

DCS

**CENTER FOR NUCLEAR WASTE REGULATORY ANALYSES**

**TRIP REPORT**

**SUBJECT:** System Administration, Networking and Security (SANS) '98 Conference  
(20-1402-158)

**DATE/PLACE:** May 7-11, 1998  
Monterrey, CA

**AUTHOR:** Ray Kotara

**DISTRIBUTION:**

CNWRA

W. Patrick  
CNWRA Directors  
CNWRA Element Managers  
R. Sanchez

NRC-NMSS

J. Linehan  
D. DeMarco  
B. Stiltenspole  
B. Meehan  
~~L. Greaves~~  
K. Stablein  
M. Federline  
M. Bell

SwRI

S. Boyanowski (Contracts)

980623

of 1  
NH15  
WM-11  
4261

Delete  
all distribution  
except  
Files  
PDR

# CENTER FOR NUCLEAR WASTE REGULATORY ANALYSES

---

## TRIP REPORT

**SUBJECT:** System Administration, Networking and Security (SANS) '98 Conference  
(20-1402-158)

**DATE/PLACE:** May 7-11, 1998  
Monterrey, CA

**AUTHOR:** Ray Kotara

### BACKGROUND AND PURPOSE OF TRIP:

The purpose of the trip was to attend select portions of the SANS '98 Conference that are or may be applicable to the CNWRA networking environment. Lectures were held in multiple locations in Monterrey, California. Selections were made in the following areas: Windows NT administration, Unix Security and Unix mail alternatives

### SUMMARY OF PERTINENT POINTS:

**Day 1: NT ADMINISTRATION COURSE**

Overview: Discuss issues on operating system functionality, architecture, boot sequences, network protocols and NT services.

**Day 2: WINDOWS NT DOMAIN AND USER ADMINISTRATION**

Overview: Discussions will include user and group management, user rights, system policies and profiles in both single and multiple domain environments.

**Day 3: FIREWALL MANAGEMENT AND TROUBLESHOOTING**

Overview: Techniques that allow you to fix firewall problems without compromising security.

**Day 4: MANAGING THE TRANSITION FROM SENDMAIL TO QMAIL**

Overview: How to fix Sendmail problems by replacing Sendmail with Qmail.

**SECURE SHELL (SSH) INTRODUCTION TO IMPLEMENTATION**

Overview: How to take advantage of SSH for secure remote access.

**Day 5: UNIX SECURITY TOOLS: USE AND COMPARISON**

Overview: Public domain security tools and how to make them work for you.

## **CONCLUSIONS:**

### **Day 1**

The lecture was very thorough and seemed to focus on presenting a "real world" administrative environment. The following are items of particular interest and relevance to the CNWRA: (i) a loop-back address should be added to the network bindings to alleviate network connection failure messages and hangs; (ii) the NetBEUI protocol relies upon broadcast packets for normal communication and should be disabled when possible; (iii) invoking the command "rdisk /s -" can automate registry backups on a domain server; and (iv) NT files inherit the permissions of the parent directory when they are created which can create confusion when comparing the NT file system permissions to a UNIX equivalent.

### **Day 2**

This lecture highlighted topics that were covered on Day 1 and focused on user administration and associated processes. The following identifies items of particular interest and relevance to the CNWRA: (i) shared drives can be set to everyone/full control since the permissions on the actual directory and files will protect it with a higher level of security than the share; (ii) setting up and modifying the "default user" profile on the Primary Domain Controller (PDC) will ease additions of new accounts; and (iii) installing the Distributed Files System (DFS), a free tool from Microsoft, allows the creation of a virtual central location for all file shares even if they are distributed on multiple servers.

### **Day 3**

The lecture focused on those commercial firewall systems that are currently available to the public and general firewall administration. Although the systems discussed are not used at the CNWRA, the lecture presented a good pro/con approach to selecting a firewall package while keeping organizational needs the primary concern. The following illustrate items of particular interest and relevance to the CNWRA: (i) replacing Sendmail with other mail packages that are considered more secure; (ii) identifying several good SPAM (junk mail) prevention sites on the Internet devoted to keeping track of known originators; and (iii) avoiding the Domain Name Service (DNS) server on NT due to its lack of stability in the current release.

### **Day 4**

This lecture emphasized the recommended substitution of the freeware program Qmail over the traditional Sendmail program that is used on most Unix mail systems. The subsequent lecture presented an in-depth look at Secure Shell (SSH). This product provides secure encrypted communications between two untrusted hosts over an insecure network. This secure communication link can be used to execute commands on remote machines, export displays, and transmit data. The following are items of particular interest and relevance to the CNWRA: (i) enhancing local mail delivery on Unix machines through the use of Qmail; (ii) replacing the standard Sendmail mail agent with Qmail for faster and flexible mail handling; and (iii) providing a link to specific hosts on the Internet with SSH could enable flexible and secure remote access to E-mail, execution/analysis of Unix runs, and file transfers.

## **Day 5**

This final lecture focused on many of the freeware tools available for Unix security and specific procedures for security audits and logging. Tools that are unavailable to the general public were not discussed. The following represent items of particular interest and relevance to the CNWRA: (i) the combination of two tools (Kuang and Tiger) can provide a good foundation for network intrusion prevention and detection; (ii) implementing TCP wrappers is necessary for the prevention and logging of hack attempts; and (iii) installing other utilities that were discussed in this lecture are well worth their constructive feedback on current network security.

### **PROBLEMS ENCOUNTERED:**

None

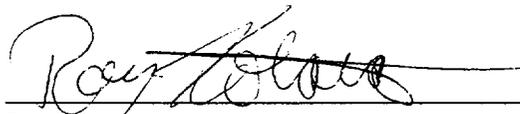
### **PENDING ACTIONS:**

None

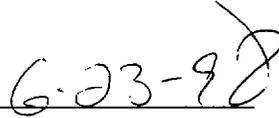
### **RECOMMENDATIONS:**

It is recommended that CNWRA IMS, as time permits, test and or implement the following: (i) reconfigure the NT Domain to eliminate NetBEUI where possible, (ii) follow and implement security enhancements for NT in the "NT Security Step By Step" book, (iii) automate nightly NT Server Registry backups with rdisk and the built in replication function, (iv) replace Sendmail with other more secure, easily manageable, and SPAM restrictive products in a test environment to determine their possible benefit to the CNWRA mail system, (v) test Secure Shell for possible remote access capability at the CNWRA, and (vi) install and use intrusion prevention and analysis tools on the protected network.

**SIGNATURES:**



Ray Kotara  
Network Administrator

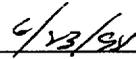


Date

**CONCURRENCE:**



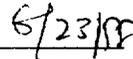
Henry F. Garcia  
Director of Administration



Date



Budhi Sagar  
Technical Director



Date