

Network Intrusion Detection for the E-Commerce Environment

Eddie Powell 2000-07-10

Introduction

"Good pings come in small packets"

As the network technology we utilize becomes more advanced so do the security issues surrounding these technologies. Evolving from the days of "sneaker net" to gigabit ethernet has introduced seemingly infinite risks associated with our public and private networks. Access control points, authentication and encryption mechanisms are only a part of the complete solution. As most security administration teams struggles daily to maintain their skill set with the latest breaches, viruses, and vulnerabilities, it is the malicious users that the administrators and consultants are "reactively learning" from. Network Intrusion Detection Systems (IDS) can provide a proactive approach for security administrators and consultants in assisting them with decisions regarding IT policies.

E-Commerce, an electronic medium that generates revenue on demand, can be demanding in maintaining security administration and management. Ensuring a desktop PC, or a server on the LAN can provide moderate challenges in securing the device, securing a device in an E-Commerce environment can prove most challenging. Whether Consumer or Business, E-Commerce provides extraordinary challenges in that your organization uses this revenue generating medium to provide a service which is highly accessible publicly and privately, and usually requires undesirable communication to be opened to these devices. The criticality of E-Data poses additional security measures, sensitive data pertaining to customers and business partners traversing private to public networks requires proactive measures to insure a secure environment. Additional communication to E-Commerce devices may be required as well from core internal systems from developers and programmers. Business processes and demand to "rush to market" must not alleviate the need for a well rounded secure E-Commerce policy. Unless physical security has been compromised, then accessing critical systems will most likely arise from the network, public and private. Network Intrusion Detection Systems when configured and implemented properly can assist in monitoring and security administration of your E-Commerce environment.

This article will discuss Network Intrusion System products by name, however this does not imply these products will be the best tool for your environment. Network Intrusion Detection is

only a part of the security solution. Thorough research is highly recommended before engaging in any costly decisions pertaining to your environment.

Overview

As the demand for E-Commerce grows on the Internet so will the increasing potential for E-Commerce sites to be maliciously attacked. The typically used business impact analysis approach (How much will this cost, if my E-Commerce web server is down) is no longer the standard as a strategic solution for implementing a well-defined security policy for the E-Commerce environment. Organizations also consider different risk factors than that of an insurance security model. The implosion of business on the Internet, has created the demand for organizations to take its product and "rush to market". This concept may introduce additional risk(s), a organization that once considered certain risk(s) as unacceptable, may now be acceptable.

With the influx of products being utilized more widely in the E-Commerce environment such as middleware programs, (i.e. Bluestone, MQseries, and Vignette) the need for additional connectivity to critical systems for critical customer data flow is now a requirement in the environment. This data flow may require connectivity to core systems, where a firewalled device may be insufficient. Denial of Service (DoS) and Distributed Denial of Service (DDoS) are becoming increasingly effective tools for malicious users to utilize against E-Commerce Infrastructure, though an unknown DoS and DDoS attack may occur, and your organizations Network Based Intrusion Detection may not posture defensively against first time denial of service attacks, IDS can provide you with statistical data for future safeguarding. As we all are aware, but it must be continually emphasized that the majority of security breaches are internal. Monitoring of key segments, **internal**, and external along with detailed logging and proactive intrusion detection are additional mechanisms in assisting in securing the E-Commerce environment.

Understanding the environment

The most challenging issues are a complete understanding of the E-Commerce environment you are attempting to secure. Security in this industry has long been considered a "consensus of opinions" and in a generalized sense is so diverse that the vast amount of information pertaining to each area, (i.e. network, application, authentication, encryption, and operating system specific) is seemingly infinite. Along with understanding security issues within your

enterprise also comes the tasks of administering and maintaining an up to date security policy. Vulnerability management alone within an enterprise may constitute the need for additional resources. Understanding the issues within your E-Commerce environment is just the beginning, understanding the communication and data flow in the environment is essential as well. Publicly, web server(s) may be only available for http and https services, however backend connections to core database or application servers with middleware products requires additional communication. As a security administrator/consultant you will find yourself being asked to research communication of data flow and applications beyond a typical LAN environment. You may be required to know "What services and/or communication will be required for a SNA /IP gateway for business process messaging to the E-Commerce web and/or application server(s), is it only SMTP?" and you may also need to understand is it only FTP and HTTP communication from a content management server to the E-Commerce web server(s), content that may be pushed across multiple communication channels such services as web, pager and cellular data.

