Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Network Security Model

The proposed Network Security Model (NSM) is a seven layer model that divides the daunting task of securing a network infrastructure into seven manageable sections. The model is generic and can apply to all security implementation and devices. The development of the NSM is important because unity is needed in securing networks, just as unity was needed in the architecture of networks with the development of the OSI model. When an attack on a network has succeeded it is much easier to locate the underlying issue and fix...

Copyright SANS Institute
Author Retains Full Rights

AD

Network Security Model

The definition of a Network Security model

Author: Joshua Backfield

Advisor: John Bambenek

© SANS Institute 2008, Author retains full rights.

© SANS Institute 2008, Author retains full rights.

Table of Contents

1.1 Introduction to the Network Security Model (NSM) 4
1.2 Why do we need a Network Security Model? 5

2. UNDERSTANDING THE NSM SEVEN LAYER MODEL: THE PHYSICAL LAYER 6

2.1 What is the Physical Layer? 6
2.2 Elements of the Physical Layer 7

3. UNDERSTANDING THE NSM SEVEN LAYER MODEL: THE VLAN LAYER 8

3.1 What is the VLAN Layer? 8
3.2 Implementing VLAN Security 8
3.3 Why is the VLAN Layer Important to Security 9

4. UNDERSTANDING THE NSM SEVEN LAYER MODEL: THE ACL LAYER 10

4.1 What is the ACL Layer? 10
4.2 Implementing ACL Security 10
4.3 Why is the ACL Layer Important to Security 11

5. UNDERSTANDING THE NSM SEVEN LAYER MODEL: THE SOFTWARE LAYER 12

5.1 What is the Software Layer? 12
5.2 Implementing Software Security 12
5.3 Why is the Software Layer Important to Security 13

6. UNDERSTANDING THE NSM SEVEN LAYER MODEL: THE USER LAYER 13

6.1 What is the User Layer? 13
6.2 Implementing User Security 14
6.3 Why is the User Layer Important to Security 14

7. UNDERSTANDING THE NSM SEVEN LAYER MODEL: THE ADMINISTRATIVE LAYER 15

7.1 What is the Administrative Layer? 15
7.2 Implementing Administrative Security 15
7.3 Why is the Administrative Layer Important to Security 15

***8.* UNDERSTANDING THE NSM SEVEN LAYER MODEL: THE IT DEPARTMENT LAYER 16**

8.1 What is the IT Department Layer? 16
8.2 Implementing IT Department Security 16
8.3 Why is the IT Department Layer Important to Security 17

9. WORKING WITH THE NETWORK SECURITY MODEL 17

9.1 The Layout of the Network Security Model and it's Similarities to the OSI Model 18
9.2 Examples of the Network Security Model and attacks 20

© SANS Institute 2008, Author retains full rights.

9.2.1 Physical Attack *20*
9.2.2 VLAN Attack *20*
9.2.3 ACL Attack *21*
9.2.4 Software Attack *21*
9.2.5 User and Administrative Attack *21*
9.2.6 IT Department Attack *22*
9.3 How the Network Security Model can be used to mitigate an attack 22
9.3.1 Initial Mitigation *23*
9.3.2 Long-Term Mitigation *23*
9.4 How to implement the Network Security Model 24
9.4.1 Introduction to implementing the NSM *24*
9.4.2 Implementing the NSM, an in-depth look *25*

10. NETWORK SECURITY LIFE-CYCLE 26

11. CONCLUSION 28

11.1 Missing IDS/IPS Layer? 28

GLOSSARY 30

© SANS Institute 2008, Author retains full rights.

Introduction

1.1 Introduction to the Network Security Model (NSM)

The Open Systems Interconnection model (OSI), developed in 1983 by the International Organization for Standardization (ISO), has been used as a framework to teach networking basics and troubleshoot networking issues for the last 25 years. It has been so influential in network development and architecture that even most of the network communication protocols in use today have a structure that is based on it. But just as the OSI model never fails us, we find that we are lacking a standard that all network security professionals can adhere to, a Network Security Model (NSM). Today's sophisticated and complex networks provide the fundamental need for the NSM.

The proposed Network Security Model (NSM) is a seven layer model that divides the daunting task of securing a network infrastructure into seven manageable sections. The model is generic and can apply to all security implementation and devices. The development of the NSM is important because unity is needed in securing networks, just as unity was needed in the architecture of networks with the development of the OSI model. When an attack on a network has succeeded it is much easier to locate the underlying issue and fix it with the use of the NSM.

