Easy protection with PASSWORD POLICIES

When I turn up at different companies I look around a typical office and it is easy to work out login names. Passwords on a system that you control however should be more secure and not too obvious.

JOHN SOUTHERN

On your Linux system the passwords are stored in the plain text file */etc/passwd*

You can view this file with any text editor. A typical line is

```
darth:x:500:100:Darth Maul:/home/darth:/bin/bash
```

This can be split up as follows:

```
darth - Login Name
x - Encrypted password
500 - UID (User IDentity number)
100 - GID (Group IDentity number)
Darth Maul - GCOS (Extra info about the user ➥
such as name etc,.)
/home/darth - Home Directory
/bin/bash - Shell used
```

As we can see the password is shown as an x which indicates that we are using shadow passwords. If we are not the password is a string which has been encrypted with the DES (Digital Encryption Standard).

The problem with just using DES is that the */etc/passwd* file is readable to everyone, otherwise they would not be able to sign onto the system. This means that they could in turn read the encrypted string in a simple text editor. By using a dictionary attack program such as Crack *ftp://ftp.cert.dfn.de/pub/tools/password/Crack/*, which tries a word from its dictionary and compares it with the encrypted string until eventually it guesses correctly.

On the other hand, this is sometimes a good way to recover passwords and really depends on just how much security you need. Shadow passwords are stored in */etc/shadow* file which only root has read permissions.

Signing on as root and looking at the file we get a typical line as

```
darth:wfR0W8eSzI1Lo:11386:0:99999:7:0::
```

Here we can see the encrypted password is wfR0W8eSzI1Lo

The 11386 refers to the last time the password was changed in the days since 1/1/70

The 0 refers to the number of days before the password may be changed.

The 99999 is used for the number of days before the password must be changed.

7 shows the number of days before a password change is forced that the user will be warned. The following 0 shows the time in days when the account is disabled after the password expires. Following this could be the number of days until the account is disabled. A final field is a reserved field.

Looking at the encrypted password: If we take an eight-letter password, for example ABCDEFGH, this is first encoded with a salt seed. The salt seed is a two-character string giving 4096 combinations. This is the first two characters of the password. The lowest seven bits of each letter of the password is then used to generate a 56-bit key for the DES algorithm to run against. The generated 11 ASCII character is added onto the seed to give the 13-character encrypted password.

Simple dictionary attacks are now fairly quick with some 500,000 words being contained in all seed combinations and sorted in order. Compared to the password this greatly aids the cracker.

To overcome this weakness, passwords should, as we all know, be random letters and characters and not make sensible words. The usual policies about changing passwords often also apply. To make the password a little more safe requires us to use the MD5 encryption method, which is a little stronger than DES.

Mind you, this is the usual case of do as recommended and not as I do. As I write this I have been roothacked.

Yet another re-install and this time I will use Tripwire. Still, on the bright side I do have a new box set distro somewhere... ■