GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Basic Novell Netware Security – By Jeff Haynie

Novell's Netware has enjoyed success as the top operating system in the file and print server arena. **Novell Netware** was designed with file and print serving in mind and handles both with great ease. Early versions of **Netware** primarily use the ***IPX/SPX*** protocol, which has the advantage of keeping the OS free from attacks via the ***Internet*** (except for very sophisticated methods that are beyond the scope of this paper). Consequently, most **Netware** exploits are run internal to the organization. However, as **Netware** begins to use **TCP/IP** as the protocol of choice it will soon face many attacks similar to those used against **Unix** and **Windows NT** systems.

Novell's Netware has a proven record of dependability and security but like most operating systems, it also has faults. This paper focuses on the past and present weaknesses of **Netware** and suggests ways to secure **Novell's** Operating System and environment.

1. Network Security Basics

Physical Access:

The security of a network is directly proportional to the competency of the system administrator. The foremost concern for any network administrator is physical access to the servers and the server room. Without basic server protection you will have little success in preserving the safety of your network's data.

To illustrate the danger, suppose an administrator fails to lock the server's system console. A hacker can completely compromise the server in a manner of minutes with access to the server console.

Easy access to your **Netware** server(s) will greatly enhance an attacker's ability to:

- Gain supervisor access
- Create back doors, bogus user names and passwords
- Obtain usernames, crack passwords
- Change configuration files
- Load "Trojan Horse" programs

On **Netware** Version 3.x machines, an intruder can boot from a floppy and delete the **Netware** Bindery. Once deleted, the intruder can restart the server, then **Netware** will detect that the Bindery is missing. **Netware** will recreate it and the new Bindery will be minus the security protection on the files and directories.

© SANS Institute 2000 - 2005, Author retains full rights.

Simple procedures and a security policy can help detect and eliminate physical attacks. For example:

- Lock down or disable floppy and CD-Rom drives and apply password protection to the **CMOS** on your server.
- Limit server access to only a select few by placing it in a secure location behind a locked door.
- Keep backup tapes in a secure offsite location.
- Keep manual log files for all system changes, like software and hardware upgrades.
- Ensure console log auditing is in place and operational on the server(s). Use **Netware's AUDITCON** for full auditing capabilities. There are third party solutions for logging file and system changes.
-

If your physical protection is not adequate, then it can be difficult to ascertain where an attack originated, and thus make the log files essentially useless.

2. Account Security:

Passwords:

Login passwords are the first line of defense against attacks on your network. Part of the administrator's job is to educate the user about the necessity of security and what makes an acceptable password choice.

Follow these password guidelines:

- Users often select less than ideal passwords. They use their children's, spouse's or pet's name, birthday, or some other easily guessed password. To defeat password cracking programs administrators should enable stringent password requirements and controls. ***See Appendix A for Utilities.***
- Passwords should be 8 or more characters long and should include letters, numbers and special characters.
- Enable intruder lockout on all user accounts and require the account to be unlocked by an administrator. ***Intruder Lockout*** is a great deterrent to password cracking and is the first notification of possible nefarious activity.
- Account time and network restrictions should be set and enforced. Time restrictions offer the ability to limit the hours a user may login to the network. You can restrict network access by groups, Network card address on a per user basis.
- Make a habit of viewing console log files daily. All intruder

© SANS Institute 2000 - 2005, Author retains full rights.

lockouts will appear in the console log.

User Configuration:

Many times an error in user configuration allows a system to be compromised. To prevent this:

- Use the "least privilege principle," only allow users the minimum rights necessary to perform their duties.
- Avoid adding specific individual rights to files or directories when possible. It is much easier to change and audit the rights for a group than for each individual account.
- There are several third party tools that allow you to audit rights for users, groups and other **NDS** objects. Hidden objects are especially of concern to an administrator. These tools can detect and eliminate these security problems.
- Unfortunately, the default version of Netware is not secure when it is first installed. You should add all necessary updates and patches immediately. For example **Netware** creates a **Guest** account during installation. This account should be removed or disabled immediately.

3. Advanced Protection:

Sometimes it is necessary to implement stronger methods of authentication for example:

- *Biometrics* - Fingerprint or retinal scans are types of unique personal identifiers that provide Biometric authentication.
- *Tokens* - A smart card is an example of a token method for secure authorization.

Current versions of **Netware** support biometric and token authorization methods.

4. Huns at the Gate!

There are far too many **Netware** exploits to cover in detail in the limited space of this article. Instead of offering a step-by-step *"How to Hack Netware"* the following topics display a few areas of concern for administrators.

A. Specific Attacks:

Physical security is just the first basic step in securing the **Netware** network. An administrator must be concerned with Viruses, worms, Denial of service, packet sniffing, spoofing, password guessing attacks,

© SANS Institute 2000 - 2005, Author retains full rights.

administrative flaws (human error), and exploitable bugs in the operating system. It is necessary to have procedures and a security policy to handle these issues.

1) Spoofing Attack:

Early versions of **Netware** (3.x) can be vulnerable to "*Spoofing Attacks*." This is easily accomplished by running **userlist /A**. Since any user has the ability to run this program it can reveal much about the network. Results from this program give you all user names and Network Card Addresses connected to the server. Once you have a Network Card Address it is simple to place it in the **NET.CFG** file. Add the network card driver, the Network Card Address you wish to spoof, **NET.CFG** and other files on a bootable floppy and you can fake your address on the Netware network.

Therefore you should move **userlist** from the **Public** folder on the **SYS** volume and place it in a folder only visible to administrators. This in itself will hinder the intruder from attaining user ID's and Network Card Addresses.

2) Viruses and Worms:

Internet connections offer great rewards but also great dangers. New viruses and worms are appearing almost daily and with users connecting to the Internet the LAN is exposed.
Install and maintain virus protection software for your servers. It is imperative that administrators continually update the latest virus patterns on the server(s) and user's workstations. Without the latest protection you're an accident waiting to happen. ***See Appendix B for a list of Antivirus Programs.***

3) Denial of Service:

These attacks apply to any attack that causes a denial of server services. There are several **DOS** attacks against **Netware.** The most dangerous one uses a spoofed packet that has its source and destination address the same. Many systems have fallen victim to this attack that was originally found to affect Windows 95 machines. No fix has been found as off this time, but you can check the following address for updates: www.njh.com/latest/9711/971120-03.html. Netware Servers won't be affected by this attack until they begin running IP protocol.

Another example is a user printing an extremely large file multiple times to a printer on the **Netware** server. This can overflow the **SYS** volume on the server and cause it to crash.

© SANS Institute 2000 - 2005, Author retains full rights.

To overcome this set space threshold limits on the server's volumes, when the threshold is reached the administrator is notified and can attempt to resolve the ***DOS*** problem before the server fails. ***See Appendix C for a list of Denial of Service Attacks.***

4) Service Exploits:

Turn off and disable all unnecessary remote access services running on your **Netware** servers, such as ***FTP*** and ***telnet***. While ***FTP*** is convenient it can be a nightmare for an administrator. Often times ***FTP*** is not configured correctly on servers or default settings on installations allow lax access privileges.

In the case of **Netware 5** newer is not always better. **NetWare 5** allows remote access to the server via telnet. ***Telnet*** uses clear-text passwords and are easily readable by any protocol analyzer. ***Telnet*** should not be enabled.

5) Remote Exploits:

Netware's Remote Console or **Rconsole** is another tool often configured incorrectly and can allow unauthorized access to the server. **Rconsole** can be used to perform duties as if the administrator was at the actual server console. The danger in using **Rconsole** is that the password encryption is not very strong and some administrators fail to change it from the default password. If an administrator leaves just one server's console unlocked, a hacker with **Rconsole** and the default password could easily gain supervisory access to the server.

If possible, remove **Rconsole** altogether. If you insist upon using **Rconsole**, you should change the password from the default and enable encryption of the password.

6) Internet Exploits:

Netware has developed several new IP protocol dependent products including a Web Server. To reduce the chance of break-ins from the Internet, consider using a firewall and proxy server. Look for more **Netware** attacks to come in the future via the Internet.

When possible you can use Network Address Translation (NAT) to map IP addresses from one group to another. Network Address Port Translation (NAPT) allows the Administrator to connect private addresses to a single

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

IP address by translating internal network IP addresses and their TCP/UDP ports into a single network address with its corresponding TCP/UDP ports. This provides the ability to hide or mask all internal addresses.

7) Software Security:

If security is critical for users consider using NCP packet signature. NCP "level 3" allows the ability to apply strict packet signature options. With this enabled, all packets are encrypted similar to a virtual private network. The advantage of NCP is the secure encryption and decryption algorithms it uses to encode and decode packets transferred between the clients and servers. Be aware this security feature comes with a performance cost and greatly slows down the sending and receiving of packets.

8) Software Bugs:

Like other operating systems it is important to keep your **Netware** server updated with the latest software patches available. Programming errors, security holes are just a few of the maladies that can be remedied.

An example of a software exploit is the use of **LDAP** version 1. The advances offered by **LDAP (*Lightweight Directory Access Protocol*)** are very appealing. However, version 1 of **LDAP** uses clear-text passwords. Any applications that use **LDAP** version 1 should be upgraded to use **LDAP** version 3. **LDAP** version 3 is supported by later versions of **NDS 7** ***(Netware Directory Services)*** and **NDS 8**.

Early versions of **Shiva** ***LAN Rover*** contained a dangerous bug. All a hacker would need is a list of users on a **Novell** server (remember **nlist**?) and wait for a user to disconnect from the **Shiva** without logging out. **Shiva** doesn't drop the connection, so the next connection will be logged in as the person who logged out incorrectly.

9) Password Cracking:

Like **Microsoft Windows NT** and **Unix**, **Netware** is susceptible to a number of password hacking programs. One notable version is the "Pandora Toolbox" program. "Pandora Toolbox" has a number of utilities which aide in the compromise of a **Novell Netware** server. ***Project Pandora***, by Simple Nomad and Jitsu-Disk, was designed to extract user info and the password hash from **Novell's NDS** files and permit password recovery through the use of a brute force or dictionary attack. "Pandora Toolbox" utilizes several programs included with the **Novell Netware** installation. In later versions ***Pandora's*** crackers could spread the attack

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

over multiple computers greatly decreasing the time needed to extract all passwords from the **NDS**.

Another program in the cracker's bag of tricks is **chknull.exe** file. This program checks for any user account using a "null" password. These tools are dangerous in the wrong hands but can aide the administrator in the detection of password omissions or the use of weak passwords.

Armed with the knowledge of past and present exploits, a **Netware** engineer is better prepared to detect, discover and prevent system compromises.

References:

Anonymous "Maximum Security - A Hacker's Guide to Protecting Your Internet Site and Network, Second Edition" August 1998

McClure, Stewart; Scambray, Joel; Kurtz, George "Hacking Exposed: Network Security Secrets & Solutions" 1999

Nomad, Simple "The Hack FAQ" 6 September 1999
URL:http://www.nmrc.org/faqs/hackfaq/hackfaq-19.html#ss19.1

Novell -"Protecting Your Network Against Known Security Threats" November 1997
URL: http://developer.novell.com/research/appnotes/1997/november/06/03.htm

Nomad, Simple "Pandora, the SATAN of Netware" 2 December 1999 URL:
http://www.nmrc.org/pandora/faq.txt

Appendix A:

The following URLs have some excellent examples of Password and security tools and tips.

http://www.sans.org
http://www.safeword.com/nwcspec.html
http://www.intrusion.com/Products/analystnt.shtml
http://bindview.com/products/bv-Control/NDS/index.html

Appendix B:

The following URLs have some excellent examples of Anti Virus software.

http://enterprisesecurity.symantec.com/products/products.cfm?productID=28
http://www.antivirus.com/products/svrprt/

© SANS Institute 2000 - 2005 Author retains full rights.

http://www.novell.com/products/vs/quicklook.html

Appendix C:

The following URLs have some excellent examples of ***Denial of Service Attacks***.

http://www.nmrc.org/faqs/hackfaq/hackfaq-23.html#ss23.1
http://www.nmrc.org/faqs/hackfaq/hackfaq-23.html#ss23.2
http://www.nmrc.org/faqs/hackfaq/hackfaq-23.html#ss23.3
http://www.njh.com/latest/9711/971120-03.html

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.