1. Change password for both user and root account
   1. passwd command
2. Disable login for root
   1. Make sure sysadmin is a sudoer
3. Change root user’s Shell in /etc/passwd from root:x:0:0:root:/root:/bin/bash

to

root:x:0:0:root:/root:**/sbin/nologin**

1. Setup Firewall (These commands in this order will drop all incoming traffic except DNS and NTP. These will also allow all outgoing traffic.) \*Note: only open port 80 on Ubuntu instead of 53 and 123
   1. iptables -P INPUT DROP

iptables -P FORWARD DROP

iptables -P OUTPUT ACCEPT

iptables -L INPUT

iptables -A INPUT -p udp --dport 53 -j ACCEPT

iptables -A INPUT -p udp --dport 123 -j ACCEPT

sudo apt install iptables-persistent

1. Forward syslog and rsyslog to splunk
   1. \*.\* @172.20.241.20 in /etc/rsyslog.conf file
2. Update both Debian and Ubuntu Machines
   1. Sudo apt update
   2. Sudo apt upgrade
3. Check users
   1. Cat /etc/passwd
4. Check shadow file
   1. Sudo cat shadow
5. Check sudoers
6. Check cronjob
   1. Cat /etc/crontab
7. Disable sshd
   1. Sudo systemctl disable ssh
8. Make sure they have a default route configured
   1. Netstat -rn
9. Backup etc folder
   1. sudo tar -cvzf etc\_backup.tar.gz /etc
   2. sudo tar -xvzf etc\_backup.tar.gz
10. install Fail2Ban
    1. sudo apt install Fail2Ban