HIDE.TXT

UNIX Abuse Collection

Written By ZeeBee Australia Jan 1990

Ok Hacksters...we all know the importance of a good understanding of the UNIX V operating system, but I find that just an understanding alone is quite simply not enough.

Our little articles are not intended for those wishing to gain an understanding of the UNIX environment. Instead, we aim to show you how to truly ABUSE the UNIX system to it's fullest potential.(And lets face it, UNIX really does have some really great abusable features!)..so....grab your UNIX accounts and passwords, and lets go!

UNIX ABUSE COLLECTION PART 01

****INVISIBILITY AND COVER UP TECHNIQUES***

One thing that really used to bug me about using a UNIX system was that I always felt like someone was watching me. It's just too easy to see what other users are doing, and as soon as you discover something good, everyone else sees what you are doing, and VOOM!...there goes your big secret. System operators too, can easily pinpoint just who is stuffing around with their system simply by seeing what processes are running under your name. So, I set out to find ways around this.

One way to cover up what you are doing is to find and copy the command that you wish to perform. As an example, just say I want to cat a whole load of bullshit to someones terminal, but I dont want anyone to see that I am executing the cat command. First of all I find the cat command. On most systems it will be somewhere in the /bin directory. Once you have found the command you must copy it (if possible) to your own directory and rename it to something inconspicuous. Most commands can be found somewhere in the /bin or /usr/bin directories, but if you cant find them, just look at your path list and see where UNIX is looking for them. (typing echo $PATH is one way to view your path list.)

Keep it in mind that not all commands are copyable (do an ls -al and look at the access flags to see if they are) if the access flags have an 'r' in the column 3rd from the far right, then you can read it, ie copy it !

One advantage to this technique is that if you find a bug with a certain command, you have a copy of the faulty code, so even if the computer staff fix the bug, you will have the old version ! Neat !

BUT! Don't worry if you can't copy the file! The following technique will do just the same job, without the need to copy the file. To do this you will need to write a program in C, compile it, and place it somewhere where it is safe for you to call whenever you want.

This is the small, and usefull piece of code:

```
main()
{
     execl("/bin/ls","a.out","-l",(char *)0);
}
```

The above piece of code will execute the ls -l command, but will generally show up as a.out -l whenever someone has a look at what you are doing!
The "/bin/ls" is the path of the 'ls' command. Put the path of any program you wish to execute here.
The "a.out" is what anyone else will think you are running. Put anything you want here. The command doesnt even have to exist!
The "-l" is the flag being passed to the ls command. You cant cover up flags which are passed. Damn!

So, by using this, you can run any program with execute access and make it look like you are running something else. You could even put in a whole path where I put the "a.out" and really confuse the shit out of people when they go looking for this great program you are running.

While we are on the topic, I would just like to stress the importance of continually checking to see what others on the system are doing. I find the "w -d" "ps -fu USERNAME" and "ps -fa" commands to be most usefull at this. On one system I was actually able to see system operators creating new accounts, and the account names and passwords were being passed. So one of the processes being executed by some priveleged user looked like this:

```
megauser  273 10:00:12  createaccount john zephyr ;
```

* In the above example, john is the account name, zephyr is the password.*

We got about 100 accounts that day !

And remember, as soon as any new toy is installed on the system, somebody will be using it, so just keep an eye on them to see what they do.