

# The Canaudit Perspective

Volume 4 - Issue 6  
(part 2)  
June 2003

## Special points of interest:

- [Gordie's top sixteen things to do to protect the UNIX operating system](#)
- [Network Segmentation](#)
- [Upcoming Events](#)
- [Learn more at our Boot Camp](#)



## **"Gordie's top sixteen" things to do to protect the UNIX system.**

Once the data is protected, the operating system needs to be hardened to prevent hackers who penetrate the network from gaining access to the machine and then elevating their capabilities to root level using exploits. Here are "Gordie's Top Sixteen" things to do to protect the UNIX operating system.

1. Ensure that all accounts have a password and that the password is not equal to the account name.
2. Ensure that trust relationships are eliminated. Seek out all copies of .rhost files, especially the root .rhost file and remove them. Then create a blank.rhost file, place it in the root directory and set the permissions to no read, no write and no execute for the owner, the group and the world. This will prevent a hacker from placing a .rhost file into the root directory and using that file to escalate their capabilities.
3. The hosts.equiv file also can be used to create a trust relationship. Empty this file and ensure that it is also properly protected.
4. In conjunction with the items above, disable the rlogin, rexec and rshell services in the Inetd file. The administrators normally object to this as they say the software will not run. We suggest that they use secure shell and tcp wrappers to create secure connections between servers. (This requires testing prior to implementation). The software vendor may need to be contacted to assist in this effort. Several of my clients have had difficulty getting the vendors to cooperate. Recently we found a solution that makes the vendor realize that you are serious and that they have to perform. If the vendor states that the software will not run without trust relationships and they are unwilling to provide a solution in a reasonable timeframe, have your general counsel send the CEO and chief legal counsel of the vendor a notice that their software is placing your environment at risk, that they were advised of this and refused to provide a solution. Therefore should there be a computer incident relating to the use of trust relationships, then your organization will hold the vendor responsible. Since the vendor was notified and generally accepted security principles mandate the elimination of trust relationships, the vendor may be deemed negligent as you provided them with prior knowledge of the risk and they refused to correct the problem or work towards a solution. Is this playing hardball? Yes, it certainly is. However, if your data is stolen because of a trust relationship and your customer data is compromised as a result, you can expect a class action suit. I don't think that a jury of 12 of your peers would accept an excuse of "The vendor software would not run if it the machine was properly secured". In fact, your organization, may be held negligent and suffer treble damage as well as loss of reputation and customers.

5. Ensure that the tftp service, which enables guests to connect to the system without authentication is disabled. If tftp is enabled, then all of the world readable files will fall into the hands of unauthorized staff, contractors or hackers as they will be able to freely download them. Also world writeable files could be altered or deleted using tftp. Get rid of this service anytime you find it.

6. Some files contain processes that execute with root capability. The two I worry about the most are the inittab and the crontab. The inittab executes the processes within the inittab whenever you boot the system. The crontab contains processes which run at prespecified times. If the permissions on any of these files are world writeable, then a disgruntled user or hacker could alter the processes to create a new account the next time the processes are run. Therefore check the permissions on all files in the inittab and the crontab to ensure that they cannot be accessed by low level users or through tftp. To launch a modified process in the crontab, you only have to wait until the scheduled task runs at the appointed time. Then your process can recreate a new root empowered account. For the inittab, the system must be rebooted. Therefore launching a denial of service attack against the machine could force a reboot and the execution of the hacker's bogus code.

There are many other UNIX risks, however the ones mentioned above are the most common ones. Ensure that you review this list with your system administrators and assist them in obtaining management approval to implement them. After all, the operating system protects the data and the programs. Without strong controls, your data may be compromised or stolen. (If you need some UNIX audit and Security scripts, [click here](#)).

Once the operating systems are hardened, the next level of security is the network itself. My book, Network Auditing: A Control Assessment Approach covers this quite well. In this article, it is necessary to cover the main points to ensure that the network and network devices protect the servers and the data. The most important control my mind is to segment the network using routers, switches or internal firewalls. **Network segmentation**, used properly, can contain a hacking incident to a single network segment. This limits the damage that can be done when the network is penetrated and increases the likelihood that the intrusion will be detected on a timely basis.

