UNIX Administration Course

Version 1.0

mapleson@gamers.org
Tel: (+44) (0)1772 893297
Fax: (+44) (0)1772 892913
WWW: http://www.futuretech.vuurwerk.nl/

Detailed Notes for Day 3 (Part 5)

Project: Indy/Indy attack/defense (IRIX 5.3 vs. IRIX 6.5)

The aim of this practical session, which lasts two hours, is to give some experience of how an admin typically uses a UNIX system to investigate a problem, locate information, construct and finally implement a solution. The example problem used will likely require:

- the use of online information (man pages, online books, release notes, etc.),
- writing scripts and exploiting shell script methods as desired,
- the use of a wide variety of UNIX commands,
- identifying and exploiting important files/directories,

and so on. A time limit on the task is included to provide some pressure, which often happens in real-world situations.

The problem situation is a simulated hacker attack/defense. Two SGI Indys are directly connected together with an Ethernet cable; one Indy, referred to here as Indy X, is using an older version of IRIX called IRIX 5.3 (1995), while the other (Indy Y) is using a much newer version, namely IRIX 6.5 (1998).

Students will be split into two groups (A and B) of 3 or 4 persons each. For the first hour, group A is placed with Indy X, while group B is with Indy Y. For the second hour, the situation is reversed. Essentially, each group must try to hack the other group's system, locate and steal some key information (described below), and finally cripple the enemy machine. However, since both groups are doing this, each group must also defend against attack. Whether a group focuses on attack or defense, or a mixture of both, is for the group's members to decide during the preparatory stage.

The first hour is is dealt with as follows:

- For the first 35 minutes, each group uses the online information and any available notes to form a plan of action. During this time, the Ethernet cable between the Indys X and Y is not connected, and separate 'Research' Indys are used for this investigative stage in order to prevent any kind of preparatory measures. Printers will be available if printouts are desired.
- After a short break of 5 minutes to prepare/test the connection between the two Indys and move the groups to Indys X and Y, the action begins. Each group must try to hack into the

other group's Indy, exploiting any suspected weaknesses, whilst also defending against the other group's attack. In addition, the hidden data must be found, retrieved, and the enemy copy erased. The end goal is to shutdown the enemy system after retrieving the hidden data. How the shutdown is effected is entirely up to the group members.

At the end of the hour, the groups are reversed so that group B will now use an Indy running IRIX 5.3, while group A will use an Indy running IRIX 6.5. The purpose of this second attempt is to demonstrate how an OS evolves and changes over time with respect to security and OS features, especially in terms of default settings, online help, etc.

Indy Specifications.

Both systems will have default installations of the respective OS version, with only minor changes to files so that they are aware of each other's existence (/etc/hosts, and so on).

All systems will have identical hardware (133MHz R4600PC CPU, 64MB RAM, etc.) except for disk space: Indys with IRIX 6.5 will use 2GB disks, while Indys with IRIX 5.3 will use 549MB disks. Neither system will have any patches installed from any vendor CD updates.

The hidden data which must be located and stolen from the enemy machine by each group is the Blender V1.57 animation and rendering archive file for IRIX 6.2:

```
blender1.57_SGI_6.2_iris.tar.gz

Size: 1228770 bytes.
```

For a particular Indy, the file will be placed in an appropriate directory in the file system, the precise location of which will only be made known to the group using that Indy - how an attacking group locates the file is up to the attackers to decide.

It is expected that groups will complete the task ahead of schedule; any spare time will be used for a discussion of relevant issues:

- Reliability of relying on default settings for security, etc.
- How to detect hacking in progress, especially if an unauthorised person is carrying out actions as root.
- Whose responsibility is it to ensure security? The admin or the user?
- If a hacker is 'caught', what kind of evidence would be required to secure a conviction? How reliable is the evidence?

END OF COURSE.