GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Developing Secure Internet Services Using Virtual Machines

John Herring
7 December 2003
GSEC Practical V.1.4b - Option 2

Abstract

This document describes the real world situations that established the need for a separate development and test environment for Internet Services. Internet Services can be anything from basic static web sites to complex applications and e-commerce sites. Security can be expensive and the provision of a duplicate production environment for developing and testing applications is no exception. A previous cost benefit analysis had deemed that the cost of a full duplicate of the production environment did not make business sense. However it did established that the risk was still real. When events triggered the situation to be re-evaluated, a cheaper alternative was sought so that security could be enhanced in a way that made business sense. This document then goes on to explain why secure application development is vital and how security infrastructure components can be built into a cost effective solution using virtual machines.

A secure Internet presence is an essential part of many companies' business offerings. Through the Internet a company can deliver its commercial offering and enhance its brand identity. Any web site or web enabled application is the view the outside world or customer has of that company. If any component of the company's Internet presence is compromised, or displays inappropriate material, the company can receive irrevocable damage. This can take the form of data loss, interruption of service or a damaged public image.
By incorporating an effective development and test environment into the companies established policies and processes all new application development and upgrades were completed in a timely fashion and without introducing yet to be identified risk or unexpected instability to the production environment. The provision of a ready made test environment and guidelines also helped developers better understand what security requirements were to be imposed on their application once in the live environment.

Background

The document focuses on one company's environment and how vulnerability in its environment was identified and what risks this posed to the company and potentially its partners and customers.

As a large multi-national company several large and complex Internet points of presence were required around the globe. The design of these Internet points of presence absolutely follows one set of global policies and procedures. These are wide ranging to be able to cover the needs of several

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

quite different businesses within the company. The application or service needs of human resources, manufacturing, sales and business partners can be very different. The infrastructure design covers many key 'defense in depth' concepts with several layers of security working together, from firewalls through to intrusion detection systems. There are also procedures in place to ensure that confidentiality, integrity and availability levels are maintained to a level that makes financial sense to the business.

The businesses within the company rely heavily on their Internet presence for many if not all of their commercial offerings as well for providing pre sales and post sales information on their products and services. They expect controls and infrastructure to be in place to prevent outages, defacements and information theft. At the end of the day, it is these businesses that pay for the companies infrastructure and there is always a limit to how much they will be prepared to spend. The real world makes reducing the risk of threats and vulnerabilities from internal and external sources an important but fine balancing act between performance, cost and security.

Processes identify problem areas

Two key operational processes are the release to production process and change management process. The goal of the release to production process is to ensure all components, from datacenter location to hardware, operating system and application are built to documented standards and that operational groups are able to support and monitor whatever is moved into production making sure that no existing services would be affected. The goal of change management in some ways is very similar but the scope of a change is more to do with controlling changes to what is already in production. In scope for a change request would be provision of supporting documentation and back out plans should a problem occur. Key to both processes is that all steps are documented to provide an audit trail of change. Note that a change control process would be used during the several stages of the release to production process, like when hardware is installed and operating systems built. Each of the processes has a regular review cycle. On successful completion of a review in either of these processes the new or updated application or service can move onto the live production environment.

Within this company, the security engineering role (my role) takes part in the review cycle of both the change management process and the release to production process. During the change management reviews two existing application owners had submitted requests for version upgrades to add functionality to the applications. When questioned on what end to end testing had been completed their answer was 'Well we tested on the internal network and it works fine but we hope to perform the final testing when we are on the production infrastructure' These change requests were not approved and subsequent testing found that the default configuration after the upgrade did not correctly enable logging to provide an audit trail of activities within the application. As both applications related to an online ordering system for partners an audit trail was a very important security feature.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The problem encountered in the release to production of one application was slightly different. The review actually took place at a mid point in the development cycle - a progress review so that an internal pilot could be carried out. Unfortunately this was actually the first time the security engineering role had been directly engaged. Two important security problems were encounters. Firstly, a lot of development had already been carried out, but the developers had previously been denied access to details of the Internet infrastructure. They had been developing almost blind to how they were going to need to integrate the application into the existing infrastructure design. Due to a misunderstanding of what constituted personally identifiable information some communication paths within the application did not require the use of an SSL encrypted data stream. The developers had also expected to be able to be able to fix any problems once they had their application infrastructure installed in the production environment.