It is imperative to maintain an up to date awareness of the security needs for your enterprise, to focus on your environment can ease some administration and management burdens to your E-Commerce critical systems. Is it necessary for the E-Commerce Security team to maintain the latest Windows NT© operating system vulnerabilities if every server in the E-Commerce environment is a Unix platform? By understanding the security challenges in your environment it will allow you to be more efficient in detecting true breaches and allow you to resource your time effectively, allowing you to focus on other responsibilities.

Understanding Network IDS Signatures

With a good understanding of what communication is being passed through your E-Commerce environment you will be able to understand attack signatures or potential intrusion. Signatures are in different formats, a port signature is a monitoring of connections to ports in the environment. The E-Commerce environment externally may require only ftp, http, and https services. Port signatures will detect connection attempts and pending your network based IDS product and configuration it can perform several functions in a proactive monitoring state, such as alerting, paging, email notification, terminate the session, reconfigure a firewall for action, or user defined. A packet header signature looks for potential malicious combinations in a packet header. A well know packet header signature is a TCP packet that attempts to start and stop a connection simultaneously, this TCP packet will have the SYN and FIN flags set. String signatures will detect a text string that may be used for a potential malicious attack, one that

may be seen in a E-Commerce environment well known to web server(s) is "GET/cgi-bin/phf".

Out of the box, products such as ISS Real Secure© and Axent NetProwler© come with several signatures preconfigured. As of this writing Axent Net ProwlerS comes with the ability of customizing your own attack signature definitions, and ISS Real SecureS allows you to customize expression strings.

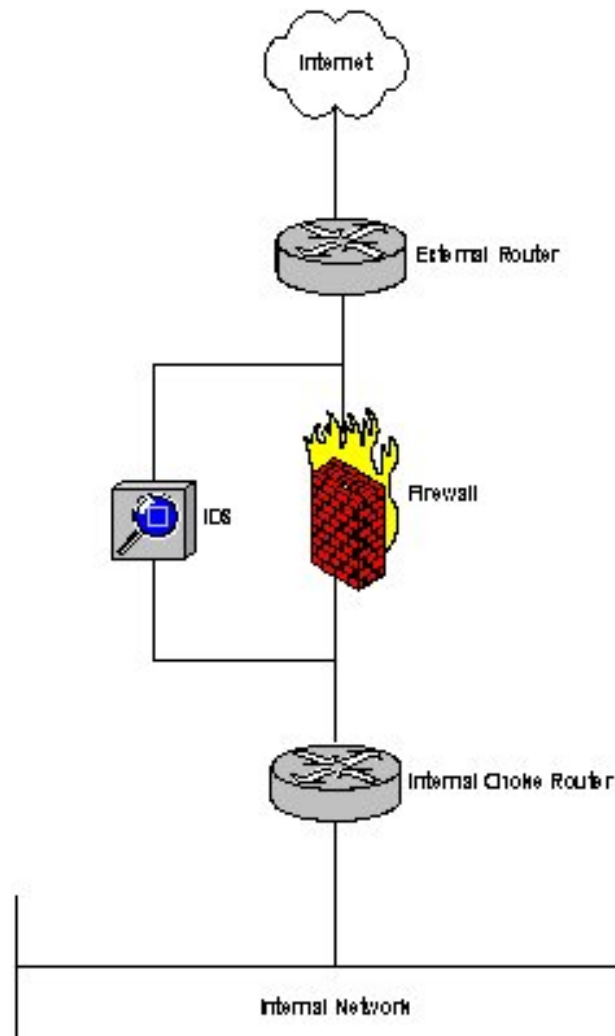
The ability to tune these signatures in your environment is essential in reducing the number of "false positives" generated. A false positive is signature that has been identified as a potential attack when it is actually a normal session. EntryPoint© formerly Pointcast was known to trigger false positives in certain environments during its update downloads, without the signature being tuned, ISS Real Secure© would recognize this event as a SYN Flood. Certain devices by nature will trigger IDS and create false positives. By tuning thresholds in a signature database and configuring the IDS product to ignore devices by either IP address or source and destination ports you can drastically reduce the number of false positives generated.

Popular signatures just as network vulnerabilities are frequently updated by IDS vendors. An up to date signature database is similar to maintaining a virus definition database, "If the anti-virus program is unaware of the virii type, what protection can it offer?"

Monitoring of key segments

In an E-Commerce environment there may be a requirement to place several network intrusion detection devices in several locations on the network. Network based Intrusion Detection Systems are only able to monitor network traffic on the network segment they reside on. The diagram below depicts a typical layered security approach in an end user access environment.

