cp-ub10-01
Solution

1. Change argus's password from Windows12 to ?Defen08
   a. Type:
      1) passwd argus
      2) New password: ?Defen08

2. Authentication
   a. Install cracklib
      1) apt-get install libpam-cracklib --force-yes -y

   b. Setup failed login attempts
      1) gedit /etc/pam.d/common-auth
      2) auth optional pam_tally.so deny=5 unlock_time=900 onerr=fail audit even_deny_root_account silent

   c. Minimum Password Length & Composition
      1) gedit /etc/pam.d/common-password

      2) password requisite pam_cracklib.so retry=3 minlen=8 difok=3 reject_username minclass=3 maxrepeat=2 dcredit=1 ucredit=1 lcredit=1 ocredit=1

   d. Password History
      1) password requisite pam_pwhistory.so use_authtok remember=24 enforce_for_root

   e. Hashing Algorithm
      1) password [success=1 default=ignore] pam_unix.so obscure use_authtok sha512 shadow

3. Change each user's password, type:
   a. passwd username
   b. New password: ?Defen08

4. Lock all users except argus
   a. passwd –l username

5. Limit root access
   a. gedit /etc/group
   b. Remove all users from the admin group except argus

6. System Patching
   a. apt-get update
   b. apt-get dist-update –y

7. Netcat Backdoor
   a. Search for a process running nc
      1) ps –ef | grep nc
   b. Search for the program that started netcat
      1) grep –l '/bin/nc' /etc/rc*
   c. Remove the line that starts netcat
      1) gedit /etc/rc.local

8. Scheduled job
   a. rm /var/spool/cron/crontabs/root

9. Service removal
   a. List running services
      1) service - -status-all
   b. Remove all services
      1) apt-get - -purge autoremove servicename