# Networking Basics

Archaict

November 2020

## Contents

# Basics of Networking

In here I'll introduce basics about networking in general.

# GNU/Linux

It is advised to use unix based system to help with understanding networking in general, since most of networking tools that will be used here are better to be used with unix based system.

**GNU** is the interfaces that is used to interract with **Linux** kernel; some call it **GNU/Linux** but here, I'll be using **UNIX** or **Linux** interchangeably to mention **GNU/Linux.**

## Privilege

### Root [#]

As a root user, you're the system admin or the owner of the machine that you're on. Basically, you have privilege that can only be obtained by, knowing the password or by doing hacking. With this privilege, you can install apps, run scripts that needed root access, or even changing configuration resided in the system.

### User [$]

It is you. User doesn't have any privilege to do things as much as root user do. For instance, you can create, delete, or even changing files that resides in your home directory without any needs to use superuser or root privilege. But as you can see, it is limited, unless you have been added to sudo group by root or another sudo group user.

## File System

### Filesystem Hierarcy Standard

Filesystem Hierarcy Standard [FHS] is maintained by Linux Foundation.

| Folder | Name | Contents |
|---|---|---|
| /bin | binary | Software and Commmands used in the system. |
| /boot | boot | Everything that's needed for booting the system. |
| /dev | devices | Device lists, disks, CD-ROM, partition (sda,sda1). |
| /etc | etcetera | System specific configuration files. |
| /home | home | Home folder for users in the machine. |
| /media | media | Automatically mounted devices. |
| /mnt | mount | Manually mounting for devices. |
| /opt | optional | Optional software that's outside from the system. |
| /proc | process | System processes and sudo files. |
| /root | root | Home directory for root user. |
| /run | run | RAM processes will be found here. |
| /sbin | sbinary | Software used for administering the system(#). |
| /tmp | temporary | Temporary copies of the session apps. |
| /srv | service | Server will store files here. |
| /sys | system | Changing settings here will be temporary |
| /usr | user | External resources under users will be found here. |
| /var | variable | All other variables related to sys and session. |

**source :** https://www.youtube.com/watch?v=HbgzrKJvDRw

### Home Directory [~]

To show hidden files use ctrl + h, you will then see hidden files that resides here. When you customize your system, you'll see all your configs here. To navigate your folder, you might need to use pcmanfm or any file manager for as GUI software, or use ranger in command-line interfaces.

## Command-Line Interface [CLI]

In unix-based system such as Linux, you might want to accustom yourself with command line interface. There are some perks using this kind of approach in managing your system, hence it'll also comes with it's own pros and cons.

### Pros

- It's fast to navigate your system once you get accustomed to it.
- Minimum RAM usage and can be opened as much as you want.
- It's known that you can run task faster here, as long as you know what to do.
- Customize everything to your heart's content.

### Cons

- Hard to use if you're here for the first time.
- No fancy animations you get from GUI application.
- Actually you can do it; ***if you have time to spare.***

### Shell

Bash is GNU Bourne-Again SHell is a language used for processing or running commands in the command-line interface. Bash, ZSH, Fish or any other flavour of Shell [sh] is using most of syntaxes that Bash is using.

Flavour that is introduced in Linux based system are mostly to make configuration that is tailored to your taste rather than one-size-fits-all solutions.

**CLI Command Lists**

| Command | Name | Usage | Options |
|---|---|---|---|
| pwd | Path to current folder | pwd | |
| cd | Change Directory | cd /home/username | |
| ls | List Directory | ls /home/username | -lash |
| clear | Clear Terminal | clear | |
| cat | Concatenate | cat anomaly.txt | |
| rm | Remove files or dirs | rm anomaly.txt | -rf |
| cp | Copy documents or dir | cp anomaly.txt | -r |
| mv | Move file or directory | mv anomaly.txt anom/ | |
| touch | Create file | touch anomaly.txt | |
| mkdir | Create directory | mkdir anom/ | |
| locate | Search for files | locate -i ano* | |
| find | Search on give dir | find /home/ -name an.txt | |
| grep | Search through text | grep anomaly ano.txt | |
| sudo | SuperUser Do | sudo apt install | |
| df | Disk space usage | df -m | -m |
| du | Disk usage | du | -h |
| head | View n-lines from head | head -n 5 anomaly.txt | |
| tail | View n-ines from bottom | tail -n 5 anomaly.txt | |
| diff | Show changes between files | diff anom1.txt anom2.txt | |
| chown | Change owner to | chown file user | user |
| chmod | Change modifiers to (-rwx) | chmod +x anom.sh | rwx |
| kill | Kill program | kill PID | |
| wget | Download things from web | wget https://link.com | |

