

Network Security Monitoring: Looking Beyond the Network

Network Security Monitoring: Looking Beyond the Network

Ian R. J. Burke: GCIH, GCFA, EC/SA, CEH, LPT

iburke@headwallsecurity.com

iburke@middlebury.edu

February 8, 2011

Abstract

Network security monitoring involves many different components. Visibility to the whole network has become as important as the basic firewall protection we build into every network design. With databases and applications leveraging the edge of the network and having wide access from a diverse user base, it is essential that they be monitored as closely as the traffic on the wire. Placing security events from any of the multiple inputs across the network into appropriate context is important if they are to have meaning and relevance. The tools to accomplish this are network flow and event correlation.

Traditionally network appliances have provided intelligence of network activity through SNMP or flow data. This has provided us with the incomplete picture we have used to support events provided to us by our IDS appliances. Today our advanced SIEM appliances can correlate that flow data against the IDS events. They can also pull in firewall logs and server logs among many other sources of information. Correlating these events against this diverse data can help provide context to where an event may have started or to what other systems might be involved. It can be used from the start of the incident handling process of identifying the incident, through forensics and again in the review process.

When network monitoring is looked at with this level of detail and is then reflected against traditional incident response frameworks or forensic best practices, it changes in relevance. In the past network monitoring has been a triggering event for incident handling. Today, a well-developed network monitoring solution may hold evidence which can be a part of the forensics and incident handling processes.

Network Security Monitoring: Looking Beyond the Network

As more networks are extending into the cloud, businesses must consider what security controls they want to pass off to the vendor that hosts their cloud solutions. Many cloud vendors offer differing levels of security controls with their applications. Some are extending those into feeds that can be pulled back into local central reporting scenarios. Security vendors are also finding new and creative ways to integrate cloud technologies into their solutions. As the integration between cloud applications and centralized networks becomes closer we as security professionals need to ensure that we incorporate these advanced technologies into our security solutions.

Keywords: SIEM, IDS, network monitoring, SNMP, vulnerability management, security monitoring, flow, database monitoring, cloud security.

Discussion

It was once said that if an attacker wants to get into our network they can and you cannot stop them. If this is true what is the point of trying to secure our networks? As security professionals we must accept that we cannot stop every attack but it is rather our goal to mitigate risk and establish an acceptable level of risk. (Bejtlich. 2004.) This is the objective of security. The challenge is to move the advantage closer to the side of security and away from the attacker.

On top of staying informed and ahead of the threat, the security professional needs to have the better defense. Sun Tzu teaches us that careful preparation can be the difference between victory and defeat. He also teaches us that strategy is essential to victory. (Giles. 1910.) To this end it is essential to develop a well thought out, layered network defense. This defense must be based on a sound understanding of the data and infrastructure that is to be protected as well as of the threats that might

Ian Burke

Network Security Monitoring: Looking Beyond the Network

be exploiting the potential vulnerabilities. By identifying the threats and vulnerabilities that can be paired together and having the knowledge of your network to provide this critical information you are better prepared to protect your infrastructure. Threat vulnerability pairs can result in loss. This combination provides for risk. It is the assessment of this information that provides the insight into the most efficient way to protect your data. (Gibson. 2010.)

No network is totally secure. The practitioner that strives for total security is destined for failure. There will always be threats and every system will always have vulnerabilities. The threat vulnerability pair results in an event. When this event results in a breach is when there is an incident. Visibility into this activity is where network security monitoring plays a critical role.

We hear discussions of defense in depth. A strong network security monitoring (NSM) solution is perhaps the true definition of defense in depth. NSM looks at data from across the spectrum of the network; from switches and firewalls to databases and applications. At the core of our networks we have an infrastructure of networking equipment built out of routers, switches and firewalls. Historically these devices were managed with SNMP and could send critical information across to central collection points with the same protocol. This was useful for gathering some network information about system state. SNMP is still used today as it gives a level of control over devices and the state information on network equipment is invaluable. Network devices have also added the value of flow data which collects more detailed information from the packet header. (Greer. 2010.) This packet header information provides valuable traffic information that might otherwise have required the use of a sniffer. Unlike the full packet data gathered by a sniffer, flow data is unidirectional packet header information. It reports on packets that contain the same source and destination address and the same port information. This is helpful in gathering traffic related information. A conversation pattern can be established between a

Network Security Monitoring: Looking Beyond the Network

source and a destination with this flow data and this is the data that is critically tracked. It can help to identify errors, the type of traffic in an event and other critical data. (Lucas. 2010.)