The NSM will provide a way to teach and implement basic network security measures and devices as well as locate underlying issues that may have allowed an attack to succeed. Traditionally we work from the bottom up to determine which layer has failed on the OSI model, but on the NSM we will work from the top down to determine which layer has failed. *See the NSM (Figure 1.1)*. Once the layer of failure is found, we can determine that all of the layers above this layer have also failed. A network security professional will be able

© SANS Institute 2008, Author retains full rights.

to quickly determine if other possible hosts have been compromised with the breech of the layer and how to secure it against the same attack in the future.

Throughout the paper we will be working from the top down describing what each layer is and how the layers of the NSM work together to accomplish complete network security.

1) Physical
2) VLAN
3) ACL
4) Software
5) User
6) Administrative
7) IT Department

Figure 1.1 – The Network Security Model

1.2 Why do we need a Network Security Model?

A well structured NSM will give the security community a way to study, implement, and maintain network security that can be applied to any network. In study, it can be used as a tool to breakdown network security into seven simple layers with a logical process. Traditional books have always presented network security in an unorganized fashion where some books cover issues that other books may completely neglect. In implementation, it can be used by network architects to insure that they are not missing any important security details while designing a network. In maintaining existing networks it can be used to develop maintenance schedules and life-cycles for the security of the existing network. It can also be used

© SANS Institute 2008, Author retains full rights.

to detect where breaches have occurred so that an attack can be mitigated.

The NSM is beneficial to all types of professionals. Let us not forget professionals who are transitioning into positions previously held by other network security professionals. Currently, learning what security techniques are implemented on a network and which ones have not can be a daunting task when the basic security structure of the network is unclear. The NSM provides that basic structure. It provides the new professional with the knowledge to discover what has been implemented and what has not been implemented from a security standpoint. Without an NSM, the network security community faces potential chaos as professionals continue to implement their own versions of secure networks without adequate structure.

2. Understanding the NSM Seven Layer Model: The Physical Layer

2.1 What is the Physical Layer?

The physical layer's primary focus is on physical security. Physical security is applied to prevent attackers from accessing a facility to gain data stored on servers, computers, or other mediums. Physical security is the first chosen layer because it is a breaking point for any network. In any scenario providing other devices, such as firewalls, will not help your security if the physical layer is attacked. For this reason we can say that if the layers below the physical layer fail the physical layer has failed as well because the attacker would be able to manipulate data as if they had breached the facility. Physical security comes in many forms including site design, access control devices, alarms, or cameras.

© SANS Institute 2008, Author retains full rights.

The physical layer is one of the easiest layers to secure because it does not require advanced technical concepts to do so. A company can be hired to install an alarm system, or an employee can be hired to stand as a security guard. We will explore the devices that the physical layer can contain in the next section.

2.2 Elements of the Physical Layer

The first form of physical security consists of site design. Site design includes features that are placed on the land around the exterior of the building. Some of these devices include fencing, barbed wire, warning signs, metal or concrete barriers, and flood lights. These forms of security are not always practical unless the facility contains highly sensitive data.

The second form of physical security consists of access control devices. Access control devices include gates, doors, and locks that are either mechanical or electronic. Locks may seem archaic but they are actually the most cost effective way to increase security. Locked doors should be placed before all areas which can either contain hosts or potentially contain hosts.

The third form of physical security is an alarm. Alarms are one of the most important features to include in the physical network security. This will provide an immediate signal that can alert the CIO or network security administrator as well as the local law enforcement that someone has entered an area that should not have been accessed.

The fourth and final form of physical security is a camera. If someone breaking in sees a camera, they are usually deterred because being caught on camera makes them easy to identify and prosecute by the police. It is the best way to determine how, where, and when

© SANS Institute 2008, Author retains full rights.

physical access was obtained. This can be useful in determining what course of action should be taken in order to mitigate an attack. How many cameras are placed in an area should be determined by the security of that area and the cost. An important area that should always have a camera is the server room.

Hiring a security guard is the only form of physical security that can be considered both an access control and monitoring measure. Security guards can warn of suspicious activity around the building or grant employees and announced visitors' access to the building. Although having a security guard on site is one of the best security measures the expense is usually too high for smaller companies.