The impact of not being approved was different for each application due to how far through the process they were but included –

- increased risk do security features not being fully set up
- delay in the production 'go live' date. Based on one of the applications predicted revenue streams, this meant many thousands of dollars a day in lost revenue
- increased development costs required for the solution rework
- security group perceived as a business roadblock instead of a business enabler.

So what went wrong?

As the requirements for more and more Internet enabled applications and services grew the company had funded a major Internet services infrastructure upgrade. Key was the alignment of the various business needs with security, infrastructure and operation policies and procedures. This is all good so far. The end result was a stable but quite complex environment using products from industry leading solution providers. A cost benefit analysis towards providing a full blown duplication of the production failed to justify the quite considerable spend required. Combine this with an internal requirement that all details of the actual design of the Internet are restricted to only the team that designed the environment. The result being that application development had effectively been cut off from the very information needed to be able to develop a functioning secure application.

What does this mean then?

Fortunately for the company existing processes picked up the security vulnerabilities and prevented the vulnerable applications from going into production. This is a very good thing. Expecting that all potential security problems are going to be isolated based solely on a paper review is not realistic. A great deal of time and effort had been wasted. A solution was needed to prevent further problems with application development. Further

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

proof was needed that security in application development is just as important as security in the supporting infrastructure.

Why Application Security is Important

Applications and web service development has had a reasonable amount over coverage over the past two years. So the proof is out there. A SANS Institute webinar titled “Is your Web App Secure? How Do You Know?” featuring Ed Skoudis (http://www.sans.org/webcasts/show.php?webcastid=90425) was aimed at increasing awareness of web application vulnerabilities. It went on to demonstrate tools that can be used to test for these vulnerabilities or flaws. An article with a similar theme by James Middleton of VUNET titled “‘Application security 'in a grim state' “(http://www.vnunet.com/News/1129340) reinforces that vulnerabilities are common and the risk of attack is rising.

Another article from Paladion Networks http://www.paladion.net/services/web_application_security.htm makes the point that much effort is often put into protecting the network, operating systems and the infrastructure, but not always the applications. These applications could be either in the form of off the shelf packages or home grown applications. The results can be very public when the applications have not had established best practice design techniques applied and then been through rigorous source code analysis (see below for a definition) and vulnerability scanning.

Source code analysis is where developers use a combination techniques and tools to ensure that the code does not contain any errors that could become security vulnerability. For example, common recent exploits have come from code that does not perform data validation of input fields. Many sources of documentation exist on what to look for. A good example is from The Open Web Application Security Project (OWASP) called “A Guide to Building Secure Web Applications” http://www.owasp.org/documentation/guide

The previous paragraph really relates to best practices. You do not have to follow them if you do not want to. This comes with its own risks but you may feel that you can put controls in place to mitigate these risks. There is a common commercial situation where best practices are an absolute requirement – financial transactions. Whether the company directly performs the transaction, or buys in services such as a credit card processing services, there are rules that must be complied with. A very good example of these rules can be found at a major global credit card company Visa USA’s web site. They have set down what they require of merchants before they will accept transactions from the merchant. They have a Cardholder Information Security Program (CISP) which amongst other things contains a section on technical Issues and answers “Visa Cardholder Security Program” http://usa.visa.com/business/merchants/cisp_tech.html. If the company is setting itself up as an ecommerce site then designing the infrastructure and applications based on these requirements should be seen as essential.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Identifying an affordable solution

So the problems have been identified and the need for a solution has been verified. Building a single fully featured test environment for application development and maintenance could possibly gain financial approval. However, because of development taking place in several countries, more than one environment would be needed. The cost of the hardware alone would be very high – potentially running into the hundreds of thousands of US dollars for each instance of the test environment. If you add on the cost of ongoing maintenance and the support time required to keep the test environment running you end up with a very expensive solution. The original environment the cost benefit analysis was preformed for was to offer a duplicate fully featured production environment. It was decided that the gains in security did not justify the expense. At the time this was over a million US dollars. If a solution could be found in the tens of thousands of US dollars this would be approved.

