

1. If in X-Window (e.g. a GUI), hit Ctrl+Alt+T to escape
2. Run **alias** to determine masked commands at your user’s level
   1. Some aliases are default, such as color highlighting flags for ls by default
   2. Run **unalias aliasedcommandhere**
3. Read dotfiles in user directory to determine any droppers
   1. **ls .\***
   2. Should contain a bash profile, history, etc, they generally execute on load
4. Elevate to root
   1. **sudo -i** if you are a sudoer, will ask for *your* password
5. Check history to see if there were any build-time leftovers
   1. **cat /root/.\*history**
   2. **cat /home/\*/.\*history**
   3. Dissect APT history in **/var/log**
      1. If needed, **apt install gzip -y**
      2. **cd /var/log/apt; gunzip \*.gz**
      3. **cat history\*|grep Commandline**
         1. Should see any apt-time install packages
      4. If that fails, **cat \*|grep Commandline**
         1. Broader to account for any version mess
      5. If all of those fail, they probably had the sense to wipe logs
6. Check for alias tampering at the root level, same as 2
   1. Run **unalias aliased\_command** to release it
7. Check for dotfiles in root
   1. **ls /root/.\***
   2. Cat as appropriate, they generally execute on load
8. Reinstall coreutils as needed
   1. apt install coreutils --reinstall
9. Check HOSTS file for DNS tampering
   1. **cat /etc/hosts**
   2. Should largely only be localhost and similar route-necessary hosts, not “ubuntu.com” or anything
10. Check integrity of apt installs
    1. **cd /etc/apt**
    2. **grep -v ^# sources.list**
    3. **grep -v ^# sources.list.d/\***
    4. **grep -v ^# sources.list.d/.\***
    5. Will output “trusted” software sources (removes comment garbage), should only be ubuntu.com sources unless of weird circumstances
    6. Comment out or remove as appropriate
    7. apt update if they change
11. **apt update** to update repos list
12. **apt upgrade** to upgrade actual software - brief downtime may occur
13. View actively running network services (listening or established) with **lsof -i -n -P**
    1. Tread carefully if it’s DHCP or DNS
14. Check for rogue users
    1. **cat /etc/passwd** to enumerate users
       1. In Linux, services etc will need their own users, but not everything should have /bin/bash
       2. **cut -d: -f1,3 /etc/passwd | egrep ':[0-9]{4}$' | cut -d: -f1** to find users over 1000, AKA “human” users
       3. Find users with passwords set
          1. **cat /etc/shadow|grep -v ':\\*:' | grep -v '\:\!\:'**
15. Check install-origin integrity to see if anything has changed since its original installation
    1. **apt install debsums**
    2. **debsums -e** to find changed configs
    3. **debsums -c** to find changed files
16. Enumerate running processes
    1. **ps aux** - amongst other fields
17. Install auditbeat
    1. <https://kifarunix.com/install-and-configure-elastic-auditbeat-on-ubuntu-18-04/>
18. Harden services
    1. DNS:
       1. Is DNS running as root? **ps aux | grep bind | grep -v '^root'**
       2. **chown -R root:bind /etc/bind**
       3. **chown root:bind /etc/bind/named.conf\***
       4. **chmod 640 /etc/bind/named.conf\***
       5. Add **version "Secured DNS server";** to named conf hide version
    2. E.x. SSH:
       1. Audit the /etc/ssh/sshd\_config settings
       2. **ls -la /home/\*/.ssh/**
19. Install Tiger IDS
    1. <https://www.tecmint.com/tiger-linux-security-audit-intrusion-detection-tool/>
20. Install tripwire
    1. <https://www.tecmint.com/install-tripwire-ids-intrusion-detection-system-on-linux/>Document encryption key
21. Dump cron
    1. **cat /etc/crontab**
    2. **cat /etc/cron.\*/\***
22. Enumerate services
    1. **service --status-all**