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

Steps to a Secure Network.
Lynn Keith
May 16, 2001
Practical v1.2d

The typical corporate security objective of the past has been to protect the Enterprise network from the Internet, but as we are reading in the news today, this has not been enough. Do not assume the only threat is from the outside. Studies show that better than 70% of network intruders are from the inside (i.e. current or past disgruntled employees or contractors), as opposed to the 17-year-old computer whiz with the virus scripting kit catching the headlines today. This is not to say that you should have a security guard standing behind everyone as they type their work, but you can protect the crown jewels of the corporation by setting realistic expectations, assessing the infrastructure and implementing measures to protect it..

As you begin to design and implement the Security infrastructure for your enterprise, it is important focus on 3 areas:

The Security Policy
The Present Infrastructure
The Future Infrastructure

The Security Policy

The first step in protecting the Enterprise is to set realistic expectations. A well-written security policy not only outlines how the network is to be utilized, but protects the users as well as the corporation. The policy should not appear to be just a set of heavy handed IS rules, but a clear concise guide to assist in getting the most out of the infrastructure. There are always going to be trade offs when applying restrictions. This is why an exception process must be included as part of the policy. The policy should be modular to allow for easy adoption to changes. Remember your enterprise, as well as business practices, will change and therefore your policy must be able to adapt to it. A reference to procedure guides should be made in your policy instead of outlining the procedure. This will assist in making it less confusing and allow for timely changes.

To be a truly effective policy, it must also protect people. Place provisions in the policy to allow for the testing. It may become necessary to violate the security policy in order to test for security vulnerabilities. Devise a provision to allow for this in a controlled manner. Incorporate the proper documentation to eliminate or drastically reduce the employee's personal liability.

To establish a working policy include members from all areas of the corporation.

Human Resources – They will be able to assist in helping you following the appropriate federal, state, local and union guidelines regarding employee activity.

© SANS Institute 2000 - 2002, Author retains full rights.

The Executive Staff – If upper management in the corporation is not supportive of the security policy, you will never have the cooperation to enforce it.

Division Representatives – They can provide information about the workflow process in their area. This will provide you with the knowledge of the tools needed for workers to complete their task.

IS Security Representative – They should be up to date on the latest vulnerabilities and be able to communicate on a non-technical level. Be flexible and supportive. If you can't explain why something is a risk, then it is not a risk to the user.

Unfortunately, there is not a canned policy that you can obtain and use. Every business has its own unique practices that will effect how implementations are made. Outside contacts and reference material can also be a great resource. Consult with individuals of whom you know from other organizations on how they may have already worked through sticking points that are effecting your implementation. There are several templates that may be obtained from organizations such as Sans to help you get started.[1]

Present Infrastructure

Knowing your infrastructure is critical in securing it. The best way to accomplish this is through documentation and analysis. This should include, but not be limited to, the OS, Applications and services on the system, Network protocols and addresses, Gateways, and security measures in place to protect the system.

You should periodically do a trend analysis of the traffic on your enterprise. If you do not know what normal traffic should be there, then you will not be able to tell when unwanted traffic exists. There are several approaches that may be taken here. Ratheon has a product called Silent Runner that discovers traffic on the network then monitors for abnormalities in the traffic and alerts administrators to those abnormalities.[2] Other options include base lining the network with readily available tools that include, but are not limited to, monitoring programs such as Network Monitor that is included with Microsoft's SMS Product, Snort, TCPDUMP, as well as systems logs and performance monitors included in the Operating Systems.

Audit the host on the network for the known vulnerabilities and make sure all updates and patches have been applied. Also check the ports currently in use in the protocol stack. Disable all unnecessary services on the systems. This will help reduce the possibility of an intruder getting in through an unnoticed back door.

A Change Control System is also essential to network security. This can be a valuable source in recovering a service that failed to function because of a bad patch or malicious code hidden in a patch. This system should track all changes and their sources.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The typical corporate infrastructure today is shown in Figure 1.

