REVIEWER FOR 1ST SEMESTER AY 2011-2012

FORESEC CERTIFICATE IN NETWORKING SECURITY

Instruction: *Select the letter of the correct answer.*

1. Your company's network just finished going through a SAS 70 audit. This audit reported that overall, your network is secure, but there are some areas that needs improvement. The major area was SNMP security. The audit company recommended turning off SNMP, but that is not an option since you have so many remote nodes to keep track of.

   What step could you take to help secure SNMP on your network?

   a. Change the default community string names
   b. Block all internal MAC address from using SNMP
   c. Block access to UDP port 171
   d. Block access to TCP port 171

2. Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into his former company's network. Since Simon remembers some of the server names, he attempts to run the axfr and ixfr commands using DIG.

   What is Simon trying to accomplish here?

   a. Enumerate all the users in the domain
   b. Perform DNS poisoning
   c. Send DOS commands to crash the DNS servers
   d. Perform a zone transfer

3. You are the security analyst working for a private company out of France. Your current assignment is to obtain credit card information from a Swiss bank owned by that company. After initial reconnaissance, you discover that the bank security defenses are very strong and would take too long to penetrate. You decide to get the information by monitoring the traffic between the bank and one of its subsidiaries in London. After monitoring some of the traffic, you see a lot of FTP packets traveling back and forth. You want to sniff the traffic and extract usernames and passwords.

   What tool could you use to get this information?

   a. RaidSniff b. Snort c. Ettercap d. Airsnort

4. George is the network administrator of a large Internet company on the west coast. Per corporate policy, none of the employees in the company are allowed to use FTP or SFTP programs without obtaining approval from the IT department. Few managers are using SFTP program on their computers. Before talking to his boss, George wants to have some proof of their activity.

   George wants to use Ethereal to monitor network traffic, but only SFTP traffic to and from his network. What filter should George use in Ethereal?

   a. net port 22
   b. udp port 22 and host 172.16.28.1/24
   c. src port 22 and dst port 22
   d. src port 23 and dst port 23

5. You are assisting a Department of Defense contract company to become compliant with the stringent security policies set by the DoD. One such strict rule is that firewalls must only allow incoming connections that were first initiated by internal computers.

   What type of firewall must you implement to abide by this policy?

   a. Circuit-level proxy firewall
   b. Packet filtering firewall
   c. Application-level proxy firewall
   d. Statefull firewall

6. George is performing security analysis for Hammond and Sons LLC. He is testing security vulnerabilities of their wireless network. He plans on remaining as "stealthy" as possible during the scan.

   Why would a scanner like Nessus is not recommended in this situation?
   a. Nessus is too loud
   b. There are no ways of performing a "stealthy" wireless scan
   c. Nessus cannot perform wireless testing
   d. Nessus is not a network scanner

7. You work as a penetration tester for Hammond Security Consultants. You are currently working on a contract for the state government of California. Your next step is to initiate a DoS attack on their network.
   Why would you want to initiate a DoS attack on a system you are testing?

   a. Use attack as a launching point to penetrate deeper into the network
   b. Demonstrate that no system can be protected againstDoS attacks
   c. List weak points on their network
   d. Show outdated equipment so it can be replaced

8. Harold is a web designer who has completed a website for ghttech.net. As part of the maintenance agreement he signed with the client, Harold is performing research online and seeing how much exposure the site has received so far. Harold navigates to google.com and types in the following search.

   link:www.ghttech.net
   What will this search produce?

   a. All sites that link to ghttech.net
   b. Sites that contain the code: link:www.ghttech.net
   c. All sites that ghttech.net links to
   d. All search engines that link to .net domains

9. Jason has set up a honeypot environment by creating a DMZ that has no physical or logical access to his production network. In this honeypot, he has placed a server running Windows Active Directory. He has also placed a Web server in the DMZ that services a number of web pages that offer visitors a chance to download sensitive information by clicking on a button.

   A week later, Jason finds in his network logs how an intruder accessed the honeypot and downloaded sensitive information. Jason uses the logs to try and prosecute the intruder for stealing sensitive corporate information.

