# Layered Security

The scope of Layered Security includes:  
1. Physical security  
2. Endpoint security  
3. Security architecture  
4. Antivirus & antimalware  
5. Server system security  
6. Attack vectors  
7. Link verification, etc.  
  
Lab Practice 1: Securing against brute force attacks on SSH port 22  
  
Change port 22 on the server system:  
a. nano /etc/ssh/sshd\_config (remove the comment on port 22, then change the number)  
b. nano /lib/systemd/system/ssh.socket (add the number that was changed in sshd\_config)  
c. systemctl daemon-reload  
d. systemctl restart ssh  
  
Lab Practice 2: Securing against attacker by creating a DMZ  
  
a. Install dependencies:  
 apt install -y iptables iptables-persistent linux-libc-dev make virtualenv python3-virtualenv libfakeroot libssl-dev libffi-dev build-essential libpython3-dev python3-minimal authbind git -y  
  
b. Configure redirect:  
 nano /etc/sysctl.conf  
 1) net.ipv4.ip\_forward=1 (remove the comment)  
 2) iptables -A PREROUTING -t nat -p tcp --dport 22 -j REDIRECT --to-port 2222  
 3) iptables-save > /etc/iptables/rules.v4  
  
c. Create DMZ user:  
 adduser --disabled-password cowrie  
 Download cowrie repository:  
 su - cowrie  
 cd /home/cowrie  
 git clone https://github.com/cowrie/cowrie.git  
  
d. Configure cowrie files:  
 cd cowrie  
 virtualenv --python=/usr/bin/python3 cowrie-env  
 . cowrie-env/bin/activate  
 pip install --upgrade -r requirements.txt  
 deactivate  
  
e. Save DMZ system on systemd (backend):  
 nano /home/cowrie/cowrie/bin/cowrie  
 Set DAEMONIZE="-n"  
 exit (till the root shell)  
  
f. Create usernames for DMZ trap:  
 nano /home/cowrie/cowrie/etc/userdb.txt  
 Add the following:  
 root:x:!root  
 root:x:!admin  
 root:x:!toor  
 root:x:!123456  
 root:x:!12345678  
 root:x:!admin123  
 root:x:!qwerty  
 root:x:!qwerty  
 root:x:!qwerty@123  
 root:x:!password  
 root:x:!p@ssw0rd  
 root:x:\*  
 tomcat:x:\*  
 oracle:x:\*  
  
g. Create hostname for DMZ trap:  
 nano /home/cowrie/cowrie/etc/cowrie.cfg.dist  
 Set hostname = ++++++  
  
h. Embed DMZ backend system on the main system:  
 nano /etc/systemd/system/DMZ.service  
 Insert the script:  
 [Unit]  
 Description=Interactive SSH Honeypot  
 Wants=network.target  
  
 [Service]  
 Type=simple  
 User=cowrie  
 Group=cowrie  
 ExecStart=/home/cowrie/cowrie/bin/cowrie start  
 Restart=on-failure  
 RestartSec=5  
  
 [Install]  
 WantedBy=multi-user.target  
  
i. systemctl daemon-reload  
j. systemctl enable DMZ.service  
k. systemctl start DMZ.service  
l. systemctl restart DMZ.service