Introduction to network analysis

Will learn:

```
.Network Basics
.How to capture Traffic
.How to analyze packets captures (PCAPs) in wireshark and TCPDump
.Work to uncover suspicious or malicious activities
```

Associated Roles:

```
Threat Hunter: Threat Hunters will analyze PCAPs and live traffic whilst hunting
for threats. This can include search for unusual communications, such as traffic,
non-standard ports, scanning activity, exfiltration, etc...
```

SOC/Security Analyst:

```
Security Analysts will be monitoring and responding to attacks over the network,
and need to be able to differentiate normal activity from suspicious activity. They
will observe and respond to port scanning, vuln´s scanning, DDoS and unusual
network traffic.

Incident Responders: Responders need to be able to identify, triage, and respond to
an endless range of security incidents, and often this will include some form of
network analysis to understand connections between compromised systems internally
or externally.
```

Penetration Testers:

```
This role involve in the identification of open ports and running services, and the
need to know how to hide their traffic both externally and when they gain access to
a system they need to pivot and move from system to system hiding from network
defenders.
```