3. Understanding the NSM Seven Layer Model: The VLAN Layer

3.1 What is the VLAN Layer?

The VLAN layer deals with the creation and maintenance of Virtual Local Area Networks. VLANs are used to segment networks for multiple reasons. The primary reason that you make VLANs is to group together common hosts for security purposes. For example, putting an accounting department on a separate VLAN from the marketing department is a smart decision because they should not share the same data. This breaks the network up into less secure and more secure areas. In the next section we will be discussing the implementation of VLANs.

3.2 Implementing VLAN Security

The first step in implementing VLANs is to determine public and

© SANS Institute 2008, Author retains full rights.

private networks. Any external facing devices should be put on public VLANs. Examples of this include web servers, external FTP servers, and external DNS servers. The next step is to place internal devices on private VLANs which can be broken up into internal user VLANs and internal server VLANs. The final step is to break down the internal user and server VLANs by department, and data grouping respectively.

3.3 Why is the VLAN Layer Important to Security

VLANs are an essential layer to the NSM because a network without segmentation contains a cluster of servers and devices without any clear organization. VLANs are used to implement access control lists in order to protect data from users that do not need access to it. Although VLANs can be implemented independently of ACLs, it is important to note that they also go hand in hand. One will usually add ACLs to a VLAN to restrict, or grant, access to/from that segment. The main reason that these two layers exist independently of each other is because VLANs should be able to change without changing the ACLs that go along with them. This is the same in the reverse as well.

VLANs are also a great way to find an exploited host. By seeing increased traffic coming from a specific VLAN, a network security professional will be able to narrow the scope of that VLAN in order to find which port the infection is possibly coming from and finally which host the infection is coming from.

© SANS Institute 2008, Author retains full rights.

4. Understanding the NSM Seven Layer Model: The ACL Layer

4.1 What is the ACL Layer?

The ACL layer is focused on the creation and maintenance of Access Control Lists. ACLs are written on both routers and firewalls. ACLs are created to allow and deny access between hosts on different networks, usually between VLANs. This makes them absolutely indispensable in the area of network security. By setting up strong access control lists, a network security professional can stop many attacks before they begin. Setting up ACLs can seem a very daunting task. There are many things to take into consideration such as return traffic or everyday traffic that is vital to operations. These are the most important ACLs that a network security professional creates. If they are not created properly, the ACL may allow unauthorized traffic, but deny authorized traffic.

4.2 Implementing ACL Security

The key to creating strong ACLs is to focus on both inbound (ingress) ACLs as well as outbound (egress) ACLs. Small companies can get by with creating very few ACLs such as allowing inbound traffic on port 80 and 443 for HTTP and HTTPS servers. They will also have to allow basic web activity outbound on ports 80, 443, and 53 for HTTP, HTTPS, and DNS respectively. Many other medium to large companies need services like VPN open for partner/vendor companies, and remote users. This can be a difficult task to implement and still maintain a level of security.

Most network security professionals focus on writing ACLs which

© SANS Institute 2008, Author retains full rights.

deny access into the company network from the internet and out of the internal network. The problem is that both of these examples are ingress ACLs. Many network security professionals do not focus on egress ACLs. Security professionals should also be focusing on writing these types of ACLs which are applied to traffic outbound to the internet as well as outbound to the internal network. For example, a Domain Controller which should be allowed port 445, 135, and 139 access to the internal network, but not to the internet on those ports should have an allow ACL for those ports on the internal ingress ACL. However, a deny should exist on the external egress ACL for those ports from that host.

A network security professional should know what ports should be allowed out of the network as well as what ports should be allowed into the network. This includes both source and destination ports. For example, network security professionals should know that ephemeral ports, ports greater than 1023, are the only source ports going into the DMZ from the internet with destination ports that are equivalent to services that are hosted in the DMZ. Likewise, only activity where the source ports are equivalent to the services running in the DMZ going outbound towards the internet with destination ports in the ephemeral range should be allowed.

4.3 Why is the ACL Layer Important to Security

ACLs are an important part of the NSM because they have the ability to allow and deny traffic for services that should and should not be seen by other networks. ACLs also protect the software layer by blocking access to services that have known vulnerabilities from networks which should not have accessing to the services. This means granting access to a Domain Controller internally to devices which need to access that specific DC; but, denying access to the Domain Controller to the internet as well as any other devices which should

© SANS Institute 2008, Author retains full rights.

not need to access that specific DC. When an attack has occurred, ACLs can be used to pinpoint a compromised host and mitigate the damage that may be caused by that host.

