# CCNA 640-802 Bible - Identify security threats to a network and describe general methods to mitigate those threats

1. What should be part of a comprehensive network security plan? A: Allow users to develop their own approach to network security. B: Physically secure network equipment from potential access by unauthorized individuals. C: Encourage users to use personal information in their passwords to minimize the likelihood of passwords being forgotten. D: Delay deployment of software patches and updates until their effect on end-user equipment is well known and widely reported. E: Minimize network overhead by deactivating automatic antivirus client updates. Correct Answers: B Explanation: Computer systems and networks are vulnerable to physical attack; therefore, procedures should be implemented to ensure that systems and networks are physically secure. Physical access to a system or network provides the opportunity for an intruder to damage, steal, or corrupt computer equipment, software, and information. When computer systems are networked with other departments or agencies for the purpose of sharing information, it is critical that each party to the network take appropriate measures to ensure that its system will not be physically breached, thereby compromising the entire network. Physical security procedures may be the least expensive to implement but can also be the most costly if not implemented. The most expensive and sophisticated computer protection software can be overcome once an intruder obtains physical access to the network. 2. Which type of attack is characterized by a flood of packets that are requesting a TCP connection to a server? A: denial of service B: brute force C: reconnaissance D: Trojan horse Correct Answers: A Explanation: A denial-of-service attack (DoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to, motives for and targets of a DoS attack may vary, it generally comprises the concerted, malevolent efforts of a person or persons to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. Among these are Network connectivity attacks. These attacks overload the victim with TCP packets so that its TCP/IP stack is not able to handle any further connections, and processing queues are completely full with nonsense malicious packets. As a consequence of this attack, legitimate connections are denied. One classic example of a network connectivity attack is a SYN Flood. 3. What are two recommended ways of protecting network device configuration files from outside network security threats? (Choose two.) A:Allow unrestricted access to the console or VTY ports. B:Use a firewall to restrict access from the outside to the network devices. C:Always use Telnet to access the device command line because its data is automatically encrypted. D:Use SSH or another encrypted and authenticated transport to access device configurations. E:Prevent the loss of passwords by disabling password encryption. Correct Answers: B, D Explanation: Whenever the trusted (inside) part of the network connects to an untrusted (outside, or internet) network, the use of a firewall should be implemented to ensure only legitimate traffic is allowed within the enterprise. SSH is a secure alternative to telnet that encrypts the traffic so that data carried within can not be "sniffed." It is always recommended to use SSH over telnet whenever possible. 4. What are two security appliances that can be installed in a network? (Choose two.) A:ATM B:IDS C:IOS D:IOX E:IPS F:SDM Correct Answers: B, E 5. Refer to the following protocols, which one can create a secure terminal connection to a remote network device? A: Telnet B: SSH C: WEP D: SNMPv1 Correct Answers: B Explanation: Secure Shell (SSH) is a protocol which provides a secure remote access connection to network devices.