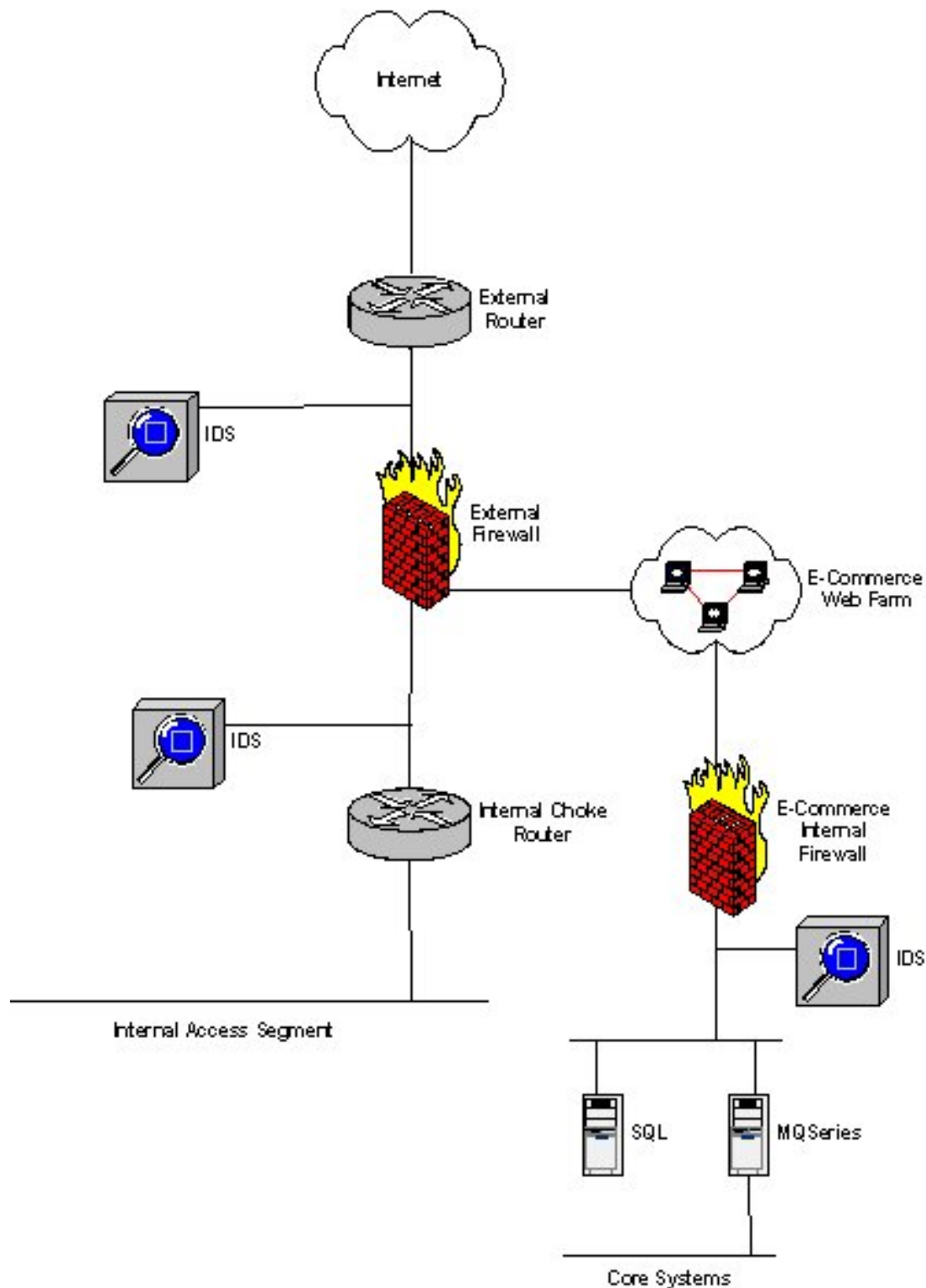
Diagram 1.



This layered methodology can provide adequate security in most environments, however a potential issue in diagram 1. though not likely if the IDS system is configured correctly, but in the event the Intrusion Detection System becomes compromised the potential malicious user can also bypass a layer of security, the firewalled device.

In the E-Commerce environment where recovery of E-Data costs are considerably more than the cost of replacing a poisoned DNS server, will require much more isolated security layering. As emphasized previously, connections to core systems and the need for internal users such as programmers and developers connecting to critical systems can pose potential security risks. The diagram shown below may depict a E-Commerce environment with connections to core and middleware systems.

