The following is a high-level comparison of our five penetration testing service tiers. Not all of these tiers are available (or applicable) to all testing services - ex. Options A and B are not available for mobile app penetration testing.

- Option A: **Automated Testing**
  - Mostly Automated - discovery (ex., hosts, services, web/API endpoints, etc.) followed by vulnerability scanning. Manual effort is limited to verifying coverage; however, individual vulnerabilities are not manually validated, which means some false positives may remain. This service is more thorough than low-cost "automated penetration testing" offerings commonly found on the market and may satisfy certain compliance requirements.
  - Typical findings distribution: ~90% informational, ~2% false positives, ~8% valid vulnerabilities requiring remediation.
  - Pricing starts at: $2,500
- Option B: **Essential Penetration Testing**
  - Partially Automated / Partially Manual - also called a vulnerability assessment. Includes all elements of Automated Testing, plus manual verification of each identified finding (e.g., penetrating the vulnerability). Reconnaissance is minimal to none. This approach is comparable to entry-level penetration testing services offered by other firms and may meet basic compliance requirements (e.g., PCI DSS).
  - Typical verified findings: ~10 (network tests) / ~8 (web app/API).
  - Pricing starts at: $5,000 for net, $8,000 for web or mobile
- Option C: **Basic Penetration Testing**
  - Mostly Manual - testing with an attacker-mindset and exploratory approach, often described as "see what the tester can find/do" or "just like an attacker." While it may incorporate some elements mentioned above, the emphasis is on simulating real-world attacker techniques often with limited knowledge, access, and hours, minimal reconnaissance, and unstructured exploration. Each finding is manually verified. Comparable with other firms' low-cost penetration testing that may satisfy compliance testing requirements.
  - Typical verified findings: This approach may surface fewer findings than Option B but often reveals unique risks that automated-heavy approaches miss. It may also incorporate some red team tactics, though a full red team engagement should be requested separately.
  - Pricing starts at: $5,000 for net, $8,000 for web or mobile
- Option D: **Standard Penetration Testing**
  - Builds on all prior tiers with additional structured testing (semi-automated and manual) and prioritized effort to uncover risks and attack vectors beyond the reach of automated tools. This service is highly likely to exceed industry-standard penetration

tests and provides coverage beyond typical compliance requirements (e.g., OWASP, NIST).
    - Typical verified findings: ~18 (network tests) / ~15 (web app/API).
    - Pricing starts at: $10,000
- Option E: **Premium Penetration Testing**
    - The most comprehensive coverage, following our Premium Testing Guide, which exceeds industry standards and aims for maximum assurance - “no stone is left unturned” where practical and applicable. Testing includes deeper reconnaissance, additional advanced techniques, thorough validation of vulnerabilities, and the highest level of quality assurance processes.
    - Typical verified findings: ~24 (network tests) / ~20 (web app/API).
    - Pricing starts at: $12,500

Additionally, see these companion resources as applicable:

- More detailed comparison of our core services: https://penconsultants.com/serviceComparisonMatrix
- Low-level Net comparison: https://penconsultants.com/netTiers
- Low-level Web App/API comparison: https://penconsultants.com/webTiers
- Other common services: https://penconsultants.com/services/