5. Understanding the NSM Seven Layer Model: The Software Layer

5.1 What is the Software Layer?

The software layer is focused on keeping software up to date with upgrades and patches in order to mitigate software vulnerabilities. Network security professionals should know what software is running on their hosts and what patch level they are currently running at to ensure that if something has happened that they can remove any unwanted software accordingly and know what vulnerabilities currently exist or have existed recently. They should also know what each new patch will do to the system it will be installed on.

5.2 Implementing Software Security

Implementing software security includes applying the most current patches and upgrades. This reduces the amount of exploits and vulnerabilities on a specific host and application. Server side software such as HTTP and HTTPS are extremely important internet facing services to keep up to date. User side software should also be kept up to date in order to protect against client-side attacks. In an example, we see a server running a web hosting application. The network security professional must keep the web server application updated to ensure that any new vulnerabilities that are found are mitigated as quickly as possible because the application is accessible at all times.

© SANS Institute 2008, Author retains full rights.

Knowing what services should be running on a host is a vital part of the software layer. If a network security professional knows that services are supposed to be running on a host and sees traffic that is anomalous to those services, they will know that something has changed and the host should be treated as if it were compromised.

5.3 Why is the Software Layer Important to Security

The software layer is an important layer on the NSM because if the software layer is compromised then an attacker can potentially get anything on that host. This is the first layer in which an attacker has gained an actual account on the network. The software layer also helps protect the user layer. If a host is patched and configured correctly, a user layer attack like a malicious pop-up will no longer be effective. The patched/configured software should disable the malicious pop-up saving the user layer.

6. Understanding the NSM Seven Layer Model: The User Layer

6.1 What is the User Layer?

The user layer focuses on the user's training and knowledge of security on the network. The user should understand basic concepts in network security. They should also learn what applications should not be run or installed on their system; likewise they should have an idea of how their system runs normally. We will cover how their knowledge of network security can assist the network security professional in determining if there is an issue on the network and if so, what that issue possibly is.

© SANS Institute 2008, Author retains full rights.

6.2 Implementing User Security

The most basic way to implement user security is to train the users on what applications should be avoided and how their computer should run normally. Applications such as Peer-to-Peer can be the difference between an infection and a clean host. As most network security professionals know many types of malware can come pre-installed into Peer-to-Peer clients. However, even more malware can be included in the files and/or applications that are downloaded through the client. Training users with this kind of knowledge can prevent them from potentially compromising a host.

Training users on how their system works is important because if they know how their system functions they will be able to detect a problem. For example, if one day their system response time has slowed down the user should notice this activity and alert the network security professional. The network security professional should then check with the user to find out what has changed in order to determine if the host has become compromised or if hardware in the system has become unstable.

6.3 Why is the User Layer Important to Security

The user layer is important to the NSM because if the user layers get compromised a user account is most likely also compromised. This can be devastating because it will give the attacker credentials to access an account on the domain and thus log into the system and see data that may not have been readily available to them before. The user layer is listed first because once the administrative layer has been breached it is not important that the user layer is still secure. Most attackers will attack the user layer before the

© SANS Institute 2008, Author retains full rights.

administrative layer because the people are the least knowledgeable about network security.

7. Understanding the NSM Seven Layer Model: The Administrative Layer

7.1 What is the Administrative Layer?

The administrative layer focuses on the training of administrative users. The administrative layer includes all members of management. It is much like the user layer except dealing with a higher level of secure data on the network. Like the user layer, administrative users should be trained on what applications should not be installed on their systems and have an understanding of how their systems run normally. They should also be trained to identify problems with the user layer. Such as recognizing an employee that installs Peer-to-Peer against security policy.

7.2 Implementing Administrative Security

Administrators should be trained the same way users are trained but with more in-depth knowledge and skill. It is important that administrators can teach a new employees security practices. Administrators should be able to effectively communicate a user's needs or problems to the network security professional. This ensures that issues are being resolved as quickly as possible, and that the network security professional is not overloaded with being 'big brother' so to speak of users.

7.3 Why is the Administrative Layer Important to Security

© SANS Institute 2008, Author retains full rights.

The administrative layer is important to the NSM because if the administrative layer is compromised an administrative account is likely also compromised. This can be devastating because it will give the attacker credentials to access and modify sensitive and secure data. The administrative layer is listed above the IT department layer because once the IT department layer has been breached it is not important that the administrative layer is still secure. Most attackers will target the administrative layer before the IT department layer because the IT department layer contains users most likely to identify the attack.

