Name: Paul A. Zocco
Certification: SANS Security Essentials
Assignment: GSEC Practical Assignment
Version: 1.2d
Group: SANS Baltimore 2001

Ten Days to Network Security

Abstract

How would you answer these questions?

- What would you do if you were given ten days to secure your network?
- You've just been to the SANS Kickstart and Level One Essentials classes and now you're back at the office. Where do you begin?
- You're a new LAN administrator and you been given the charge of "securing" the network. What would be the most effective plan of action in the shortest period of time? What could you do to make your network more secure quickly?

This paper will present ten days of effective tasks, with a quick task and long term task each day. Each essential security action listed below in the day-by-day tables has three characteristics:

- Focuses on real threats rather than theoretical threats
- Can be implemented quickly and inexpensively
- Are proven and effective

Overall, what occurs is the development of a comprehensive security program. According to Pipkin[1], the five parts of a security program are:

- Inspection
- Protection
- Detection
- Reaction, and
- Reflection.

As the days progress, each of the five parts begin to get fulfilled, some at a greater level than others.

Introduction

Network security is not a product that you can purchase it's a process. A long process that you continually update, improve, and monitor. A process that has a policy to define and guide as you manage risks, not avoid them. Starting the process is difficult. In fact, you may not know where to start, what to do first, how to do it. You need to pace yourself but it's nice to have a guide. This paper is such a guide. Whether you're just starting out to protect your network or you're a seasoned professional who needs a refresher, this paper will guide you with tasks to complete along the way and checklists to assist you in making sure all procedures are complete. In ten business days, you will be on your way to a secure network. The day-by-day tables in this paper provide a quick and long-term security task that can be performed each day. Long-term tasks take more time, involve more planning and people, and are more difficult to accomplish. But they can be done in parallel with the quick tasks, which pay immediate benefits. The quick tasks are less intrusive then the long term tasks and can be completed in a short amount of time by one person. Mounted on your office or server room wall, the checklists are a quick reference guide, which along with the day-by-day tables, provide a solid foundation for network security. Even though every aspect of network security can't be covered in ten days, you'll find that the matrix covers the most effective tasks to secure your network in a short time, as well as helping you write a complete security policy.

Like any important project, you can't secure your network in a vacuum. You must form a team of people and get them involved. The team must then lobby management as to the seriousness and importance of network security and get their buy-in.

Each quick task will have a time, cost, and interference factor (from 1 to 5 icons). The time factor (↑ takes into account how quickly a security task can be implemented, the cost factor ($) takes into account whether something is free or easy to do or must be budgeted, and the interference factor (👽) has to do with whether a client or group of clients is inconvenienced as the security change or changes are made. For example, if a client desktop PC or a server has to be rebooted for changes to occur, this would be considered a higher interference factor than if the security administrator completes a task in the background, such as resetting the ACL on a directory, and a user only has to login again for changes to take effect.

SANS recommends protection at all perimeters, that is, host, network, and router. As you will see, each of the quick tasks builds the perimeter defenses immediately while each long-term task develops the information security program for the organization. Once the information security program is in place after the tenth day, procedures and checklists are there to constantly and consistently keep the quick tasks up-to-date. Let's get started!

DAY 1

Day	Quick Task	Time	Cost	Interference	Long Term Tasks
Day 1	Create more secure passwords	↑	$	👽	Information Security Program Development 1- Information assessment, threat (risk) analysis, vulnerability assessment

Quick Task-Create more secure passwords

The username/password combination is typically the first line of defense against intruders. If your network only uses usernames and passwords for protection, it could be viewed as an "eggshell", that is, having a hard outer shell but a soft center. However, the username/password task is where you should start on Day 1 since it is the easiest to do and involves all of your users, hopefully creating buy in to greater security. Passwords are "low-hanging" fruit that are attractive to crackers and the cracking of just one user's password is enough to compromise any system. Securing this first line of network authentication reaps many benefits.

Considering that there are a variety of ways to have users learn a new, harder-to-crack password, there are immediate benefits in promoting this quick task. Passwords to consider changing on a regular basis are:

- Username passwords, especially any administrator or root password
- Any hub, switch, or router passwords
- Any SNMP community password (especially away from the standard "public" password)
- Any print server password
- Any screen saver password

One section of the overall security policy to be developed should contain a password policy. Basics of the password policy must include:

- What group of departmental and LAN administrators are allowed to change what passwords
- User passwords should be forced to be changed at least every 30 days
- User accounts should be locked after 3 failed attempts, for at least up to 15 minutes
- Passwords must contain one alpha (uppercase and lowercase), one number, one special character or punctuation
- Passwords on an NT or W2K system should be at least 14 characters, taking into consideration that the password is hashed at 7 characters
- The user can't reuse the last 5 passwords
- Administrator accounts should be renamed, secured with a good password, and audited for logon attempts
- Passwords should not be written down or sent via email
- Any OS tools that encrypt password storage (such as SYSKEY) should be used
- A common phrase or verse to a poem or favorite song makes it easy to remember a password. For example, "Strawberry Fields, forever" could make the password **StrFie#4ever**. Take the first three letters of the first two words (including uppercase), add the # symbol as your punctuation mark, and append on forever, but change the "for" to a number 4.

Long Task- Information Security Program Development 1- Information assessment, threat (risk) analysis, vulnerability assessment

The development of an information security program starts in earnest. The first part of the task is an information assessment, that is, a resource inventory. You must determine the security classification of all information resources by assigning a value to them and considering what risks you might incur. This is the main assessment of information in your organization. Ask yourself these questions:

- How sensitive is the information?
- What is the consequence of disclosing this information?
- Are there any legal or contractual obligations and penalties concerning the information?
- Are there any industry, government, local, or organizational standards and guidelines that

might help determine how this information is classified?
- What is the lifetime of this information?

