10.3.12 DoS Countermeasure Facts

Unlike many of the other attacks we've discussed, denial-of-service attacks are not frequently used by ethical hackers. So, why study them? Well, because it's hard to fight against something you don't know about. Understanding how the denial-of-service attacks work will help you to provide countermeasure recommendations to your clients.

This lesson covers the following topics:

- DoS and DDoS attack prevention
- DoS and DDoS attack protection
- DoS and DDoS attack response

DoS and DDoS Attack Prevention

There are two ways to prevent DoS and DDoS attacks:

Method	Description
Limit access points	Limit the number of servers that are accessible from outside the network.
Limit services	Disable unnecessary services on live systems.

DoS and DDoS Attack Protection

Method	Description
Enable router throttling	Router throttling limits the potential impact of a DoS attack and can provides a bit of additional response time for administrators to respond to an attack.
Reverse proxy	All traffic is redirected to the reverse proxy before being forwarded to the real server. In the event of an attack, the proxy takes the impact.
Threat management systems and intrusion prevention systems	Threat management and intrusion prevention systems provide numerous protections, including VPNs, anti-spam, and load balancing.
Anti-malware tools	Anti-malware tools help to reduce the risk of Trojan infections and bot installations.
Anti-spoofing measures	Anti-spoofing measures ensure that spoofed packets are unable to infiltrate your network.
RFC 3704	Blocks packets from IP addresses that are not being used (typically performed by the ISP).
Black hole filtering	Creates an area of the network, also known as a black hole, where offending traffic is forwarded and dropped.

DoS and DDoS Attack Response

It is important to be prepared for a DoS attack. These attacks are becoming more common, and although the large-scale attacks against large companies catch the spotlight, small and mid-sized companies are also seeing an increase in attacks.

Method	Description
Response plan	Your response plan should include a checklist of all threat assessment tools and hardware protections you have in place. This way, you know where to go to find information about what exactly you're up against. You'll want to have a pre-determined group of people defined as your response team. All members of this team should know what their role is in the response and where to find the information they need. You'll also want a communication plan. Who needs to know what information? When do they need this information? Some attacks may have a quick and simple fix, but others may escalate quickly, so you'll want to have an escalation plan in place. At what point do you switch over to your redundant systems? At what point do you decide to completely shut everything down? Response plans are extremely important, and as an ethical hacker, you'll probably play a large part in helping companies develop their response plans.
Attack absorption	Add extra services such as load balancing and excess bandwidth so that you have too much for the attacker to be able to flood. Of course, this is a pricey option, as it requires extensive resources and planning.
Service degradation	Set services to throttle or even shut down in the event of an attack.

Backup provider	Have more than one upstream connection to use as a failover in the event of a flooding attack.