Linux OS Hardening

- User Account
- Remove un-wanted packages
- Stop un-used Services
- Check on Listening Ports
- Secure SSH Configuration
- Enable Firewall (iptables/firewalld)
- Enable SELinux
- Change Listening Services Port Numbers
- Keep your OS up to date (security patching)

By: Imran Afzal
www.utclisolutions.com

OpenLDAP Installation

- What is OpenLDAP?
- OpenLDAP Service
  - `slapd`
- Start or stop the service
  - `systemctl start slapd`
  - `systemctl enable slapd`
- Configuration Files
  - `/etc/openldap/slapd.d`

By: Imran Afzal
www.utclisolutions.com

Trace Network Traffic (traceroute)

- The traceroute command is used in Linux to map the journey that a packet of information undertakes from its source to its destination. One use for traceroute is to locate when data loss occurs throughout a network, which could signify a node that's down.
- Because each hop in the record reflects a new server or router between the originating PC and the intended target, reviewing the results of a traceroute scan also lets you identify slow points that may adversely affect your network traffic.

- Example

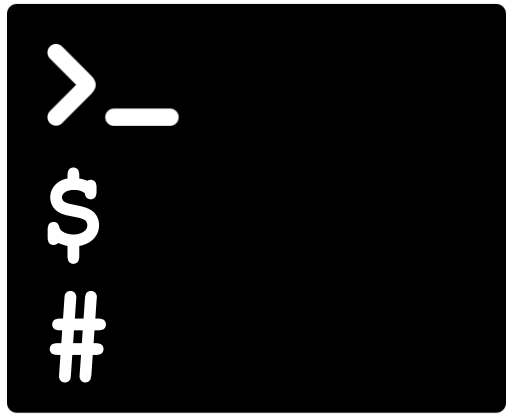
```
# traceroute www.google.com
```

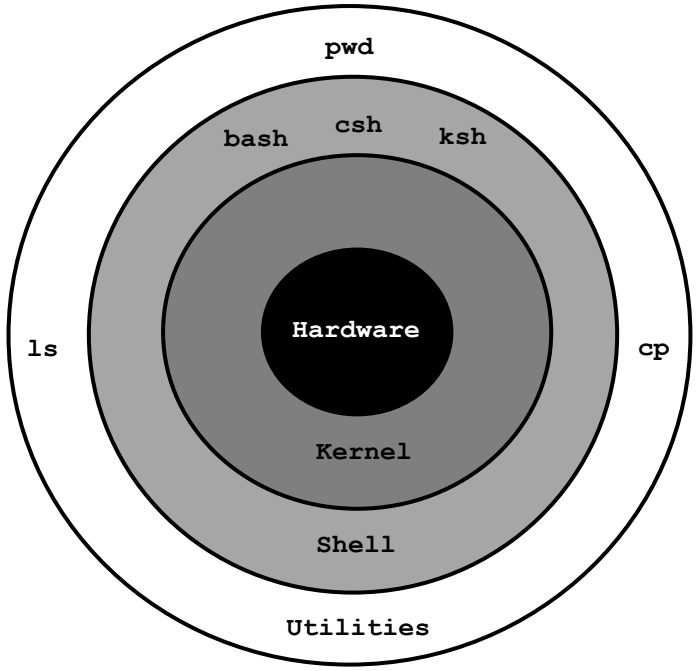
By: Imran Afzal
www.utclisolutions.com

Configure and Secure SSH

- **SSH**
  - SSH stands for secure shell

provides you with an interface to the Linux system. It takes in your commands and translate them to kernel to manage hardware





- Open SSH is a package/software
- Its service daemon is sshd
- SSH port # 22

By: Imran Afzal
www.utclisolutions.com

Configure and Secure SSH

- SSH itself is secure, meaning communication through SSH is always encrypted, but there should be some additional configuration can be done to make it more secure
- Following are the most common configuration an administrator should take to secure SSH

✓ **Configure Idle Timeout Interval**

Avoid having an unattended SSH session, you can set an Idle timeout interval

- Become root
- Edit your **`/etc/ssh/sshd_config`** file and add the following line:
- **`ClientAliveInterval 600`**
- **`ClientAliveCountMax 0`**
- **`# systemctl restart sshd`**

The idle timeout interval you are setting is in seconds (600 secs = 10 minutes). Once the interval has passed, the idle user will be automatically logged out

By: Imran Afzal
www.utclisolutions.com

Configure and Secure SSH

- ✓ **Disable root login**

  Disabling root login should be one of the measures you should take when setting up the system for the first time. It disable any user to login to the system with root account

  - Become root
  - Edit your **`/etc/ssh/sshd_config`** file and replace PermitRootLogin yes to no
  - **`PermitRootLogin no`**
  - **`# systemctl restart sshd`**

By: Imran Afzal
www.utclisolutions.com

Configure and Secure SSH

✓ **Disable Empty Passwords**

You need to prevent remote logins from accounts with empty passwords for added security.

- Become root
- Edit your **`/etc/ssh/sshd_config`** file and remove # from the following line
- **`PermitEmptyPasswords no`**
- **`# systemctl restart sshd`**

By: Imran Afzal
www.utclisolutions.com

Configure and Secure SSH

✓ **Limit Users' SSH Access**

To provide another layer of security, you should limit your SSH logins to only certain users who need remote access

- Become root
- Edit your **`/etc/ssh/sshd_config`** file and add
- **`AllowUsers user1 user2`**
- **`# systemctl restart sshd`**

By: Imran Afzal
www.utclisolutions.com

Configure and Secure SSH

✓ **Use a different port**

By default SSH port runs on 22. Most hackers looking for any open SSH servers will look for port 22 and changing can make the system much more secure

- Become root
- Edit your **`/etc/ssh/sshd_config`** file and remove # from the following line and change the port number
- **`Port 22`**
- **`# systemctl restart sshd`**

By: Imran Afzal
www.utclisolutions.com