By looking into how other areas of Information Technology are reducing their costs you quite quickly come across references to the use of Virtual Machines running on single hardware platforms. This is especially true in the areas of infrastructure consolidation, rapid deployment and testing.

Why Virtual Machines

Virtual machine software is an application that runs on a physical host under control of the host's operating system. The virtual machine software divides up the host into compartments in which separate operating systems can run in effective isolation.

VMWare products were selected for several reasons including -

- The virtual machine software runs on the common Intel IA-32 architecture.
- Many developers are already familiar with the VMWare workstation products for Microsoft Windows and for Linux clients.
- VMWare provided an extract from the USA's National Security Agency (NSA) Tech Trend Notes on how to use VMWare to provision an environment called NetTop. This environment was designed by the NSA to be able to provision multiple isolated environments and configurations on one hardware package. (VMWare / NSA "Tech Trend Notes - Preview of Tomorrow's Information Technologies Volume: 9 Edition: 4" http://www.vmware.com/pdf/TechTrendNotes.pdf) Having the NSA say they are prepared to use VMWare in certain situations requiring enhanced security was seen as a big help in getting approval.

The ESX product from VMWare was specifically chosen as it is their enterprise class product with advanced options to control what machines, both physical and virtual, can access what resources. The ESX operating

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

system is a customised Linux kernel. The ability to isolate or allocate networks and storage to specific virtual machines and / or the host operating system was also very desirable. More information on the VMWare ESX product can be found at their FAQ page
http://www.vmware.com/products/server/esx_faqs.html

For the rest of this document the term host refers to the hardware and operating system that is acting as the virtual machine host. The term client refers to the virtual machine running its own operating system within the confines of the virtual machine host.

Designing the 'Virtual' environment

The exact network build any company's network is often required to be kept internal at all times so should not appear in a white paper such as this. However, as most will actually be designed using the many established best practices, the network drawn out in figure 1 on page 13 does actually contain many of the important security features required. Figure 1 is in fact the original proof of concept used for justification to move forward with a project to design and build the Virtual Internet Application Development Platform.

The reasons behind the design of the network diagram in Figure 1 on page 13 are –

- A minimum of two firewalls or network devices with access control lists (ACL's) must exist between the external or unprotected network and the internal protected network. The reason behind this is a malicious person or piece of code must defeat two physical devices. The use of the word physical still applies as there is no way to tell from the external network if potential target is running on real hardware or virtual hardware. It is possible and in fact quite desirable to hide the default or standard responses the network gives at the IP network level. This can be done to a greater or lesser extent in the virtual client (or physical for that matter) operating system with network driver configurations.
- The two firewalls will be based on different architectures and preferably be from different manufacturers. This is to reduce the risk of a single vulnerability being exploited allowing a malicious person or piece of code to traverse from the external network to the internal network. This can also reduce the risk of a common fault from interrupting service.
- All firewalls and routers must have the default rule set to drop all applied. Only specific service to specified destinations should be enabled. For example only ports 80(HTTP) and port 443 (SSL) to the Web server.
- All device and client management traffic be encrypted. Secure Shell (SSH) is a commonly used program for providing strongly encrypted authentication data for managing devices. Controlled access to all the virtual clients is also possible via the ESX server console operating system.
- The networks should be compartmentalised or split up into specific functions or application types. This allows for rule creation on the firewalls

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

to restrict what data can flow to what network. This minimises the damage that can be done if a system is compromised.

- Different applications should not reside on the same platform. In the case of a virtual environment this distinction extends to the virtual client due to compartmentalisation within the virtual machine software.
- All devices that are capable of generating logging data should log back to a central logging server. A Syslog server is one of the most common and is the preferred option.
- Network segments should be monitored with Intrusion Detection Systems (IDS) to monitor for unexpected or malicious patterns in network traffic. If security is compromised on a firewall or system an IDS system can detect and raise an alert for action to be taken. Note that to be effective the configuration of IDS is essential to avoid false positive alerts. While many rule sets are available, these systems and the administrator will inevitably have to 'learn' about the network they are monitoring.

