# Module 2: Linux Fundamentals PT12

*Understand the following*

Hex char symbol conversion to binary (top or bottom)

| 0 | 0000 |
|---|------|
| 1 | 0001 |
| 2 | 0010 |
| 3 | 0011 |
| 4 | 0100 |
| 5 | 0101 |
| 6 | 0110 |
| 7 | 0111 |
| 8 | 1000 |
| 9 | 1001 |
| A | 1010 |
| B | 1011 |
| C | 1100 |
| D | 1101 |
| E | 1110 |
| F | 1111 |

*What's another name for a daemon?*
- **process or service**

Most services end with d... except **apache**

*What can you tell me about systemd?*
- PID starts with 1. First service that starts up.

*Service types*
- Unit
- Target

*How to enable a service?*
- systemctl enable servicename

*How to start firewalld?*
- systemctl start firewalld

*Systemctl options*
- Start
- Stop
- Status
- Enable
- Restart = start and stop
- Reload = start

**Firewall** – "filter"
- Allows certain traffic to come in or go out.
- You can filter on IP addresses (Network Layer), tcp/udp (Transport layer), port number (Application layer) – *an access control list*

**Services running in a soho(small office/home office)**
- Routing
- Firewall
- DHCP (Dynamic Host Configuration Protocol)
- DNS (Domain Name Server)
- NAT  (Network Address Translation)

**PfSense –** a software for setting up firewalls.

*3 types of Linux firewalls*
*Netfilter* – Linux firewall core – very complex
*IPTables* – firewall app that is pre-installed on most Linux distros
- app tool builds upon Netfilter

*Uncomplicated Firewall (UFW)* – provides user-friendly framework for managing Netfilter
- GUI

*firewalld* – front-end controller for IPTables

# _Identity Access Management_

_4 main components of IAM_
1. Make a claim
2. Prove the claim
3. Permissions
4. Accounting

---

**SSH** – port 22 – Public and Private key pair work in tandem. Give out the public key and keep the private key stored.

**nc/ncat** – shows open ports but not details, if the port on the other side is also listening then you can send commands

**nmap** – shows details on port such as Port, State and Service