts could then be received by a syslog server, network monitoring station or network management station and would incorporate the events and alerts of several devices to be parsed and formatted for reporting. Snort network intrusion detection utilizes a format similar to tcpdump, but adding the packet payload to the output. Snort can also use syslog for its logging format, requiring a unique reporting tool to parse and format the tcpdump raw data or syslog information. Often host-based intrusion detection software will have data parsing and formatting integrated into the package, using its own, perhaps proprietary, format. Network management stations pull statistical and status information from devices via SNMP and various logging methods to parse and format the information for its own style of reporting as well. Even though all of this data requires similar parsing and formatting and the communications are distributed in much the same way, there still remains discordance between them.

The Problem

This requires manual accumulation and organization of the various elements, individual analysis of each device's logs, and manual integration of the resultant data to form a composite of the network and its current security status. Sometimes the ability exists to import data from one format into another, but this is often not the case due to some products being proprietary or others just being self-aware. There are a lot of products and projects out there, each trying to satisfy a requirement while claiming to be a solution in itself. With the fast pace of the security industry, these products and projects are often pushed out to the public as quickly as possible and rarely contain the ability to integrate with other products and projects. In any event there are sometimes even different groups that are responsible for capturing and analyzing a particular part of the network security solution using one of these products. As an example, the personnel responsible for intrusion detection may only have access to or an understanding of the information from the intrusion detection devices. The firewall personnel may only have knowledge and access to the firewall information, and so on. To compound the issue, this separation of duty results in misinformation and lack of desired information between the responsibilities. The firewall person may not have the knowledge to understand what information is beneficial, or even crucial, to the intrusion detection person and vice versa. Thereby the same diversity and distribution that is meant to hinder attackers can also prove to be a challenge to the security staff.

This lack of coordination and oversight can make for a substantially weakened, if not failed, security posture. Because of their lack of knowledge, communication and integration of information, there are numerous voids in the security of the network that can, and probably will,

be exploited. This defeats the purpose of defense in depth at its core and is a result of improper implementation, either through policy or procedure. The characteristics of an attack can come from various symptoms of the network and have different threat vectors. With knowledge of only one threat vector or symptom out of several, the attack may go undetected and result in a compromise. The core of defense in depth is to provide several sources and levels of alerting to recognize a majority of the threat vectors and symptoms of an incident, which makes getting around them without being noticed a magnitude more difficult, if not impossible. This raises the awareness and integrity of the network when it is properly implemented, tightening the security of the network and its resources. Without the integration of security efforts and communication to provide reference and status information, the integrity of the network begins to fail, resulting in weakened security.

Looking Down the Road

The result is a requirement for an additional tool or methodology to unify, correlate and aggregate the resultant data from all of the sources in order to provide an accurate and complete representation of network activity and security. This would then make the various components of the network security structure appear as virtual co-operative agents that report normalized data to a central console or area which in turn aggregates and subsequently analyzes that data for anomalous behavior and/or signatures that may or may not represent an incident. By working in concert with each of the other devices, a true and complete representation of the security status of the network is portrayed. Centralizing the data ensures the continuity and detailed near real-time awareness of the network. In contrast, if the data were analyzed independently, perhaps even by different groups or in different geographies, there would be a lack of correlation between, and aggregation of, events that could indicate an incident. This could then lead to a realized, though previously unrecognized, security incident and cost a great deal more time, money and effort in containment, eradication and recovery than if it were detected in its early stages through correlation. Also, by normalizing or unifying the data, it could be integrated into a database, allowing the power of defense in depth to realize its full potential. Queries could be made on any number of elements to provide historical data on individual events or incidents as they relate to current events or incidents or even vulnerabilities. Having this information in a database would add current and historical statistical analysis as well as enhanced reporting and more focused data retrieval. As well, false positives, or false alarms which result from normal operations that were not configured for and subsequently generate alerts, would be able to be quickly negated or confirmed through detailed historical analysis instead of continued testing and tracking. Correlations could quickly and easily be queried and realized that may associate the signature of an event with an attacker from the past or previously recorded threat vectors, thus providing evidence for legal action or forensics. This type of detailed information, when collected and associated, also provides a method of profiling, in which the common traits of an attacker are logged and categorized for later reference to identify the attacker at a later date, should the need arise. Lastly, through a compilation of network information and auditing, new and previously undiscovered or unknown exploits and attacks could be recognized, with their historical signature captured and documented, for release to, and analysis by, others. Having the ability to share information such as this with a greater degree of accuracy and speed would enhance the network

security community in its awareness and overall defense posture.

