The following is a high-level comparison of our four penetration testing service tiers. Not all of these tiers are available (or applicable) to all testing services - ex. Options A and B-sub1 are not available for mobile app penetration testing.

- Option A: **Automated Testing**
  - Mostly-automated discovery (hosts, services, web/API endpoints, etc.), followed by a vulnerability scan, with manual verification of coverage, but no manual vulnerability verification. It will contain some false positives and is a step up from the ultra-low-cost "automated penetration testing" services commonly found on the market, which may meet certain compliance testing requirements. On average, ~94% are informational findings and observations, another ~2% are false positives, while ~8% are true positive findings in need of mitigation.
  - Pricing starts at: $2,500
- Option B: **Basic Penetration Testing**
  - Comparable with other testing firms that offer low-cost penetration testing that may meet your compliance testing requirements. It includes manual verification of each finding (e.g. penetrating the vulnerability). Testing services at this tier are generally unavailable during Q4, deadlines treated as best-effort in Q1 and Q3, while Q2 is the only quarter with a guaranteed testing timeline. The client chooses **one** of the following approaches:
    - Sub Option #1: Partially Automated / Partially Manual - This is also called a vulnerability assessment. Includes everything from above (Automated Testing) and manual verification/penetration, but very minimal recon. There are an average of 12 verified findings for network tests, and 10 for web app/API.
    - Sub Option #2: Mostly Manual - This is a "see what the tester can find/do" approach. It may include some of the elements mentioned above, but primarily focuses on testing from a "just like an attacker" perspective, often with limited knowledge and access, a small number of budgeted hours, minimal recon, and taking an unstructured approach to testing. There are often less findings from this approach. *Note: This testing is similar to red teaming but is limited in scope, time, and lacks specific goals. Rather than months of testing, it spans only a few hours. For a more thorough assessment, please ask about our full red teaming services.* Optionally: *These hours could be increased within a larger budget or include other requested testing customizations.*
  - Pricing starts at: $5,000 for net, $8,000 for web or mobile
- Option C: **Standard Penetration Testing**
  - Includes everything from above, but it also prioritizes a number of semi-automated and manual testing hours to identify risky vulnerabilities and attack vectors not otherwise detectable by automated tools. This is near-certain to surpass the thoroughness of other vendors' testing and will exceed your compliance testing

Copyright 2013 - 2025 PEN Consultants, LLC
Confidential & Proprietary

requirements. There are an average of 20 verified findings for network tests, and 17 for web app/API.
    - Pricing starts at: $10,000
- Option D: **Premium Penetration Testing**
    - Includes everything from above, but performs all applicable and practical testing from our premium testing guide, which exceeds all industry testing standards and thoroughness. The goal of this coverage is that “no stone is left unturned”. There are an average of 28 verified findings for network tests, and 24 for 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/

Copyright 2013 - 2025 PEN Consultants, LLC
Confidential & Proprietary