Linux Checklist v1.0

Notes

If a command errors or fails, try it again with `sudo` (or `sudo !!` to save typing)

Google anything and everything. If you don't know or understand something, google it

When you see the syntax `$word`, do not type it verbatim, but instead substitute the appropriate word (usually referenced in a previous command).

When the order of steps does not matter, bullet points have been used instead of ordinals.

To edit files, run `gedit`, a graphical editor akin to notepad; `nano`, a simple command-line editor; or `vim`, a powerful but less intuitive command-line editor. Note that vim may need to be installed with `apt-get install vim`.

Checklist

1. Read the readme

   Note down which ports/users are allowed.

2. **Do Forensics Questions**

   You may destroy the requisite information if you work on the checklist!

3. Secure root

   set `PermitRootLogin no` in `/etc/ssh/sshd_config`

4. Secure Users

   1. Disable the guest user.

      Go to `/etc/lightdm/lightdm.conf` and add the line

      ```
      allow-guest=false
      ```

      Then restart your session with `sudo restart lightdm`. This will log you out, so make sure you are not executing anything important.

   2. Open up `/etc/passwd` and check which users

      - Are uid 0
      - Can login
      - Are allowed in the readme

   3. Delete unauthorized users:

      ```
      sudo userdel -r $user
      ```

      ```
      sudo groupdel $user
      ```

   4. Check `/etc/sudoers.d` and make sure only members of group sudo can sudo.
   5. Check `/etc/group` and remove non-admins from sudo and admin groups.
   6. Check user directories.
      1. cd `/home`
      2. `sudo ls -Ra *`
      3. Look in any directories which show up for media files/tools and/or "hacking tools."

   7. Enforce Password Requirements.

      1. Add or change password expiration requirements to `/etc/login.defs`.

```
 PASS_MIN_DAYS 7
PASS_MAX_DAYS 90
PASS_WARN_AGE 14
```

   2. Add a minimum password length, password history, and add complexity requirements.
      1. Open `/etc/pam.d/common-password` with sudo.
      2. Add `minlen=8` to the end of the line that has `pam_unix.so` in it.
      3. Add `remember=5` to the end of the line that has `pam_unix.so` in it.
      4. Locate the line that has pam.cracklib.so in it. If you cannot find that line, install cracklib with `sudo apt-get install libpam-cracklib`.
      5. Add `ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-` to the end of that line.
   3. Implement an account lockout policy.
      1. Open `/etc/pam.d/common-auth`.
      2. Add `deny=5 unlock_time=1800` to the end of the line with `pam_tally2.so` in it.
   4. Change all passwords to satisfy these requirements.

      `chpasswd` is very useful for this purpose.

5. Enable automatic updates

   In the GUI set Update Manager->Settings->Updates->Check for updates:->Daily.

6. Secure ports

   1. `sudo ss -ln`
   2. If a port has `127.0.0.1:$port` in its line, that means it's connected to loopback and isn't exposed. Otherwise, there should only be ports which are specified in the readme open (but there probably will be tons more).
   3. For each open port which should be closed:
      1. `sudo lsof -i :$port`
      2. Copy the program which is listening on the port. `whereis $program`
      3. Copy where the program is (if there is more than one location, just copy the first one). `dpkg -S $location`
      4. This shows which package provides the file (If there is no package, that means you can probably delete it with `rm $location; killall -9 $program`). `sudo apt-get purge $package`
      5. Check to make sure you aren't accidentally removing critical packages before hitting "y".
      6. `sudo ss -l` to make sure the port actually closed.

7. Secure network

   1. Enable the firewall

      ```
      sudo ufw enable
      ```

   2. Enable syn cookie protection

      ```
      sysctl -n net.ipv4.tcp_syncookies
      ```

   3. Disable IPv6 (Potentially harmful)

      ```
      echo "net.ipv6.conf.all.disable_ipv6 = 1" | sudo tee -a /etc/sysctl.conf
      ```

   4. Disable IP Forwarding

      ```
      echo 0 | sudo tee /proc/sys/net/ipv4/ip_forward
      ```

   5. Prevent IP Spoofing

      ```
      echo "nospoof on" | sudo tee -a /etc/host.conf
      ```

8. Install Updates

   Start this before half-way.

   - Do general updates.

      1. `sudo apt-get update`.

        2. `sudo apt-get upgrade`.

    - Update services specified in readme.

        1. Google to find what the latest stable version is.
        2. Google "ubuntu install service version".
        3. Follow the instructions.

    - Ensure that you have points for upgrading the kernel, each service specified in the readme, and bash if it is vulnerable to shellshock.

9. Configure services

    1. Check service configuration files for required services. Usually a wrong setting in a config file for sql, apache, etc. will be a point.

    2. Ensure all services are legitimate.

        ```
        service --status-all
        ```

10. Check the installed packages for "hacking tools," such as password crackers.

11. Run other (more comprehensive) checklists. This is checklist designed to get most of the common points, but it may not catch everything.

Tips

- Netcat is installed by default in ubuntu. You will most likely not get points for removing this version.
- Some services (such as `ssh`) may be required even if they are not mentioned in the readme. Others may be points even if they are explicitly mentioned in the readme