Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

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

OK, So I Need Security. Where Do I Start?

This paper is not designed to be an end-all solution to your problems, but it can be used to begin identifying and fixing some of the glaring (i.e.. most easily compromised) security holes on your network and then what to do after that. There are numerous other papers on the SANS Reading Room website (http://www.sans.org/infosecFAQ/index.htm) that can provide a more thorough examination of each topic in much greater detail.

Copyright SANS Institute
Author Retains Full Rights

AD

Automate more Web application scanning.
watchfire

Lyde Andrews
GSEC Practical Assignment Version 1.2f

Title: "OK, So I Need Security. Where Do I Start?"

If you're anything like me, you've always heard about how important security is and how a secure infrastructure is so crucial. You've probably also been rather overwhelmed with all the terms, systems, and marketing material proclaiming how one vendor's system can solve all of your security problems. However, the one thing that you're not sure of is where to start. With all the threats, potential security holes, and snake oil solutions being sold, a core question continues to linger, "What can I do right now to at least begin securing my network?"

This paper is not designed to be an end-all solution to your problems, but it can be used to begin identifying and fixing some of the glaring (ie. most easily compromised) security holes on your network and then what to do after that. There are numerous other papers on the SANS Reading Room website (http://www.sans.org/infosecFAQ/index.htm) that can provide a more thorough examination of each topic in much greater detail.

When taking steps to protect your network, understand that there are three major security objectives that you need to account for. These are:

- Confidentiality – making sure that private data stays private
- Integrity – insuring that data and systems have not been altered in an unauthorized manner.
- Availability – insuring that systems and data are there when needed

Note: The National Institute of Standards and Technology (NIST) adds two additional objectives to the list: Accountability (all actions must be traceable) and Assurance (insuring that the other elements above are in place) [1]. As you evaluate different tools, systems, and processes, be sure to apply them within the context of these security objectives.

Five steps that you can take to make your network more secure.

1. Identify and protect your most valuable assets first

When starting down the road of network security, it's tempting to reach for the proverbial, "low hanging fruit" by focusing on those systems that you are more comfortable in making more secure. You may have a higher comfort level in applying a service pack on NT than shutting down an IP service port on UNIX, but one of the first areas that you want to focus on is to identify and protect those systems that maintain your most valuable assets in terms of data.

For example, the company that I work for has over sixty NT servers; however, the company's core financial, client, and employee data resides on two UNIX servers. In this case, it probably makes more sense to initially focus on the UNIX servers before tackling the NT systems.
It's good to have the most secure NT print servers possible, but you may want to focus first on locking down the network's core business systems. During this step, make sure to get feedback from senior management in terms of what they view the most critical systems to be from a

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

business perspective, since what you deem crucial may differ slightly from how they view the situation.

2. Secure the perimeter

Make no mistake about it; you ARE being probed. If you don't believe this and want to prove it to yourself, download a copy of a personal firewall, such as ZoneAlarm (www.zonelabs.com), install it on a PC directly connected to the Internet (dial-in, cable, DSL, etc.), then turn on logging, sit back and watch. As you will see, within 48 hours chances are that you will have been probed multiple times. The same thing is happening at your company, so make sure that you identify all of the access points to your network and protect them.

Firewalls:

One of the primary ways to protect the perimeter is to install a properly configured firewall solution (notice that I did not say to buy a firewall and install it using the default configuration entries). Once you have a secure firewall in place, identify and route as many external network entry points into your firewall as possible. You can have the most solid firewall solution, but if a hacker can easily enter through your dial-up server (or even worse, a modem directly connected to one of your systems), then the firewall will be virtually useless. As Bruce Schneier states in his book, "Secrets & Lies," one of the best ways to defeat a firewall is just to go around it [2]. Once you have consolidated as many connections as possible through the firewall, reexamine your configuration again to insure that the connections are properly protected.

Intrusion Detection Systems:

In addition to a solid firewall solution, an Intrusion Detection System is a very important tool that can monitor the network for suspicious activity and alert you of any potential access compromises. In there publication entitled, "Intrusion Detection Systems," NIST identifies three main types of Intrusion Detection Systems with each type having its own distinct set of advantages and disadvantages. These three main types are:

- Network-based IDSs
- Host-based IDSs
- Application-based IDS [3]

There are many companies offering Intrusion Detection Systems that range from very good to deplorable. Make sure to investigate IDSs in detail before planning a full-scale deployment. SNORT is one example of an excellent open source network IDS (www.snort.org).

3. Secure the core systems

Once you have protected both your most critical systems and protected your perimeter, the next step is to provide protection for your core/internal systems. The main point to remember is that the default installation of ANY Operating System is NOT secure!

