

# Glossary terms from week 3 & wrap-up

Nice job finishing this section!

Let's review what you've learned so far.

We discussed how to secure networks.

We also learned about network intrusion tactics like malicious packet sniffing and IP spoofing.

Finally, we discussed how a security analyst can protect against these attacks.

You've learned about DoS and DDoS attacks like ICMP flooding, SYN attacks, and the ping of death, which try to overwhelm a network by flooding it with unwanted data packets.

Now, just think about everything you know already about network attacks.

What you've learned in these videos will be essential in your work as a security analyst.

Coming up, you'll learn about how security analysts can protect the network using various security hardening techniques.

## Terms and definitions from Course 3, Week 3

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

**Botnet:** A collection of computers infected by malware that are under the control of a single threat actor, known as the "bot-herder"

**Denial of service (DoS) attack:** An attack that targets a network or server and floods it with network traffic

**Distributed denial of service (DDoS) attack:** A type of denial or service attack that uses multiple devices or servers located in different locations to flood the target network with unwanted traffic

**Internet Control Message Protocol (ICMP):** An internet protocol used by devices to tell each other about data transmission errors across the network

**Internet Control Message Protocol (ICMP) flood:** A type of DoS attack performed by an attacker repeatedly sending ICMP request packets to a network server

**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 a network

**Network Interface Card (NIC):** Hardware that connects computers to a network

**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

**Packet sniffing:** The practice of capturing and inspecting data packets across a network

**Passive packet sniffing:** A type of attack where a malicious actor connects to a network hub and looks at all traffic on the network

**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 64KB

**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 ICMP packets

**Synchronize (SYN) flood attack:** A type of DoS attack that simulates a TCP/IP connection and floods a server with SYN packets

---

Revision #1

Created 3 July 2023 07:12:20 by naruzkurai

Updated 3 July 2023 10:29:21 by naruzkurai