8. Understanding the NSM Seven Layer Model: The IT Department Layer

8.1 What is the IT Department Layer?

The IT department layer contains all of the network security professionals, network technicians, architects, and support specialists. These are all of the people that make a network operational, and maintain the network, and all of the hosts that reside on that network. The IT department layer is like the administrative layer except the IT department has accounts to access any device on the network. For example, an IT department user can have read, write, and modify access to a database table structure, where an administrator or user only has read, write, and modify access to the records within that table structure.

8.2 Implementing IT Department Security

Each person in the IT department layer should have some type of

© SANS Institute 2008, Author retains full rights.

background in network security. The network structure and security policy should be well defined to users in the IT department layer. Minimal training may be necessary for a new employee to learn the structure and design of the network. The IT department is responsible for the implementation and maintenance of all network layers including the physical layer, VLAN layer, ACL layer, software layer, user layer, and the administrative layer. The IT Department should also know as much as it can about its users requests and needs.

8.3 Why is the IT Department Layer Important to Security

The IT department layer is important to the NSM because if the IT layer fails the attacker will have system level access to all devices on the network. Devices such as routers, firewalls, proxies, and VPN devices with become vulnerable. This can be devastating because it will give the attacker the ability to completely paralyze and disable a network. It can also cause massive financial loss to a company because client trust has been affected. An example of a devastating IT department layer attack would be using a drop table command to completely destroy records and information.

9. Working with the Network Security Model

In this section, we will be examining how to effectively work with the network security model. This will cover the layout of the NSM as well as how attacks against a network can be profiled with the use of the model. We will also discuss how the model can be used to mitigate attacks that have already happened. Finally we will look at how to implement the NSM on a new network.

© SANS Institute 2008, Author retains full rights.

9.1 The Layout of the Network Security Model and it's Similarities to the OSI Model

Each layer of the NSM is built upon the layer below it, much like the OSI model, if one layer fails all layers above it will fail as well. We will look at the NSM versus an inverted OSI model as shown in *Figure 9.1* to show how each model relates and differs.

Network Security Model (NSM)	OSI Model (inverted)
Physical	Physical
VLAN	Data Link
ACL	Network
Software	Transport
User	Session
Administrative	Presentation
IT Department	Application

Figure 9.1 – Network Security Model (NSM) vs. OSI Model (inverted)

The first layer is the physical layer from the NSM and the physical layer from the OSI model. Both work with the physical aspects of the network. The physical layer from the NSM deals with physical securities where the physical layer from the OSI deals with physical network connections. Both layers are very self explanatory and very easy to deal with.

The second layer is the VLAN layer from the NSM and the data link layer from the OSI model. Both work similarly by dealing with MAC addressing and VLANs. The VLAN layer from the NSM deals with VLAN segmentation. This splits LAN's across switches and segments based on the data link layer from the OSI model which covers MAC addressing.

© SANS Institute 2008, Author retains full rights.

The third layer is the ACL layer from the NSM and the network layer from the OSI model. Both work similarly by dealing with IP addressing and LAN's. The ACL layer from the NSM deals with ACL implementation which is used to allow or deny access based on the network layer from the OSI model which covers IP addressing.

The fourth layer is the software layer from the NSM and the transport layer from the OSI model. Both deal with the actual connection on the network from host to host. The Software layer from the NSM deals with the software and the patches that allow the software to not be exploited while the Transport layer from the OSI model describes the connection between the both ends of the software connection.

The fifth layer is the user layer from the NSM and the session layer from the OSI model. Both deal directly with the local host where the user layer from the NSM deals directly with the user who is able to utilize that local machine. The Session layer from the OSI model deals directly with communication on that local machine.

The sixth layer is the administrative layer from the NSM and the presentation layer from the OSI model. Both deal with administrative functions. The administrative layer deals with the administrative users who have the ability to direct users and the presentation layer deals with how the data is directed.

The seventh and final layer is the IT department layer from the NSM and the application layer from the OSI model. The IT department layer deals directly with the maintenance of all layers and making sure that the entire network works correctly from NSM model and all layers of the OSI model. The Application layer from the OSI model deals with the actual display of the data.

© SANS Institute 2008, Author retains full rights.

9.2 Examples of the Network Security Model and attacks

We will now look at some examples of attacks against a network and how the layers work by example.

