Network+ Guide to Networks, Seventh Edition

Chapter 8, Solutions

Review Questions

1. Your organization has just approved a special budget for a network security upgrade. What procedure should you conduct in order to make recommendations for the upgrade priorities?

A. Data breach

B. Security audit

C. Exploitation

D. Posture assessment

Answer: D. Posture assessment

2. What wireless attack might a potential hacker execute with a specially configured transmitter?

A. Jamming

B. Vulnerability

C. Evil twin

D. Zero-day exploit

Answer: A. Jamming

3. What kind of vulnerability is exploited by a ping of death?

   A. Zero-day exploit

B. Buffer overflow

C. Social engineering

D. Backdoor

Answer: B. Buffer overflow

4. Which type of DoS attack orchestrates an attack using uninfected computers?

A. DDoS (distributed DoS) attack

B. Smurf attack

C. DRDoS (distributed reflector DoS) attack

D. PDoS (permanent DoS) attack

Answer: C. DRDoS (distributed reflector DoS) attack

5. What software might be installed on a device in order to authenticate it to the network?

A. Operating system

B. Security policy

C. NAC (network access control)

D. Agent

Answer: D. Agent

6. What feature of Windows Server allows for agentless authentication?

A. Active Directory

B. ACL (access control list)

C. IDS (intrusion detection system)

D. Network-based firewall

Answer: A. Active Directory

7. What kind of firewall blocks traffic based on application data contained within the packets?

A. Host-based firewall

B. Content-filtering firewall

C. Packet-filtering firewall

D. Stateless firewall

Answer: B. Content-filtering firewall

8. What of the following features does *not* distinguish an NGFW from traditional firewalls?

A. Application Control

B. IDS and/or IPS

C. User awareness

D. UTM (Unified Threat Management)

Answer: D. UTM (Unified Threat Management)

9. At what layer of the OSI model do proxy servers operate?

A. Layer 3

B. Layer 2

C. Layer 7

D. Layer 4

Answer: C. Layer 7

10. What kind of virus runs in place of the computer’s normal system files?

A. Worms

B. Macro viruses

C. File-infector viruses

D. Boot sector viruses

Answer: D. Boot sector viruses

11. What unique characteristic of zero-day exploits make them so dangerous?

Answer: The vulnerability is exploited before the software developer has the opportunity to provide a solution for it.

12. What characteristic of ARP makes it particularly vulnerable to being used in a DoS attack?

Answer: ARP performs no authentication.

13. A neighbor hacks into your secured wireless network on a regular basis, but you didn’t give him the password. What loophole was most likely left open?

Answer: The default password was not changed.

14. Regarding managing security levels, why do network administrators create domain groups?

Answer: To simplify the process of granting rights to users

15. What kinds of issues might indicate a misconfigured ACL?

Answer: Connectivity and performance issues between two hosts in which some applications or ports can make the connection while others can't

16. Any traffic that is not explicitly permitted in the ACL is _______________, which is called the ______________________.

Answer: denied, implicit deny rule

17. What's the difference between an IDS and an IPS?

Answer: An IDS can only detect and log suspicious activity. An IPS can react when alerted to such activity.

18. What causes most firewall failures?

Answer: Firewall misconfiguration

19. What are the two primary features that give proxy servers an advantage over NAT?

Answer: Content filtering, file caching

20. What distinguishes a virus from other types of malware?

Answer: A virus can replicate itself with the intent to infect more computers.