On early networks protection of a firewall was sufficient. Today we see web filters, IDS and other network security appliances sitting across the fabric of the network from the edge to the core. This equipment can provide many different aspects to the security picture. Not only does much of it provide blocking functions to threats, but it also provides data that can be passed back to a central collection point and compared or combined with the flow data from the network equipment to gain better insight into the activity on the network. This combined information is starting to provide a better image of activity on the network. For example, an IDS placed on the edge of the network may fire an alert for firewalking. When combined with flow data from the firewall of packets with diminished TTLs the alert is more meaningful and less likely to be a false positive.

Intrusion detection equipment today, like many of these security appliances have also come a long way to improving their technology. Many of these older systems were simple packet sniffers that would apply signatures to the traffic collected. When a packet or sequence of packets matched a signature they would fire an alert. These newer more advanced devices, not only can now block when they detect a violation to a rule, but their rules are more advanced. Beyond simple signatures the IDS of today applies advanced algorithms that look for behaviors, trends, and traffic patterns that are indicative of malicious traffic.

To this point we have looked at network information. Much of the significant activity that an incident handler would look at would happen at the application level. Inspecting a database or an application is a significant source of information for threat visibility. Adding this level of information to the NSM picture can bring the threat analysis from where on the network the threat was initiated to what application or even to what user the threat was initiated from. It may also help to narrow the

Network Security Monitoring: Looking Beyond the Network

scope of what systems or files may have been compromised. A database monitoring solution goes beyond looking at the logs of a database and will track the SQL commands being sent to and from the database. Depending on the implementation these solutions can track the user and the privilege level of the user sending the commands. Database monitoring solutions come in multiple forms. Some of the more advanced solutions function similar to sniffers systems that are targeted to database traffic. These solutions sit in front of a database environment and record the traffic passing through. Unlike IDS solutions which look at layers 2 through 7 of the OSI model, (Caswell, Beale, Foster. 2003.) database monitoring focuses on the application layer. The focus of a database monitor is the user traffic and the SQL commands being sent to and from the database. With database monitors that are not network based but rather reside on the database themselves, much of the metadata associated with the traffic may be lost, but the pertinent SQL information is still attainable. In either solution, the key benefit of a database monitoring solution is that all of this data can be sent to a central correlation system for alerting and reporting.

As we have seen a big part of NSM is about visibility. This picture would not be complete without visibility to the vulnerabilities across our infrastructure. Vulnerability management is a critical part of NSM. Vulnerability management is focused on awareness of the current weaknesses in the assets across your infrastructure. The tools available for this task have the ability to look at configuration of systems and applications installed on systems as well as current CVE information on these solutions. The CVE database is maintained by Miter. Miter also maintains a list of vendors that provide vulnerability management software. (CVE. 2010) This software can be used to add value to the NSM solution.

The tool that combines all of this data is a security information event manager (SIEM). These tools have advanced significantly from the log managers of a few years ago. With the ability to take data feeds from most security technologies as well as server logs and flow data they can correlate massive

Network Security Monitoring: Looking Beyond the Network

amounts of data quickly and accurately. The differentiating factors behind SIEM appliances and technologies today are mostly based on the scale of the solution, their ability to write rule sets, and their database engines. These systems combine massive amounts of data and help to elevate the truly significant security events to the top. They have the ability to look at the IDS event and link it to the flow data and the database monitoring event. They can also look at whether the database has the needed patches. With all of this data in one location it becomes much easier to identify an incident from an event and to isolate the scope of the incident as well. SIEM solutions are evolving from two camps. There are those which are event driven and those which are compliance driven. Historically SIEM solutions have evolved from either security providers or log management solutions. This may have a lot to do with the two different approaches. The event driven solutions are built on extensible databases. They are event driven and focus a lot of effort on elevating events based on correlated data.

Compliance driven solutions are often based on log management or log collection solutions. These systems architect large database solutions that can gather large amounts of log data and parse across that data for related events. From this related data they then correlate relevant events and report on compliance issues. In many respects it achieves the same end goal. The focus is the key difference of these two approaches. When architecting a solution, the role the SIEM will play in your security program may help to decide what approach is best for your objective.

As SIEM technology advances new features are being built into the solutions. SIEM appliances are being developed to communicate with more vendors and technology feeds from across the network. They are building in technology to support emerging technologies. Some vendors are focusing on reporting and compliance. Other vendors are focusing their solutions on remote connectivity and alerting. Most solutions are starting to find ways to support cloud technology.