Working Towards a Solution

The two methods that are appearing through companies and on the Internet are a second party analysis or consultation and the use of integrated products. Some of the entrants in the second party analysis option include the Internet Storm Center at http://www.incidents.org, Dshield at http://www.dshield.org/ and the Security Intelligence Alert Service/Aris Predictor at http://www.securityfocus.com/premier/ - PREDICTOR. These three sites are based on the premise that they host a central repository of current and relevant information in a central source for reference and distribution. This allows administrators the ability to quickly and effectively compare the symptoms of any questionable network activity with a collection of known and analyzed exploits as referenced from these sites. From this, it can be determined whether there is actually an exploit or undocumented false positive to contend with. If there is still a concern that this may be a new exploit or need further investigation, the packet captures and resultant logs/data can be submitted to the sites to be analyzed by a conglomeration of experts in the field. This allows for the security community to promote itself and its abilities through cooperative information sharing, which also affords the benefit of a higher degree of accuracy through redundancy. The second party analysis option provides for dynamic response to threats as well as a wealth of varied knowledge to find the solutions to counter these threats. It is inexpensive in terms of resources, but it lacks the depth to adequately respond to all but the lower echelon of incidents in-house.

There are a couple of integrated products available today that appear to be working towards some variation of centralizing network management and/or network security. One of these is Analysis Console for Intrusion Databases (ACID), which "is a PHP-based analysis engine to search and process a database of security events generated by various IDSes, firewalls, and network monitoring tools" (Danyliw). This tool provides packet analysis and historical data from various types of 'sensors' that combine their data to present a relevant network security status (see Figure 2). Another function of ACID is to process Snort intrusion detection alerts, tcpdump binary logs, Cisco Pix events, Linux ipchains-based events, and Linux iptables-based events into its database to provide a more comprehensive analysis of the health and security of the network. Although it has a finite pool of supported devices, it is clearly on its way to providing an impressive product. Another product is Demarc PureSecure, which incorporates network management with network intrusion detection alerting to provide network stability as well as network security information (see Figure 3). Demarc PureSecure provides an interface to Snort-based sensors, file integrity scanner, and log analyzer, among other things, and integrates it all into a relational database for analysis and reporting. Even though Demarc PureSecure is approaching this solution from a slightly different perspective, it too is developing in a positive direction towards centralized management. Consideration must be made to understand that these products are not a total solution to integrate into any network, but they are beginning to realize the utility and necessity for centralized network security management. The initial basis and organization of centralized network security management, therefore, needs to be established through policy and procedure

and then complimented with the appropriate tools to support and present it in an informative and relevant way.

Starting Blocks

One of the policy and procedure methodologies available to establish a solid foundation for centralized network security management is the dispersal of data and distribution of analysis. In this scenario, the various groups that are responsible for their part of the network security solution would frequently distribute their data and analysis to the other security group(s) as well as receive data and analysis from the other security group(s). This would spawn redundant analysis for validation, comprehensive data inclusion in the analysis to assist in identifying distributed attacks and aggregate attacks, and provide multiple backups of the data in the event of a compromise through multiple copies. Although this does not provide real-time or even near real-time alerting, it does promote a more thorough analysis of the network security state and provides a wealth of interrelated data to aid in better detection, incident analysis, and historical trend analysis. This also promotes open communication and collaboration of the various elements, which is crucial. The more information that is shared between separate groups, which all share the responsibility of securing the network, the greater their control and understanding of the overall security state of the network. As a byproduct, this policy/procedure would encourage configuration management practices to help in assuring that all devices were patched or upgraded as needed in order to protect against current and future vulnerabilities. Audits and awareness can be shared to facilitate the most current and reliable implementation of security measures. A more formal procedure would need to be implemented in order to safely and reliably back up the data regularly for historical purposes. In circumstances where new resources may not be available or the personnel hierarchy cannot be changed easily, this would at least provide improved security awareness, even if it were not the best solution.

The best methodology available to establish a solid foundation of centralized network security management is the consolidation of the groups responsible for the various layers of defense into a unified department or think-tank group, preferably in its own physical workspace. This would enable a centralized data collection effort, correlated and aggregated analysis, response as a composite and coordinated unit, patch and update uniformity and currency, a heightened and more accurate awareness of the status of network security through centralized reporting, and near real-time or even real time alerting of incidents and events via centralized collection and analysis. Having this advantage, particularly the near real time awareness, can be the difference between thwarting an attack and having to do a forensics investigation and recovery of lost data and resources. Although there is a reduced level of redundancy and a single point of failure with this methodology, this can easily be avoided through redundant data collection stations, redundant analysis via teams, providing an escalation chain, and regular archival of harvested data and/or analysis. This solution provides a higher level of security, as the various layers of defense are coordinated, cooperative and cohesive. There is also a broader collective of knowledge on which to develop, monitor and improve security awareness and integrity as the security personnel interact just as the devices themselves, sharing information and ability. This solution embodies

the practice of team building and sharing of knowledge within the group to help advance all parties in all aspects of security, as well as ensure completeness and accuracy through being able to have checks and balances from the input and correction of others in the group.