| Command | Name | Usage | Options |
|---|---|---|---|
| uname | Linux system information | uname -a | -a, -r |
| history | CLI Command history | history | |
| htop | See running processes | htop | |
| man | Manual page for everything | man bash | |
| zip | zip files | zip -r anomaly.zip anom | -r |
| unzip | unzip files | unzip anomaly.zip | |
| echo | Echo data input to | echo ``Lorem Ipsum'' | |
| hostname | Check hostname | hostname | |
| useradd | Add user | useradd anomaly | |
| userdel | Del user | userdel anomaly | |

There are things called alias that use .bash_aliases file in home directory to do shortcut to combine options and command. As an example, you can use :

[.bash_aliases]

alias ls='ls --color=auto --group-directories-first'

What this alias mean is, when you type ls by itself, it'll then run ls --color=auto --group-directories-first along with it. This way you won't need to type all these long command to call ls with options that you mostly use, just put it in .bash_aliases file, and you're good to go. You can check alias that you've been specified by typing `alias' in your terminal, and it'll show your aliases.

## Distros or DE?

Distribution manage all your packages. You might want to use Debian based distros if you're new to linux.

| Base | Package Manager | Usage |
|---|---|---|
| Arch | package-manager | pacman -Syyu |
| Debian | aptitutde | apt-get install |
| Fedora | Dandified YUM | dnf install |

There are tailored distros that are based on above mainline ditros, they might be tailored for specified category in mind, like gaming, studio, and so on.

| Flavour | Tailored For |
|---|---|
| PopOS! | Gaming |
| Manjaro | Easy to use Arch Based Desktop |
| PeppermintOS | Reviving old laptops |
| RedHat | Servers |
| Ubuntu Studio | Studio |
| Kali Linux | Network & Hacking |

Desktop Enviornment or Desktop interfaces is the graphical interface that you'll be interacting with.

| Desktop Environment | Best Distro |
|---|---|
| GNOME | PopOS! / Ubuntu |
| KDE Plasma | Kubuntu |
| Xfce | Manjaro / Mint |
| Deepin Desktop | UbuntuDDE |
| Budgie | Solus |
| Cinnamon | Mint |
| Pantheon | Elementary OS |
| MATE | Ubuntu |

| Desktop Environment | Best Distro |
|---|---|
| LXDE/LXQt | PeppermintOS |

**Youtube Sources :**

- Infinitely Galactic
- Chris Titus Tech

# Networking

## IP Address

In this day and age, we have devices that always have a conversation over the network, internet connection that always on. For each devices, we have addresses associated with them, in this case, it'll be IP Address. There's two kind of IP Addresses associated with every device :

- **Public IP Address**

  Devices that are connected always have this kind of IP Address, it's what Internet Service Providers [ISP] give to your devices. This IP can be used by public if they know your Public IPs, so it's best to never show this IP to anyone but yourself.

- **Local IP Address**

  This IP is associated with your device if you're connected to the router, your router will give you IP Addresses based on their own subnet, usually this will be 192.168.1.0/24. Typical IP for router will be like this.

| IP Address | Device |
|---|---|
| 192.168.1.1 | Router |
| 192.168.1.2 | Smartphone |
| 192.168.1.3 | Laptop |
| 192.168.1.4 | Desktop |

This ip usually will be allocated based on who connected first to the router network, and then any device after that will be listed under the connected device. This setting can be configured in your device if you want to connect to the same IP Address everytime you connect to the router, this approach use

static IP instead of dynamic IP that are used by the router. For each config that you want to use, please refer to your router provider or company manual.

ifconfig

By running this command, you'll see an example of what your network might look like. Most of the network will provide some IPs and interfaces or network card device that'll be associated with what type of network they use.

For instance you have three interfaces built-in to your device.

```
lo: flags=##<UP,LOOPBACK,RUNNING>  mtu ######
        inet 127.0.0.1  netmask 255.0.0.0

wlan: flags=##<UP,BROADCAST,RUNNING,MULTICAST>  mtu ######
        inet 192.168.1.XX  netmask 255.255.255.0  broadcast 192.168.1.255
```

**lo**

Lo stands for localhost, here you'll see your localhost IP, it'll always be 127.0.0.1 it's used as a loopback address, if you want to open software that are using port 8888 to open a Jupyter Notebook, you'll then type localhost:8888 it'll then resolve to `127.0.0.1:8888', but you won't see 127.0.0.0.1 in your browser, if you type localhost because of DNS resolver.

