GIPMC®
GLOBAL INSTITUTE OF PROFESSIONAL MANAGEMENT CERTIFICATION

Exam Name - Certified Information Systems Penetration Tester (CISPT)™

Sample Exam

1. What is the main purpose of a Rules of Engagement (RoE) in a penetration test?

A. List vulnerabilities found
B. Define scope, permissions, constraints
C. Set firewall configurations
D. Provide daily progress reports

Answer **B**

2. Which technique involves gathering system info without direct interaction?

A. Active OS fingerprinting
B. SQL injection
C. Passive OS fingerprinting
D. Service enumeration

Answer **C**

3. Which tool is best suited for passive OS fingerprinting?

A. Nmap
B. Superscan
C. NBTscan
D. p0f

Answer **D**

4. What distinguishes penetration testing from vulnerability scanning?

A. Identifies general threats vs. exploits

B. Vulnerability scanning is active; pen testing is passive

C. Scans only web apps

D. Only pen testing requires legal approval

Answer **A**

5. Which describes grey-box testing?

A. Tester has no system knowledge

B. Full knowledge of internal system

C. Partial system knowledge (e.g. architecture)

D. Automated tool only

Answer **C**

6. What is the correct sequence of penetration testing phases?

A. Reconnaissance → Scanning → Exploitation → Privilege escalation → Reporting

B. Exploitation → Reconnaissance → Reporting → Scanning

C. Scanning → Reconnaissance → Reporting → Exploitation

D. Reporting → Reconnaissance → Exploitation

Answer **A**