



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 permitted 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>

Introduction

As information technology communication evolves and corporate networks restrict permissions and bandwidth to lock down vital resources, security or lack thereof is becoming the dominant topic of discussion in networking circles. The headlines and airwaves are buzzing with articles and discussions about network attacks, electronic theft, corporate spying, social engineering, software piracy, industrial espionage, and various other types of black hat crime. Cyber warfare is exponentially rising and administrators are rapidly implementing advanced solutions to defend against such attacks. Consequently, the network security book publishing industry is also expanding to an unseen level. There are literally hundreds of publications released each year to help administrators understand the complexities of staunchly protecting resources while allowing the free flow of data and information to enhance productivity. Ironically, hackers also have access to these resources and are using them to expose network vulnerabilities at an alarming rate.

The information outlined below offers basic insight, practical guidelines and applications in order to help administrators properly understand and secure their networks. Conclusions drawn from the following information show the significance of administrator awareness and vigilance in setting up and configuring defenses toward a higher level of network protection. The key to success in this area is to develop a systematic approach toward optimally effective security while being mindful of the delicate balance between data integrity, availability, and confidentiality.

What is Security?

Modern Secure Networks use layers of physical, administrative, electronic, and encrypted systems in order to protect valuable resources. Effective security is achieved when there is a balance between protection and availability of these resources. It is entirely possible to allow unrestricted access to a system, so that the system is available to anyone, anywhere, anytime, through any means. However, this kind of random access poses a danger to the integrity of the information. On the other hand, complete security of an information system would not allow anyone access. To achieve balance, the level of security for an organization must allow reasonable access, yet protect against real or potential threats.

It is extremely important to realize that security is also not a single configuration or technology. An administrator cannot go to the grocery store or mall to purchase some security. Security is ultimately a mindset; it is a combination of feeling safe, knowing data is secure, and being as sure as

possible that the network will not go down during any given moment. These are mostly intangible concepts that involve feelings and state of mind.

Security, therefore, can also be defined an emotion. Just as it may be hard to understand why some people feel comfortable or uncomfortable leaving their front door unlocked while sitting on the back porch enjoying the sunset, it is equally hard to define when the administrator of a network can feel secure in the knowledge that their systems are not likely to be compromised when they are not on site. (Peterson, p.2) The need for security in this context is also found in Abraham Maslow's hierarchy of needs, a widely recognized psychological theory taught in many business and administrative courses.

Computers and the network environments in which they operate have evolved into highly sophisticated and complex systems of operation. Consequently, the complexity of the relationship between computer system and network is proving to be an area of immeasurable vulnerability. Therefore, it is essential that security remains a top priority for any given organization and network.

In general, security is the quality or state of being secure and free from danger. It means protection from adversaries from those who would do harm intentionally or otherwise. The United States National Security Program is an example of a multi-layered system that protects the sovereignty of a state, its assets, resources, and its people. In the same manner, achieving the appropriate level of security for an organization depends on a multifaceted system.

A successful organization should have the following multiple layers of general security in place to protect its day-to-day operations:

- Physical Security
- Personal Security
- Operations Security
- Communications Security
- Network Security
- Information Security (Whitman, p.9)

Secure Networks Wanted

The National Strategy to Secure Cyberspace recently released by the Federal Bureau of Investigation is sure to gain global attention of network administrators. The FBI, the highest level of law enforcement in the United States, best known for its criminal most wanted list and inept use of information technology, is currently working to build awareness of cyber security and promote positive security hygiene. In his recent News Commentary entitled "Keeping Hackers at Bay," Arvind Krishna, Vice President in charge of Security Products for Tivoli Software at IBM, quoted from the FBI's list of five common mistakes that leave company and employee data vulnerable:

1. Default installations.
2. Weak passwords.

3. Incomplete data back-up.
4. Unnecessary ports left open.
5. Unfiltered packets.

While this short list states the obvious, it is disconcerting that these mistakes are still being made on a continual basis.

Further information required to keep hackers at bay can be found at:
<http://zdnet.com.com/2100-1107-958397.html>

Layers of Security

Contrary to popular belief, the first line of defense for a well-protected system has nothing to do with packets flowing in and out of the network. The first line of defense of any system is the security policy. Many Information Technology professionals consider the firewall the first line of defense, however, a firewall cannot be properly configured and administered without a security policy. Effective security in any network begins with having a clear statement of purpose. The security policy must address who, when, why, how, and where. The security policy must also state clear objectives for every piece of equipment used in the defense of a network including configuration parameters. The policy is a document or set of documents that describes the security controls to be implemented in an organization. Ultimately, the security policy will not be effective unless it is enforced. Therefore, network users should be required to sign a clearly written document that explains what they are allowed and not allowed to do on the system. At a minimum, a good security policy should include an overview, a statement of purpose and a scope of applicability, while using statements according to the guidelines discussed below:

Security Policy Essentials

Any enforced security policy should be committed to protecting the employees, partners and company from illegal or damaging actions by individuals, either knowingly or unknowingly. The intention for publishing a Security Policy should not be to impose restrictions that are contrary to the established culture of openness, trust and integrity. Internet, Intranet, and Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts electronic mail, browsing, and FTP, are property of the Company. These systems are to be used for business purposes in serving the interests of the company and its clients in the course of normal operations. Effective security requires a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know the guidelines, and to conduct their activities accordingly.

