1. **Password Reset on Linux Box**
    - https://swordfish.wordpress.com/2006/06/23/openbsd-hack-single-user-mode-reset-root-password/ (openbsd)
    - Hold Left-shift
    - Get in the grub config file
    - Look for line "Linux /boot/vmlinuz … **init=/bin/bash**"
    - Press Control-X
    - mount -o rw,remount /
    - passwd <change-password>

2. **Change passwords for all user accounts**
    - cat /etc/passwd
    - cat /etc/shadow #check for hashes
    - passwd
    - Check accounts for empty passwords
        i. cat /etc/shadow | awk -F: '($2==""){print $1}'
3. **Check sudoers file**
    - Remove sudo root without password authentication
    - Check /etc/group
    - sudo EDITOR=vim visudo
4. **Check cronjobs**
    - crontab -l (for each user)
    - ls -la /etc/cron.*
5. **Check bash history**
    - history
    - tail /var/log/auth.log
6. **Set bash history to be erased after logging out**
    - unset BASHHIST
    - unset BASHFILE
7. **List running services**
    - ps ax (list all running procs)
    - ps aux username (specify a user to see their procs)
    - **Turn off unnecessary**
        i. service <serviceName> stop
        ii. chkconfig <serviceName> off

8. **List open ports**
    - netstat -tulpn
    - netstat -anp | grep LISTEN | grep -v STREAM
    - lsof -nPi (show all listening ports in lsof, not sure the diff here)

9. **Host firewall**
    - **Save IPtables to a file**
        i. sudo sh -c "iptables-save > /etc/iptables.rules"
    - **Restore ip tables**
        i. iptables-restore < /etc/iptables.rules
        ii. iptables-save
    - **Inside /etc/iptables.rules**
    - iptables -t filter -F
    - iptables -t filter -X
    - iptables -P INPUT DROP
    - iptables -P FORWARD DROP
    - iptables -P OUTPUT DROP
    - iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
    - iptables -A INPUT -p tcp -m tcp --dport <port #> -j ACCEPT
    - iptables -A INPUT -i lo -j ACCEPT
    - iptables -A OUTPUT -o lo -j ACCEPT
    - iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
    - iptables -A OUTPUT -p udp -m multiport --dport <port#>,<port2#>,<begin#:end#> -j ACCEPT
    - iptables -A OUTPUT -p tcp -m multiport --dport <port1#>,<port2#>,<begin#:end#> -j ACCEPT

    - https://help.ubuntu.com/community/IptablesHowTo
    - man iptables
    - man iptables-extensions
    - **Block ip-address**
    - iptables -A INPUT -s <ip-address> -j DROP
    - iptables -A OUTPUT -d <ip-address> -j DROP

10. **Kernel patches / kernel protection**
    - **Update**
    - sudo apt-get update
    - sudo apt-get dist-upgrade

    - **Patch and protect Kernel**
    - # Turn on execshield
    - kernel.exec-shield=1
    - kernel.randomize_va_space=2
    - # Enable IP spoofing protection
    - net.ipv4.conf.all.rp_filter=1
    - # Disable IP source routing

- net.ipv4.conf.all.accept_source_route=0
- # Ignoring broadcasts request
- net.ipv4.icmp_echo_ignore_broadcasts=1
- net.ipv4.icmp_ignore_bogus_error_messages=1
- # Make sure spoofed packets get logged
- net.ipv4.conf.all.log_martians = 1

11. **Change folders and ssh settings**
    - **Check for malicious scripts here** /tmp/
    - **For ssh**
    - vim /etc/ssh/sshd_config
        i. PermitRootLogin no
        ii. AllowUsers <username>
        iii. Protocol 2
    - ~/.ssh/authorized_keys
    - /root/.ssh/authorized_keys

12. **Check for users inside**
    - last
    - w #how logged users
    - Who -p

13. **Check logs**
    - tail - f /var/log/message – Where whole system logs or current activity logs are available.
    - tail - f /var/log/auth.log – Authentication logs.
    - tail - f /var/log/apache/error.log

    - /var/log/kern.log – Kernel logs.
    - /var/log/cron.log – Crond logs (cron job).
    - /var/log/maillog – Mail server logs.
    - /var/log/boot.log – System boot log.
    - /var/log/mysqld.log – MySQL database server log file.
    - /var/log/secure – Authentication log.
    - /var/log/utmp or /var/log/wtmp : Login records file.
    - /var/log/yum.log: Yum log files.

Logging Procedure

mkdir -p ~/logs/initial (make a folder in your home directory called logs, inside it make a folder called initial)

cd ~/logs (change working dir to that new folder)

sudo cp -R /var/log/ . (copy the whole log folder!)

mv log initial (rename the newly copied folder to something different (preferably that indicates time stamp) yay nested parens)
diff -r /var/log initial (compare the current /var/log dir with your copy)

14. **Change mysql settings**
15. **Disable ipv6**
    - # vi /etc/sysconfig/network
    - NETWORKING_IPV6=no
    - IPV6INIT=no

    - **Disable IPv6:**
    - open file /etc/modprobe.d/aliases
    - vi /etc/modprobe.d/aliases
    - Find the line:
    - alias net-pf-10 ipv6
    - Replace with:
    - alias net-pf-10 off
    - alias ipv6 off
    - Save and close the file.

16. **Possibly chattr i shadow file**

17. **Install fail2ban**
    - apt-get update && apt-get upgrade -y
    - apt-get install fail2ban
    - (fedora) dnf install fail2ban
    - (centos) yum install fail2ban

18. **Common-tasks:**
    - Check for no passwords
    - Setuid binaries
        i. #See all set user id files:
        ii. find / -perm +4000
        iii. # See all group id files
        iv. find / -perm +2000
        v. # Or combine both in a single command
        vi. find / \(-perm -4000 -o -perm -2000 \) -print
        vii. find / -path -prune -o -type f -perm +6000 -ls
    - ASLR

19. **Block an ip address**

- iptables -A INPUT -s 202.54.20.22 -j DROP
- iptables -A OUTPUT -d 202.54.20.22 -j DROP