**eth0 [wired]**

This is your ethernet connection, if you're not having eth0 in your ifconfig results, then it means your device doesn't have eth0 installed, it's the case for newer laptops that're ditching ethernet for a slimmer device. To use eth, in this case you might want to buy a separate ethernet adapter dongle so you can connect with ethernet wired connection.

**wlan0 [wireless]**

It is strange that if your laptop, smartphone, or any device post-2010 that doesn't have wlan0. This can be found in any devices that you might have right now, though in some cases you might not found this if you're using desktop. This should come with most of your devices without the needs for buying a wireless adapter, but if you're in cyber security or any environment that might need a second wireless card, you might want to buy one that have monitoring support that comes with it, most Alfa wireless adapter comes with this already configured out-of-the-box.

| Device | IP Adress |
|---|---|
| Router IP Address | 192.168.1.0/24 |
| Localhost | 127.0.0.1/24 |

## DNS

Computer is recognized by numbers not name, to understand this, they use DNS or Domain Name System to be used as an alias to call an IP Address that are associated with it. DNS is used for resolving name to numbers, for example:

IP Address xxx.xxx.xxx.xxx is associated with Google.com

By doing this it'll cache xxx.xxx.xxx.xxx to dns server, and whenever you ask for Google.com, it'll go to the IP Address associated with it and show that you're connected to Google.com.

But Domain Name System Servers not all knowing, so they made a hierarcy sorted by Root Servers (.org, .com, .edu, etc.).

Google.com (com will be the root)

IP Address are leased to a DHCP server, if the address associated with the device is still present, then the lease attached with it, will be renewed. On

the other end, once DHCP server know that the IP associated with the device is not in use, or disconnected, the IP Address will then be back to IP Addresses pool to be used again with another computer.

## Router & Hub

> Hub is dumb, don't be like hub. Send one to ALL. Router is smart, be like router. Send one to ONE.

## Protocols

### TCP/IP

***Transmission Control Protocol*** // this internet protocol is often used in http or https, it is known to be reliable and precise in its execution. TCP use sequence when it sends a packet, it'll reduce congestion in the traffic and easier for receiver to understand the packet it receive.

### UDP

***User Datagram Protocol*** // often used in DNS because it's faster in its execution, but it's not as reliable as TCP, it's because there is no sequencial packet sending. UDP relies on its speed to send packets, without using any sequence, so the packet that the reciever get, might be hard to understood, not by human language, but *their* language.

### OSI Layer

| OSI Layer | Analogy | What they do? [analogy] |
|---|---|---|
| Application | Letter (Browser) | Letter or Package you want to send? |
| Presentation | Packaging (Filetypes) | Packaged in Envelope or Box ? |

| OSI Layer | Analogy | What they do? [analogy] |
|---|---|---|
| Session | Address Checking | Local or International address? |
| Transport | Stamp | Which stamps are you using? |
| Network | Post Office (TCP/UDP) | Post office, post box? |
| Datalink | Transportation | Transported by truck, plane, boat? |
| Physical | Delivery | Who will deliver the letter? |

**Analogy Example**

You want to send a letter to a friend in another country. You specify that what you're going to use is letter. After you choose what kind of package you want to send, then what will it be covered in? You choose that it's best to just use envelope to send it, since it'll be just the letter. Then you write their address in the envelope. After you create your letter, put it inside the `envelope' and write the address, then you put stamps in your letter, but since you want to send it over with a courrier, they will put your envelope inside their envelope to indicate that envelope will be then delivered. To deliver this, the courrier will send it to the Post Office to then transport it with a plane since it's faster. This will then be delivered to the nearby Post Office on the receivers end.

On the reciever ends, once the postman put it in the nearest gateaway from the airport, it'll then transported by truck into the nearest Post  Office, by checking stamps and envelope that are given by the courrier, it is then sent to the address with the mailer envelope and the letter will reach it's destination.

**Application**

This layer is where you define what application are you using for viewing contents, your browser belongs here. Letter is analogy of the things that you want to

send.

**Presentation**

This is where your file will be presented, your filetypes (.pdf, .docs, etc.) are resides in this layer. This is where your envelope comes in, because you choose to send it as a `letter' with an envelope.

**Session**

This is where the you throw your address in and to insure that the receiver can recieve the letter or not. This is where statuses comes in, if the receiver status is down, then the intended message won't reach at all.