9.2.1 Physical Attack

First we will look at a physical break-in. In this example an attacker breaks in through a locked door after everyone has gone home for the evening. No other physical security measures are in place. The hacker gains physical access to the network by using a laptop plugged into a network jack. He can scan the local area network for servers and gain access to data. In this scenario other physical measures should have been used to deter the attacker from getting physical access. Your physical layer has failed. A camera needs to be added, possibly a security guard, or even an alarm system.

9.2.2 VLAN Attack

Second we look at a VLAN attack. Let us assume that the attacker has exploited the physical layer and has a laptop plugged into the network that is scanning for machines vulnerable to the MS03-026 exploit[1]. Since the attacker has a machine on the local network he or she will attempt to exploit devices on the subnet that he or she currently resides on. The attacker will only attempt to infect the local subnet because scanning other subnets may make the attacker more visible and may take extended time. If the servers are not segmented from the local network with the use of VLANs the attacker has a direct way to scan the server. Correct VLANs will force the

[1] http://www.microsoft.com/technet/security/bulletin/MS03-026.mspx

© SANS Institute 2008, Author retains full rights.

attacker to scan multiple networks. Once the VLAN layer has failed, we know that the physical layer has failed as well.

9.2.3 ACL Attack

Third we look at an ACL attack. A network administrator configures ACLs on a device inbound from the internet to a web server that also contains a MSSQL database of people visiting the website. The attacker knows that the web server exists and scans the IP address for open ports. The ACLs have not been setup properly so the attacker is actually scanning the entire box. Proper ACLs, like only allowing port 80 activity to the web server would have prevented this ACL layer failure. It no longer matters that the web server is on a different network (through the use of VLANs) because the attacker has full access to the box.

9.2.4 Software Attack

Fourth we look at a software attack. The attacker attempts to exploit a web server that they know is running Apache. They attempt to run an /etc/passwd retrieval attack on the web server. Because the Apache software has not been patched the attacker is successful in downloading the password file. The attacker uses this password file to log in to web server. Patching software properly could have prevented this attack. ACLs could not have prevented this attack because the attacker was successful through port 80 that was allowed.

9.2.5 User and Administrative Attack

Fifth we look at a user and administrative attack. Because education of the users and administrators is the primary foundation

© SANS Institute 2008, Author retains full rights.

of these layers we can put these attacks together. The attacker spoofs an email from the IT department stating that a user's password has been lost and needs to be changed to 'blah'. Because of lack of education, the user believes the email and changes their password to 'blah' right away. This gives the attacker a working accessible account on the network that they can use to login remotely. Patching software properly could not have prevented this attack because this was a user error.

9.2.6 IT Department Attack

The sixth and final attack is the IT department attack. An attacker mails a CD with database of records supposedly from 'client X'. The network administrator uploads the records to the database without noticing that a root kit runs automatically in the background. The root kit eventually gives the network administrators username and password to the attacker through some source. The attacker has a network username and password that they know is a high level administrator account. The attacker can now access more devices, servers, and services than a normal user on the network. Now than an IT account has been breached the attacker does not need a user or administrator account, they have an account that is much more powerful.

9.3 How the Network Security Model can be used to mitigate an attack

In this section we will be looking at how the Network Security Model can be used to mitigate an attack that has already happened. We will be looking into a specific example, however, the concept remains the same and only the starting layer changes. The exploit we will be looking at is the MS03-026 exploit which is at the software layer;

© SANS Institute 2008, Author retains full rights.

this specific exploit allows remote access to a Windows device through vulnerability in a specific Windows port/service. Since the attack is directed at the software layer, this is the layer that has been compromised. We will need to go through the layers from the top to the bottom to mitigate the attack.

9.3.1 Initial Mitigation

We start with the physical layer by removing the infected host and determining what malware is running on the system by running root kit detectors as well as checking anti-virus software. We also look to see if there was a physical break-in to see if the attacker may have infected any other hosts at the same time. Once this process has been completed we should look at the specific VLAN the host resided on. Here we also look for other hosts that could be infected. We will mitigate these hosts the same as the original host, each host that is possibly compromised should be isolated from the network and scanned for possible malware. Next we should look at the ACLs used on the router/firewall to see if this host could have infected any other networks. If the ACLs do not block this activity to other VLANs, those VLANs should be investigated to see which hosts, if any, are infected.

