HP 9000 Security

HP-UX 10.20 and 11.00

Case Study

NAV CANADA

Jeff Baggs and John Richer

About NAV CANADA

1. Canada’s provider of civil air navigation services
2. Operations coast to coast providing air traffic control, flight information, weather briefings, airport advisory services and electronic aids to navigation
3. World’s first fully commercialized system

Environment

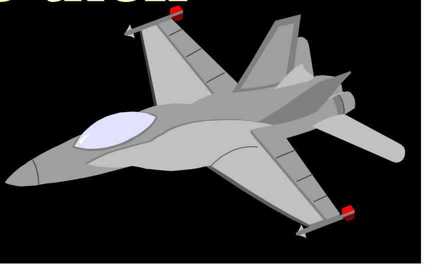
- HP 9000 servers (D, K, N and T classes)
- HP-UX 10.20 and 11.00
- NIS and NFS not used
- Not using Trusted System
- Firewall

Number 1 Vulnerability

- Passwords
- Passwords
- Passwords

Easily guessed Passwords

- Use some password cracking tool such as Crack on a regular basis to find easily guessable passwords.
- Obtain management’s consent before cracking passwords.
- Run a unix script to force users who have easily guessable passwords to change their passwords upon next login.



Script to force users to change password

- Copy file containing login ids of cracked passwords to /tmp/passwd.sh
- Create /tmp/passwd.exscript file:

  ```
  %s/^/passwd -f -x 28 -n 7 /
  ```

- ex - /tmp/passwd.sh < /tmp/passwd.exscript
- Execute /tmp/passwd.sh

Sample /tmp/passwd.sh

```
Passwd -f -x 28 -n -7  user1
Passwd -f -x 28 -n -7  user2
Passwd -f -x 28 -n -7  user3
Passwd -f -x 28 -n -7  user4
```

Two Fence Rule

- Gives you an added layer of protection in protecting Root access
- You have to login as a “normal” user then su to root to gain root access.
- Hacker now has to guess another userid and crack another password.

/etc/securetty

Console

Check for accounts with no password

```
Awk -F: ‘length($2)<1 {print $1}  <  /etc/passwd
```

W Command

```
$ w


user1   ttyp2    8:52        -sh
orafin  ttyp3  9:38am    sqlplus apps/dft1&4
```

History File

- Password may show up in history file
- sqlplus apps/dft1&4

Lastb

- Lastb can give away passwords
- User can inadvertently type their password as their userid
- This will show up with lastb

World Writeable Files

- find / -perm -0002 -print
- find / -perm -0020 -print

- Run Medusa

Medusa

- HP security tool
- Lists vulnerabilities in Security and suggestions on how to fix them

Network Services

- “As delivered by most vendors, Unix is intended to be a friendly and trusting operating system; by default, network services are offered to every other computer on the network”

/etc/services

- Make copies of any configuration files before you make any changes
- A lookup table for ports
- Some services no longer in widespread use
- If you do not know what a service does, you may want to turn it off

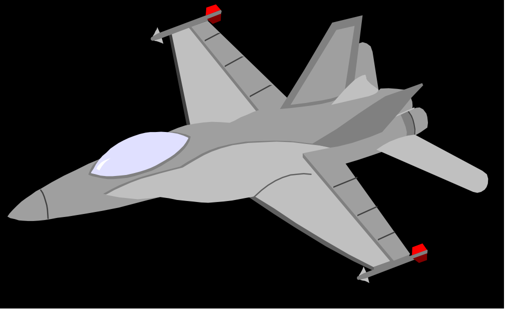
/etc/inetd.conf

- Specifies which networking services can be used by other systems to access the host

/var/adm/inetd.sec

- Allows selective network access to the host for selective systems

```
ftp    deny   15.24.62.*
login  deny
```



Umask

- Set it to 022
- Set it in /etc/profile
- OR in users’ profiles

Misellaneous

- Keep patches up to date
- Subscribe to HP’s Security Bulletins Digest at

  us-support.external.hp.com
- Subcribe to Cert Alerts at

  www.cert.org

Changing Oracle Application Passwords

- Have all users log out of the system
- Backup and export

  APPLSYS.FND_USERS

  APPLSYS.FND_ORACLE_USERID
- Recover these tables if anything goes wrong

Changing Oracle Application Passwords (con’t)

- Shutdown Concurrent Managers
- Shutdown the Listener
- Login to Oracle Financials as Sysadmin
- Navigate to:

  \Navigate\Security\Oracle\Register
- Go to form “Register Oracle Ids”

Changing Oracle Application Passwords (con't)

- Important:

  When the dialogue box appears with Yes/No choice, simply move to the next field.

- Repeat for APPLSYS and APPS, do NOT save at this point.
- The passwords of APPLSYS and APPS MUST be the same at all times
- Save all three changes now

Changing Oracle Application Passwords (con't)

- IMPORTANT:
    1. Re-query the form
    2. Keep this application session open (in case there are problems)
- If one of the two passwords are not correct you will not be able to login into the application

Changing Oracle Application Passwords (con’t)

- Hence, the reason we always leave a Session open.

Changing Database level password

- Use secure account (e.g SYSTEM or SYS)
- Login into SQL*plus
- Change the password for APPLSYS and APPS
- The password must be changed to the same password specified in the Application session

Verify Password Changes

- Start a new session and verify that you can login to the Application (remember to leave a session open)
- If not, reset the database level password again, most often it's a typing error
- Should this fail, I recommend resetting them to their original passwords both in the application and database and start over

Changing Passwords of other Userids

- The other Application users/schemas do NOT have to match APPLSYS or APPS
- Change passwords at the database level while keeping the Applications sessions open using the SQL*plus script
- Recovery:

  If you have exhausted all your options, drop and import the 2 tables mentioned previously

AND

- Don’t forget to PRAY…

- Questions ???

Thank-you for coming !

Contact Information:

richerj@navcanada.ca

baggsj@navcanada.ca