The purpose of a security policy is to outline the acceptable use of computer equipment at the organizations corporate and branch offices. The rules

must be defined in such a way as to protect the employee and the organization in the event of a security breach. Inappropriate use exposes systems and employees to risk including virus attacks, compromise of confidential data, network systems and service disruptions, as well as potential legal ramifications.

A list of prohibited activities should be presented to employees before they sign an acceptable use policy with a clear exemption of certain restrictions due to the course of legitimate job responsibilities (e.g., systems administration staff may have a need to disable network access of a host if it is disrupting production services). However, under no circumstances should an employee of the company be authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing organizationally owned resources.

The scope of the policy should encompass employees, contractors, consultants, temporary, and other workers at the company including all personnel affiliated with third parties. The policy should also apply to all equipment that is owned or leased by the company.

Further information on how to develop an effective security policy can be found at: <http://www.sun.com/software/whitepapers/wp-security-devsecpolicy/>

After the security policy has been created, disseminated, and enforced, the physical implementation of the layered defense mechanisms can begin, which includes the following components:

- [The Router](#)
- [The Firewall](#)
- [The Proxy Server](#)
- [The Demilitarized Zone](#)
- [Intrusion Detection System](#)
- [Password Security](#)
- [Anti-Virus Solution](#)
- [Physical Security](#)

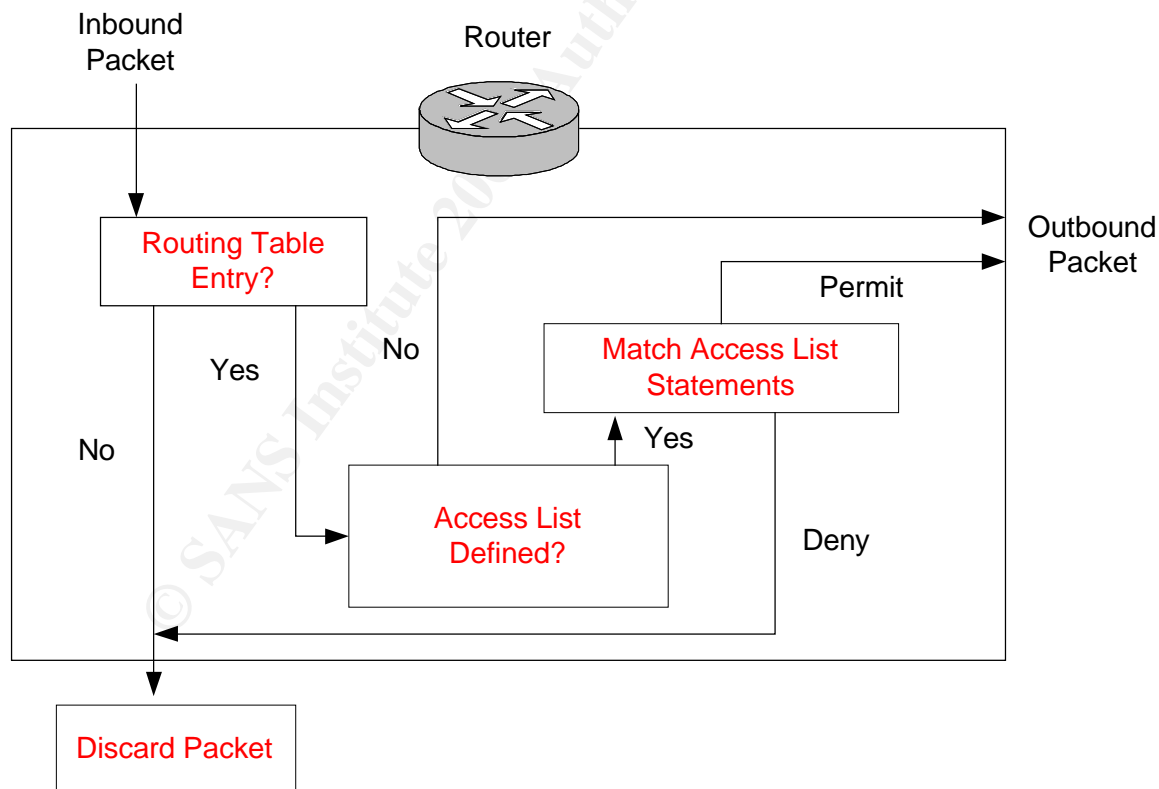
The Router

On the edge of the network are the routers. A router is a device that forwards data packets along private networks and the Internet. Routers are connected to at least two networks, commonly called Local Area Networks or Wide Area Networks and are located at gateways, the place where these two or more networks connect. A router may also connect networks containing different media technologies. For example, one part of an office may have computers with Token Ring cards wired to a Multi-Station Access Unit. To connect this network segment to another part of the building running Ethernet, you must have a router that can speak both Ethernet and Token Ring. When data from the Token Ring reaches the router, it can be sent out on the Ethernet segment and so on. Ultimately, routers use headers and forwarding tables to determine the best path

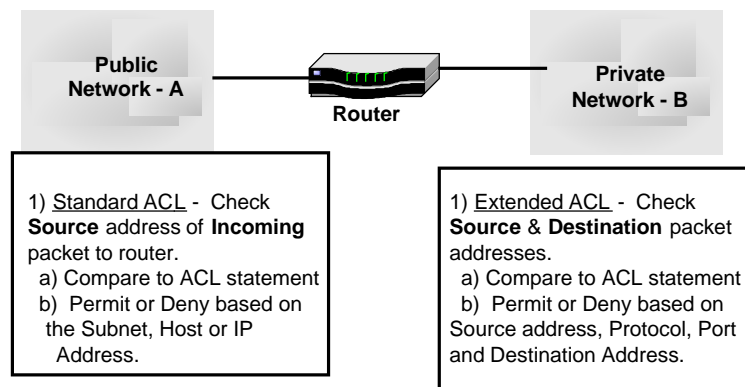
for forwarding the packets, and they use protocols to communicate with each other and configure the best route between any two hosts.

Understanding routers and routing requires the examination of a router from two different perspectives: physical and logical. From a physical perspective, routers contain many different parts, each having its own function. From a logical perspective, routers perform many functions, including finding other routers in the network, learning about potential destination networks and hosts, discovering and tracking potential routes, and forwarding packets to their specified destination. (Cisco, P. 530)

Even though very little filtering of data is done through routers, they can be used in the layered defense model through the use of access control lists (ACLs). Access control lists enable administrators not only to control access from a security standpoint, but also to restrict bandwidth use on critical links. An ACL is a packet filter that compares a packet with a given set of criteria such as limiting ICMP traffic that is allowed to pass through the router. As the packet enters the router, the routing table is checked and if there is no route, the packet is dropped. If the packet is routable, the router will check to see if the interface has an access list defined and if there is no list, the packet is routed out through the appropriate interface. If there is a list, the packet is verified to decide if it should be permitted to pass or dropped.



Access Control Lists are divided into two main categories: Standard and Extended. The Standard ACL has a value between 1 and 99. The Extended ACL has a value between 100 and 199.



If a packet filter rule is configured to deny a specific network, then it must be followed with a permit statement for all remaining networks. It is critical that an access control list operate from the top down. If the first statement of an access list is checked, and the packet doesn't match the rules of that statement (Permit or Deny), the packet is sent to the next list. This process will continue through all the rule statements of each list until there is a match. If there is a match, the packet will follow that particular rule.

In the event there are two rules within the same access control list that apply to the same packet, the first will be the rule the packet will follow. Also, there will always be a match since the end of every access list is an implicit deny. This means that every list must have at least one permit statement or all packets will be denied. The following are examples of Access Control rules:

Standard ACL rule to deny access from the 172.168.0.0 network and allow all other traffic:

```
Access-list 50 deny 172.168.0.0 0.0.255.255
Access-list 50 permit any
Access list 50 deny 0.0.0.0 255.255.255.255 (Implicit Deny)
Interface Ethernet 0
IP access-group 50 out
```

Extended ACL rule to deny 171.168.37.45 from using FTP to the Internet while also allowing it to use FTP to the rest of the network:

```
Access-list 100 deny tcp 171.168.37.45 0.0.0.0 0.0.0.0 255.255.255.255 eq 20
Access-list 100 deny tcp 171.168.37.45 0.0.0.0 0.0.0.0 255.255.255.255 eq 21
Access-list 100 permit ip any any
Interface Ethernet 0
IP access-group 100 out
```

Extended ACL rule to deny telnet access between 210.93.105.0 and 223.8.151.0.

```
Access-list 101 deny tcp 210.93.105.0 0.0.0.255 223.8.151.0 0.0.0.255 eq telnet
Access-list 101 permit ip any any.
Interface Ethernet 1
IP access-group 101 out
```

The Firewall

The next device in the layered defense configuration is the Firewall. A Firewall is a device that blocks or allows information flowing in and out of the organization. A Firewall is usually a computing device that prevents information from entering or exiting the network based on a set or mix of predefined rules. Firewalls are usually placed on the security perimeter just behind the edge of the gateway router.

