**Gold Team**

**Ubuntu Hardening Checklist**

| **GOLD LINUX TEAM** | |
|---|---|
| Server Name: | |
| IP Address: | |
| Team Member | |
| Fax number: | |

| | |
|---|---|
| ☐ | Change Root Password |
| ☐ | Create 2 users: dbAdmin, netAdmin |
| ☐ | Add new users to ‘wheel’ Group |
| ☐ | Set new users passwords |
| ☐ | Install Firewalld |
| ☐ | Turn on Firewalld |
| ☐ | Install Security Updates |
| ☐ | Install AppArmor |
| ☐ | Turn on AppArmor |
| ☐ | Install Fail2ban |
| ☐ | Configure Fail2ban |
| ☐ | Modify /etc/sysctl.conf |
| ☐ | Install clamav |
| ☐ | Update clamav (sudo freshclam) |
| ☐ | Run a full system scan. |
| ☐ | Install Cockpit |
| ☐ | Turn on Cockpit |

1. Log in as root (admin user supplied by the competition)
2. Type **passwd**
3. Type in current password
4. Type new password from list
5. Retype new password from list
6. Add netadmin and dbadmin
7. Type **sudo adduser dbadmin**
8. When prompted, enter and re-enter the password
9. Just hit enter until asked to accept and then accept (y)
10. Type **sudo adduser netadmin**
11. Repeat steps 7 and 8
12. Add user to sudo group: **usermod -aG sudo netadmin**
13. Add user to sudo group: **usermod -aG sudo dbadmin**
14. Log out and log in to netadmin
15. Disable root login, run **sudo chsh root -s /sbin/nologin**
16. Disable all acounts, except root, listed after this command **awk -F: '($3 == "0") {print}' /etc/passwd**
17. List all users by typing **cut -d: -f1 /etc/passwd**
18. Remove all unneccesary users by typing **passwd -l <username>**
19. List all users for sudo using **getext group sudo**
20. Remove all users not dbadmin and netadmin by typing **deluser <username> sudo**
21. Install and enable Firewalld by typing the following commands:
    a. **sudo apt -y install firewalld firewall-config firewall-applet**
    b. **sudo systemctl unmask --now firewalld.service**
    c. **sudo systemctl enable --now firewalld.service**
    d. **sudo firewall-cmd --permanent --zone=public --add-port=22/tcp**
    e. **sudo firewall-cmd --zone=public --add-port=22/tcp**
    f. **sudo firewall-cmd --permanent --zone=public --add-port=80/tcp**
    g. **sudo firewall-cmd --zone=public --add-port=80/tcp**
22. Install Security Updates by typing the following commands:
    a. **sudo apt install unattended-upgrades**
23. Install and enable AppArmor by typing the following commands:
    a. **sudo apt -y install apparmor**
    b. **sudo apt -y install apparmor-profiles**
    c. **sudo apt -y install apparmor-utils**
    d. **sudo systemctl start apparmor**
    e. **sudo aa-enforce /etc/apparmor.d/!(lxc*)**
24. Install Fail2ban
    a. **sudo apt-get -y install fail2ban**
25. Install Clamav and run scan. (Once scan is started, open a new connection and continue with the checklist because it will take a while.)
    a. **sudo apt-get -y install clamav**
    b. **sudo freshclam**
    c. **clamscan -r --remove /**
26. Modify /etc/sysctl.conf
    a. See Attached Table
27. Install and enable Cockpit

a. **sudo add-apt-repository ppa:cockpit-project/cockpit**
b. **sudo apt-get update**
c. **sudo apt-get -y install cockpit cockpit-networkmanager cockpit-storaged cockpit-packagekit cockpit-dashboard**
d. **sudo systemctl enable cockpit.socket**
e. **sudo systemctl start cockpit**