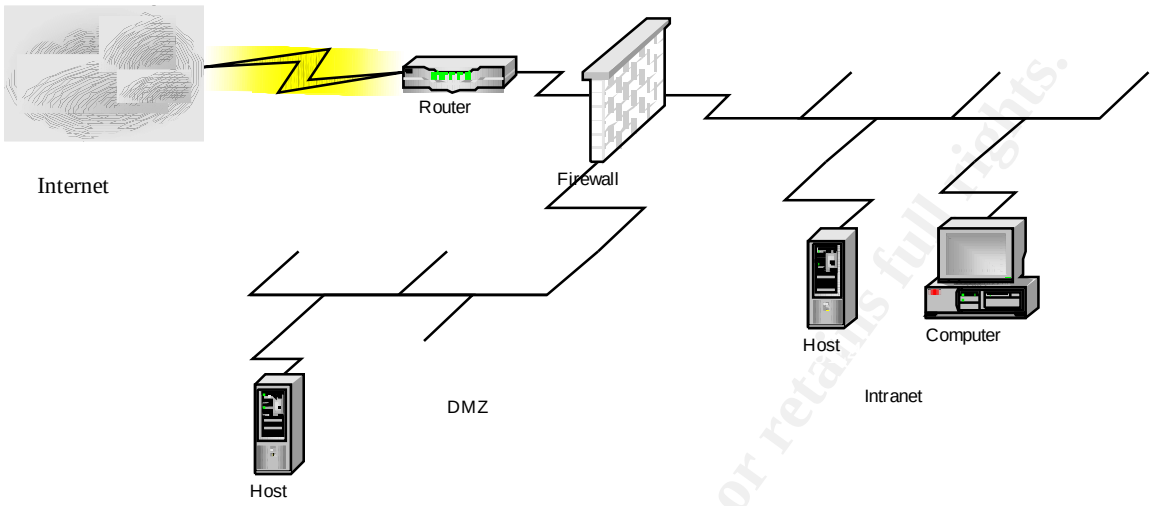

Figure 1

This leaves the network open to an extensive variety of internal vulnerabilities. Most network switches today have the capability of segmenting the network through the use of VLANS. This network segmentation allows traffic to be isolated to only the necessary areas. Then a port is configured to trunk VLANS through the IEEE 802.1q protocol, or a proprietary protocol such as Cisco's ISL Trunking Protocol. This coupled with the internal use of firewalls and router access list will provide a multi-tiered approach to protecting your network. This will go a long way toward assuring that the user community only has access to the information necessary to their job.

By placing backend host on a secure segment protected by a firewall, only designated users can achieve system access. This is accomplished by enabling only the ports necessary for communication to the host. In the example of Microsoft Exchange 5.5 server, you would perform the following task on the Exchange system:

1. Backup the registry on your Exchange server.
2. You will make 3 Registry entries on the Exchange server. [3]
   a. Add the following entry **TCP/IP port REG_DWORD DATA: *port number to assign*** Under **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeDS\Parameters**

   b. Add the following entry **TCP/IP port REG_DWORD DATA: *port number to assign*** Under **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeIS\ParametersSystem**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Then on the firewall complete the following:

1. Open TCP port 135 on your firewall.
2. Open the other 2 ports above 1024 that you chose to use in the registry entries above.

Another thing to consider in protecting the internal network is the low cost of intelligent hubs and switches. A platform should be implemented to allow managed ports to give the ability to turn off all unused ports. This will keep unauthorized systems from attaching to the network. It is also important to monitor log information and network trend analysis reports. If a system goes for 10 minutes of Internet traffic a day to 6 hours a day (or a user constantly has to change passwords), then an investigation is warranted.

The acquisition or manipulation of data is not the only threat to corporate resources. Remember, someone with a vendetta will take pleasure in creating complications for an organization. Reducing or eliminating the ability to access corporate resources can also achieve this type of hardship and is classified as a Denial of Service.

When someone mentions an operating system the first thing that usually pops to mind is some form of Windows or Unix, but all computing systems have an operating systems including network routers. This being said, there are several things that should be done to assist in the prevention of Denial of Service attacks. The first place to start is staying up to date on the security advisories[4] and applying the current patches/upgrades for your equipment. The CERT organization issued an alert[5] for the sadmind/IIS Worm virus on May 08, 2001, that takes advantage of vulnerability in the Solaris operating system allowing it to replicate and a weakness in IIS allowing it to deface a NT based web site. The patch for Solaris[6] has have been available for over 2 years and the patch for IIS[7] has been available since November of 2000.

The next safety measure is through good security configuration practices. Cisco Systems provides some excellent white papers on preventing denial of service attacks.[8] [9] The access lists in the white papers are formatted specifically to Cisco's equipment but they provide excellent information on how these attacks work.

The Future Infrastructure

With more and more end users traveling between corporate locations and working from home, wireless networking has started to play an interesting role in the network. End users are requesting wireless connectivity in meeting rooms as well as at home. A Gartner Group study shows that 36 Million wireless network systems will be in place by 2003. The wireless systems consist of 3g systems, IEEE 802.11 systems and Bluetooth systems. With the 3G systems still costly and the Bluetooth designed more for secure data synchronization with handheld devices, we will concentrate on the 802.11 systems.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The 802.11b wireless devices are rapidly becoming the most popular of the wireless connectivity due largely to price and easy to use. Users want connectivity in corporate meeting rooms and to their LAN modems at home to give them the mobility they desire while maintaining necessary communication avenues. Most of the wireless systems today can be taken out of the box and connected to a network with no configuration. This type of setup using the system defaults offers no security and lends an easy access point for unauthorized users on the network. This is why the IS department must take an active role in the deployment of these systems.

Never use the default configuration in a wireless access point. Simply change the SSID to something easy to remember, but not obvious (i.e. do not use a company name, etc…) to someone trying to gain access to your network. Limit the number of connections allowed to the access point. If this is a home system with only one connection and the user is not able to connect, then this is a warning sign to possible unauthorized access. Placing a router with a firewall feature set between the access point and the rest of the network will allow for time- based access, as well as providing firewall protection for any locally connected host. In the Cisco router, defining a time range statement and including it in the access list do this.

The following is an example of a time based access list that permits access from 8 to 5 Monday through Friday:

```
Time-range http-permit
        Periodic weekdays 8:00 to 17:00

Ip access-list extend strict
        Permit  tcp any any http time-range http-permit
```

The standard WEP encryption is better than nothing at all, but does have known security vulnerabilities.[10 11] I would also recommend filtering on the MAC address as an extra measure though this could be spoofed. If possible, use a system that allows for Radius authentication. Some Radius systems also allow for time-based connectivity, and when the office is closed - so is the access point. The Cisco ACS2000 is an excellent system that integrates with Microsoft's Active Directory, or can handle the authentication through its own database. For the budget conscious, you might try a free product from freeradius.org but it is still in the development stage. Mobile clients requiring wireless should connect through a VPN solution. This will provide secure communications back to the corporate infrastructure.

In Closing:

© SANS Institute 2000 - 2002, Author retains full rights.

The changes we discussed brings our Infrastructure to resemble figure 2

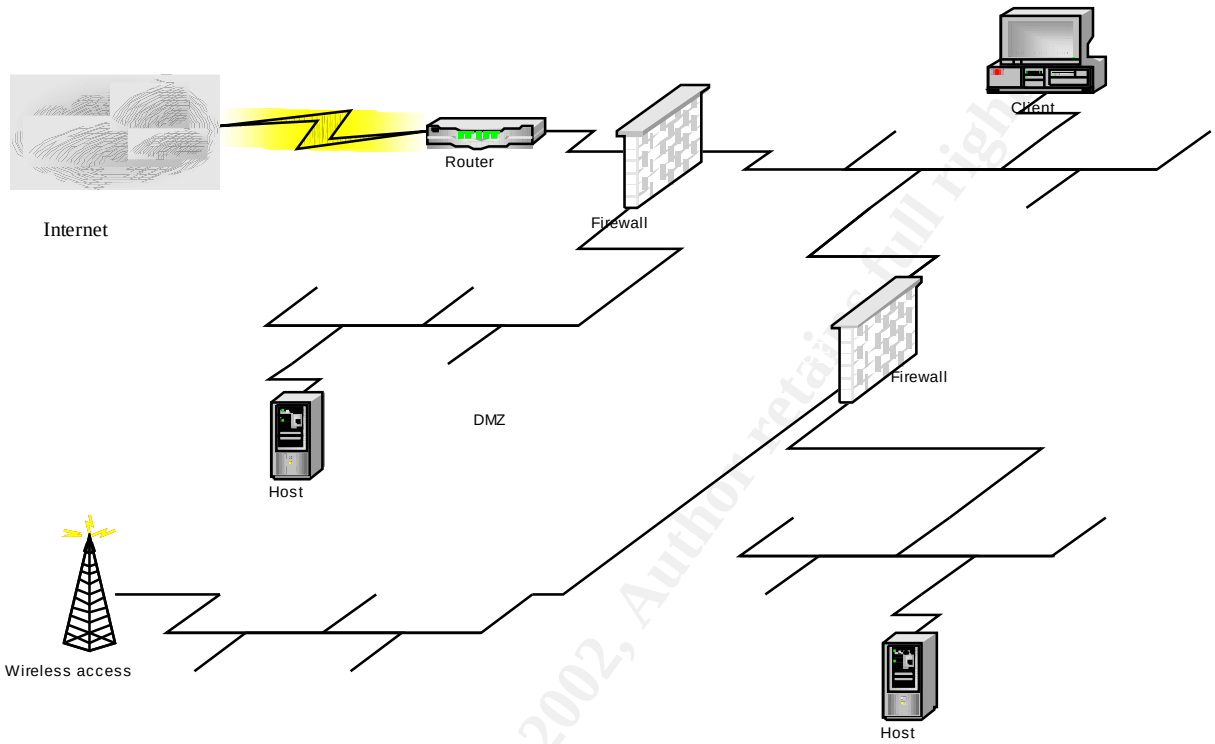

Figure 2

Knowing how your equipment works and how it should perform in your environment is the most critical aspect of network security. A team approach is essential; no individual can know everything, so utilize all of your resources. Continue to monitor and evaluate your infrastructure, this includes at least 4 internal and 1 external audits per year. Some smaller organizations do not have the resources to fund of these ventures. A possible solution would be to team up with other IS departments in the area to perform neutral committees for technical training and review, as well as joint auditing of the groups enterprise networks. By making your resources available to other organizations, and utilizing their resources to assist your organization, you may obtain a wealth of knowledge at a greatly reduced costs for all involved. This coupled with user education will provide a more secure system infrastructure.

[1] The Sans Institute
http://www.sans.org/newlook/resources/policies/policies.html

[2] Silent Runner
http://www.silentrunner.com

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

[3]The Microsoft Knowledge base Q155831 - XADM: Setting TCP/IP Ports for Exchange and Outlook Client Connections Through a Firewall

[4] Cisco Systems, Internet Security Advisories
http://www.cisco.com/warp/public/707/advisory.html

[5] Cert Advisory CA-2001-11 sadmind/IIS Worm
http://www.cert.org/advisories/CA-2001-11.html

[6] Sun Security Bulletin #00191
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doctype=cool&doc=secbull/191&type=0&nav=sec.sba

[7] Microsoft Security Bulletin MS00-78
http://www.microsoft.com/technet/security/bulletin/MS00-78

[8]Cisco Systems, Strategies to Protect Against Distributed Denial of Service Attacks http://www.cisco.com/warp/public/707/newsflash.html , Cisco Systems. February 2000

[9]Cisco Systems. Defining Strategies to Protect Against TCP SYN Denial of Service Attacks http://www.cisco.com/warp/public/707/4.html , Cisco Systems

[10] Princy C. Mehta. Wired Equivalent Privacy Vulnerability
http://www.sans.org/infosecFAQ/wireless/equiv.htm , April 2001

[11] Nikita Borisov, Ian Golberg, and David Wagoner. Security of the WEP Algorithm.
http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html , University of California Berkeley. February 2001

© SANS Institute 2000 - 2002, Author retains full rights.