Security Testing

Vulnerability Assessments are passive

Look for known weaknesses: Open ports, weak passwords, misconfigured or default settings.

Penetration Testing is active

Attempt to exploit weaknesses found, often from vulnerability assessment

The role of a tester is to document weaknesses found Remediation should come from elsewhere (Separation of Duties)

White box: mimics what an admin could do—full network knowledge

Black box: mimics an external user with no knowledge of environment

Grey box: what a user with basic permissions could do—some knowledge of environment

3 rules of security testing (In this order)

1. Meet with Management and discover objectives of test
2. Define Rules of Engagement
3. GET WRITTEN PERMISSION from senior management or other authorized entity

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Network Analysis

Sniffers

System with Network card in “promiscuous” mode. Means that the NIC can pick up ALL traffic, not just what is addressed to it.

Sniffer + Analysis Engine is an IDS

Host-based IDS (HIDS) only examines a single system—overhead, and doesn’t scale well

Network based (NIDS) examines a network segment. Uses analysis engines:

Pattern Based—matches a known pattern (for instance, a signature—like a virus definition file)—can’t detect new malware (zero-day attacks)

Profile based (behavior-based systems) look for network anomalies—May have false positives (Systems alert that a type of traffic attack, but it is actually incorrect and the traffic is actually normal network behavior. A false negative is when a system fails to detect an attack. Both are negative, so those should be minimized.