That said, there are some key issues on the network side that must be addressed. One of my biggest concerns is that Simple Network Management Protocol (SNMP) will be active when it is not needed. If SNMP is enabled on your network, tools such as Solar Winds can be used to quickly document the network. Network equipment, servers, workstations, printers and other devices that use a community string (SNMP password) can bleed information if the community string can be guessed or brute forced by Solar winds or other tools.

Many of our clients have a community string of public which enables us to see information such as account names, services running on the machine and network routes that exist. With a community string of private, we can often download network device configurations enabling us to modify the configurations or worse, take control of the network devices. If you are using SNMP on the inside of your network, make sure that the community strings are complex (eight characters long, with a special character in positions 2 through 6. Also, the SNMP password should be changed on a regular basis, especially when there is network staff turnover.

Another control would be to set up a honey pot on the inside of the network. This will identify when a machine is scanned with a product such as Solar winds or Super Scan. I like a free tool called Back Officer Friendly which tells me when my box is being scanned. There are commercial versions of this product and other products that perform the same function. The point to remember here is that normally an SNMP or port scan is one of the first things a hacker will do when they penetrate a network.

I love controls that are free, because that often is the budget for network security. One of my favorite free controls is the ability to use router encryption to encrypt and decrypt data before it is transmitted across

network segments. Encrypting this data prevents hackers and other nefarious people from sniffing accounts, password or data off the network.

Normally, I would cover modems and wireless at this point. However, wireless controls appeared in a previous Canaudit Perspective article and Modems will be covered in next month's issue. Just remember to ensure that modems and wireless connections are minimized and secured.

This article is based on our new seminar Control and Security of Enterprise Wide E-Commerce. An expanded version will be available in my new book, Control and Security of E-Commerce, which is currently in the process of being published by John Wiley and Sons. IT will include a full set of Risk / control tables and audit checklists to assist you with your audit or security review. When you attend one of my Canaudit or Chapter events, I will be pleased to dedicate and sign your copy of this book if you bring it to the class.

Best regards, Gord

If you would like to learn more about how to protect your data including your customer and client information the Canaudit IT Audit and Security Boot Camp is a five-day workshop that covers all the items in this article in greater depth. There are over 1300 pages of material as well as several hands on exercises. This workshop will provide you with the concepts, tools and methodologies you need. We are holding public classes for this course in Fairfax, VA July 21-25, 2003 and Minneapolis, MN October 6-10, 2003. We look forward to seeing you there. For any questions or to register please contact [Jennifer@canaudit.com](mailto:Jennifer@canaudit.com) or 805-583-3723 or visit us at [www.canaudit.com](http://www.canaudit.com)

## UPCOMING EVENTS

It's time to register for one of Canaudit's public classes

**The Ultimate Network Penetration Class**  
(5-days)

[Lake Tahoe, CA - September 15-19,2003](#)

**IT Audit & Security Boot Camp**  
(5-days)

[Fairfax, VA – July 21-25, 2003](#)  
[Minneapolis, MN – October 6-10, 2003](#)

### **Professional Development Weeks:**

**Simi Valley, CA - August 11-14, 2003**

- [Understanding & Preventing Electronic Fraud](#)
- [Control & Security of Telecommunication Networks](#)
  - [Control & Security of Web Applications](#)
  - [Cyberterrorism and Electronic Espionage](#)
- [Computer Forensics For Security and Audit Professionals](#)
- [Control & Security of Wireless Networks](#)

**Minneapolis, MN – October 6-10, 2003**

- [Control & Security of Windows 2000](#)
- [Control & Security of Wireless Networks](#)
  - [Control & Security of Unix](#)
  - [Control & Security of the Internet](#)
- [IT Audit & Security Boot Camp](#)



**Canaudit, Inc.**  
AUDITS • SEMINARS • CONSULTING

P.O. Box 2110 – Simi Valley – California – 93062-2110 - Phone: 805-583-3723 Fax: 805-582-2676 [www.canaudit.com](http://www.canaudit.com)

© Canaudit, Inc. 2003