Linux Network Configuration for Penetration Testers

1. Introduction

Understanding Linux network configuration is essential for penetration testers. It helps in setting up environments, manipulating traffic, and discovering or exploiting vulnerabilities.

2. Network Interfaces

- Tools: `ifconfig`, `ip`
- Information: IP addresses, netmasks, interface status
- Configuring Interfaces:

```
sudo ifconfig eth0 up
sudo ip link set eth0 up
sudo ifconfig eth0 192.168.1.2
sudo ifconfig eth0 netmask 255.255.255.0
sudo route add default gw 192.168.1.1 eth0
```

3. DNS Configuration

Edit `/etc/resolv.conf` for temporary DNS changes:

```
nameserver 8.8.8.8
nameserver 8.8.4.4
```

Make persistent DNS changes using network management tools or by modifying `/etc/network/interfaces`.

4. Static IP Setup

Example `/etc/network/interfaces`:

```
auto eth0
iface eth0 inet static
  address 192.168.1.2
  netmask 255.255.255.0
  gateway 192.168.1.1
  dns-nameservers 8.8.8.8 8.8.4.4
```

Apply changes:

```
sudo systemctl restart networking
```

5. Network Access Control (NAC)

Access Control Models

Type	Description
DAC	Resource owners define permissions.
MAC	OS enforces strict access based on labels.
RBAC	Role-based access simplifies user privilege management.

6. Network Monitoring Tools

- `syslog`, `rsyslog`, `ss`, `lsof`
- ELK Stack: Elasticsearch, Logstash, Kibana
- Purpose: detect breaches, misconfigurations, or data leaks

7. Troubleshooting Tools

- `ping`: Test host connectivity.
- `traceroute`: Discover network paths.
- `netstat`: View active connections and listening ports.
- `tcpdump`, `wireshark`: Analyze traffic.
- Common issues include DNS misconfiguration, hardware failures, and congestion.

8. Hardening and Security Mechanisms

SELinux

- MAC system enforcing policies at kernel level.
- High granularity and security; complex configuration.

AppArmor

- MAC system using user-friendly profiles.
- Easier to manage but less granular than SELinux.

TCP Wrappers

- Simple IP-based service access control.
- Lightweight but limited compared to SELinux/AppArmor.

9. Recommendation

Practice configuring security tools in a VM with snapshots. Hands-on experimentation deepens understanding.