Password cracking

Windows password recovery

1. You have inadvertently forgotten your WindowsXP password and can't log in to your system. You really need to obtain access to your system. You also need to figure out passwords for others in the system.
    - Begin by cloning the windows vm that I tell you to.
    - One easy way to regain access to the system is simply resetting the password or blanking it out.
        - Blanking the password seems to work better, but you can try resetting it to something else as you follow the instructions below.
        - Boot your newly cloned vm with a hacking cd inserted `citv bootvm mynewlyclonedvm d hirens`
        - I would just blank the password for a single user and see if you can login as that user.
        - Also try to promote a user (make them an administrator)
2. Using your newly found windows password, boot windows and:
    - take screenshots of being logged

SAM file cracking

Getting the hashes for a Windows machine is the first step. It is pretty fun though. Boot your windows machine with parrot in the d drive. When parrot has loaded, mount the windows filesystem, then run run the `bkhive` and `samdump2` commands. TO do this, `cd` into the mounted directory and run `bkhive Windows/System32/config/SYSTEM ~/key` then run `samdump2 Windows/System32/config/SAM ~/key > ~/win_hash.txt`.

See if you can crack any passwords. Some programs that you might try are: l0phtcrack, hashcat, or multiforcer. You could look for any program that understands NTLM hashes. You could even scp it over to an OS that has john installed on it and try it. `John` should be installed on parrot.

To Submit

- Prove to me that you did all of the above. (Maybe some print screens, or other descriptions)
- List all the users with their passwords (as much as you were able to decipher)
- One document please (preferrably PDF). No zip or tar.