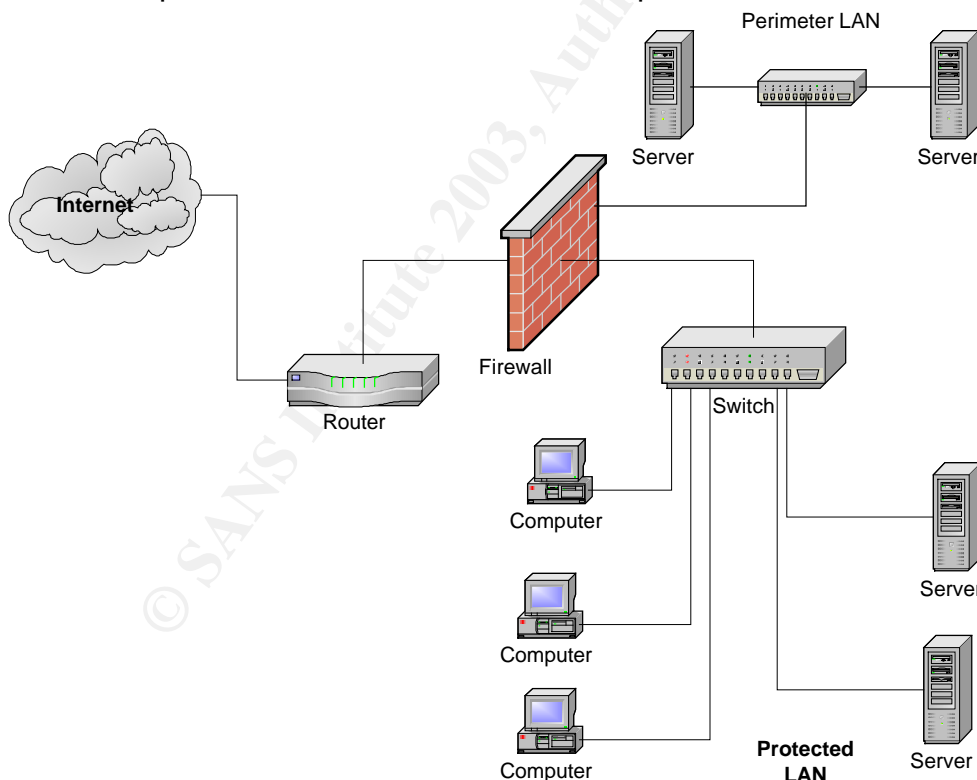
There are many types of Firewalls, normally classified by their ability to filter certain types of information. A Firewall might be a piece of turn-key hardware, or it might be a function included in software running on a special server. Firewall software is also available for a variety of Operating Systems. Firewalls can be packet filtering, proxy, or application level. A Firewall can also be a single device or compiled of multiple systems forming a buffer between the inside and outside networks.

The need for a Firewall indicates that your company is connecting its local area network (LAN) to the Internet. The key to formulating a specific design is by assessing and analyzing the types and number of communication links you expect to configure between the LAN and the Internet. Some of the determinations you should make when designing a Firewall solution include:

- a. Determine file download policy.
- b. Determine file upload policy.
- c. Determine whether you should deny access to particular users.
- d. Determine if your network will include Internet accessible Web pages.
- e. Determine if your Site will include Telnet support.
- f. Determine if your site will include FTP support.
- g. Determine ongoing employee access to the Internet and Web.
- h. Determine Worst Case Scenario if the Network is Compromised.
- i. Determine whether dedicated staff will monitor Firewall Security.
- j. Determine hardware or software solutions (Jamsa, p.97)

The best configuration for the Firewall service is to segment the network into at least three parts. The Internet connection enters the Firewall on a separate LAN adapter that gives the Firewall total control over the routing of those packets. The Firewall can then host another LAN adapter for connections to other corporate LANS on the perimeter and the third connection links the Firewall to the protected corporate internal LAN.

Behind the Firewall, the corporate LAN looks very much like an Internet Service Provider (ISP). However, services such as DNS, DHCP, and WINS that are normally set up on separate servers in an ISP can be combined in the Intranet to perform those services for the corporate LAN.

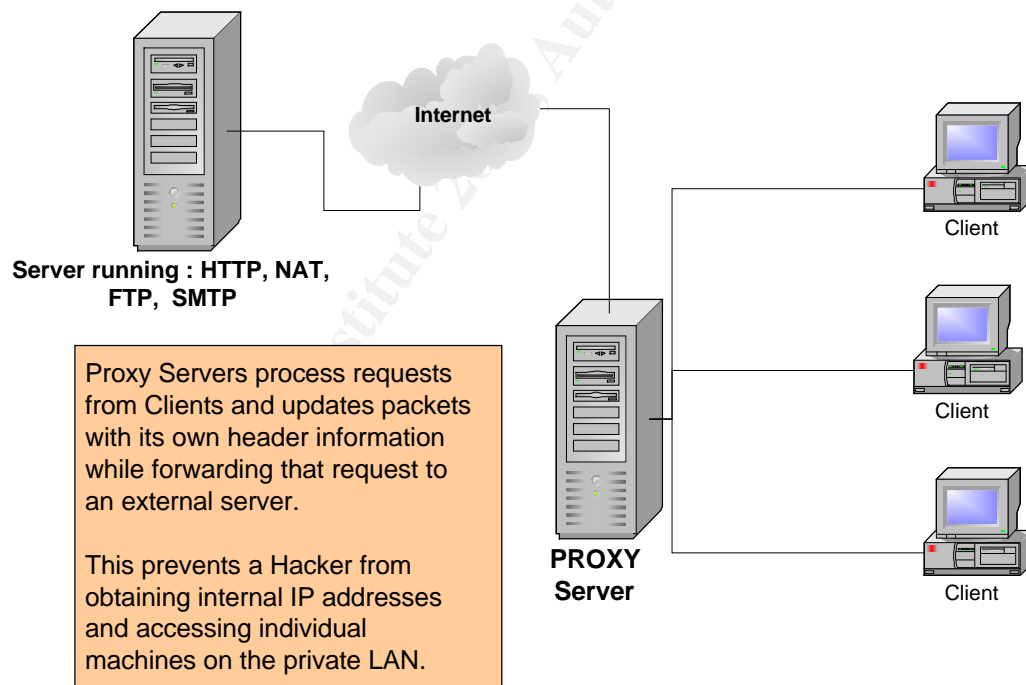


Packet filtering technology has been around since organizations first started using Firewalls. This type of Firewall has the ability to permit or deny packets based on simple rules created by the administrator. The disadvantage to

this type of configuration is that the filter will only look at the header of the packet. The problem with this type of filtering is that the administrator might create a rule set that would block the File Transport Protocol (FTP) but not the put command in FTP. This is where a Proxy server can be beneficial to the layered defense approach.