**Transport**

TCP and UDP resides here, to send packets, server will then determine, if you're using a browser to access https, to use TCP. The courrier will send the envelope to the Post Office but before that, he's encapsulating the enveloped letter with another envelope so it'll be safer. Stamps indicate ports that it'll be using, since you're accessing https, it'll be using port 443.

**Network**

In here, you'll be seeing Source and Destination IPs, this is where your `Post Office' comes in, you'll be seeing Source IP Address and its Destination IP Address.

**Datalink**

What interface you're accessing this packet with, wlan0 or eth0 resides here. The letter is transported by plane from origin to receiver.

**Physical**

This is where the postman comes in, he'll then delivering it to the nearest gateaway in the airport. This is where you know how the letter will then be

delivered. This also where the packet actually sent to the receiver, maybe from eth0 to eth0.

# Penetration Testing

There are some preparation before we go into Penetration Testing as a whole, as you might see before, there are various distros catered to this needs as penetration tester. Hacking in general doesn't always meant to be virtual or over the network, hacking can also be used in physical senses. Breaching the perimeter through virtual or physical spaces means that you have to do some researching beforehand, this kind of approach we often call it as **reconnaissance phase.**

## Phases

There are 7 Phases that'll be discussed here, in which is :

| Phases | Categories |
|---|---|
| Reconnaissance | Pre-Engagement |
| Scanning and Enumeration | Pre-Engagement |
| Exploitation | Engagement |
| Post-Exploitation | Engagement |
| Writing Reports | Post-Engagement |

### Reconnaissance

This phase include all pre-engagement knowledge, most of the time, you'll spend more time gathering data here rather than doing an attack. You might want to refer this like when you're in a military. You might be doing the operation

for 1 hour or so, but the gathering phases starts around 6-12 month before the engagement even happen. In our case as cybersecurity penetration tester, you might gather data for a good amount of time, it might take 1 or 2 weeks before you're ready to do the engagement phases. There are some thing that you have to prepare here before moving up to the next phases. This phases often called as passive information gathering or footprinting.

- Gather data through *OSINT* (Open Source Intelligence)
- Gather information about the company (Shifts, servers, systems)
- Contact (Email address phone numbers, job postings)
- Employee that is unhappy about the job (Sentimental data)

| Name | Usage | Commands |
|---|---|---|
| NsLookup | DNS Server records | nslookup google.com |
| Traceroute | Measuring route to target | traceroute google.com |
| Ping | Check if host is alive or not | ping google.com |
| Whois | Domain and IP address info | whois google.com |
| Maltego | Easy to use OSINT GUI | maltego |
| Google | Dorks inside google search engine | insert query with opts |
| Social Media | Instagram, Twitter, Facebook, etc. | |
| Sherlock | Username search in multiple sites | sherlock username |

**Scanning and Enumeration**

Once you know all the information outside of the system, now we need to know what we will expect inside the system that we're going to breach. In this phase, we might need to use some tools that can be used for enumerating a system such as nmap. Once you know which port are open and what you're going to do with it, we can then go into exploitation phase. Always search for any details inside the

system, you might want to refer to this results from scanning metasploitable 2 system.

As a root user or if you have sudo privilege, run this command to do enumeration to the system, I use 192.168.56.101 because it's the IP's of vmbox for metasploitable 2.

```
user@hostname # nmap -O -sV -T4 192.168.56.101
```

| Port | Name | Product // Version |
|---|---|---|
| 21 | ftp | vsftpd 2.3.4 |
| 22 | ssh | OpenSSH 4.7p1 Debian 8ubuntu1 |
| 23 | telnet | Linux telnetd |
| 25 | smtp | Postfix smtpd |
| 53 | domain | ISC BIND 9.4.2 |
| 80 | http | Apache httpd 2.2.8 |
| 111 | rpcbind | 2 |
| 139 | netbios-ssn | Samba smbd 3.X - 4.X |
| 445 | netbios-ssn | Samba smbd 3.X - 4.X |
| 512 | exec | netkit-rsh rexecd |
| 513 | login | |
| 514 | shell | Netkit rshd |
| 1099 | java-rmi | GNU Classpath grmiregistry |
| 1524 | bindshell | Metasploitable root shell |
| 2049 | nfs | 2-4 |
| 2121 | ftp | ProFTPD 1.3.1 |
| 3306 | mysql | MySQL 5.0.51a-3ubuntu5 |
| 3632 | distccd | distccd v1 |
| 5432 | postgresql | PostgreSQL DB 8.3.0 - 8.3.7 |
| 5900 | vnc | VNC |

| Port | Name | Product // Version |
|---|---|---|
| 6000 | X11 | |
| 6697 | irc | UnrealIRCd |
| 8009 | ajp13 | Apache Jserv |
| 8180 | http | Apache Tomcat/Coyote JSP engine 1.1 |
| 8787 | drb | Ruby DRb RMI |
| 33206 | nlockmgr | 1-4 |
| 40304 | mountd | 1-3 |
| 57133 | status | 1 |
| 57741 | java-rmi | GNU Classpath grmiregistry |