Building the host hardware

VMWare ESX server runs on Intel IA-32 architecture systems. While ESX server is very resource efficient, the more resources that you can add the better the performance and the more virtual machine you can realistically run at the same time. The configuration in table 1 is a good starting point.

Part description	Quantity
Dual or Quad processor Intel Pentium P4 system	1
4 Gb system memory	1
SCSI RAID controllers	2
36Gb disk array	1
20Gb disk array	1
200Gb disk array	1
Network Interface cards	1
200Gb capable backup device (Disk or tapes)	1

Table 1

Table 2 describes the configurations to provision all the components listed in the network diagram in Figure 1.

© SANS Institute 2004, Author retains full rights.

System	OS	Memory	Disk
VM Host	ESX Console OS	384Gb	36Gb + 200Gb
FW1	Windows 2003	256Mb	6Gb
FW2	Red Hat Linux	256Mb	6Gb
EXT IDS	Red Hat Linux	256Mb	6Gb + 4Gb
INT IDS	Red Hat Linux	256Mb	6Gb + 4GB
Scanner	Red Hat Linux	256Mb	6Gb
Web	Windows 2003	256Mb	6Gb
SQL	Windows 2003	256Mb	6Gb + 20GB
Logs	Red Hat Linux	256Mb	6Gb + 4Gb
Proxy	Windows 2003	256Mb	6Gb
VPN	Windows 2003	256Mb	6Gb
Win98	Windows 98	128Mb	4Gb
eCom	Windows 2003	256Mb	6Gb
FTP	Windows 2003	256Mb	6Gb
NT4	NT 4 Workstation	128Mb	4Gb
WXP	Windows XP Pro	256Mb	6Gb
Linux	Red Hat Linux	128Mb	4Gb
	Totals	4080Gb	106Gb

Table 2

For more detail on installation, operational and best practice guides you can refer to the VMWare document site http://www.vmware.com/support/esx2/doc/

Providing almost double the minimum disk space required allows the creation of multiple 'versions' or states to be kept for several of the client virtual machines. Most the space required for each client virtual machine is for the machines disk. This disk is stored as a file on the host.

The second SCSI RAID controller only has the smaller 20Gb array connected to it as this will be 'bound' to the virtual machine used by the SQL server providing effectively dedicated hardware.

Building the Virtual Infrastructure

Once the hardware is built and what the ESX product calls the Console Operating System (OS) is installed, it is time to configure ESX to have the correct hardware devices set to the correct operating mode – such as dedicated to the host, clients or shared between host and the clients. Note that one of the network interface cards will become dedicated to the ESX console OS. Table 3 lists how the networks need to be allocated for correct operation.

To provide the SQL database server with its own dedicated storage you have to set the ESX configuration to not share the second SCSI RAID controller.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Name	Host	Host / NIC	Address	Mask
External Net	vmnet_2	Host	192.168.2.0	/255
Ext App Net	vmnet_3	Host	192.168.4.0	/254
Out Net	vmnet_4	Host	192.168.6.0	/255
Trans Net	vmnet_5	Host	192.168.7.0	/255
Int App Net	vmnet_6	Host	192.168.8.0	/254
DB Net	vmnet_7	Host	192.168.10.0	/255
Intra Net	vmnic2	NIC	192.168.11.0	/255

Table 3

As the design includes IDS systems and network scanner systems, the virtual network interface cards (NIC) will need to be set to promiscuous mode. This is where the card processes all the network traffic it can see whether or not it is actually bound for it. You have to turn promiscuous mode on for the required NIC within the console OS. The command is -

echo "PromiscuousAllowed yes" > /proc/vmware/net/vmnic0/config

You then have to disable promiscuous mode for the MAC address of each system with that NIC that must not use promiscuous mode. The command is -

echo "PromiscuousAllowed no" > /proc/vmware/net/vmnic0/<MACAddress>

The <MAC address> is of the format 00:05:69:XX:YY:ZZ Identifying the MAC address for a particular virtual client easiest once the client operating systems are built.