9.3.2 Long-Term Mitigation

Now we begin looking into long-term mitigation, this means that we should be looking at what failed and what should be fixed so the issue does not happen again. Since the Software layer was the actual layer which failed; we will start by looking into this layer. Was an update available which could have prevented this attack? If so, we should attempt to push out the update in order to mitigate this type of attack from happening again. We should make sure all machines are updated with the most current patches. Next we should be looking

© SANS Institute 2008, Author retains full rights.

into the ACL layer to see if an ACL could have prevented this attack. If so, we should put this ACL in to make sure that any other attempts on other hosts which may not be patched yet do not occur. Next we will look at the VLAN layer to see if something should be changed in the VLANs which can prevent a network wide outbreak. This would also include checking to see if VLANs could have protected servers from the attack. All VLANs should be re-evaluated and reconfigured. Finally, the physical security should be checked; did this the host get compromised by a physical break-in? If so, how can this be prevented in the future.

9.4 How to implement the Network Security Model

9.4.1 Introduction to implementing the NSM

Implementing the NSM should be a consistent strategy. This means that all layers should be implemented as soon as possible and no layer should get more focus than another. The idea is that a basic level of security should be implemented for each layer of the NSM. After the basic level; all the layers should consistently be increased in security by developing a Network Security Life-Cycle which will be discussed later. Basic ACLs should be expanded to include newer ACLs which will be more specific to the company as well as VLANs which will eventually include the perfect amount of host usage. Physical security should be increased to match the security needed for future attack attempts. For example, new locks can be put in place which can include upgrading from basic locks to ID Badges that have RFID’s in them to go with accountability as well as actual authentication for the person entering the restricted area.

© SANS Institute 2008, Author retains full rights.

9.4.2 Implementing the NSM, an in-depth look

The first step is to implement all layers at a basic level. First, the IT department, Administrative department, and all users should begin learning and reading literature about network security. This should be fairly non-technical for the people outside of the IT department and more technical for the IT department itself. Second, all software should be checked and upgraded so it is up to date at its most current update/patch level. Third, in the ACL layer, the network security professional should check to see if ACLs are currently being used. If they are implemented they should be evaluated to discover any potential needs or discrepancy. If there are no ACLs, the network security professional should begin creating generalized ACLs. Fourth, in the VLAN layer, the network security professional should check to see if VLANs are currently being used and if they are where they are implemented as well as where they are not and if the VLANs are actually useful. At this point, if there are no VLANs currently being used; the network security professional should begin creating generalized VLANs. Finally, the network security professional should check to see if any physical security is in place; if not, they should try implementing some type of general security measures.

The second step is to begin working on the layers more in-depth. This means that the IT department, administrators, as well as users should begin learning more about network security and how it effects their day-to-day operations. This will ensure that the human layer will be stronger since everyone from the IT department down to the users will have working knowledge of network security. Although the IT department should be educated through a technical background, the user layer should be fairly non-technical so they are not thrown into technical jargon that they must learn. In the software layer, the network security professional should begin looking at the

© SANS Institute 2008, Author retains full rights.

software currently running on systems in order to start making decisions like what should be removed from the systems as well as what permissions all system users should have. We can combine the ACL and VLAN layer into a "Network" layer since they will work side by side in implementation. New VLANs should be created in order to segment the network as needed and new ACLs should be put into place in order to control the flow of traffic. Of course, before VLANs are added, ACLs should be placed at the edge in order to stop traffic from coming in that is completely unwanted. As new VLANs are created, new ACLs should be put on them to restrict access to only what is needed. At the physical layer, locks should be put on doors leading to protected data areas; also cameras should be put up around these areas in order to keep track of people using these devices.

As previously stated; no one layer should be halted in progress of another layer. A network security professional should not wait to implement their ACLs and VLANs until all system configurations have been completed. It is not necessary to implement network security measures in a specific order at all. Instead, ensure that all layers are working in a coordinated effort. As previously shown, the NSM is much like the OSI model and all layers must work correctly in order to have the desired result, complete network security.

10. Network Security Life-Cycle

Once the network security model has been implemented; a network security professional can begin a network security life-cycle. This should contain checks and balances to make sure that all layers continue to be as secure as possible. The life-cycle should begin with a look at all the layers from a technical standpoint. This means that the network security professional should look at the current Network Security Model to find any problems or improvements

© SANS Institute 2008, Author retains full rights.

that need to be done. New vulnerabilities that may have been released from the time of the last upgrade should be addressed.

