# Cybersecurity 701

## ip/ifconfig Lab

# ip/ifconfig Materials

- This lab will explore the ifconfig command in a Linux Terminal
- Materials needed
  - Kali Linux Machine
- Software Tools used
  - ip (Linux Command)
  - hostname (Linux Command)
  - ifconfig (Linux Command)

# Objectives Covered

- Security+ Objectives (SY0-701)
  - Objective 5.5 - Explain types and purposes of audits and assessments
    - Penetration testing
      - Reconnaissance
        - Passive
        - Active

# What is ip/ifconfig?

- The **`ip`** command shows/manipulates the routing, network devices, and interfaces
  - **`ip`** stands for **I**nternet **P**rotocol
- The **`ifconfig`** command can configure a network interface
  - **`ifconfig`** stands for **I**nter**F**ace **CONFIG**ure

```
IP(8)                                    Linux                                    IP(8)

NAME
       ip - show / manipulate routing, network devices, interfaces and tunnels

SYNOPSIS
       ip [ OPTIONS ] OBJECT { COMMAND | help }

       ip [ -force ] -batch filename

       OBJECT := { link | address | addrlabel | route | rule | neigh | ntable | tunnel |
                tuntap | maddress | mroute | mrule | monitor | xfrm | netns | l2tp |
                tcp_metrics | token | macsec | vrf | mptcp }

       OPTIONS := { -V[ersion] | -h[uman-readable] | -s[tatistics] | -d[etails] | -r[es-
                olve] | -iec | -f[amily] { inet | inet6 | link } | -4 | -6 | -I | -D | -B |
                -0 | -l[oops] { maximum-addr-flush-attempts } | -o[neline] | -rc[vbuf]
                [size] | -t[imestamp] | -ts[hort] | -n[etns] name | -N[umeric] | -a[ll] |
                -c[olor] | -br[ief] | -j[son] | -p[retty] }

OPTIONS
       -V, -Version
              Print the version of the ip utility and exit.
```

```
IFCONFIG(8)               Linux System Administrator's Manual               IFCONFIG(8)

NAME
       ifconfig - configure a network interface

SYNOPSIS
       ifconfig [-v] [-a] [-s] [interface]
       ifconfig [-v] interface [aftype] options | address ...

DESCRIPTION
       Ifconfig is used to configure the kernel-resident network interfaces.  It is used at
       boot time to set up interfaces as necessary.  After that, it is usually only  needed
       when debugging or when system tuning is needed.

       If  no arguments are given, ifconfig displays the status of the currently active in-
       terfaces.  If a single interface argument is given, it displays the  status  of  the
       given  interface  only;  if a single -a argument is given, it displays the status of
       all interfaces, even those that are down.  Otherwise, it configures an interface.

Address Families
       If the first argument after the interface name is recognized as the name of  a  sup-
       ported  address  family, that address family is used for decoding and displaying all
       protocol addresses.  Currently supported address families include inet (TCP/IP,  de-
       fault), inet6 (IPv6), ax25 (AMPR Packet Radio), ddp (Appletalk Phase 2), ipx (Novell
 Manual page ifconfig(8) line 1 (press h for help or q to quit)
```

# ip/ifconfig Lab Overview

- Set up Environment
- The **`ip`** Command
- The **`hostname`** Command
- The **`ip`** Command (Routes)
- The **`ifconfig`** Command

# Set up Environment

- Log into your range
- Open the Kali Linux Environment
  - You should be on your Kali Linux Desktop
  - Open a new Terminal

# The `ip` Command

- Just entering the ip command will show the following result:

```
ip
```

```
┌──(kali@10.15.60.24)-[~]
└─$ ip
Usage: ip [ OPTIONS ] OBJECT { COMMAND | help }
       ip [ -force ] -batch filename
where  OBJECT := { address | addrlabel | fou | help | ila | l2tp | link |
                   macsec | maddress | monitor | mptcp | mroute | mrule |
                   neighbor | neighbour | netconf | netns | nexthop | ntable |
                   ntbl | route | rule | sr | tap | tcpmetrics |
                   token | tunnel | tuntap | vrf | xfrm }
       OPTIONS := { -V[ersion] | -s[tatistics] | -d[etails] | -r[esolve] |
                    -h[uman-readable] | -iec | -j[son] | -p[retty] |
                    -f[amily] { inet | inet6 | mpls | bridge | link } |
                    -4 | -6 | -I | -D | -M | -B | -0 |
                    -l[oops] { maximum-addr-flush-attempts } | -br[ief] |
                    -o[neline] | -t[imestamp] | -ts[hort] | -b[atch] [filename] |
                    -rc[vbuf] [size] | -n[etns] name | -N[umeric] | -a[ll] |
                    -c[olor]}
```

- Notice all the options? Find the current version of the ip utility using “-V”

```
ip -V
```

```
┌──(kali@10.15.60.24)-[~]
└─$ ip -V
ip utility, iproute2-5.14.0, libbpf 0.4.0
```

# The `ip` Command

- Show the status of various network interfaces of this system
  **`ip addr show`**
- Here, the first network is **`lo`**, which is the loopback address
  - On Linux, this will always be the first address
  - The address of **`lo`** is always **`127.0.0.1`**
- The second network is **`eth0`**, which shows this has a wired connection
  - **`wlan0`**, would signify it's a wireless connection
- This is where you will find the IP Addresses assigned to the current host

```
┌──(kali@10.15.60.24)-[~]
└─$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 100
0
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc mq state UP group default qlen 1
000
    link/ether 0a:cc:0a:f4:8a:f1 brd ff:ff:ff:ff:ff:ff
    inet 10.15.60.24/17 brd 10.15.127.255 scope global dynamic eth0
       valid_lft 2306sec preferred_lft 2306sec
    inet6 fe80::8cc:aff:fef4:8af1/64 scope link
       valid_lft forever preferred_lft forever
```

IPv4 Address  IPv6 Address

# The `ip` Command

- To show the IP address for your network connection

  **`ip addr show`** **`<network_name>`**

- Notice the loopback is not displayed. (How might you show the loopback?)

```
┌──(kali@10.15.60.24)-[~]
└─$ ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc mq state UP group default qlen 1
000
    link/ether 0a:cc:0a:f4:8a:f1 brd ff:ff:ff:ff:ff:ff
    inet 10.15.60.24/17 brd 10.15.127.255 scope global dynamic eth0
       valid_lft 2224sec preferred_lft 2224sec
    inet6 fe80::8cc:aff:fef4:8af1/64 scope link
       valid_lft forever preferred_lft forever
```

- Shorten the results with the **`-br`** flag (brief result)

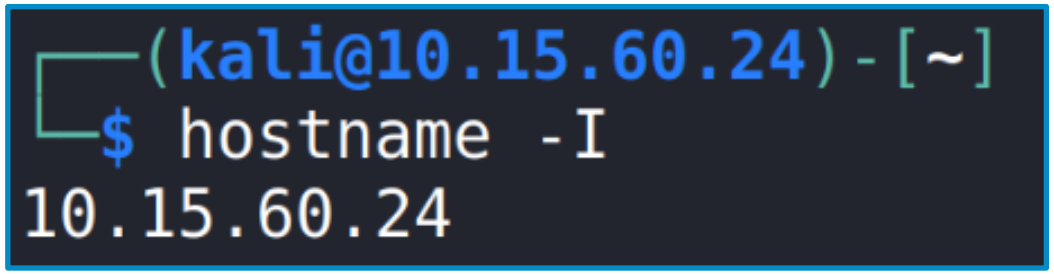
  **`ip -br addr show`** **`<network_name>`**

```
┌──(kali@10.15.60.24)-[~]
└─$ ip -br addr show eth0
eth0             UP             10.15.60.24/17 fe80::8cc:aff:fef4:8af1/64
```

# The `hostname` Command

- While the `ip` command is very powerful, what if you want to show only the assigned IP Address?
- Use the following command to show only the IP Address*:
  - **`Hostname -I`**

*Note: You may also receive the MAC address with this command!



# The `ip` Command (Routes)

- List the ip routes
  **`ip r`**
- Add an ip route*
  **`sudo ip r add <New_Route_IP> via <Default_IP>`**
- Show the route
  **`ip r`**

*Change **`add`** to **`del`** to delete the route

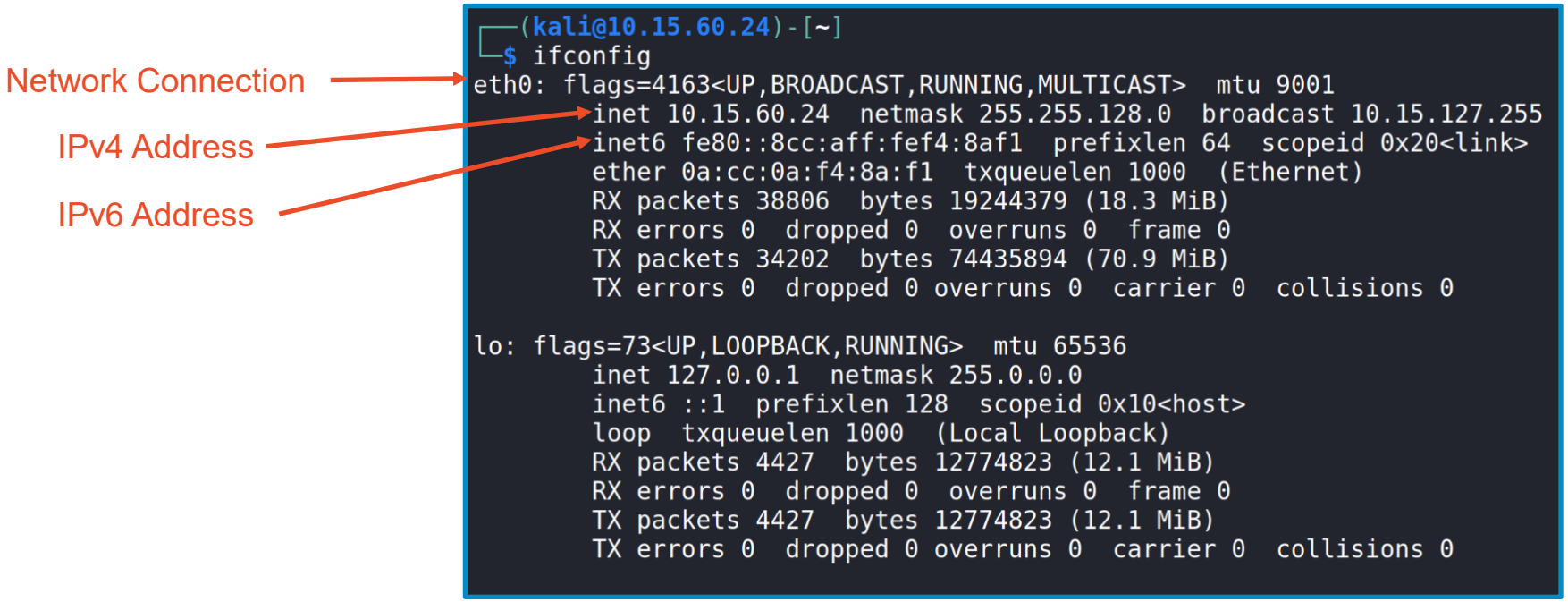
```
┌──(kali@10.15.60.24)-[~]
└─$ ip r
default via 10.15.0.1 dev eth0
10.15.0.0/17 dev eth0 proto kernel scope link src 10.15.60.24

┌──(kali@10.15.60.24)-[~]
└─$ sudo ip r add 10.15.58.213 via 10.15.0.1

┌──(kali@10.15.60.24)-[~]
└─$ ip r
default via 10.15.0.1 dev eth0
10.15.0.0/17 dev eth0 proto kernel scope link src 10.15.60.24
10.15.58.213 via 10.15.0.1 dev eth0
```

The new route

# The `ifconfig` Command

- Use the **`ifconfig`** command to show the interfaces

  **`ifconfig`**



# The `ifconfig` Command

- To show stats for a specified network interface:
  - `ifconfig <Network_Name>`

```
┌──(kali@10.15.60.24)-[~]
└─$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 9001
        inet 10.15.60.24  netmask 255.255.128.0  broadcast 10.15.127.255
        inet6 fe80::8cc:aff:fef4:8af1  prefixlen 64  scopeid 0x20<link>
        ether 0a:cc:0a:f4:8a:f1  txqueuelen 1000  (Ethernet)
        RX packets 39011  bytes 19264747 (18.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 34429  bytes 74650384 (71.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

# The `ifconfig` Command **up** and **down**

- The following command will turn a network on:

  **sudo ifconfig <Network_Name> up**

- The following command will turn a network off*:

  **sudo ifconfig <Network_Name> down**

  *Please Note: This will turn the internet connection off, if you are using a cyber range that is utilizing a remote desktop, you will lose access to the system