Once all the virtual devices are prepared, all of the virtual machines can be configured to the details set out in tables 2 and 3 and the network diagram in figure 1. Too greatly speed up the operating system build process, take an ISO image of the operating system CD and copy it onto the ESX server console operating system file system. A useful tool for creating ISO Images is UltraISO from EZB Systems (http://www.ezbsystems.com/ultraiso/index.html). The virtual hardware configuration tool lets you point the virtual clients CD / DVD drive to either the actual physical CD / DVD drive or an ISO image.

When you start building the operating system onto the virtual clients you will need to ensure you have valid licences for each operating system installed. These are still real PC's and operating systems – only the hardware is virtual! The same license requirement applies to any applications you install onto the virtual clients. As this really is a development environment, subscribing to the Microsoft MSDN subscriptions services (http://msdn.microsoft.com/) provides a very cost effective software licence option.

To assist with the build and configuration stage of the operating system an extra NIC was added to the virtual configuration so that all the latest updates

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

could be downloaded. Once built this NIC was removed from the virtual client configuration.

The order of building the virtual clients is not too important but starting with the two firewalls and linking up the networks is a good first step followed by the Logs server, Nessus scanner and IDS boxes. The basic infrastructure is in place when these are built and configured. Table 4 lists the major applications used in the building of the network on Figure 1. Where the application is prefixed with MS this refers to Microsoft products.

System	Application	Function	Link
VM Host	VMWare ESX 2.0.0	Virtual Machine Host	Link
FW1	MS ISA Server 2000	Firewall	Link
FW2	Firewall Builder 1.1.1	Firewall	Link
EXT IDS	Snort 2.0.5	IDS	Link
INT IDS	Snort 2.0.5	IDS	Link
Scanner	Nessus 2.0.9	Vulnerability Scanner	Link
Web	MS IIS 6	Web server	Link
SQL	MS SQL Server 2000	Database server	Link
Logs	Simple Event Correlator	SysLog analysis	Link
Proxy	MS ISA Server 2000	Web Proxy server	Link
VPN	MS Routing and Remote Access MS ISA Server 2000	Remote connectivity Firewall	Link Link
FTP	MS IIS 6	FTP server	Link

Table 4

Provisioning the environment

Once the environment was built basic testing was carried out to ensure all components worked as required. A rule set was added to both FW1 and FW2 to match rules in the production environment. All of the virtual clients were scanned to make sure the builds had completed correctly. Extensive documentation about the build and configuration of the environment was created and another test was performed just to make sure the documentation matched the actual environment.

When all the tests completed satisfactorily a full backup of the virtual machine host was taken. This backup became the ‘Master Image’ for the development and test environment.

A document set was created and posted on an access controlled web site for use by the company’s authorised developers. The set included not only information on the environment but also the company policies on required coding practices and security community best practices on coding practices such as guide from The Open Web Application Security Project “A Guide to Building Secure Web Applications V1.1.1” (Sept 2002)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

(http://www.owasp.org/documentation/guide) and pointers to sites detailing the current top vulnerabilities such as the SANS Institute Top 20 Vulnerabilities site (http://www.sans.org/top20/)

Now the development groups had not only the environment but also the documentation needed to be able to develop applications securely and in a way that matched the company's policies and procedures.

Then when you need to provide a consistent development and test environment to a development group all you need is –

- the list of hardware equipment to order (Table 1)
- the pointer to the document store
- the Master Image
- Financial justification – the environment is still not free.

The use of the development and test environment was added as required steps in the Release to Production process and the Change Management process for Internet applications and services.

Maintaining the environment

To ensure that the development and test environment kept up to date with the ever changing security requirements a version control and tracking system was established for the components within the environment and the environment Master Image. The Release to Production process and the Change Management process require that the application be developed to particular versions of the development and test environment.