As you can see on this table, there are ports that you can choose from to do some exploitation. Beware, this is example of a vulnerable built system. In your case, when you're enumerating and scanning a machine or system, it might not be look like this machine, it might only have some ports open, so you might want to refer to your system and penetration test lab for open ports.

Other ways to do enumerating is by providing web-based social engineering and sending scripts that once run will connect you to the machine that you're going to exploit.

We can use Wireshark to help with scanning and enumerating we have access to a WiFi hotspot, that way, we can sniff the traffic and understand what's happening inside the network we're in. This is especially useful for checking if there's telnet, ftp, or any deprecated and unsecure service is running.

**Exploitation**

To exploit a system, you might need scripts that are tailored to vulnerabilities that you found. It'll be easier for you to run nmap scans to know the service

they're using before doing this. Refer to CVE information for more understanding about the exploit that you want to use, since there are 145197 CVE's as of 2020.

There are many resources that you can find to learn about CVE's and exploitation in general.

There are many types of attack that you can do once you enumerate the target system. In Cipher, there are some exploits that we can use :

- Web Application Attacks
- Network Attacks
- Memory-based attacks
- Wi-Fi attacks
- Zero-Day Angle
- Physical Attacks
- Social engineering

Once you're inside the system, there are some things that we should do :

1. Privilege Escalation

   Obtain root privilege, see (root [#]) for more info about what we can do as root user. This will lead in owning the system. To do this, first you have to check what kind of privilege you've gained. If it's based on user rather than root, then you have to use some exploit such as meterpreter , look for `/etc/passwd' file, or brute-forcing (not recommended).

2. Maintaining Access & Backdoors

   As a penetration tester, this part is usually skipped, because you don't want to use access to the system again until they patch the system and ask you to do it again. This part is generally if you're in need of accessing the system again if the vulnerabilities hasn't been patched.

### Post-Exploitation

After you do all exploits, you might want to do some post exploitation to either maintain access, or retracing all the command you used for documentation. This phase is where targets system has been exploited.

### Writing Reports

Starts by documenting what you do before you write the actual writeups for reports. By doing this, not only you'll learn about the processes as a whole but reproducibility just in case they want to try it themselves.

## Distribution

To start, it's easier to use distro that is tailored specifically for Offensive Security & Defensive security. Distros that are specifically used for hacking are already installed with bunch of tools that can be used for Red or Blue Teaming alike.

Word of Caution! Please don't use these distros as your mainly driver if you don't know what you're doing, since usage of this without any monitoring might lead to vulnerabilites in your system. Also these distros are advised to be used inside a vmbox or live cd's as per their nature of offensive part of networking distros. You've been warned.

| Flavour | Tailored For | Links |
|---|---|---|
| Kali Linux | Hacking | https://www.kali.org/downloads/ |
| Parrot OS | Security & Privacy | https://www.parrotsec.org/download/ |
| Black Arch | Network & Hacking | https://blackarch.org/downloads.html |

Although it is advised to use this distros for built in out-of-the-box tools, as

long as you know how to search for packages and repos, it's possible to just use any mainline based distros to just add repos for each respective distros and use it, it's not advised but possible.

## Tools

### WiFi Cracking

This will be where you make choices to pawn your target wifi, this used in ***Reconnaissance Phase***. This way, if you're around the perimeter where you can use targets wifi, then use this tools.

**CLI Tools :**

- wifite
- aircrack-ng [airmon-ng, airodump-ng, aireplay-ng]

**GUI Tools :**

- fern wifi cracker
- kismet
- wireshark (monitoring)

**Source:**

- Newhorizons - Networking Basics
- Hostinger - Bash Commands
- Metasploitable2
- NetworkChuck - OSI Layer
- Network Direction - OSI Layer

English is not my primary language, since I wrote this for public use, I try to use English as much as I can. Sorry for any grammatical errors, happy Learning!