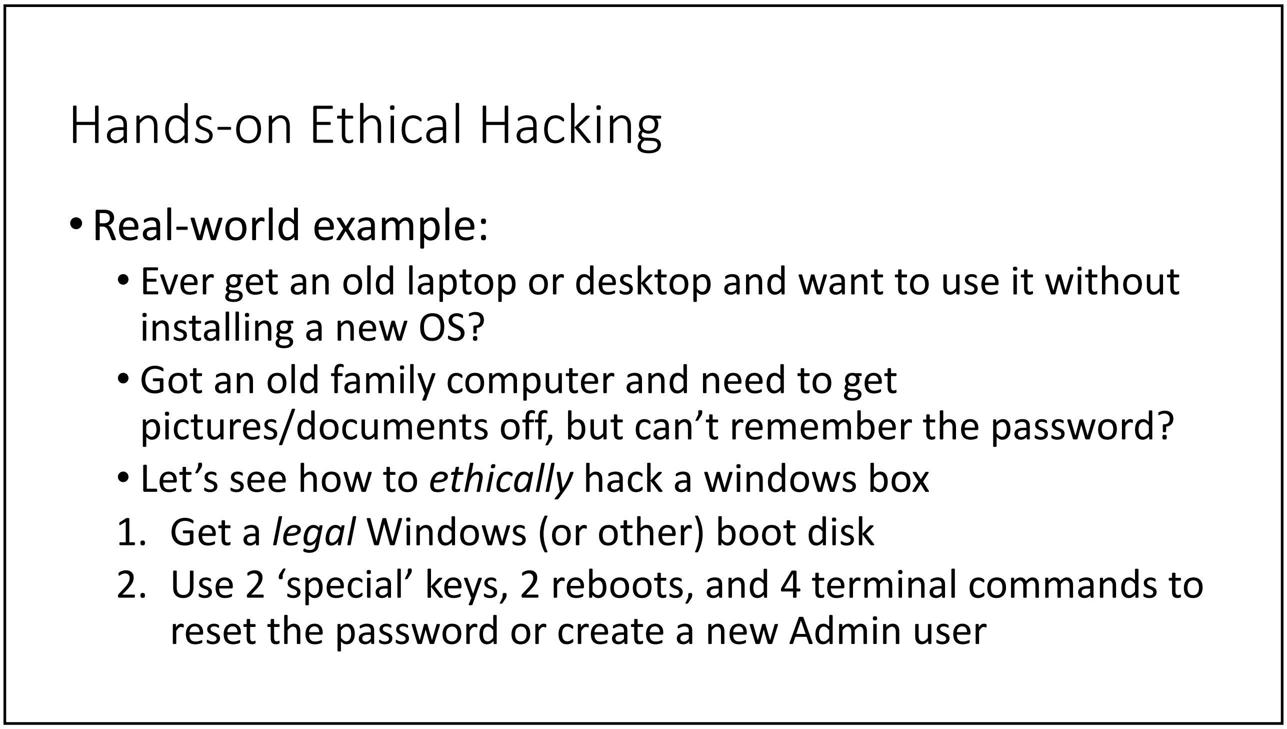
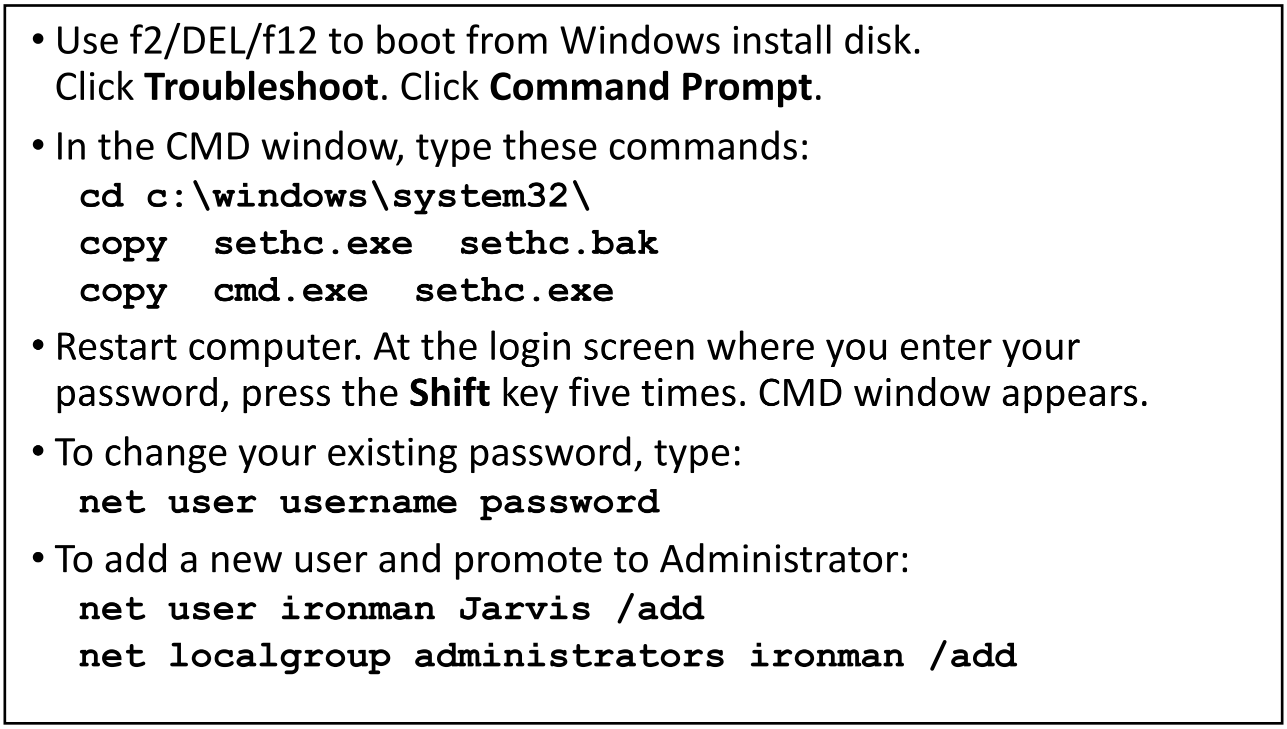


Hands-on Ethical Hacking

- Real-world example:
  - Ever get an old laptop or desktop and want to use it without installing a new OS?
  - Got an old family computer and need to get pictures/documents off, but can’t remember the password?
  - Let’s see how to *ethically* hack a windows box
  1. Get a *legal* Windows (or other) boot disk
  2. Use 2 ‘special’ keys, 2 reboots, and 4 terminal commands to reset the password or create a new Admin user



- Use f2/DEL/f12 to boot from Windows install disk.
  Click **Troubleshoot**. Click **Command Prompt**.
- In the CMD window, type these commands:

```
cd c:\windows\system32\
copy  sethc.exe  sethc.bak
copy  cmd.exe  sethc.exe
```

- Restart computer. At the login screen where you enter your password, press the **Shift** key five times. CMD window appears.
- To change your existing password, type:

```
net user username password
```

- To add a new user and promote to Administrator:

```
net user ironman Jarvis /add
net localgroup administrators ironman /add
```