The Proxy Server

Proxy servers can enhance the layered defense configuration through the use of software that can intercept network traffic destined for given applications and can make decisions based on more than the header of the packet. The proxy acts as a go between for the client and server so there is never a direct connection between the two. Initially, proxy servers were used to cache commonly visited web pages, speeding up the network and Internet use. They have since evolved into cache web pages as well as becoming an element of a network security system. The proxy server acts at the application layer and is able to provide services to the network. The proxy acts as a gateway for all packets to flow through. A significant distinction between a packet filter and proxy server is that the proxy understands the application or service that is used and the packet filter does not. The proxy service can permit or deny packets based on the actual function the user is trying to perform.



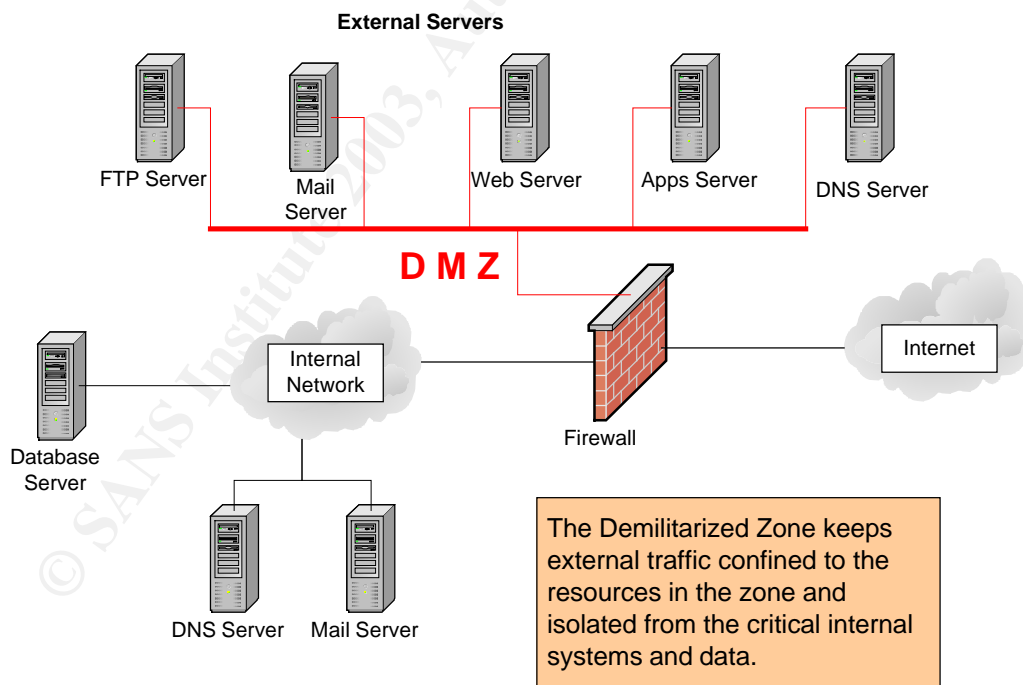
One of the most crucial issues with proxy servers is the single point of failure. If the entire network is running through the same proxy, that machine becomes quite critical, and must be configured and backed-up properly.

The Demilitarized Zone

The Demilitarized Zone (DMZ) is considered the buffer space against outside attacks. Physically, it is the area that exists between the inside and outside networks where some organizations place Web servers and other services. These servers provide access to organizational Web pages without allowing traffic to enter the internal networks. (Groth, p.366)

A standard DMZ setup has three network cards in the Firewall computer. One adapter card is directly connected to the Internet, the second is connected to the network segment with the external servers, and the third is connected to the internal network. When hackers break into the DMZ, they will only be able to see public information, not internal corporate information on the private network. Additionally, the e-mail messages traversing the internal network are secure because the messages are stored and viewed on e-mail servers inside the network.

An example of a DMZ in military terms is the zone between North and South Korea. This zone is defined along the Military Demarcation Line established by the Armistice agreement in 1953 at the end of the Korean War. It is the 4 km wide by 250 km long corridor extending from east to west across the Korean peninsula. The Military Armistice commission rigidly enforces the DMZ that separates the two Koreas, preventing any type of human intrusion.



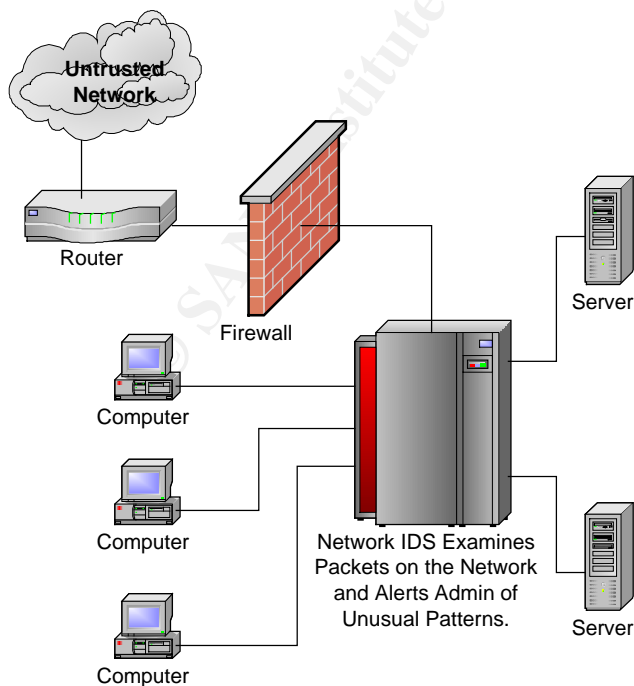
Intrusion Detection System

In an effort to detect unauthorized activity within the boundaries of the inside network or on specific machines, many organizations implement intrusion

