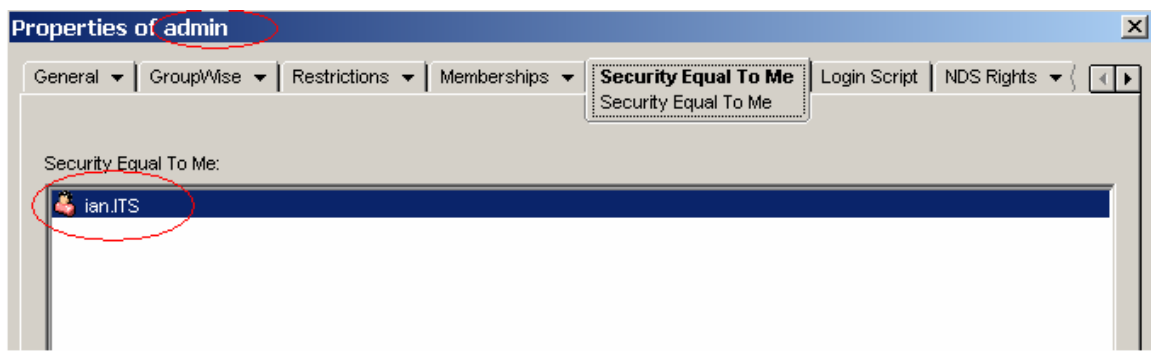


Escalation of Privileges (Netware 5)

Introduction

The goal of every privilege escalation attack on any network operating system is to achieve root access to the system; in Linux it's a matter of cracking the root password to the system, with a Windows NOS adding a user to the administrators group is the best way to escalate your privileges. In Netware the holy grail of escalation of privileges is the security equal to admin property (illustrated bellow)



By having the username shown in this property box the user is effectively has the same rights to the system as admin does, meaning (in this example) the user ian has unfettered access to system resources and can make any changes to the edirectory that is required.

This section of the article will outline how the user belder will achieve admin access to the system. It will outline the steps taken and the methodology outlined in achieving root access to the server.

Please note the user belder is not a member of the admin group and all escalation attacks will be carried out using this user.

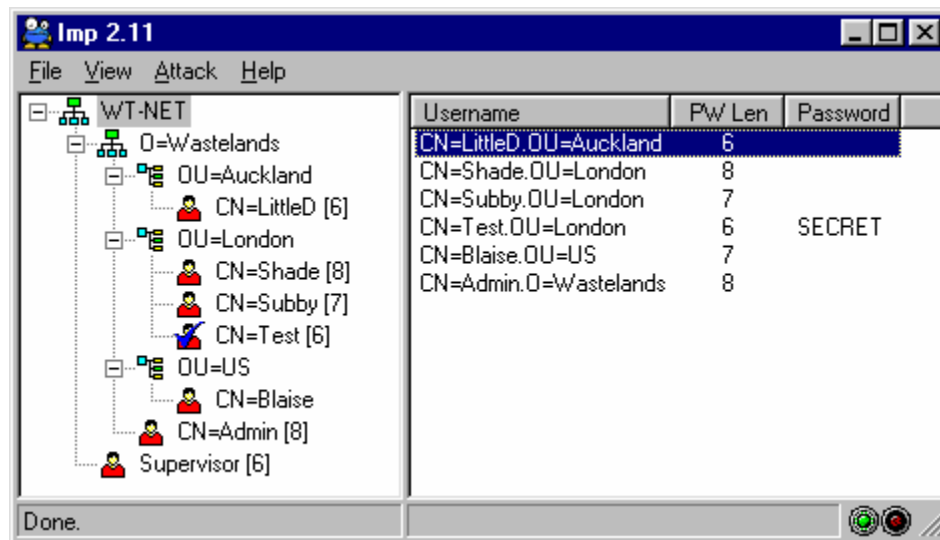
Auditing of Passwords

In every Netware system there is a hidden system directory that cannot be accessed via any client computers or the directory listing on the server console, this includes the admin user of the system, this directory (SYS:_NETWARE) can only be accessed by using a set of system NLM files on the Netware server console. This directory contains 4 files that hold all the information on the Netware server:

- 0.DSD contains system Entry Title information or more specifically the database title entries.
- 1.DSD contains the value information for each of the titles or e-directory objects
- 2.DSD contains block information of the file system
- 3.DSD contains partition information about the server.

As mentioned in previous sections any user can access console1 and in most out of the box networks can access the remote control software bundled with Netware. However if console security is properly implemented the user should not be able to access the console.

Once the user has access to the SYS:_NETWARE directory, the above mentioned files must be copied out of the directory, and copied to a Netware workstation, After the files are copied the user then launches the Netware password tool such as IMP or Pandora



This program will audit the files and report the passwords as illustrated in the figure above

Once the user has the password of the admin user all that is required is to login and escalate there privileges through console1