Microsoft Windows NT/2000:

There are several actions that you can take to make Windows NT and Windows 2000 more secure. Some of these are:

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

a) Service Packs and hotfixes – It takes some effort to keep up to date on the latest service packs and hotfixes, but Microsoft has provided a tool called Qchain (http://support.microsoft.com/support/kb/articles/Q296/8/61.asp) that allows you to install multiple hotfixes without having to reboot after each install (even though you will still need to reboot at least once).

b) Harden your system – Again, the default install is NEVER secure!
If installing a new server, determine what its specific role will be and then turn off/uninstall any services and ports that are not needed. Microsoft also has very good checklists for setting up both Domain Controllers and member servers. For example, the checklist for NT 4.0 member servers is located at: http://www.microsoft.com/technet/security/mbrsrvcl.asp. Just be sure to customize the checklist to meet your own specific needs.

Microsoft has also recently released a tool called HFNetChk that enables an administrator to check the patch status of all the machines in a network from a central location. It covers NT 4.0, Windows 2000, IIS, SQL, and IE 5.
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/tools/hfnetchk.asp
Another excellent reference for hardening Windows 2000 servers is Philip Cox's "Hardening Windows 2000" [4]. In this paper, he goes into greater detail regarding installation, system policies, service removal, and tightening TCP/IP.

c) Auditing
In order to insure that unauthorized activity is not occurring on your systems, you need to enable auditing. Whether it's detecting unauthorized activity or just proving to your users that "the network" didn't delete their files, it is crucial that you enable auditing for events such as file creation/deletion, failed login attempts, notification of users trying to access prohibited directories, etc. Just remember that auditing doesn't do you any good if you do not monitor and review the audit logs regularly.

d) Password and account policies
One of the most common ways intruders get access into the network is through exploiting existing user accounts along with their associated passwords. By enforcing strong passwords and account policies you can significantly reduce the chances of intruders gaining access to the network. One way to effectively reduce the chance of someone either stealing or guessing passwords is to implement account lockout, which locks a user's account if someone enters the wrong password a specified number of times. This measure will help prevent brute-force password attacks.

You can enforce stronger passwords by using tools such as passfilt and passprop, but be sure that you have thoroughly tested them before implementing them in production. For example, if you enforce strong passwords through the use of passfilt then systems that use pass-through authentication (ie. simultaneous logins to Novell and NT) may not function properly.

You can also test the relative strength of users passwords by using password-cracking tools, such as L0phtcrack. Their newest product is LC3 http://www.atstake.com/lc3, and it can

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

crack virtually any NT password within a few weeks. However, one productive use of these tools is to effectively determine how vulnerable the user account passwords are.

e) Vulnerability scanners

There are a number of tools on the market that can assist you in identifying areas of vulnerability on the network. These scanners can look for systems that have not been properly updated with the necessary updates, identify open service ports that may pose a potential threat to attack, and a number of other useful items depending on what specific scanner is used.

Products such as Retina (http://www.eeye.com/html/Products/Retina/index.html) and others can help in identifying and resolving many of these vulnerabilities. Again, you will be amazed at how many of these problems would be fixed just by keeping current on Service Packs, hotfixes, and disabling unneeded services and ports.

Special Note of Caution: Make sure that you get written permission from a senior member of management BEFORE you run these tools (password crackers and vulnerability scanners)! There are some scary stories of well-intentioned administrators who found themselves in deep trouble because they did not get the proper authorization beforehand.

UNIX:

Even though Microsoft tends to get its fair share of the spotlight when it comes to security flaws, there are a number of areas where UNIX can also benefit from some healthy due diligence. Just as there are password-cracking tools for NT, there are also similar tools for UNIX.

Two of the most well known password-cracking tools for UNIX systems are Crack and John the Ripper (or just "John"), which looks at the contents of the password file on UNIX and attempts to make educated guesses regarding the most commonly used passwords. These small, easy-to-use tools can apply over 2400 rules to a dictionary list to guess passwords [5]. However, there are several ways that you can protect your UNIX systems against these types of threats. Some of these are:

- Enforce strong passwords by using tools such as passwd+
- Maintain a solid password policy (ie. password expiration, etc.)
- Use shadow files, which stores encrypted passwords in a separate file from the default password file (etc/passwd)

Another step than can be taken to strengthen the security of both UNIX and NT systems is to identify and remove unneeded IP service ports. For example, if you are not using any type of email programs on your UNIX systems, then you would want to insure that port 25 is not open. You can run a port scanner utility that will identify any open ports on your systems (UNIX and/or NT).

Desktops:

When it comes to protecting your desktops from unauthorized access, one of the main areas to focus on from a configuration standpoint is to turn off file and print sharing! By disabling this feature, you prevent most of the desktops from broadcasting their existence and, therefore, opening themselves up to attack. Just as with other operating systems, it is imperative to stay

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

current on service packs, hotfixes, and other security updates. Also, you can save yourself many a sleepless night by installing and maintaining an updated version of virus protection software. There are many excellent virus protection systems on the market (my personal favorite is Trend – www.trendmicro.com) that can provide broad coverage across desktops, servers, and e-mail systems.

4. Simplify

As a rule, the simpler network is easier to manage and secure than the more complex one. When I first started work at my company, it had three different connections to the Internet with three different firewalls (Border Manager, Guantlet, and PIX). Even though some people could try to claim that this combines the strengths of the three systems, it actually combines all the weaknesses of these systems since hackers could exploit the weakest link or whichever is easiest for them to break into.

Some people proclaim that having a complicated network helps to confuse a would-be hacker. You will also hear people state that since they are not a big company then no one would be interested in gaining access to their network. The main point to keep in mind in this regard is that "Security through Obscurity" does not work! Remember the earlier example of connecting a PC directly to the Internet and installing ZoneAlarm? If you have a presence on the Internet (and even if you're not), you will be probed. Bruce Schneier succinctly states it, "Complexity is the worst enemy of security" [6]. The overall point is that the simpler your network is, the better you will be able to understand, manage and protect it.

5. Continue learning

The information that I have covered here does not even begin to show the tip of the iceberg. Security is such a vast subject and covers so many different areas that it is impossible for any single individual to know everything. I'm not trying to slap down some shameless plug for SANS, but if you're serious about understanding the threats, vulnerabilities, and solutions to overcome your network's security issues, then SANS training is a solid, non-vendor based organization that will provide objective assessment and evaluation of what solutions work and which do not. They also offer certifications corresponding to the different systems that many companies are looking for when evaluating candidates, so these training courses and certifications can also significantly increase your marketability in the industry (which never hurts!).

Summary:

So there you have it – five steps that you can take right now to begin securing your network.

1. Identify and protect your most valuable assets first
2. Secure the perimeter
3. Secure the core systems
4. Simplify
5. Continue learning

As I stated earlier, these steps are not the final destination, but they will be a good start to establishing a secure network environment. While you are following these steps that are focused

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

on directly improving the network, there is one other recommendation that I would make as you move along the path in understanding more about security.

Don't try to go it alone; get professional help. If no one in your company has any security experience then do not try to tackle the problem alone. There are just too many vulnerabilities and the tools that are available to be used against your network are too easy to use even by inexperienced people (ie. script kiddies). Just be sure to verify that the security company that you are dealing with has a solid, proven reputation. If all a security consultant is going to do is come into your network and run some basic vulnerability scanners that he or she downloaded from the Internet then find someone else. You want someone who is going to take the time to understand your organization, your network configuration, and your current processes before they bring out some fancy tool.

Understanding security and implementing a secure networking infrastructure can be daunting, but if you take the time to understand your network, fix the major entry points and core systems, and then change your processes to incorporate security into all phases of your projects, then you will have made great strides in providing a solid, secure networking environment.

© SANS Institute 2001, Author retains full rights.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Appendix:

Hyperlinks to tools mentioned:
Zone Alarm (personal firewall)– http://www.zonelabs.com
SNORT (IDS) – http://www.snort.org
QChain (Microsoft hotfix installer) –
http://support.microsoft.com/support/kb/articles/Q296/8/61.asp

Windows NT 4.0 Member Server Configuration Checklist -
http://www.microsoft.com/technet/security/mbrsrvcl.asp

HFNetChk (Microsoft security assessment tool)-
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/tools/hfnetchk.asp

LC3 (password-cracking tool for NT)- http://www.atstake.com/lc3
Retina (vulnerability scanner)- http://www.eeye.com/html/Products/Retina/index.html

Crack (password-cracking tool for UNIX) –
ftp://ftp.cerias.purdue.edu/pub/tools/unix/pwdutils/crack

John the Ripper (password-cracking tool for UNIX) – http://www.openwall.com/john
Trend (virus protection software) – http://www.trendmicro.com/

Bibliography:
1. "Underlying Technical Models for Information Technology Security". 15 May 2001. URL: http://csrc.nist.gov/publications/drafts/UnderlyingModels-ITSecv0.2.doc (29 June 2001): 4-5

2. Schneier, Bruce. Secrets and Lies. New York: John Wiley and Sons, Inc., 2000. 190

3. Bace, Rebecca and Mell, Peter. "Intrusion Detection Systems". August 2001. URL: http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf (21 August 2001): 16-20

4. Cox, Philip. "Hardening Windows 2000". 25 May 2001. URL: http://www.securityfocus.com/data/library/hardenW2K12.pdf (27 June 2001): 18

5. Scambray, Joel. Hacking Exposed, Second Edition. Berkeley: McGraw-Hill, 2001: 341

6. Schneier, Bruce. Secrets and Lies. New York: John Wiley and Sons, Inc., 2000. 372

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 19th, 2013

Upcoming SANS Training

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

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