Summary

Operating a commercial Internet environment requires you to maintain a high awareness of the risks you can exposed to. The network, system and application components must be designed and operated in a coordinated and security aware way. However the adding of many security features is a very expensive requirement. Careful cost benefit analysis must be performed with the company's own businesses to ensure that what you are spending on protection does not exceed the value of what you are protecting. Too much protection wastes the company's money and too little exposes the company to the risk of unacceptable loss.

By using virtual machine technology to reduce the cost of providing enhanced security to the company you are helping to reduce the exposed attack surface and providing a better return on security investment.

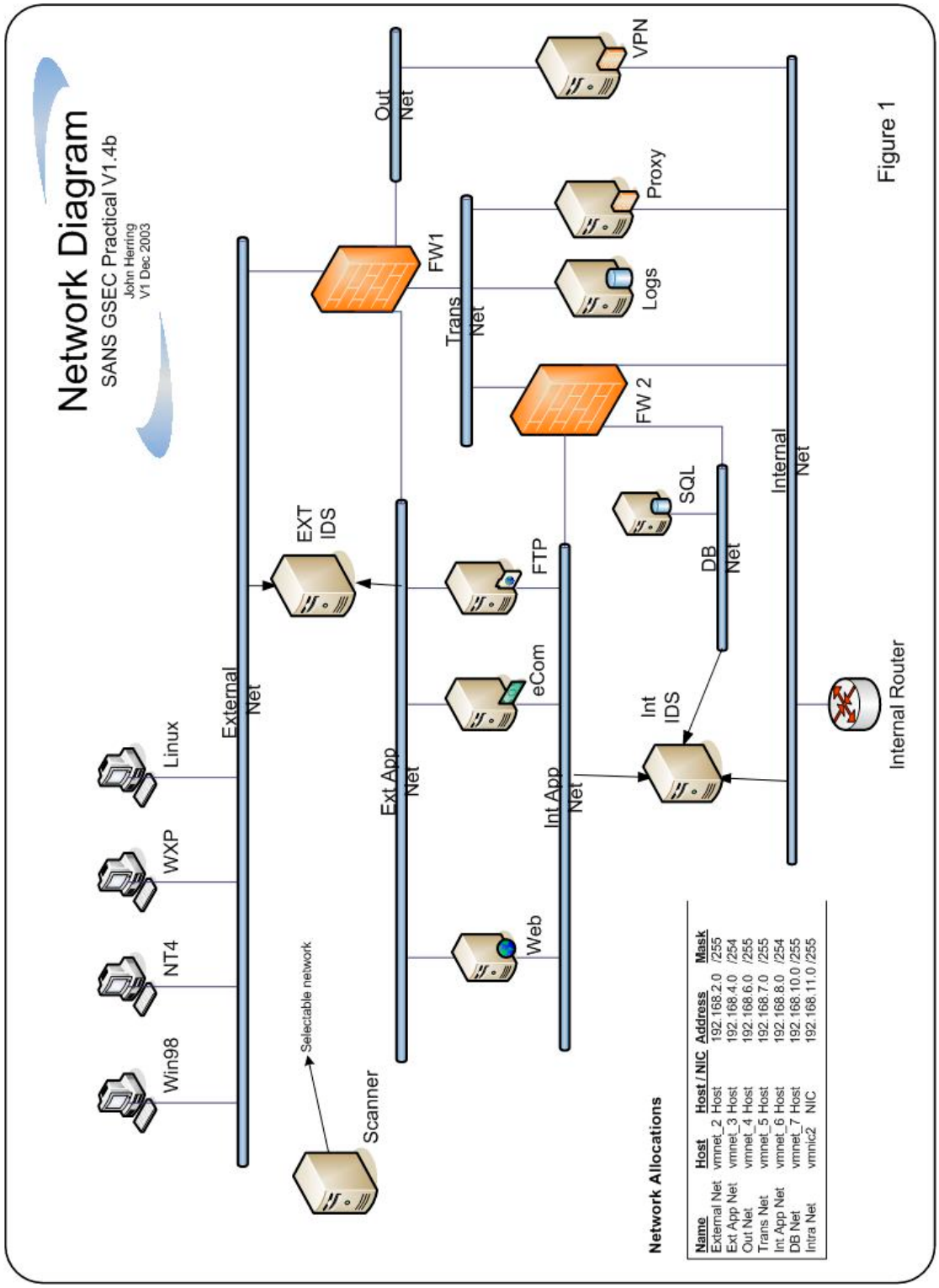
The public Internet and for that matter the companies internal network can, and probably will, expose web applications to a myriad of possible attacks to an ever mounting list of vulnerabilities. If application development does not take action to prevent the well established vulnerabilities for being exploited