Keep the assessment as simple and straightforward as possible. Determine how vulnerable you would be if your information were compromised. Use the formula:

Risk = Impact X Probability.

Keep it simple by assigning a value of 1, 2, or 3 to Impact and to Probability, with 1=lowest and 3=highest. The higher the product of **Impact X Probability**, the greater the **Risk**, the greater the vulnerability. Design a simple matrix of information resources and place it in the first section of your security policy.

DAY 2

Day	Quick Task	Time	Cost	Interference	Long Term Tasks
Day 2	Implement Virus Protection-on all desktops, servers, email servers	↑↑	$$$	👽 👽	Information Security Program Development 2 – Policies-Passwords, Acceptable Use, Incident Response, System Admin, Configuration Management, Online Warnings

Quick Task- Implement Virus Protection-on all desktops, servers, email servers

The second quick task is to purchase and implement an anti-virus solution for all desktops and servers, especially email servers. In today's computing environment, this task is a no-brainer. It must be done, no questions asked. Several anti-virus products, once installed on a server, implement a console that allows anti-virus updates to be pushed to users automatically. In this respect, you are building on user loyalty. For example, by pushing virus updates to your users, they'll like knowing they have up-to-date virus protection and this security process will have more value to them. Educate your users on how email attachments can easily spread viruses and consider setting email client software to not open attachments automatically. Don't forget to share with your users the web addresses of virus and hoax protection sites. Hoaxes, in terms of destruction, are harmless but are a great drain on Internet bandwidth. As users share email about hoaxes, productive time is taken away from your day and their day. Empower your users to limit these emails by educating them on the web sites that explain hoaxes in detail.

The anti-virus part of your security policy would include:

- Anti-virus protection on every desktop, server, and email server.
- Automatically push anti-virus updates to users
- Educate users about email attachments
- Educate users about viruses and hoaxes and what web sites help distinguish between the

two

Long Task- Information Security Program Development 2- Policies-Passwords, Acceptable Use, Incident Response, System Admin, Configuration Management, Online Warnings

This day is where we begin the development of security policy. If you break the security policy into pieces, it will be easier to write. Consider pieces such as a master root policy that oversees the other parts, a password policy, an acceptable use policy, an incident response policy, a system administrator policy and set of procedures, a policy for managing machine configuration changes, a system policy for what software should and shouldn't belong on a machine, a personal hacking policy, and a set of online warnings for internal and external users of your systems.

Remember, your security policy give systems and network administrators a fall back during a crisis and a guide for the mundane but essential day-to-day decisions and actions. Policies should also provide and contain:

- Well thought out approaches to problems that have been tested over time,
- A method to bring a business closer to understanding its computer and network business requirements and risks,
- A framework for re-evaluation as requirements and risks change,
- A grounding in reality,
- The vehicle that provides security in a manageable way while delivering required services and ensuring profitability,
- A method for continual updating, and
- Metrics to measure compliance.

The more simple and straightforward your policies are, the more likely they are to be understood, followed, and accepted. As explained in the first day of SANS Level One Security Essentials, each policy should contain these parts:

- Purpose
- Related documents
- Cancellation (of old policies)
- Background
- Scope
- Policy statement
- Action
- Responsibility
- Security procedures and checklists
- Clear, concise, realistic steps
- Consistency with higher-level policy and guidance
- Forward looking, able to change
- A review schedule
- Be readily available

Another way to look at security policy is what Avolio[2] suggests. Start with a Root Security Policy, that is, a framework that tells us what has to be done. It addresses known requirements and threats and suggests a “Do what’s possible today, tag residual risks and note tasks to be accomplished later” attitude. The root is where risk assessment and business requirements come together and differences are worked out and it addresses how an organization handles information, who may access it and how, it specifies allowed and denied behavior, and lists controls that are in place. You then develop Security Architecture Guidelines, that is, a part that specifies countermeasures to the threats discovered in risk assessment and lists the assurances that are in place, the auditing, and the controls. An Incident Response Procedure should describe what is considered an incident and who gets called and when. Acceptable Use Policies, meant for end users, explain what actions are permitted and which are prohibited. These policies try to name the service, system or subsystem it is regulating, then state in clearest terms behavior that is and is not permitted. They must also tell the consequences of breaking the rules. Finally System Policies and System Administration Procedures (sometimes called lock-down guides) describe what software must and must not be in place and how systems are to be backed up and administered.

Remember, a reasonable security policy strikes a balance between security and productivity. Make security processes have value to your users. For example, push virus updates to them. They’ll like knowing they have up-to-date virus protection. When a restrictive security measure must be put in place, you’ll have the edge to explain to users why it’s necessary. Your security policy is a living document. Use resources like www.sans.org and www.cert.org to keep your policy up-to-date. Most important, get management buy-in. Since computer, network, telephone costs are seen today as part of the investment for doing business, so must management see security costs. Senior management must ratify every policy, document, and guideline.

DAY 3

Day	Quick Task	Time	Cost	Interference	Long Term Tasks
Day 3	Install latest OS Patches, Updates, and Hotfixes on Desktops and Servers, Disable Unnecessary Services, Use Vulnerability Tools	↑↑↑	$	👽👽👽👽	Information Security Program Development 3 – User education and training (include social engineering)

Quick Task- Install latest OS Patches, Updates, and Hotfixes on Desktops and Servers, Disable Unnecessary Services

The third quick task keeps building up the defense in depth. You must take a close look at all the services running on your servers and determine what ones are absolutely necessary to provide the proper service. Default installations of most operating systems tend to install more services than are required for secure operation. Run vulnerability assessment tools such as nmap, to determine what weaknesses you currently have. For example, it is rare that a web server needs to run an SMTP service or that an email server needs to run an HTTP service. Most default installations install SNMP services, which are rarely secured properly and in most instances are not necessary. Microsoft NT servers typically install the NetBEUI protocol but all that is necessary for most applications and Internet usage is TCP/IP. Locking down unnecessary services also holds true for desktop machines (no need for file and print sharing), and switches and routers (beware of built-in HTTP engines) that need to have HTTP access restricted. In other words, "If you aren't using it, turn it off."

