Pablo Hernandez
ITEC4390.13086

NIST 800-42
Assignment

1. **What is the purpose of Network Security Testing?**

   Testing serves several purposes. One, it allows discovery of exploitable flaws which will always be present or surface over time. Two, security testing is important for understanding, calibrating, and documenting the operational security posture of an organization. Three, security testing is an essential component of improving the security posture of your organization.

2. **Describe basic capabilities and limitations of vulnerability testing.**

   Vulnerability testing may result in many false positive scores, or it may not detect certain types of problems that are beyond the detection capabilities of the tools.

3. **Why is security testing results valuable?**

   Security testing results are valuable because they provide insight to how secure the tested environment may or may not be, limited only by the tools used. For example, if you use basic tools to perform a vulnerability assessment your results may fair well. However, if you use more sophisticated tools along with a penetration test the results may differ. Once you have discovered any vulnerabilities then you can subsequently repair them.

   Specifically, security testing results can be used in the following ways:
   - As a reference point for corrective action,
   - In defining mitigation activities to address identified vulnerabilities,
   - As a benchmark for tracing an organization's progress in meeting security requirements,
   - To assess the implementation status of system security requirements,
   - To conduct cost/benefit analysis for improvements to system security, and
   - To enhance other life-cycle activities, such as risk assessments, Certification and Authorization (C&A), and performance improvement efforts.

4. **What does a comprehensive network scan produce?**

   A list of all active hosts and services, printers, switches, and routers operating in the address space scanned by the port-scanning tool, i.e., any device that has a network address or is accessible to any other device.

Pablo Hernandez
ITEC4390.13086

5. **What does network scanning enable an organization to do?**

   Organizations should conduct network scanning to:
   - Check for unauthorized hosts connected to the organization's network,
   - Identify vulnerable services,
   - Identify deviations from the allowed services defined in the organization's security policy,
   - Prepare for penetration testing,
   - Assist in the configuration of the intrusion detection system (IDS), and
   - Collect forensics evidence.

6. **Describe the types of corrective actions that may be necessary as a result of network scanning.**

   The following corrective actions may be necessary as a result of network scanning:
   - Investigate and disconnect unauthorized hosts,
   - Disable or remove unnecessary and vulnerable services,
   - Modify vulnerable hosts to restrict access to vulnerable services to a limited number of required hosts (e.g., host level firewall or TCP wrappers), and
   - Modify enterprise firewalls to restrict outside access to known vulnerable services

7. **Compare and contrast port and vulnerability scanners.**

   Network scanning involves using a port scanner to identify all hosts potentially connected to an organization's network, the network services operating on those hosts. While vulnerability scanners take the concept of a port scanner to the next level. Like a port scanner, a vulnerability scanner identifies hosts and open ports, but it also provides information on the associated vulnerabilities (as opposed to relying on human interpretation of the results). Most vulnerability scanners also attempt to provide information on mitigating discovered vulnerabilities.

8. **Describe a vulnerability scanner. In your answer, include possible scanner capabilities.**

   Vulnerability scanners provide system and network administrators with proactive tools that can be used to identify vulnerabilities before an adversary can find them. A vulnerability scanner is a relatively fast and easy way to quantify an organization's exposure to surface vulnerabilities.

Vulnerability scanners provide the following capabilities:

- Vulnerability scanners provide the following capabilities:
- Identifying active hosts on network
- Identifying active and vulnerable services (ports) on hosts.
- Identifying applications and banner grabbing.
- Identifying operating systems.
- Identifying vulnerabilities associated with discovered operating systems and applications.
- Identifying misconfigured settings.
- Testing compliance with host application usage/security policies.
- Establishing a foundation for penetration testing.

9. Describe the types of corrective actions that may be necessary as a result of vulnerability scanning.

The following corrective actions may be necessary as a result of vulnerability scanning:

- Upgrade or patch vulnerable systems to mitigate identified vulnerabilities as appropriate.
- Deploy mitigating measures (technical or procedural) if the system cannot be immediately patched (e.g., operating system upgrade will make the application running on top of the operating system inoperable), in order to minimize the probability of this system being compromised.
- Improve configuration management program and procedures to ensure that systems are upgraded routinely.
- Assign a staff member to monitor vulnerability alerts and mailing lists, examine their applicability to the organization's environment and initiate appropriate system changes.
- Modify the organization's security policies, architecture, or other documentation to ensure that security practices include timely system updates and upgrades.

10. What is the purpose of penetration testing?

The purpose of penetration testing is to identify methods of gaining access to a system by using common tools and techniques used by attackers.