Reaping the Benefits

The operational benefits of centralized management include the ability to train relatively quickly as there is expertise in all disciplines centrally located and available; the vast array of skills and information required is centrally located and integrated for a more comprehensive understanding; there is a wealth of historical and trend analysis available as a means of tracability and accountability, including the capture of evidence; there is communication between the security personnel that reinforces redundancy and oversight to provide checks and balances as well as a coordinated effort; and all of the tools utilized are immediately available for reference and guidance in a central location. The drawbacks are that there is a large knowledge base required to facilitate the information from the various layers of defense and centralization results in a lot of information to parse and analyze. As a by-product of the group becoming its own functional unit, though, the information flows more freely and solutions are realized more quickly and effectively, since all affected parties are in concert. The large amount of information to parse can be distributed throughout the group to ease in the workload of the group and strengthen their interaction. Possible or potential threat vectors and incidents can be escalated within the group and appropriate attention made available to react with countermeasures relatively quickly. Immediate action can take place as soon as one person knows or a decision is made, since the rest will know as well, by default of working together as a coordinated and integrated group, and having an escalation chain. In essence, centralized network security management attempts to help the security community mirror the actions of attackers, particularly of recent, whom attack in coordinated groups and distribute their presence, threat vectors and attacks. These groups share tools and information to formulate distributed attacks, which are far more challenging to recognize and counter because of the subtlety of its signature and possible interference or diversion by other group members. Now the security team can have a distributed presence and coordinated defense to counter the efforts of attackers and minimize incidents, all the while avoiding duplication of effort. The distribution and integration of the security team strengthens the security status of the network. Add to that the centralization of the security team's tools and reporting and you have a near impervious network that most attackers will retreat from in search of easier and more vulnerable prey. Tie this in with the distribution of information to other repository and analysis entities, like www.incidents.org, and you help to strengthen the whole security community and diminish the availability of targets for attackers.

Conclusion

In summary, there are several factors that support centralized network security management. Policy and procedure are the biggest factors in building a solid foundation and effective security implementation. In addition, the granular analysis and aggregate data of centralization makes for a complete view and assessment of the security status of the network; maintenance and

operational security become tied together to improve stability; training becomes a diverse and rich exposure to complete security implementations and practices; diverse solutions and devices provide a fertile ground for growth, improvement and general awareness; a cohesion of the security team is developed which provides a coordinated approach to the implementation of best practices and support; and overall awareness and preparedness for security events and incidents becomes focused and honed. Although there is the liability of a single point of failure, this can be overcome through redundant data stores and archiving. The drawbacks that may arise from implementing centralized security management pose less of a threat when the results of improving security awareness and tightening security protection are manifest. The result is a highly aware and secure network that can react quickly and effectively, without any degradation in user service or operational latency. With a few careful considerations for data redundancy and archival, centralized network security management can take advantage of the full power and potential for defense in depth and a hardened security posture.

References

Hulme, George. "Centralized Security Management On The Way." (28 May 2001).
URL: http://www.informationweek.com/839/security.htm (16 Jan 2002).

Frederick, Karen Kent. "Network Monitoring for Intrusion Detection." (28 Aug 2001).
URL: http://www.securityfocus.com/infocus/1220 (20 Jan 2002).

"TCP/IQ." Socket Workbench – Port Numbers. (2002)
URL: http://www.tcpiq.com/tcpiq/res/tcpip-ports.asp (17 Jan 02).

Roesch, Martin. "Snort – Lightweight Intrusion Detection for Networks."
URL: http://www.snort.org/docs/lisapaper.txt (23 Jan 2002).

"Distributed Intrusion Detection System." (07/2000). URL: http://www.dhshield.org
(18 Jan 02).

"Demarc Security." URL: http://demarc.org (20 Jan 02).

Galik, Capt. Dan, USN. "Defense in Depth: Security for Network-Centric Warfare." (April 1998).
URL: http://www.chips.navy.mil/archives/98_apr/Galik.htm (22 Jan 02).

"Defense Logistics Agency: Information Assurance Modernization."
URL: www.dtic.mil/jcs/j4/projects/gcss/2f-dla_ia_tool.ppt (18 Jan 2002).

Bass, Tim; Robichaux, Roger; Liberman, Cheryl. "IEEE MILCOM 2001 - Defense in Depth Revisited: Qualitative Risk Analysis Methodology for Complex Network-Centric Operations."
Final Draft, Paper #403. URL: http://www.silkroad.com/papers/pdf/milcom2001-430.pdf
(11 Jan 2002).

"Incidents.org." SANS Emergency Incident Handler. URL: http://www.incidents.org
(24 Jan 02).

Musich, Paula. "Micromuse Gets Into Security Management." (25 Jan 02).
URL: http://www.eweek.com/article/0,3658,s%253D701%2526a%253D21746,00.asp (27 Jan 02).