At this point, the Network Security Model should be tested by a penetration test in order to find any exploits or holes that may have been missed. It should be noted that a penetration test should always be done since it will run every type of test necessary to discover network holes. If any exploits are found from the penetration test these issues should be dealt with as if they were a true break-in and the NSM was breached.

Finally, the network security professional should look at ways to update layers as the company expands. Condensing or expanding ACLs or VLANs as needed, improving physical security, looking for new versions of software that is available as well as running tests to make sure that no unauthorized software applications are running on systems. Training for all IT department, administrative departments, and user departments should continue to be done to ensure that new employees know about network security as well as refreshers for older employees.

This strategy will ensure that all layers are constantly under scrutiny and all layers are as secure as they can be. Since it is a life-cycle, there will be a point at which any network security professionals Network Security Model becomes obsolete and must be redone in order to compensate for the growth of a company as well as the high demands of the security industry. No set timeline should be given to the life-cycle; the time it takes is based on the company. A smaller company would have a longer but more dynamic life-cycle since it will be easier and more cost efficient to change large portions of the Network Security Model at once. A larger company would have a shorter but more static life-cycle since it will be easier to change small details in the Network Security Model causing

© SANS Institute 2008, Author retains full rights.

small to no disruption of service. This does not apply to every case and there are also instances where a smaller company would want to go with a life-cycle more dedicated to what a larger company would use. For example if a small company were a 24x7 operation, then it would need to run a larger company based life-cycle in order to maintain that 24x7 operation.

11. Conclusion

Currently there is no model for network security; this paper has defined and proven a possible Network Security Model which will allow general network security to be implemented and maintained by any size company. This is a framework and each layer can be modified to include company specific issues and details which may not be outlined here.

11.1 Missing IDS/IPS Layer?

One thing that is not included with the model is a section for IDS/IPS. IDS' would fall under the Physical layer because an IDS will only tell you after an attack has happened providing forensics for where and when much like a camera. IPS' were not included as they would fall under the ACL section since they perform the same type of action; blocking hosts going from one network to another.

The most important issue here is that IDS/IPS systems are still not 100% accurate and provide quite a few false positives. This makes it uncertain if they should be included in a network or not. IDS/IPS developers are making strides everyday to become more and more accurate, but there are still too many ways to circumvent them to rely on them solely.

© SANS Institute 2008, Author retains full rights.

Appendix A

Network Security Model	Exploit type
7) Physical Layer	Physical break-in
6) VLAN Layer	Network scanning local internal
5) ACL Layer	Network scanning complete internal
4) Software Layer	Software specific exploit (MS03-026)
3) User Layer	Social Engineering an User
2) Administrative Layer	Social Engineering an Administrator
1) IT Department Layer	Social Engineering and IT Professional

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2008, Author retains full rights.

Glossary

1. ACL – see Access Control List.
2. Access Control List – List of access controls which allow services to be accessed from IP addresses.
3. Compromise – This is used to describe when an attacker has taken control of the host, or the attacker has gotten a password and username on the host.
4. IDS – see Intrusion Detection System
5. IPS – see Intrusion Prevention System
6. Infection – Usually used to describe what has happened to a machine which has a virus or rootkit installed on it.
7. Intrusion Detection System – System which uses a list of signatures to detect known attacks or known anomalies and alert accordingly.
8. Intrusion Prevention System – System which uses a list of signatures to detect known attacks or known anomalies and prevent the traffic from traversing the network.
9. Mitigation – Preventing an attack from progressing further into the network.
10. Private Data – Data which is stored data which is only accessed by authorized users and is extremely sensitive. This data is usually not accessed outside of the network; if it is accessed externally it is accessed through secure channels and authorization and is accessed internally through authorization and secure channels as well.
11. Protected Data – Data which is available to the authorized users. This data is sometimes able to be changed by the authorized user; this data should only be accessed inside of the network without authorization and accessed externally through authorization.
12. Public Data – Data which is readily available to the public without any kind of access restrictions. This is usually also protected and is not changed by the public. An example is an unencrypted website.

© SANS Institute 2008, Author retains full rights.

13. Site Design - includes features that are placed on the land around the exterior of the building.

14. VLAN – see Virtual Local Area Network.

15. Virtual Local Area Network - A logical grouping of two or more nodes which share the same IP network.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2008, Author retains full rights.

Last Updated: May 23rd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced