



NCI-Frederick Communications
ABCC, SAIC Frederick
Frederick, Maryland

Computer Security Policies and Recommendations

Services Installed on NCI-Frederick Computers and Servers (i.e. HTTP, Telnet, FTP)

- Services such as, but not necessarily limited to, HTTPD (web server), TELNETD, and FTPD, shall not be on personal computers or servers unless approved and registered by the LAN and Security Group and CSS.
- All Administrators that require HTTP, Telnet, or FTP servers to run on the NCI-Frederick network must report these systems to the NCI-Frederick LAN Office for registration and approval.

Anti-virus Software Configuration at NCI-Frederick

- All personal computers and servers must have anti-virus software (standard NIH approved with site license) installed and must be configured to be updated and upgraded on a weekly or more frequent basis. The NIH has site licenses for anti-virus software for the Windows, Macintosh, Linux, and Solaris operating systems.
- Network Associates anti-virus software is the current NIH standard for personal computers (Macintosh, Microsoft Windows, and Linux). In light of this, new computers should not be purchased with other anti-virus software, such as Norton, since it cannot be updated with new virus definition files and programs through the NIH site license.
- Standard procedures will be implemented for installing and configuring anti-virus software on all personal computers at the NCI-Frederick campus.
- For more information about using Anti-Virus software at NCI-Frederick, see <http://comm.ncifcrf.gov>.

Malicious Attacks against NCI-Frederick Network Computers

- In an event of a computer attack on NCI-Frederick computers (worm, virus, denial-of-service, etc.), the ABCC and CSS shall pursue a joint effort in determining priorities and procedures for combating the attack and allocation of resources.

NCI-Frederick File Sharing Security

Description

This guidance is intended to prevent hacker attacks on NCI-Frederick file servers. The purpose of file servers at NCI-Frederick is to provide for the transfer and storage of files for legitimate users. However, malicious users can take advantage of incorrectly configured file servers to store hacker programs, copyrighted data, and/or pornographic material without the knowledge of NCI-

Frederick users. As a result, other NCI-Frederick systems can be compromised and used for malicious purposes, causing embarrassment to NCI-Frederick.

Recommendation

The guidance below provides solutions to minimize these problems at NCI-Frederick while causing no disruption to the NCI-Frederick mission.

The transfer and storage of files has been commonly performed at NCI-Frederick by:

- Anonymous access to File Transfer Protocol (FTP) servers
- Community access to Network File Sharing (NFS) exports
- Community access to Server Message Block (SMB) shares

Unfortunately, anonymous/community access on file servers often is configured to allow for global read/write permissions to the servers/exports/shares. The following guidance directs administrators at NCI-Frederick on how to apply controls that can decrease vulnerabilities in file servers.

1. **Anonymous FTP servers shall be discouraged. Where required, all directories shall be either read only, write only, or restricted by IP address.** When systems/users need the ability to exchange files, they should set up a user account with a secure password and make it available to those users they work with. For the UNIX platform, it is recommended that the FTP service be protected through the use of TCP Wrappers.
2. NFS exports shall be restricted to only NCI-Frederick host computers. The host list shall be the minimum required to support the mission.
3. SMB shares for both servers and local user drives shall be protected from the outside reading or writing. For Windows 9X systems, a password shall be supplied for each share. For Windows NT/2000, all shares will be controlled by password-protected accounts.

For additional guidance on this matter, contact the ABCC Helpdesk at x5555.

Web Based Email

Description

Web based email (such as, but not limited to, Hotmail, AOL, Yahoo!, or Excite accounts) poses a threat to the NCI-Frederick campus by allowing an entry point for mail that circumvents current security controls that are in place to prevent the spread of malicious code, viruses, and worms. Unfortunately, we currently do not have control over web-based email that enables users to read personal email and open attachments on their government desktops. By allowing this type of access to online web based email accounts inside our network, we are providing a gaping hole for malicious software, Trojan horses, and other viruses and worms into and out of our environment without our knowledge.

Recommendation

It is therefore the recommendation at this time by the NCI-Frederick Security Team that NCI-Frederick users do not use web-based email on their government machines or while logged into the network from their dial-up account.

Instant Messaging**Description**

Instant Messaging is a means by which NCI-Frederick users communicate in a chat-like atmosphere to coworkers and friends from their government systems. There are many security and productivity concerns that need to be addressed if NCI-Frederick users are to install and use Instant Messaging on their government systems. A few of these are:

1. When using Instant Messaging for business purposes, employees are often not aware that they are sending their conversations across a public network.
2. While communication is in transit, messages are stored as open text in server buffers at services such as AOL and Yahoo!. Not only can packet sniffers read Instant Messaging content, but also unencrypted logs of conversations can easily be stolen.
3. Instant Messaging software announces information, including IP address, about the user and his machine whenever he logs on. This opens up the machine to potential targeting by malicious attackers and advertises to the world that it is running Instant Messaging software from a government registered IP address range.
4. Because of the file transfer capabilities, viruses can be easily transmitted from one machine to another. As people are copying files from machine to machine, any virus that they've picked up along the way can propagate. The issue here is there is no way to filter what types of files are being transferred to computers running Instant Messaging software. Attachments and file transfers cannot be blocked and machines may become infected through a hole in our security architecture, without our knowledge or control.
5. Users may end up with shared directories and/or file server capabilities on their machines. This may cause both privacy issues and bandwidth issues. If the service discovers that your machine has a lot of disk space and a large amount of bandwidth, you could end up not only downloading a file you wanted, but also then becoming the server for others who want to download that file. Even AOL Instant Messenger, which is chat based rather than file based, gives you the option to become a file server and contains a directory that is shared by default.
6. As business users add unauthorized clients to their machines, they can open up their networks to unsecured traffic. While the administrator think that he is safe (or at least relatively so) by setting up firewalls and intrusion detection, the user has initiated a connection that will get through the firewall, and allow not only conversation, but also file movement. Suddenly there is a large gap that potentially harmful traffic can flow through.

Recommendation

It is the recommendation of the NCI-Frederick Security Team to discourage the use of Instant

Messaging programs on NCI-Frederick government computers or while accessing the network through their dial-up accounts.

Secure Shell Suite (SSH)

Description

SSH is a client and server for secure encrypted communications. It is designed to replace FTP, Telnet, and the r-services (rlogin, rcp, rsh). There are two parts to SSH: the client program on the machine the user is connecting from, and the server program on the machine the user is connecting to.

FTP - The File Transfer Protocol (FTP) was designed to move files between machines to increase collaboration and to shield users from the differences in the way operating systems handle files. By design, FTP is an unsecured protocol. The transfer and authentication processes are unencrypted. Risk: passwords can be intercepted and used for malicious intent.

Telnet - Allows remote users to log on to the system and run console programs using the command line. Telnet is not a secure protocol and passwords are sent across the wire in plaintext. Risk: potential for unauthorized remote command line access and passwords sent unencrypted across the network.

Rlogin - Remote Login allows an authorized user to login to other UNIX machines on a network and to interact as if the user were physically at the host computer. Once logged in to the host, the user can do anything that the host has given permission for, such as read, edit, or delete files. Rlogin uses a file `.rhosts` that resides on the host machine and maintains a list of terminals allowed to login without a password. Risk: if this list is compromised, any machine can be added to this list and log in with permissions as if physically at the host computer. Communication is in plaintext and can be easily viewed without the knowledge of the user.

Most computer systems rely on passwords as their first line of defense against intruders. Telnet and similar applications send all information, including passwords, in an unencrypted form between computers. This allows would-be intruders to sit and watch the network, waiting for passwords to go by on network traffic. Special software tools called sniffers make eavesdropping a popular method for breaking into computers. SSH protects the user from eavesdroppers by encrypting all data between the client and server machines, including the user's password.

Recommendation

It is the recommendation of the NCI-Frederick Security Team for all campus users to use the Secure Shell (SSH) Version 2 Suite in place of Telnet, FTP, and Rlogin. If you log in to your computer accounts remotely, you should be using SSH, unless you are already using a Virtual Private Network (VPN).

Making an SSH connection requires that you have an SSH client on your local computer. If you already have a full version of SSH installed on the machine, you are ready to go. If not, see [Obtaining, Installing, and Configuring OpenSSH](http://comm.ncifcrf.gov) at <http://comm.ncifcrf.gov>.

Wireless Technologies

Description

With the popularity and proliferation of wireless communication products on the market today, it is not surprising that NCI-Frederick users are interested in installing wireless network equipment in their environments. Unfortunately, there are many issues that need to be addressed and planning that must take place prior to installing wireless products in your environment.

Recommendation

Wireless technologies are relatively new and due to communication interference issues and security concerns, it is the recommendation of the NCI-Frederick Security Team for wireless products not to be added to the network without prior review and approval by the NCI-Frederick LAN Office. Network ESSIDs, hopping sets, frequency settings, and Wired Equivalent Privacy (WEP) levels need to be approved and registered through the NCI-Frederick LAN Office.

For more information and an Application for Installation, please see the [NCI-Frederick Wireless Policies](http://comm.ncifcrf.gov) at <http://comm.ncifcrf.gov>.