© SANS Institute 2000 - 2005 Author retains full rights.

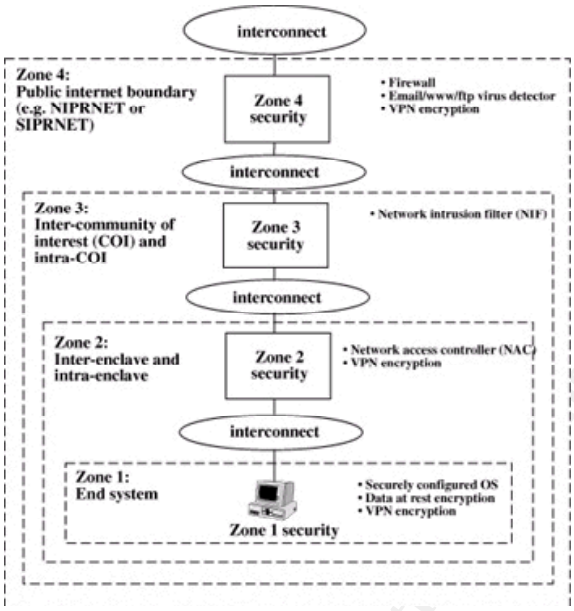

Figure 1. Defense in Depth Structure (Galik)

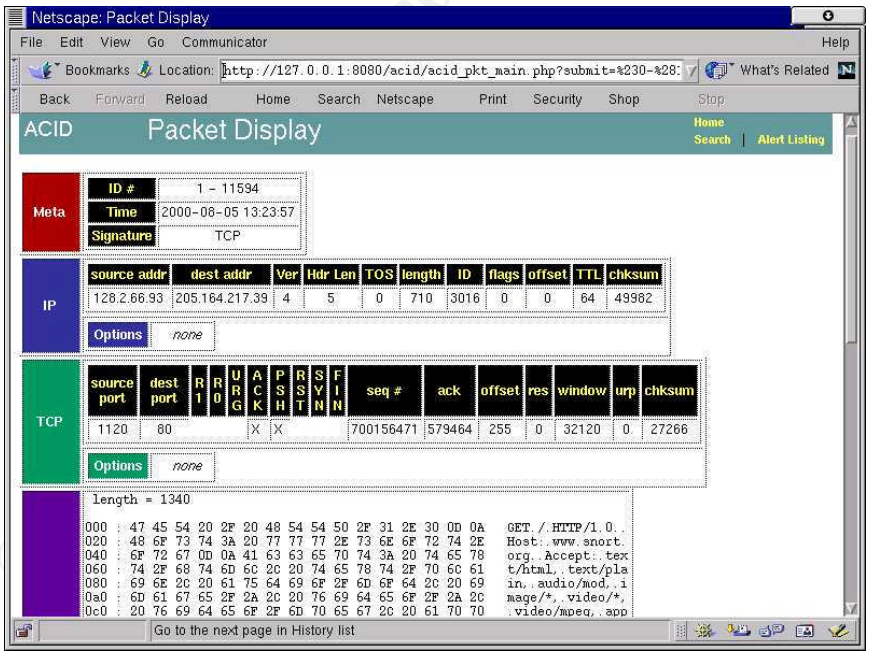

Figure 2. ACID Packet Display

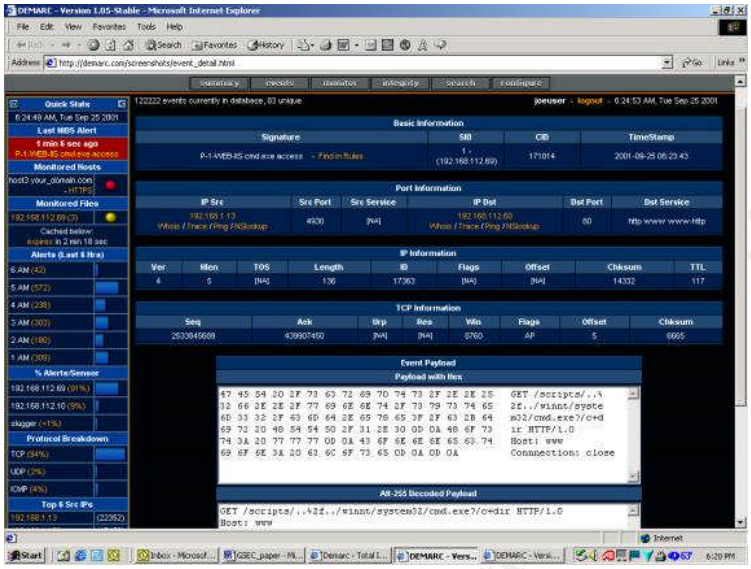

Figure 3. Demarc Event Detail