Operating systems patches, updates, and hotfixes are typically provided free via vendor's web sites. Take advantage of email notification services provided by these vendors and other security lists to keep you informed of the latest fixes. As with any operating system update, evaluate whether you need the particular patch. Typically vendors release multiple fix releases called Service Packs, which take care of several, operational and security fixes in one package. Check newsgroups and other trusted sources to make sure the latest service pack has had widespread acceptance and success before installing on production machines. Updates, sometimes known as hotfixes, are typically patches released after a service pack. Most security updates come in the form of hotfixes and administrators must determine, on a case-by-case basis, if the hotfix in question, is necessary to bolster network security. To summarize:

- As for server services, "If you aren't using it, turn it off."
- Improve on your host-based perimeter by asking, "Is there a business requirement for this service?"
- Tighten systems settings, implement latest OS service packs, patches, and hotfixes

Long Task- Information Security Program Development 3 – User education and training (include social engineering)

User education and training are critical to the success of your security efforts. Training is your best defense against security lapses. Get the word out to users that they are a valuable part of the security infrastructure. Having vigilant users is a great defense. Train users with the following thoughts in mind:

- Any acceptable use policy you write is meant for your end users. Explain actions that are permitted and those which are prohibited.
- Tell the consequences of breaking the rules.
- Educate users on social engineering and how crackers use it to subvert security measures.
- Train the trainers, the helpdesk, and the end users not to give out information over the phone, email, or casual conversation unless they know the recipient and can verify his or her authenticity
- Make sure processes have value to your users.
- Outline the users' roles and responsibilities
- Consider physical security
- Consider how you dispose of information
- Consider laptop and wireless use

DAY 4

Day	Quick Task	Time	Cost	Interference	Long Term Tasks
Day 4	Herd Users into Groups, Assign Permissions to all Files/Directories, Remove Old Accounts, Check All Configurations	↑↑↑	$	👽 👽	Information Security Program Development 4 – Network Design-DMZ and Firewalls

Quick Task- Herd Users into Groups, Assign Permissions to all Files/Directories, Remove Old Accounts, Check All Configurations

Permissions on files and directories determine what users have what kind of access to what information, that is, what information the users are authorized to use. Herd users into groups, using your OS tools. Create user groups based on the types of information they should have access to, possibly depending on department, job function, business unit, or most important, a need to know basis. You should:

- Plan user groups based on a need to know. This overrides department, business function, or job classification.
- Start by giving no one permission. Give permission as it is needed.
- Determine group permissions on all directories, particularly system files and crown jewel files.
- Delete old user accounts and user groups along the way.
- Check for permission misconfigurations. If a user group needs only to see files, give Read access, not Change access.
- Only give the right Access Control when absolutely necessary. Access Control allows a user to assign others rights to that directory.

Long Task- Information Security Program Development 4 – Network Design-DMZ and Firewalls

If your organization doesn't have a firewall, get one. Whether you get a firewall appliance (like an Axent Velociraptor or a Cisco PIX) or a more traditional firewall (Checkpoint Firewall-1 or Symantec [Axent] Raptor) that you load on an NT server, you will get the opportunity to segment and subnet your network into a demilitarized zone, also known as a DMZ. A DMZ is where administrators can locate publicly accessible machines, such as email and web servers, so that they are separated from the machines on the internal LAN, thereby providing another layer of defense.

Try to get the most sophisticated firewall that you can. Protocol-level or packet-level firewalls check each packet as it passes through the firewall. Stateful packet-level firewalls not only check each packet but keep track of the state of each packet. Application proxy firewalls intercept traffic at the application level and essentially answer each packet as a proxy. Firewalls typically have at least three interfaces: one for incoming traffic, one for access to the DMZ, and one that connects to your protected network, your LAN. Firewalls typically add a layer of privacy by concealing a network's inside IP address scheme from the outside through Network Address Translation (NAT). NAT allows you to use private IP addresses (IP addresses that aren't routable) on your internal network that translate to typically one valid IP address for the outside world to see.

Crucial to firewall success is proper configuration. Most firewalls are configured by rulesets, that is, groups of rules that describe what TCP/IP ports can and can't get through the firewall to the DMZ machines or to the machines on the internal LAN. But as stated on the SANS Roadmap poster, don't fall prey to these common firewall and DMZ security perimeter problems:

- Assuming that a firewall alone provides sufficient security
- Allowing some network services, such as ftp and http, to pass through the perimeter unscreened
- Not logging connections through the perimeter or not reviewing the logs regularly
- Allowing support personnel to use telnet or other unencrypted protocols to manage the firewall or DMZ machines.

DAY 5

Day	Quick Task	Time	Cost	Interference	Long Term Tasks
Day 5	Configure Routers and Firewalls-Ports, Rulesets, Egress Filtering	↑↑↑	$	👽	Information Security Program Development 5 – Secure physical access

Quick Task- Configure Border Routers

Your border routers and firewalls need to be configured to deny all unnecessary incoming traffic. Establish rule sets to block most malicious traffic. In this manner, the firewall inspects all traffic that tries to pass to and from your network, permitting only authorized traffic to pass. Think of it as a noise filter. To prevent Distributed Denial of Service (DdoS) attacks, also configure egress filtering on your router. Make sure that traffic leaving your network comes only from your network. Important points are:

- Deny all ports on your routers and firewalls and allow necessary ports one at a time.
- Configure only ports 25 (SMTP), 110 (POP3), 80 (HTTP) as a minimum through your firewall. Don't open port 21 (FTP), in fact, don't even consider an FTP server.
- On an NT network, block TCP and UDP ports 137, 138, 139 that allow outsiders to see what devices you have via NETBIOS protocol.
- Use Network Address Translation (NAT) on your internal LAN so that only the minimum of IP addresses is disclosed to the outside world.
- The maximum number of IP addresses to disclose to the Internet is one, that is, your router. If you have an email server and web server, you'll have to disclose those IP addresses, too.

Long Task- Information Security Program Development 5 – Secure physical access

Physical access to your servers and desktops provides people with many opportunities to undo your hard work in securing your network. For servers, provide a room that is at least under key and lock and preferably under an access control system that monitors and logs who is in the server room and when. Only allow authorized personnel into the server room and log off of any servers when not in use.

As for desktops, train staff to log off or lock their workstations during any break away from their machine. Set screen savers to require a password for entry. Provide secured bins for depositing unused sensitive media. Provide a shredder for any paper that needs to be securely discarded. Discourage all users from writing down passwords. Lock up floppy disks, CD-ROMs and other storage media from prying eyes and hands.

DAY 6

Day	Quick Task	Time	Cost	Interference	Long Term Tasks
Day 6	Backup and Restore-Use special backup agents-test and implement	↑↑	$$$$	👽	Information Security Program Development 6 – Controlled environment (HVAC, fire, UPS)

Quick Task- Backup and Restore-Use special backup agents-test and implement

If you don't have third-party backup software for your NT/2000 server, consider Cheyenne's (Computer Associates) ArcServe or Veritas Backup Exec. Each tool provides a comprehensive backup and restore package that allows for scheduled full, differential, and incremental backups as well as partial and full restores. If you have email or database servers, consider purchasing the special backup agents for these systems, as they allow for backup while the files are open or in use. Use a media-rated (125 degrees F) data safe to store backup media and store at least a weeks worth of tapes, including a full backup of all systems, offsite. Or consider contracting with a storage service to pickup, deliver, and store backup media offsite.

Proper tape rotation is important. Consider a daily, weekly, monthly tape rotation as follows:

- Consider full backups each day, if possible
- The last Friday of each month is the monthly backup
- Following the last Friday of each month, the next week start with tape Week 1-Monday, Week 1-Tuesday, etc.
- Succeeding weeks follow as Week 2-Monday, Week 2-Tuesday, etc.
- Typically almost five weeks worth of tapes are needed per month.

Remember these points about backup:

- Use a third-party backup software package
- Install special email and database backup agents
- Test partial and full backups and also partial and full restores
- Rotate tapes on a daily, weekly, monthly basis

- Manage offsite storage of backup tapes, whether you take them home or a service picks them up
- Make sure all system administrators know how to run backups and restores
- Document procedures for how you conduct, secure, and make available normal backups

Long Task- Information Security Program Development 6 – Controlled environment (HVAC, fire, UPS)

As you work on the secure physical access of the server room in Long Task 5, make sure you control other aspects of the server room environment. An uninterruptible power supply (UPS) is essential for any server operation. Not only should a UPS provide clean, regulated electrical power, free from sags, brownouts, surges, and over voltages, it should also provide a logging and alerting mechanism for system administrators of any of these adverse power conditions. Temperature and humidity must also be controlled and monitored by a commercial-grade air conditioning unit.

- Controlled environment (temperature, humidity, fire protection)
- Controlled electricity (proper power supply)

DAY 7

Day	Quick Task	Time	Cost	Interference	Long Term Tasks
Day 7	Provide clean electrical power	↑↑↑	$$$$	👽👽👽👽	Information Security Program Development 7 – Web Server Security

Quick Task- Provide clean electrical power

Your servers are critical to your organization and you should do all that you can to protect them. Like any electronic device, computers depend on clean, steady electrical power to run reliably and safely. One of the least expensive and least time consuming quick tasks you can do to protect your network is to provide each server with an uninterruptible power supply, a UPS. According to American Power Conversion (APC)[3], there are six types of UPS designs. Two of these designs are most popular for workstations and server; Standby and Line Interactive. For servers under 5 kVA (kilo Volt-Amperes), the Line Interactive UPS is recommended. Line Interactive units provide good line conditioning, are highly efficient, come in a variety of sizes, and can be extended with additional battery packs for longer run times when the power goes out. UPS units will typically protect against sags, brownouts, surges, and over voltages. Some units will even boost power is there is a sag or brownout condition without having to resort to battery power. Most units come with a serial port to connect to a serial port on your server. With UPS monitoring software (usually included), an administrator can monitor the power going into and out of the UPS and set alarm and logging parameters for notification in case of power problems or outages. Most UPS software will shut down a server safely after a preset time lapse but before batteries are drained.

Most UPS manufacturer's sites provide UPS sizing tools or selectors that allow you to choose your actual server with accessories, choose a desired run time, and choose a future expansion capacity. Once chosen, the selectors typically provide you with a choice of UPS units with various features. Some things to look for in a UPS:

- Size the UPS for additional capacity and extended run time– most power problems are transient but storms or bad weather can call for long battery run times
- Check the Amperage rating and plug type of the UPS and make sure your electrical circuit has the proper capacity and outlet
- Select a UPS that has surge, sag, brownout, and over voltage protection.
- Look for units that boost under voltage conditions without using battery.
- Select a unit with software that monitors power, logs readings, sends alerts, and performs shutdowns in case of power outage.

Long Task- Information Security Program Development 7 – Web Server Security

Web servers are a security problem because we need to give the public access to them over TCP port 80 if we want to advertise our organization or institution. Talk about an open door to a major system on our network! Having said that, there are several tasks that can be done to minimize the security risks inherent in a web server.

First, check out the Microsoft security web site at www.microsoft.com/security and look for the IIS v4.0 and IIS v5.0 security checklists. Some of the more important items on that list are:

- Install minimal Internet services – To use IIS, the following services must be running:
    - Event Log
    - License Logging Service
    - Windows NTLM Security Support Provider
    - Remote Procedure Call (RPC) Service
    - Windows NT Server or Windows NT Workstation
    - IIS Admin Service
    - MSDTC
    - World Wide Web Publishing Service
    - Protected Storage
- Select the appropriate authentication method for your application (in order of increasing trust)
    - Anonymous
    - Basic
    - Windows NT Challenge/Response
    - Client Certificates
- Set proper directory permissions for CGI, script, include, static files
- Make sure IIS log files have proper ACLs
- Disable or remove all sample applications
- Secure the anonymous IIS account (IUSR_computername) – use only a local account

DAY 8

Day	Quick Task	Time	Cost	Interference	Long Term Tasks
Day 8	Host and Network Audits and Logging	↑↑↑	$	👽 👽	Information Security Program Development 8 – Secure Remote Access

Quick Task- Host and Network Audits and Logging

Why do you need to do audits and turn on logging? As said in the SANS Windows NT Security Step-by-Step book, "If you don't see the problem, you cannot fix it." Turning on logging and auditing such events as: Logon and Logoff, success and failure, File and Object Access failure, Use of User Rights failure, Security Policy changes, success and failure, Startup, Shutdown, and System, success and failure will allow you to see several events. You'll be able to answer these questions: Who has logged in unsuccessfully? Who has accessed what important files on your servers? Who has started up or shut down a server? Who has made a change to the security policy? Remember, you'll only be able to see all of the above events only if you view the logs.

Start by adjusting the size of the log files to a large size to save several days or weeks worth of data. What you want to do is save enough events in a log file to determine if there are any trends and to give you experience in what people are doing in your network. Turn off any options that do cycling logging (logs that overwrite themselves after so many days.) Also, turn off any options that shut down the server if the audit logs are full.

To summarize:

- Adjust log files to large sizes for system, security, and applications
- Save the log files in a format suitable for later analysis, such as a comma-separated-value format
- Turn on auditing of basic events, adjusting as necessary depending on volume of events recorded:
    - Logon and Logoff, success and failure
    - File and Object Access failure
    - Use of User Rights failure
    - Security Policy changes, success and failure
    - Startup, Shutdown, and System, success and failure
- System audits and audits for crown jewels
- Review Section 5 of Level One Essentials, Day 3 to see how to read logs daily with free tools, such as tools from the NT Resource Kit and tools like NTLast
- Set up a regular schedule for reviewing logs for failed logon attempts
- Centralized your monitoring to view all sights in one location

Long Task- Information Security Program Development 8 – Secure Remote Access

Every situation and every user can't demand a private line to communicate with your LAN. You'll have to use the public Internet to do your work. Using a Virtual Private Network (VPN) will allow you to conduct your business over the Internet. By creating what is known as a VPN tunnel, combinations of qualities such as IP Security (IPsec), the Layer 2 Tunneling

Protocol (L2TP), and the Point-to-Point Tunneling Protocol (PPTP) can be used to provide a secure connection and still offer three important security services:

- Authentication – to prove the integrity of the tunnel endpoints
- Encryption – to protect sensitive information transferred, and
- Integrity checks – to ensure that the data has not changed in transit.

Think about the following deployment considerations:

- Difficulty of deployment – Consider if you need multi-protocol support. Consider the impact on network addressing, routing, firewall configurations
- Integration – Check for methods of authentication and if your VPN supports privately addressed networks
- Client software – The desktop environment can dictate what VPN solution you select.
- Flexibility – Determine your authentication, message integrity, and encryption requirements up front to narrow your choices and reduce your costs
- Performance – VPN technologies are taxing as they add packet overhead and make use of encryption. Perform trials of the product if possible.
- Transparency and ease-of-use – If end users are to use any product, it has to be easy to use and well defined. If it's troublesome, it won't be used.
- Scalable management – Being able to track usage and provide updates is important to promoting the success of your VPN.

Some resources are:

"Redefining the Virtual Private Network (VPN)" a Check Point white paper at www.checkpoint.com

"Virtual Private Networks: Your Guide to the New World Opportunity" a white paper from Cisco at www.cisco.com

"A Practical Guide to the Right VPN" from ZDNet IT Resource Centers at http://techguide.zdnet.com

"VPNs: The Good, The Bad, and The Ugly", Information Security magazine, May 2001, pp 49-64.

DAY 9

Day	Quick Task	Time	Cost	Interference	Long Term Tasks
Day 9	Personal Firewalls (Host Defense)	↑↑	$	👽	Information Security Program Development 9 – Disaster Recovery

Quick Task- Personal Firewalls (Host Defense)

If you continue to think Defense in Depth, personal firewalls provide another layer of protection right at the host level. Most personal firewalls available today are a combination of a packet-filtering or application-level proxy firewall and an Intrusion Detection System (IDS). An IDS is used to monitor network connections in real-time, giving you warning when someone is trying to pry where they shouldn't. An IDS also offers logging for all entries which provides evidence if prosecuting attackers.

Two popular personal firewalls are Network ICE BlackICE Defender (www.blackice.com) and Zone Labs' ZoneAlarm (www.zonelabs.com) . BlackICE Defender is a packet-filtering firewall and IDS in one and has a stateful inspection capability that allows it to monitor your network connection for signatures of popular attacks. When an attack is blocked, BlackICE Defender will log the attack and all packets, and even try to get the host name and MAC address of the attacker. BlackICE Defender does provide an editable configuration file for more advanced users. ZoneAlarm is free for personal use and intervenes at the application level when your machine tries to contact the Internet. It checks to see if a rule has been set up for an application and is configured "on the fly". Once the rule is configured and saved, ZoneAlarm remembers if you have left that traffic through before and doesn't question you again when you use the application in question. Both Internet and local access traffic are tracked.

Concerning personal firewalls, you should:

- Take advantage of free or low-cost personal firewalls
- Look for a personal firewall that combines a packet-filtering or application-level proxy firewall with an IDS
- Use Deny All, Allow as Needed
- Block for port scanners, if possible
- Create rules to watch the most commonly exploited ports
- Check logs regularly for suspicious activity

Long Task- Information Security Program Development – Disaster Recovery

Whether it's a flat tire, being stuck in a snow bank, or locking your keys in your car, there's nothing worse then being unprepared with your car in the above situations. A simple spare tire, a shovel in the car trunk, or a spare key in your wallet or purse are all it takes to be prepared in case mishaps strike at the wrong time. With computer networks, as with driving, planning and preparation make the difference. Create a disaster recovery plan and keep it with your security policies. Here are some things to consider:

- Keep a change log on each server's desktop to track changes you've made. Copy the change log to another location (floppy, another server) for safe keeping in case the server goes down.
- Keep a copy of any configuration files for servers and routers on floppy in a protected place.
- Keep a spare hard disk on hand for all the types of disks in your servers. (Here's a vote for keeping server purchases uniform.)
- Purchase servers with dual power supplies, if possible. One takes over instantly in case the other fails.
- Disk structures should be at a minimum RAID 1 or RAID 5. A hot spare is best.

- Use server monitoring software (usually comes with server) to watch server health.
- Use a larger enough UPS to allow server to run for a short time if power goes out.
- Make sure all backup logs are checked daily. Test restoring from a backup tape at least once a month.
- Place a phone in your server room for easy access to vendor or support help when needed.
- Replace backup tapes as needed.
- Clean all tape drives at least once a week. (Especially DAT drives.)
- Keep operating system software, all service packs, patches, hotfixes, and drivers in a safe place in case of disaster. It will keep you from running around trying to hunt down resources when you most need them.
- Prepare an emergency repair disk and system boot disk in case internal files (such as an NT registry) need to be repaired.
- If you have a number of servers, always keep an extra monitor, keyboard, and mouse on hand.
- When you purchase a server, extend the basic service contract to at least three years with a four-hour response time.
- When disaster strikes, take a deep breath and relax. Get a pad of paper, assess the situation and draw out a plan of attack. Saving a few minutes to rush a fix can sometimes make matters worse.

DAY 10

Day	Quick Task	Time	Cost	Interference	Long Term Tasks
Day 10	Subscribe to Security Bulletins	↑	$	👽	Information Security Program Development 10 – Intrusion Detection/Self hacking

Quick Task- Subscribe to Security Bulletins

Security bulletins are a must if you are to stay abreast of all that is going on in the security. Trends as well as immediate notifications are important to keeping your network safe. Here are some of the security bulletins you must subscribe to and some of the web sites you must visit:

NT Bugtraq – Well moderated list that tracks NT security problems	www.ntbugtraq.com www.securityfocus.com
CERT Advisories – Computer Emergency Response Team from Carnegie Mellon University	www.cert.org
Windows NT Security: Step-by-Step – from the SANS Institute	www.sans.org/ntstep.htm
Viruses and Hoaxes – Symantec AntiVirus Research Center (SARC)	www.sarc.com

Viruses and Hoaxes – Data Fellowes site	www.datafellowes.com

Long Task- Information Security Program Development – Intrusion Detection/Self hacking

To be able to protect your systems as much as possible, you need to be able to detect and analyze any attacks directed at your organization. Then, you need to be able to react to that attack accordingly, strengthening your defenses based on your analysis of the attack. For these two reasons, you need to install an Intrusion Detection System (IDS). Most likely, you'll want to install a network-based IDS, to monitor all of your network traffic, searching for any traffic pattern that looks suspicious, such as a port scan or a denial of service attack. At that moment, the IDS should alert you with an alarm.

A good IDS should give you more control and visibility. Control lets you manage you network traffic and network access. Visibility lets you see and understand your network's nature and its traffic, and allows you to make decisions about resource allocation. Where routers and firewalls give you control on who enters your network, IDSs add visibility by checking those that get through the firewall by applying additional rules to the traffic, sometimes called signatures. Signatures such as a threshold barrier, that is too much traffic from one source (possibly a denial of service, profiling (create base profiles for most users and looking for the suspect ones, and known attack signatures (such as invalid TCP headers, mass mailings from many users, or TCP scans) are the components that the IDS uses to judge the validity of traffic and whether or not an alert should be sent out.

As IDSs have evolved, they've added new levels to network visibility. IDSs examine packets within the data stream to identify threats from authorized users, back-door attacks, and hackers who thwart the perimeter defenses. Best-of-class IDSs fully decode protocols to completely expose packets and their contents to the scrutiny of large attack-signature databases tuned to the specific environment, and alert security professionals to suspected threats.

Like firewalls, IDSs can also block specific data streams that are suspect. Unlike perimeter defenses, which completely block user access, IDSs discriminate and thereby minimize the risk of blocking authorized users who have made a benign mistake

At some point, you have to play the bad guy. Once your IDS is set up, you need to try to hack yourself. But first get permission. As part of your security policy, include a "personal" security policy, signed by your management that gives you permission to hack your own network. The personal security policy is a necessity, giving you an out in case something happens to the network.

Conclusion

This paper is not the definitive answer on security. It is intended to be a well-defined starting place and handy reference. Some important areas of security that were not brought up include most notably encryption, privacy, Public Key Infrastructure, denial of service attacks, email security, and telecommunications security. Hopefully, the reader will pursue the security web sites listed and not avoid the challenge ahead.

Checklists

Day	Quick		
1	☐ Consider all types of passwords that need to be secure ☐ What administrators are allowed to change what passwords? ☐ Force password change at least every 30 days ☐ User account locked after 3 failed attempts, for at least up to 15 minutes ☐ Passwords must contain one alpha (uppercase and lowercase), one number, one special character or punctuation ☐ Passwords on an NT or W2K system should be at least 14 characters, taking into consideration that the password is hashed at 7 characters ☐ User can't reuse the last 5 passwords ☐ Rename Administrator account, secure with a good password ☐ Audit Administrator account for logon attempts ☐ Passwords should not be written down or sent via email ☐ Use OS tools that encrypt password storage ☐ Use a phrase or verse from a poem or song to remember password	A Security Administrator magazine (part of Windows 2000 magazine) article on setting passwords	http://www.secadministrator.com/Articles/Index.cfm?ArticleID=20204

2	☐ Install anti-virus protection on every desktop, server, and email server. ☐ Automatically push anti-virus updates to users ☐ Educate users about email attachments ☐ Educate users about viruses and hoaxes ☐ Tell users what web sites help distinguish between viruses and hoaxes	Symantec-Developers of Norton AntiVirus	www.symantec.com www.sarc.com
		McAfee VirusScan	www.mcafee.com
		F-Secure AntiVirus	www.datafellows.com
		Hoaxes – a great resource on hoaxes that travel the Internet	http://www.datafellows.com/news/hoax/
		Hoaxes – another very good source on hoaxes	http://www.symantec.com/avcenter/hoax.html
3	☐ As for server services, "If you aren't using it, turn it off." ☐ Improve on your host-based perimeter by asking, "Is there a business requirement for this service?" ☐ Tighten systems settings, implement latest OS service packs, patches, and hotfixes	Microsoft's site on updates, patches, and hotfixes	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/current.asp
		Security checklists and tools for Microsoft servers	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/tools/tools.asp
		Home of the Microsoft Download Center	http://www.microsoft.com/downloads/search.asp
4	☐ Plan user groups based on a need to know. This overrides department, business function, or job classification. ☐ Start by giving no one permission. Give permission as it is needed. ☐ Determine group permissions on all directories, particularly system files and crown jewel files. ☐ Delete old user accounts and user groups along the way. ☐ Check for permission misconfigurations. If a user group needs only to see files, give Read access, not Change access.	Microsoft security site settings for files and directories	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/tools/mbrsrvcl.asp
		TrustedSystems.com site to download a few papers on setting permissions	http://www.trustedsystems.com/downloads.htm
		Boran Systems overall NT Security guide	http://www.boran.com/security/nt1.html

5	☐ Deny all ports on your routers and firewalls and allow necessary ports one at a time. ☐ Configure only ports 25 (SMTP), 110 (POP3), 80 (HTTP) as a minimum through your firewall. Don't open port 21 (FTP), in fact, don't even consider an FTP server. ☐ On an NT network, block TCP and UDP ports 137, 138, 139 that allow outsiders to see what devices you have via NETBIOS protocol. ☐ Use Network Address Translation (NAT) on your internal LAN so that only the minimum of IP addresses is disclosed to the outside world. ☐ The maximum number of IP addresses to disclose to the Internet is one, that is, your router. If you have an email server and web server, you'll have to disclose those IP addresses, too.	An article on demilitarized zones for your network	http://www.zdnet.com/enterprise/stories/main/0,10228,2717224,00.html
		An article on setting proper firewall rules	http://www.8wire.com/headlines/?AID=1798
		A good article on choosing a firewall	http://www.zdnet.com/enterprise/stories/main/0,10228,2694089,00.html
		Security Portals enterprise firewall page – much information about many vendors	http://securityportal.com/firewalls/enterprise/
		A comprehensive ports list from Security Portal	http://securityportal.com/firewalls/ports/
6	☐ Use a third-party backup software package ☐ Install special email and database backup agents ☐ Test partial and full backups and also partial and full restores ☐ Manage offsite storage of backup tapes, whether you take them home or a service picks them up ☐ Make sure all system administrators know how to run backups and restores ☐ Document procedures for how you conduct, secure, and make available normal backups	Computer Associates, developers of Cheyenne ArcServe	www.ca.com
		Veritas, developers of Backup Exec	www.veritas.com
		Iron Mountain, providers of safe, offsite storage of backup media and pick-up and drop-off services.	www.ironmountain.com

7	☐ Size the UPS for additional capacity and extended run time–most power problems are transient but storms or bad weather can call for long battery run times ☐ Check the Amperage rating and plug type of the UPS and make sure your electrical circuit has the proper capacity and outlet ☐ Select a UPS that has surge, sag, brownout, and over voltage protection. ☐ Look for units that boost under voltage conditions without using battery. ☐ Select a unit with software that monitors power, logs readings, sends alerts, and performs shutdowns in case of power outage.	American Power Conversion	www.apcc.com
		Best Power	www.bestpower.com
		Tripp Lite Corporation	www.tripplite.com
		APC’s useful UPS selector	http://www.apcc.com/template/size/apc/