Network Security Monitoring: Looking Beyond the Network

To date most of these NSM solutions look at the physical networks as integrated into our infrastructure. Security is lagging behind the business model which is moving to the cloud. More networks are extending to the cloud each day. The question yet to be answered by these network monitoring solutions and the cloud solution providers is how the cloud network solutions will be protected. Many cloud vendors are offering API's to pull some information down to local reporting environments. Many SIEM vendors are working on finding ways to integrate these API's into their solutions. Is this the next wave of NSM integration? However it is supported this is an area that vendors need to address and on which security professionals need to keep a watchful eye.

Cisco talks about the borderless network and how we can protect these emerging networks. They identify that access control is going to be a key component to securing these networks. They also point out that application, database and endpoint control are going to be key components to controlling these borderless networks. (Gillis. 2010.) As we look to cloud solutions we need to assess how we develop our borderless networks. Do we embrace applications provided by cloud vendors where we have little control or do we embrace cloud solutions where we can host our endpoint solutions? As we walk through the risk assessment for these solutions we need to assess the security implications offered by each solution.

Jeremy Conway of Nitro Security commented that it is important to remember that the cloud is still just a network and that monitoring it is technically no different than monitoring a local network. (personal communication, February 4th, 2011.) As he pointed out, the big question with monitoring networks in the cloud becomes who owns the assets and the data.

The Internet has come to offer one additional advantage to NSM which more vendors are integrating into their solutions. This is intelligence over emerging threats and real-time global intelligence pulled from sensors across the Internet. As vendors integrate this type of intelligence into

Network Security Monitoring: Looking Beyond the Network

their solutions they add an asset that allows security personal to contrast their correlated events against threats from across the Internet to quantify the viability of a threat and add global intelligence to their perspective of their NSM picture.

Conclusion

Network security monitoring is the process of defending across your entire infrastructure by correlating the gathered intelligence from security and network tools collectively. To be effective NSM should include data from the full spectrum of network appliances, network security tools and application aware security tools. As we extend our networks into the cloud it is increasingly important that we find ways to pull the data from our endpoints and integrate the visibility from those cloud vendors into the data that we correlate in our SIEM solutions. Increasingly SIEM vendors are working to integrate the API feeds from cloud vendors, but as we assess the different cloud solutions we need to identify the risks that are appropriate for our organizations.

Security is a cyclical process about finding the acceptable risk level for the organization. Network security monitoring is a powerful tool that provides visibility to the threat vulnerability pairs across the infrastructure and helps to move the risk equation in favor of the security professional and the business.

References

Anonymous. (2001.) *Maximum Security, 3rd Edition*. Sams Publishing. US.

Bejtlich. (2004.) *The Tao of Network Security Monitoring Beyond Intrusion Detection*. Addison-Wesley Professional. MA.

Caswell, Beale, Foster. (2003.) *Snort 2.0 Intrusion Detection 2nd Edition*. Syngress. MA.

CVE. (2010.)Miter. Retrieved from: <http://cve.mitre.org/>.

Domain Information and Management APIs. Google. Retrieved from: <http://code.google.com/googleapp>
Ian Burke

Network Security Monitoring: Looking Beyond the Network

[s/docs/index.html#domain](#)

Gibson. (2010.) *Managing Risk in Information Systems*. Jones and Bartlett Learning. MA.

Giles. (1910.) *On the Art of War*. By Sun Tzu. Tomsoft. Ebook retrieved from the Apple Store.

Gillis. (2010.) *Securing the Borderless Network: Security for the Web 2.0 World*. Cisco Press. IN.

Goodall, Lutters, Rheingans, Komlodi. (2006.) *Focusing on Context in Network Traffic Analysis*. University of Mayland. IEEE. Retrieved from: <http://www.securedecisions.com/Members/admin/context-in-network-traffic-analysis/>.

Greer, Chris. (2010.) *How Should I Monitor My Network: SNMP, Flow Analysis, or Packet Analysis?*. Fluke Networks. Retrieved from: http://www.flukenetworks.com/fnet/en-us/Community/Packets_in_Paradise?plckPostId=blog:1d69ff7a-abce-4694-9d65-915308c354a3Post:aaeb3741-3ad3-4c78-8cda-9685d240990f&plckController=Blog&plckScript=blogScript&plckBlogPage=BlogViewPost&plckElementId=blogDest

Kim, Love, Spafford. (2008.) *Visible Ops Security: Achieving Common Security and IT Operations*. IT Process Institute, Inc. OR.

Lucas. (2010.) *Network Flow Analysis*. No Starch Press, Inc. CA.

Nothcutt, Zeltser, Winters, Kent, Ritchey. (2005.) *Inside Network Perimeter Security*. Sams Publishing. US.