detection systems. With a myriad of commercial Intrusion Detection systems (IDS) available, the network administrator has many critical decisions to make. These decisions range from allocation of funds to deciding the speed of response to new types of incidents such as the Slapper Worm or code Red virus. The fee of such programs is generally the driving factor in the decision making process. Some products run from a few thousand dollars to over a hundred thousand dollars.

The Snort IDS program has many benefits. Aside from the fact that there is no fee associated with the use of this product, it is written in an open-source format that allows for quick modifications. The rules for Snort can be written by anyone and posted to the Web for widespread distribution. Whenever a new threat is identified, an administrator or programmer can write a new rule and post it that day. Additionally, the Snort community can analyze, download and implement it. This IDS tool and associated applications can be found at www.snort.org.

Another benefit of snort is ease of installation. In less than 10 minutes Snort can be installed, configured, and up and running. The three items required for a Windows installation are the Snort application, WinPcap file, and a utility called IDS Center. The WinPcap is a self-extracting executable packet capture driver and can be found at www.snort.org. The power of Snort as an IDS lies in its ability to create and use rule sets from the command line. However, for those who are not comfortable using a command-line program, a tool called IDS center has been created to provide a Graphical User Interface (GUI) environment for Snort in Windows. Since Snort and WinPcap are already installed, the rest of the setup for IDScenter is very straightforward. IDScenter can also be found at www.snort.org.



Network-based IDS look at patterns of network traffic and attempt to detect unusual activity based on previous baselines. This may include packets coming into the organization with a valid address from machines inside the network (IP Spoofing) or it may detect high volumes of information leaving the network (Data Theft). IDS can also detect denial of service attacks targeted against internal network servers. Network-based IDS can use a catalog of common attack signatures and develop a database of normal activity on the network for comparison with future activity.

Host based IDS are usually installed on computers they protect and monitor the status of various files stored on that system. The IDS will learn the configuration of the system, assign priorities to various files depending on their value, and alert the administrator of successful or failed attempts to access the files or data. In a host-based IDS, the system can create a database of file attributes to use as a baseline, as well as maintain a catalog of common attack signatures and methodologies.

Password Security

The very first line of defense against unauthorized access to computer systems is authentication and password protection. Like any other aspect of network security, passwords must be managed. Managing passwords involves ensuring that all passwords for user accounts follow security guidelines so that they cannot be easily guessed or cracked as well as implementing features of your network operating system in order to prevent unauthorized access. This can very easily become the weakest link in the security hierarchy if something goes wrong. The problem is that users want simple and easy to remember passwords for their accounts. Most users would like to settle on one password, and use it for all of their accounts while they also write them down for quick reference. Unfortunately, for the system administrator, this is not effective password management from a network security standpoint. The reality is that password security requires almost constant attention to provide a minimum level of comfort.

The most important password on a server-based system is the administrator's password, usually known as super-user or root. Anyone who knows it will have full access on remote systems, and possibly other systems on the local network. For business systems, it is wise to limit number of people who hold the "root" password for integrity, and security.

Passwords should be at least six characters long but some of the stronger passwords have a minimum of 8 characters. Only the first eight characters of a password are recognized on most UNIX systems. The one thing to remember is that under no circumstance should your account names or passwords be written down. The only person who should know them is you, and they should be memorized! To consistently get strong passwords, you can use auditing tools, such as a crack program that tries to guess passwords. If you use weak passwords, the crack program will have little difficulty making a guess. Good crack programs strip off the leading and trailing characters of every password it

attempts to break so make sure to use special numbers and characters in the middle of your password schemes to prevent them from being cracked.

