CYBS 7357 Lab 05 Quiz

\*Answers are shown in yellow

1. Penetration testing tests the strengths and weaknesses of the IT security, as well as the:

a. readiness of the facility and/or employees to respond to an attack.

b. readiness of white-hat hackers to respond to an attack.

c. ability of white-hat hackers to make successful attacks when necessary.

d. ability of personnel to complete the time-consuming job of typing commands.

2. Which of the following statements is true regarding penetration testing?

a. It is considered an art, but not a science.

b. It is only done by individuals outside the organization, not by employees.

c. It can be done by black-hat hackers as a part of their targeting rituals.

d. It is too sophisticated to be done by script kiddies searching for a story to tell.

3. Which step of penetration testing includes the remediation of the vulnerabilities?

a. Reconnaissance

b. Scanning

c. Vulnerability analysis

d. Post-attack activities

4. What is another term used to describe the vulnerability analysis step of penetration testing?

a. Exploitation

b. Enumeration

c. Examination

d. Scanning

5. Which step of penetration testing includes the actual attack?

a. Exploitation

b. Enumeration

c. Examination

d. Scanning

6. Which of the following statements is true regarding the automated tools used for penetration testing?

a. Pen testers typically use automated tools after attacking a system to identify the various vulnerabilities that have been exploited.

b. Automated tools are all the same in terms of the target environments they work against.

c. Pen testers often use more than one tool to help identify vulnerabilities from a number of sources.

d. Automated tools have completely replaced humans typing specialized commands for specialized circumstances.

7. Which of the following statements is true regarding the security configuration of an organization?

a. White-hat hackers generally know nothing about the security configuration of the IT system they are trying to penetrate.

b. There are many possible security postures of any network and its constituent parts, from highly secure to not secure at all.

c. It is not a good idea for pen testers to have advance information about the security configuration of a network.

d. Actual attackers are likely to know as much about the environment as employees or those who are hired to protect that environment.

8. Which of the following rules exist to identify the type of traffic from the private (inside) network at 172.30.0.0/24 that should be allowed to pass through the firewall?

a. Inbound rules on the LAN

b. Outbound rules on the WAN

c. Outbound rules on the LAN

d. Inbound rules on the WAN

9. Domain Name Service runs on port:

a. 21.

b. 25.

c. 53.

d. 110.

10. Which of the following rules exist to block or permit the public (outside) traffic from coming into the 172.30.0.0 network?

a. Inbound rules on the LAN

b. Outbound rules on the WAN

c. Outbound rules on the LAN

d. Inbound rules on the WAN

11. For defenders, the last step in penetration testing is \_\_\_\_\_\_\_\_\_\_, during which vulnerabilities are fixed and the pen test steps are repeated to ensure the attack can’t occur again.

a. covering their tracks

b. remediation

c. exploitation

d. validation

12. For attackers, the last step in penetration testing is often \_\_\_\_\_\_\_\_\_\_, during which log files or other forensic information is destroyed or modified.

a. covering their tracks

b. remediation

c. exploitation

d. validation

13. Which of the following is the first phase in the attacker “kill chain” process?

a. Reconnaissance

b. Weaponization

c. Delivery

d. C2 (command and control)

14. In which of the following phases of the attacker “kill chain” process do attackers use a combination of technical and social engineering approaches to develop specific tools, such as spear-fishing e-mails or mobile apps?

a. Reconnaissance

b. Weaponization

c. Delivery

d. Exploitation

15. A probe or even a full pen test is often a precursor to which phase in the attacker “kill chain” process?

a. Reconnaissance

b. Weaponization

c. Delivery

d. C2 (command and control)

16. In which of the following phases in the attacker “kill chain” process is the attack actually unleashed?

a. C2 (command and control)

b. Weaponization

c. Delivery

d. Exploitation

17. Which of the following phases in the attacker “kill chain” process includes a component during which the results of exploitation are reported but can also include additional targeting and tasks?

a. C2 (command and control)

b. Weaponization

c. Delivery

d. Exploitation

18. The Nessus report summary includes \_\_\_\_\_\_ :

a. forensic evidence against black-hat hackers.

b. a comparison of findings over several scans.

c. a ranking of the network’s security.

d. both a bar chart and a pie chart showing the distribution of vulnerability findings.

19. In the lab, the detailed vulnerability information in the Nessus reports provided a(n):

a. hexadecimal description of the problem and no solution possibilities.

b. plain-English, high-level description of the problem and a hint at the solution.

c. encrypted description of the problem and a hint at the solution.

d. highly detailed description of the problem but no solution possibilities.

20. Which of the following statements is true regarding pen testing?

a. Pen testing is only considered marginal as a security control.

b. It is not necessary to re-scan a system or network to validate changes.

c. It is not necessary to re-scan a system after patching programs.

d. Closing some vulnerability issues can expose other vulnerabilities.

NAME:

Natnael kebede