   Why will this not be viable?
   a. Intruding into a honeypot is not illegal
   b. Entrapment
   c. Intruding into a DMZ is not illegal
   d. Enticement

10. Which of the following actions best describes the term IP spoofing?
    a. Trying to guess a password.
    b. Pretending to be someone you are not.
    c. Capturing TCP/IP traffic.
    d. Trying to crack an encryption key.

11. Harold wants to set up a firewall on his network but is not sure which one would be the most appropriate. He knows he needs to allow FTP traffic to one of the servers on his network, but he wants to only allow FTP-PUT. Which firewall would be most appropriate for Harold? needs?

    a. Application-level proxy firewall
    b. Data link layer firewall
    c. Packet filtering firewall
    d. Circuit-level proxy firewall

12. When setting up a wireless network with multiple access points, why is it important to set each access point on a different channel?
    a. Avoid cross talk
    b. Avoid over-saturation of wireless signals
    c. So that the access points will work on different frequencies
    d. Multiple access points can be set up on the same channel without any issues

13. A packet is sent to a router that does not have the packet destination address in its route table, how will the packet get to its properA packet is sent to a router that does not have the packet? Destination address in its route table, how will the packet get to its proper destination?
    a. Root Internet servers
    b. Border Gateway Protocol
    c. Gateway of last resort
    d. Reverse DNS

14. You are a security analyst performing reconnaissance on a company you will be carrying out a penetration test for. You conduct a search for IT jobs on Dice.com and find the following information for an open position:

    7+ years experience in Windows Server environment
    5+ years experience in Exchange 2000/2003 environment Experience with Cisco Pix Firewall, Linksys 1376 router, Oracle 11i and MYOB v3.4 Accounting software are required MCSA desired, MCSE preferred
    No Unix/Linux Experience needed

    What is this information posted on the job website considered?
    a. Information vulnerability
    b. Social engineering exploit
    c. Trade secret
    d. Competitive exploit

15. John and Hillary works at the same department in the company. John wants to find out Hillary's network password so he can take a look at her documents on the file server. He enables Lophtcrack program to sniffing mode. John sends Hillary an email with a link to Error! Reference source not found.

    What information will he be able to gather from this?

    a. The SID of Hillary's network account
    b. The network shares that Hillary has permissions
    c. The SAM file from Hillary's computer
    d. Hillary's network username and password hash

16. Terri works for a security consulting firm that is currently performing a penetration test on First National Bank in Tokyo. Terri's duties include bypassing firewalls and switches to gain access to the network. Terri sends an IP packet to one of the company's switches with ACK bit and the source address of her machine set.

    What is Terri trying to accomplish by sending this IP packet?

    a. Poison the switch's MAC address table by flooding it with ACK bits
    b. Enable tunneling feature on the switch
    c. Trick the switch into thinking it already has a session with Terri's computer
    d. Crash the switch with aDoS attack since switches cannot send ACK bits

17. Tyler is setting up a wireless network for his business that he runs out of his home. He has followed all the directions from the ISP as well as the wireless router manual. He does not have any encryption set and the SSID is being broadcast. On his laptop, he can pick up the wireless signal for short periods of time, but then the connection drops and the signal goes away. Eventually the wireless signal shows back up, but drops intermittently.

    What could be Tyler issue with his home wireless network?
    a. 2.4Ghz Cordless phones
    b. Satellite television
    c. CB radio
    d. Computers on his wired network

18. You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe.

    What are you trying to accomplish here?
    a. Enumerate domain user accounts and built-in groups
    b. Establish a remote connection to the Domain Controller
    c. Poison the DNS records with false records
    d. Enumerate MX and A records from DNS

19. Why is it a good idea to perform a penetration test from the inside?
    a. It is easier to hack from the inside
    b. It is never a good idea to perform a penetration test from the inside
    c. To attack a network from a hacker's perspective
    d. Because 70% of attacks are from inside the organization

20. Meyer Electronics Systems just recently had a number of laptops stolen out of their office. On these laptops contained sensitive corporate information regarding patents and company strategies. A month after the laptops were stolen, a competing company was found to have just developed products that almost exactly duplicated products that Meyer produces.

    What could have prevented this information from being stolen from the laptops?
    a. SDW Encryption b. EFS Encryption c. DFS Encryption d. IPS Encryption