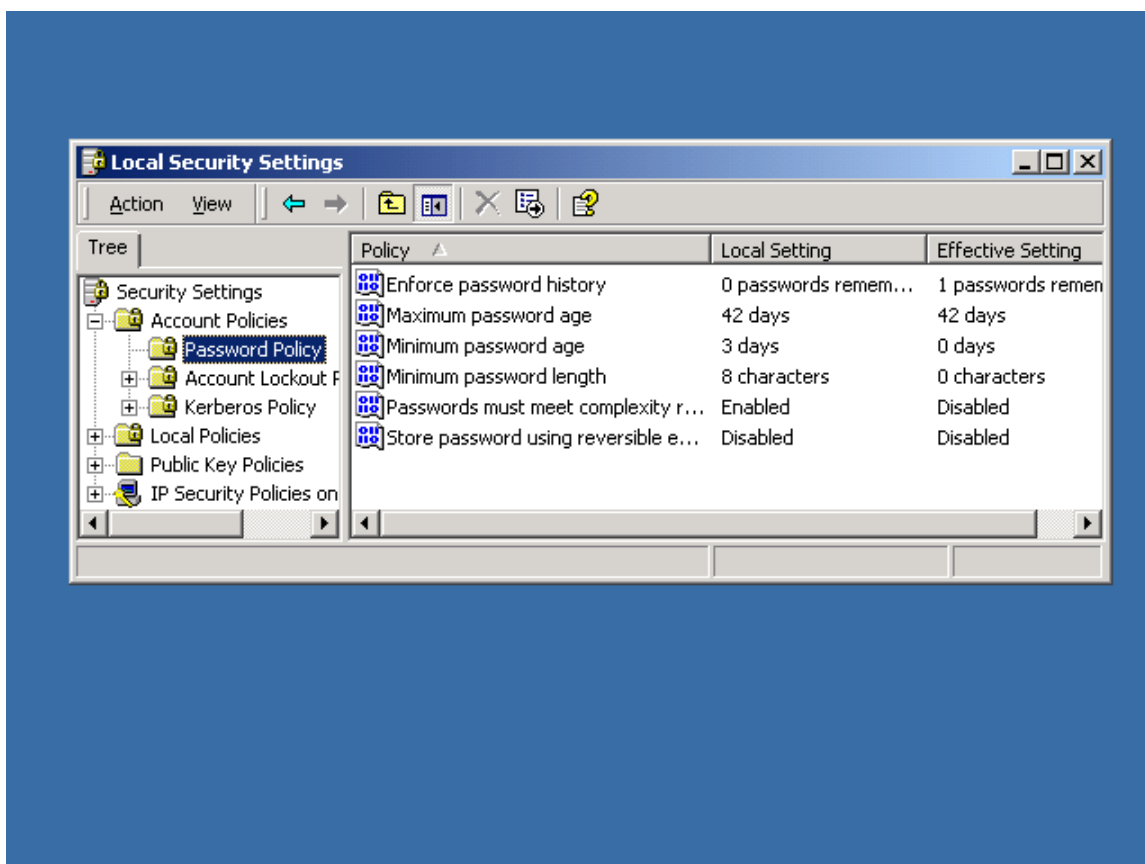
Hackers use many different attempts to decrypt passwords, and it has been proven very routine to purchase or download a program that attempts to guess a password. A decent Windows password crack program called LC4 can be found at <http://www.atstake.com/research/lc/>. There is no fee for the standard program unlike the Brute Force option. Of course, to deter this type of program from being successful, users should remember that if their password is long and complex, these types of programs take longer to succeed and will usually be noticed by the administrator and shut down.

Some examples of password cracking programs are Brute Force attacks and Dictionary attacks. The application of computing and network resources to attempt every possible combination of options of a password is called a Brute Force attack. Since this is often an attempt to repeatedly guess passwords to commonly used accounts, it is sometimes called a password attack. The dictionary attack narrows the field by selecting specific accounts to attack and uses a list of commonly used passwords to guess instead of random combinations.

Even the best passwords do not age well over time. Passwords can be guessed if they are never changed. The impact of someone guessing your password is reduced if passwords are set to expire after a certain amount of time. The procedure an administrator can use to stop this type of guess attack is to give all passwords a limited lifetime. If all users are forced to change their passwords after a set amount of time, it makes it harder for the programs to work on repeated attacks. The flip side is that it may also encumber the administrator's job because users will write down their new passwords each time they are required to change them.

Windows 2000 Server Local Security Password Policy Setting

© SANS Institute 2003



In the Windows 2000 Server, the password settings can be accomplished from the Local Security Settings, but if Domain Level Policies are defined, they override Local Policy Settings. Whenever you make a policy change in Windows 2000 or .NET Server, you must use the Security Editor (secdit) utility from the command prompt to refresh and implement the policy.

C:\>secdit /refreshpolicy machine_policy

Group policy propagation from the domain has been initiated for this computer. It may take a few minutes for the propagation to complete and the new policy to take effect. Please check Application Log for errors.

The general rule for setting passwords is to never choose anything that someone could guess by knowing you, such as your name, address, social security number, family member's name, phone number, driver's license, birthday, etc. These are the first targets used by a hacker or system cracker. Passwords with numbers, alphanumeric characters, and special punctuation characters usually serve as hard to crack combinations. Some great examples of strong passwords are "!andrew", "%40assign", and "big!fish."

Anti-Virus Solution

When monitoring security-based websites like SANS Institute and McAfee, you will find new Viruses, Trojan horses, and Denial of Service (DOS) attacks added by the day if not hour. There are many people out on the Internet who are quite willing to break into your network. Some are doing it simply for the challenge, while others are planning malicious attacks.

Anti-Virus programs protect your network computers in two ways. They work in an active seek and destroy mode or a passive sentry mode. When ordered to seek and destroy, the program will scan the computers' boot sector and files for viruses, and if any are found, it will present you with available options for removing or disabling them. Anti-Virus programs can also operate as virus shields that passively monitor your computer's activity, checking for viruses only when certain events occur, such as a program executing or a file being downloaded.

The computer virus is one of the most well known dangerous risks associated with computers and Network Security today. Similar to the human virus influenza that spreads through the population by contact, the computer virus spreads through the network infecting hard drives and programs indiscriminately. For the systems that are inoculated with the latest Anti-Virus software, the impact of a full-scale virus attack may be minimal at best. For those systems that are unprotected, the results of an attack can be devastating.