Diagram 2.



This may appear to be an "overkill" environment, however this type E-Commerce environment provides multiple solutions, by placing Network Intrusion Detection Systems on key segments this allows monitoring as in diagram 1. and reduces the possibility of complete breaches if a single IDS system is compromised or if the resource becomes unavailable. The backend connectivity from the web server(s) to the internal network provides multiple solutions as well. Sensitive E-Data communicated from middleware and core systems are not traversing the public firewall, segregating this data to it's own segment. This also allows this E-data, sensitive

to network performance to be uncongested with other traffic on that network segment. Also if necessary the communication that may be necessary to administer and maintain the web server (s) can traverse the internal firewall through a separate communication channel as well, this communication also again is being monitored by IDS. Internal users are also monitored by IDS.

The above aforementioned solutions may not be the adequate solution for your E-Commerce environment, again thorough research should be done in order to provide your organization with a best fit scenario.

Fingerprinting, The Hackers toolbox? The Security Administrators toolbox?

TCP/IP stack fingerprinting is widely used as the choice methodology for potential malicious users to gain information in order to compromise devices on your network. Fingerprinting allows potential malicious users to extract information on devices by probing the stack of the networked device. One of the widely used fingerprinting tools of choice is [Nmap](#). As our technology increases so do the exploits and tools designed to find these exploits, one of the latest tools used in fingerprinting is [Queso](#). This tool has quite extensive tests and separates the OS fingerprints from the code, allowing it to add an additional OS easily. What information is extracted from the TCP/IP stack? It provides potential malicious users with information on operating systems which a potential malicious user to exploit that OS. For instance just obtaining simple information through an ftp session may instigate an attempted exploit on the ftp server in question. The sample ftp connection below indicates OS type and ftp version information.

```
c:\>ftp ftp.nai.com
Connected to ftp.nai.com.
220 ftpcal6 Microsoft FTP Service (Version 4.0).
User (ftp.nai.com:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password: *****
230-*****
230-230-WARNING
```

At this point a warning banner is issued by the system. However application banners still provide information regarding the ftp application. There are several methodologies for

Fingerprinting. Certain methodologies may also include mixing techniques from different Fingerprinting methods. By producing this statistical information potential malicious users can utilize this information to exploit your environment. Fingerprinting has an upside as well. These tools are not for hackers alone. Security Administrators can utilize these tools to identify the potential exploits and then take this information to secure the environment. By fingerprinting your environment you can generate statistical data to be utilized to configure your Intrusion Detection Systems.

As this information is very useful in the hacker community, it is a valuable tool in aiding the Security Administrator/Consultant as well. By using passive fingerprinting in your E-Commerce environment you can obtain this same statistical information that hackers learned from your environment, it can be most helpful to determine what operating system and platform you are being attacked from.

Conclusions

Implementing security methodologies pertaining to your E-Commerce environment is not a simple project. Research alone is very time consuming. Network Intrusion detection should also be complemented with it's counter-part Host based Intrusion Detection. IDS alone will not ensure a secure environment. A layered approach with firewalls, hardened routers, and other security mechanisms will assist in securing and administering the environment.

What next generation of technology will be available for Intrusion Detection, ample forethought has to be given to this arena as E-Commerce is evolving with new technology. Wireless E-Commerce with wireless application protocols (WAP) present additional challenges in securing this communication. Will the future of Network Intrusion detection not only be able to monitor the network promiscuously on it's own segment, will it be able to detect eavesdropping in the wireless E-Commerce environment? Automatically notifying your service provider with information regarding a potential attack?

This article was to provide high level insight information pertaining to Network based Intrusion Detection. As Network Security Administrators/Consultants we will continually become burdened with administrative and maintenance duties and responsibilities. It is imperative to maintain and keep up to date with issues pertaining to your environment. Along with poorly configured devices, not up to date devices can be your biggest demise in a potential malicious compromise.

Eddie Powell is a Senior IT Security Consultant for IBM. Eddie has been in the IT security consulting industry for seven years, and a consultant for eight years. When Eddie is not playing "road warrior" he can usually be found in the water underground in his home state of Florida, as Eddie is an avid cave diver.

Relevant Links

[Subscribe to FOCUS-IDS Mailing List](#)

SecurityFocus.com

[Privacy Statement](#)

Copyright 2006, SecurityFocus