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

then the problems will not go away. Remember that if an application designer has access to common vulnerabilities and details on the best working practices to secure web applications and service so does the hacker and criminal community and you can be sure they will test every possible attack surface possible even if the developer or security group does not.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References

The SANS Institute webinar “Is your Web App Secure? How Do You Know?” featuring Ed Skoudis (http://www.sans.org/webcasts/show.php?webcastid=90425) (7 Dec 2003)

James Middleton, VUNET “Application security 'in a grim state' “(Feb 2002) URL: http://www.vnunet.com/News/1129340 (7 Dec 2003)

Paladion “F.A.Q.'s on Application Security Assessment” URL: http://www.paladion.net/services/web_application_security.htm (7 Dec 2003)

The Open Web Application Security Project “A Guide to Building Secure Web Applications V1.1.1” (Sept 2002) URL: http://www.owasp.org/documentation/guide (7 Dec 2003)

Visa USA “Visa Cardholder Security Program” URL: http://usa.visa.com/business/merchants/cisp_tech.html (7 Dec 2003)

VMWare / NSA “Tech Trend Notes - Preview of Tomorrow’s Information Technologies Volume: 9 Edition: 4” (Fall 2000) http://www.vmware.com/pdf/TechTrendNotes.pdf (7 Dec 2003)

VMWare ESX server Version 2 FAQ URL: http://www.vmware.com/products/server/esx_faqs.html (7 Dec 2003)

VMWare ESX server documentation URL: http://www.vmware.com/support/esx2/doc/ (7 Dec 2003)

Microsoft MSDN Subscriptions Service URL: http://msdn.microsoft.com/ (7 Dec 2003)

SANS Institute - The Twenty Most Critical Internet Security Vulnerabilities ~ The Experts Consensus URL: http://www.sans.org/top20/ (7 Dec 2003)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Product References

VMWare ESX Server 2.0
URL: http://www.vmware.com/products/server/esx_features.html (7 Dec 2003)

Microsoft Windows Operating Systems
URL: http://www.microsoft.com/windows/default.mspx (7 Dec 2003)

Red Hat Operating systems
URL: http://www.redhat.com/ (7 Dec 2003)

Microsoft ISA Server
URL: http://www.microsoft.com/ISAServer/ (7 Dec 2003)

Microsoft Internet Information Service (IIS)
URL: http://www.microsoft.com/WindowsServer2003/iis/default.mspx
(7 Dec 2003)

Microsoft Internet Information Server
URL: http://www.microsoft.com/WindowsServer2003/iis/default.mspx
(7 Dec 2003)

Microsoft SQL Server 2000
URL: http://www.microsoft.com/sql/ (7 Dec 2003)

Microsoft Routing and Remote Access (VPN)
URL:
http://www.microsoft.com/windowsserver2003/technologies/networking/vpn/default.mspx (7 Dec 2003)

Firewall Builder
URL: http://www.fwbuilder.org/ (7 Dec 2003)

Nessus Vulnerability Scanner
URL: http://www.nessus.org (7 Dec 2003)

Snort Intrusion Detection
URL: http://www.snort.org (7 Dec 2003)

Simple Event Correlator
URL: http://sourceforge.net/projects/simple-evcorr/ (7 Dec 2003)

EZB Systems UltraISO CD Image Editor
URL: http://www.ezbsystems.com/ultraiso/index.html (7 Dec 2003)

© SANS Institute 2004, Author retains full rights.