Most viruses always have some type of signature for which the anti-virus software can search. When you purchase and install anti-virus software, the software comes with a database of virus signatures. As new viruses emerge, the software companies add the corresponding signatures to the anti-virus software database files you can normally download from the Web, in order to keep your system's virus-signature database current. Anti-Virus software works by examining the contents of files that reside on your disk, programs you have loaded into memory, and the contents of e-mail messages you receive. When the Anti-Virus software examines a file, it looks for a Virus Signature, something unique that corresponds to a virus.

Further information on how Computer Viruses work can be found at:

<http://www.howstuffworks.com/virus.htm>

Further information on Virus Prevention, Recognition, and Removal can be found at: www.virusbtn.com/index.html

Further information on Virus removal Tools can be found at:

www.symantec.com/avcenter/tools.list.html

Physical Security

Physical security addresses the design, implementation, and maintenance of countermeasures that protect the physical resources of an organization. This

includes the physical protection of the people, the hardware, and the supporting system elements and resources associated with the management of transmission, storage, and processing information. Most technology based security controls can be circumvented by gaining access to computers and routers physically. Some computers are constructed in such a way that it allows access to the hard drive and other components of the PC. Hand held USB devices capable of holding more than a gigabyte of information can also be plugged into the back of a computer to download sensitive or otherwise proprietary data. Special care should be taken to prevent access by unauthorized personnel at the work site. If someone can walk into the computer center and access the system unchallenged, then the system administrator has a major problem. By controlling access to computers, servers, and more importantly routers, you can make it all the more difficult for someone to steal or damage either data or equipment.

A major part of an administrator's responsibility should be to establish physical access policies for the computing facilities, and then educate the users who would be affected by such policies. An example of this is on U.S. Navy ships where financial, personnel, military, and secret information systems are isolated and kept physically secure. Compartments housing mainframes and other such servers are guarded and kept secure leaving access to very few people. As a result, when the users are educated, they will be able to report any unauthorized activity they may witness, and may challenge users they don't recognize using the system.

Additionally, computer components on Navy ships and in other industrial environments are particularly sensitive to many types of physical environmental conditions such as fire, smoke, and moisture. Considerations for the purchase of smoke detectors, air filtration and automatic fire suppression systems to ensure quick responses in the event of an emergency are paramount.

Just as with any other area of security, physical security requires sound organizational policy for direction. Policy guides the planning of physical security in the development life cycle and serves as a reference to organizational objectives through ongoing maintenance and use.

Further information regarding Physical Security can be found at:
<http://www.andrewernst.com/Research/networks/english/physical.htm>

Conclusion

Even though the aforementioned approach to layered security appears straightforward and basic, effective layers of security may take months or years to completely develop. The strong foundation and multiple layers of protection may compliment the present topology, however, as connections increase among business partners, the number of connections required to support remote access grows, and the quantity of services offered to customers rise, the original set of security policies and procedures in network architectures can turn into a

complicated array of security mechanisms and formulations that require constant attention and updating.

Furthermore, perfect security is a goal that few people pursue due to the fact that most security professionals realize there is no such thing. The concept of perfect security cannot exist for one simple reason: As human beings, we are imperfect and unpredictable with the freedom to make decisions, both good and bad. All we can do is strive for this elusive perfection, which in effect, increases both physical and emotional system security.

Further information pertaining to Security Layers can be found at:

<http://www.infosecurymag.com/2002/jun/insecurity.shtml>

Further information pertaining to Best Security Practices can be found at:

<http://www.infonetwork.com.au/securityadvisor.htm>

Credits

Peterson, Warren. Network Security Fundamentals. elementk, 2001.

Whitman, Michael. Principles of Information Security. Thompson, 2003.

Cisco Networking Academy, First-Year Companion, Cisco Press, 2001.

Groth, David. Network + Study Guide. Sybex, 2001.

Jamsa, Kris. Hacker Proof. Thompson, 2002

Krishna, Arvind. "Five Steps for keeping Hackers at bay." 18 Sep 2002.

URL: <http://zdnet.com.com/2100-1107-958397.html>

Avolio, Frederick. "Best Practices in Network Security." 20 Mar 2000.

URL: <http://www.nwc.com/1105/1105f2.html>

"How to develop a Network Security Policy."

URL: <http://www.sun.com/software/whitepapers/wp-security-devsecpolicy/>

Mackey, Richard. "Security Architecture." Jun 2002.

URL: <http://www.infosecurymag.com/2002/jun/insecurity.shtml>

"Security Advisor." Jan 2000.

URL: <http://www.infonetwork.com.au/securityadvisor.htm>

"Ten Best Tips on Security."

URL: <http://www.infonetwork.com.au/security10tipc.htm>

Ernst, Andrew. "Physical Security." Dec 2002.

URL: <http://www.andrewernst.com/Research/networks/english/physical.htm>

“How Computer Viruses Work.”

URL: <http://www.howstuffworks.com/virus.htm>

“Virus Bulletin.”

URL: www.virusbtn.com/index.html

“Virus Removal Tools.”

URL: www.symantec.com/avcenter/tools.list.html

© SANS Institute 2003, Author retains full rights.