8	☐ Adjust log files to large sizes for system, security, and applications ☐ Save the log files in a format suitable for later analysis, such as a comma-separated-value format ☐ Turn on auditing of basic events, adjusting as necessary depending on volume of events recorded: ☐ Logon and Logoff, success and failure ☐ File and Object Access failure ☐ Use of User Rights failure ☐ Security Policy changes, success and failure ☐ Startup, Shutdown, and System, success and failure ☐ System audits and audits for crown jewels ☐ Review Section 5 of Level One Essentials, Day 3 to see how to read logs daily with free tools, such as tools from the NT Resource Kit and tools like NTLast from www.foundstone.com ☐ Set up a regular schedule for reviewing logs for failed logon attempts ☐ Centralized your monitoring to view all sights in one location	NTLast, a tool to help read NT log files on a daily basis.	http://www.foundstone.com/rdlabs/tools.php?category=Forensic
9	☐ Take advantage of free or low-cost personal firewalls ☐ Look for a personal firewall that combines a packet-filtering or application-level proxy firewall with an IDS ☐ Use Deny All, Allow as Needed ☐ Block for port scanners, if possible ☐ Create rules to watch the most commonly exploited ports ☐ Check logs regularly for suspicious activity	Creators of ZoneAlarm and ZoneAlarm Pro	http://www.zonelabs.com
		Creators of BlackICE Defender	http://www.networkice.com/

10	☐ Subscribe to several security mailing lists, especially the ones that track viruses, patches, and hotfixes ☐ Visit security web sites on a daily basis	NT Bugtraq – Well moderated list that tracks NT security problems	www.ntbugtraq.com www.securityfocus.com
		CERT Advisories – Computer Emergency Response Team from Carnegie Mellon University	www.cert.org
		Internet Security Systems – Well Organized List of Security Mailing Lists	http://xforce.iss.net/maillists/otherlists.php
		MOREnet-Missouri Research and Education Network-great compilation of security sites	http://www.more.net/security/general.html
		Boran Systems great guide to overall network security	http://www.boran.com/security/
		8wire.com – Good security web site	http://www.8wire.com/headlines/?AID=1798
		Search Security – A great source to search	www.searchsecurity.com
		Security Portal – Organized, searchable site	www.securityportal.com
		SANS Institute Windows Security Step-by-Step	www.sans.org/ntstep.htm

Footnotes

[1] Donald L. Pipkin, Information Security: Protecting the Global Enterprise, (Prentice Hall PTR, 2000), pp 17-18.

[2] Frederick M. Avolio, "Best Practices in Network Security," Network Computing magazine, URL:http://www.networkcomputing.com/shared/printArticle?article=nc/1105/1105f2full.html

[3] "The Different Types of UPS Systems", APC Technote. URL:http://sturgeon.apcc.com/technotes.nsf/For+External/E9BBFEE399C39C7585256A5C007A1430?OpenDocument

Bibliography

Allen, Julia. "CERT System and Network Security Practices." Carnegie Mellon University, Software Engineering Institute. URL: **http://www.cert.org/archive/pdf/NCISSE_practices.pdf**

Avolio, Frederick M. "Best Practices in Network Security." Network Computing magazine. URL:http://www.networkcomputing.com/shared/printArticle?article=nc/1105/1105f2full.html (5-Jul-2001)

Culp, Scott. "The Ten Immutable Laws of Security." Microsoft Corporation. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/columns/security/10imlaws.asp

Culp, Scott. "The Ten Immutable Laws of Security Administration." Microsoft Corporation. URL: **http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/columns/security/10salaws.asp**

Dinino, Gregg J. "Initial Network Security Steps Don't Require Techies." URL:http://www.bdmp.com/itg/publications/06.htm (5-Jul-2001)

"Dress Your E-Security in Layers." Earthweb IT Management: Security. URL:http://itmanagement.earthweb.com/secu/article/0,,11953_791191,00.html

Ferrarini, Elizabeth M. "The Five-Access Point Security Plan." Earthweb Networking and Communications. URL:http://networking.earthweb.com/netsecur/print/o,,12084_752421,00.html (5-Jul-2001)

Genusa, Angela. "12 Keys for locking up tight." CIO magazine. **URL:http://www2.cio.com/archive/030101/keys_content.html** (5-Jul-2001)

Gardner, Rick. "Computer Network Security must be an ongoing process." Houston Business

Journal. **URL:http://houston.bcentral.com/houston/stories/2001/03/18/focus2.html** (5-Jul-2001)

Martin, Jim. "Top Ten Best Security Practices for Windows NT." Coordinator Technology Conference 1999. **URL:http://www.more.net/security/nt10/sld001.htm**

"Microsoft Windows 2000 Network Architecture Guide." Systems and Network Attack Center (SNAC), National Security Agency. Report Number: C4-051R-00

"Network Security Policy: Best Practices White Paper." Cisco Corporation. URL:http://www.cisco.com/warp/public/126/secpol.html

Norton, Peter. Peter Norton's Network Security Fundamentals. SAMS, 2000.

Packer, Ryon. "Network Intrusion Detection, Part 1: Laying the Groundwork." URL: http://www.8wire.com/article_render/?aid=2026

Pipkin, Donald L. Information Security: Protecting the Global Enterprise. Prentice Hall PTR, 2000.

Reeder, Paul. "Intrusion Detection: Adding Depth to Network Defense." URL: http://www.8wire.com/article_render/?aid=1954

SANS Level One Security Essentials. SANS Institute, 2001.

SANS Institute. "Essential Security Actions: Step By Step." URL:http://www.sans.org/newlook/resources/esa.htm (5-Jul-2001)

Sunbelt W2Knews Electronic Newsletter from Sunbelt Software. May 10, 2001

"The Different Types of UPS Systems." APC Technote. URL:http://sturgeon.apcc.com/technotes.nsf/For+External/E9BBFEE399C39C7585256A5C007A1430?OpenDocument

"VPNs: Virtually Anything?" Core Competence. URL:http://searchnetworking.techtarget.com/originalContent/0,289142,sid7_gci540868,00.html