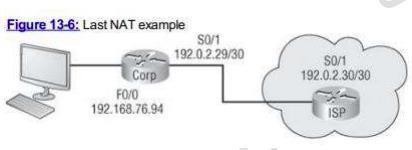


6.Explain with Command

A. DONE



Module 10 CCNA - Security threat landscape

# Beginner Question

1. Explain Security Threat
   1. A security threat is a malicious act that aims to corrupt or steal data or disrupt an lranization’s system or the entire organization.
2. What is mitigation Techniques?
   1. Mitigation is the reduction of something harmful or the reduction of its harmful effects. It may refer to measures taken to reduce the harmful effects of hazards that remain in potentia, or to manage harmful incidents that have already occurred.

# Intermediate Question

* + 1. Explain DoS Attacks
       1. A denial of service [DOS] attack is an attack meant to shut down a machine or network

making it inaccessible to its intended users.

* + 1. Explain DDoS
       1. A distributed denial of service [DDos] acctack s a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.
    2. Explain IP spoofing
       1. IP spoofing, or IP address spoofing, refers to the creation of Internet protocol [IP] packets with a false source IP address to impersonate another computer system.

# Advance Question

* + - * 1. What is social Engineering Attack?

Social engineering is the tactic of manipulating, influencing, or deceing a victim in order to gain control over a computer system, or to steal personal and financial information.

* + - * 1. Explain Man-In-The Middle Attack

A man in the middle (MITM) attack is a general term for when a perpetrator positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway.