Heber Paz
22 MAR 07
NIST 800-42

Answer 10 of 12

1. What is the purpose of Network Security Testing?
The purpose is to prevent incidents from happening at all.
2. Describe basic capabilities and limitations of vulnerability testing.
The limitations include not being able to detect certain types of problems or may result in positive scores (in the testing) which are false.
3. Why are security test results valuable?
They are valuable to help to point out vulnerabilities in a network that would otherwise go unnoticed. The cost of the tests would be offset by the amount saved on an incident response.
4. What does a comprehensive network scan produce?
It produces a list of all active hosts and services, printers, switches, and routers operating in the address space. Some scans provide the OS, versions, and open ports.
5. What does network scanning enable an organization to do?
It enables "an organization to maintain control of its IP address space" and ensures its hosts "run only approved network services."
6. Describe the types of corrective actions that may be necessary as a result of network scanning.
Corrective actions include "closing discovered and exploited vulnerabilities, modifying… security policies, creating procedures to improve security practices, and conducting security awareness training."
7. Compare and contrast port and vulnerability scanners.
"Port scanners identify active hosts, services, applications" and OS. Both scanners identify hosts and open ports. Vulnerability scanners provide information on the vulnerabilities associated with the hosts and open ports while port scanners rely on human interpretation to find vulnerabilities.
8. Describe a vulnerability scanner and possible scanner capabilities.
N/A
9. Describe the types of corrective actions that may be necessary as a result of vulnerability scanning.
You can patch to mitigate vulnerabilities. You can improve configuration management program and procedures to upgrade systems routinely. You can monitor vulnerability alerts and mailing lists that apply to the organization's environment. You can modify the organization's security policies and architecture to include appropriate system updates and upgrades.
10. What is the purpose of penetration testing?
The purpose is to uncover hidden vulnerabilities that are not found by vulnerability testing.
11. Compare and contrast blue teaming and red teaming.
Blue teaming and red teaming are both types of penetration testing. Blue team is overt with the knowledge and permission of the IT staff. Red team is covert without knowledge of the IT staff but with consent from upper management.
12. Select a few of the General Information Security Principles. Present them. Elaborate on their importance.
N/A