Weekly challenge 3 **Due** Jun 25, 11:59 PM +08 Graded Quiz • 50 min

defense

intrusion

44 sec

Introduction to network intrusion Congratulations! You passed! tactics Go to next item Secure networks against Denial of Service (DoS) attacks Quiz • 50 min Network attack tactics and **Review Learning Objectives** Review: Secure against network 1. What happens during a Denial of Service (DoS) attack? 1/1 point Video: Wrap-up The attacor successfully impersonates an authorized user and gains access to the network. Reading: Glossary terms from week Try again The target ជ្រានអ្នក ខ្មែរក្រុម ខេត្តក្រុម ខេត្តក្រក្រុម ខេត្តក្រុម ខេត្តក្រាម ខេត្តក្រុម ខេត The network is infected with malware. Quiz: Weekly challenge 3
10 questions The data packets containing valuable information are stolen as they travel across the network. **Receive grade** Your grade **View Feedback ⊘** Correct To Pass 80% or higher We keep your highest score (DDoS) attacks? Select three answers. A DDoS attack may use multiple devices in different locations to flood the target network with unwanted traffic. **⊘** Correct ☑ In both DoS and DDoS attacks, if any part of the network is overloaded, the attacks are successful. **⊘** Correct A DoS attack targets a network or server. **⊘** Correct A DoS attack involves multiple hosts carrying out the attack. X This should not be selected Please review <u>the video about DoS attacks</u> ☐. 3. A security team discovers that an attacker has taken advantage of the handshake process that is used to establish a TCP connection between a device and their server. Which DoS attack does this scenario describe? O Ping of Death On-path attack O ICMP flood SYN flood attack **⊘** Correct 4. Fill in the blank: The maximum size of a correctly formatted IPv4 ICMP packet is \_\_\_\_\_, as opposed to the 1 / 1 point oversized packet that is sent during a Ping of Death attack. 64KB 15Gb O 64TB 32KB **⊘** Correct **5.** Which of the following statements correctly describe passive and active packet sniffing? Select three answers. 0.75 / 1 point Passive packet sniffing allows malicious actors to view the information going in and out of the targeted **⊘** Correct Active packet sniffing involves data packets being manipulated in transit. **⊘** Correct ✓ Using a VPN to encrypt data offers a business protection from packet sniffing. **⊘** Correct The purpose of active packet sniffing is to read data packets while in transit. X This should not be selected Please review the video about malicious packet sniffing [2]. 6. As a security professional, you take steps to stop an attacker from changing the source IP of a data packet in order to impersonate your authorized system. What type of network attack are you working to prevent? Active packet sniffing Passive packet sniffing IP spoofing O Ping of Death **⊘** Correct 7. What are some common IP spoofing attacks? Select all that apply. 0 / 1 point on-path attacks **⊘** Correct replay attacks **⊘** Correct smurf attacks **⊘** Correct KRACK attacks X This should not be selected Please review the video about spoofing  $\Box$ . 8. In which attack would a malicious actor place themselves in the middle of an authorized connection and intercept 1/1 point the data in transit? Smurf attack O Packet flooding attack Malware attack On-path attack **⊘** Correct 9. Fill in the blank: The \_\_\_\_\_ network attack occurs when an attacker intercepts a data packet in transit, then 1 / 1 point repeats it at another time. On-path replay O SYN flood smurf **⊘** Correct 10. Which combination DoS and IP spoofing attack can bring down an entire network by flooding an authorized user's 1/1 point IP address with packets? Replay attack Smurf attack On-path attack O Ping of Death **⊘** Correct