

Int

## Introduction to network intrusion tactic

### What you'll learn

- Network security
- Network intrusion tactic
- Network attack protection

### The case for securing network

#### Common network intrusion attacks

- malware
- Spoofing
- Packet sniffing
- Packet flooding

Attack can harm an org. by

- Leaking valuable or confidential information
- Damaging an organization reputation
- Impacting customer retention
- Costing money and time

## Secure networks against denial of service attack

### Denial of service attacks

An attack that targets a network or server and floods it with network traffic

### Distributed Denial of service attack (DDoS)

A type of denial of service attack that uses multiple



device or server in different location to flood the target network with unwanted traffic.

Syn (synchronize) flood attack

A type of DoS attack that simulates a TCP connection and floods a server with SYN packets.

Internet Control Message Protocol (ICMP)

An internet protocol used by devices to tell each other about data transmission errors across the network.

ICMP Flood

A type of DOS attack performed by an attacker repeatedly sending ICMP packets to a network security server.

Ping of death: A type of DOS attack caused when a hacker pings a system by sending it an oversized ICMP packet that is bigger than 64 KB.



## Network attack tactics and defense

### Malicious packet sniffing

Passive packet sniffing : The type of attack where data packets are read in transit.

Active packet sniffing : A type of attack where data packets are manipulated in transit.

IP spoofing : A network attack performed when an attacker changes the source IP of a data packet to impersonate an authorized system and gain access to network.

Common :

- on path attack
- Replay attack
- Smurf attack

On path attack : An attack where a malicious actor places themselves in the middle of an authorized connection and intercepts or alters the data in transit.

Replay attack : A network attack performed when a malicious actor intercepts a data packet in transit and delays it or repeats it at another time.

Smurf attack : A network attack performed when an attacker sniffs an authorized user's IP address and floods it with packets.