PEN Consultants

PEN Consultants, LLC
13423 Blanco Rd #3124
San Antonio, TX 78216
https://penconsultants.com
Office: 830-446-3411

The following is a high level comparison matrix of our core services. Across the top are the core services, down the left side are the parameters and details of those services.

Our standard & premium services are not ad hoc, time boxed to 1-2 weeks, “see what we can find”, shoot-from-the-hip tests. We meticulously follow and run-to-completion our testing guides which are based on industry testing standards, methodologies, and processes. To be clear, most of our tests do include a portion of “free styling”, but that is balanced with the need to also be thorough in our coverage.

If a parameter is labeled “Required” or “Highly Recommended”, but that is not compatible with your policy, then you will want to look at a different service. If no core service fits exactly what you are in need of, that is not a problem! We can follow the “Custom Approach” column and call the service something like “Security Testing w/Penetration”.

You can find a general comparison of our penetration testing services here: https://penconsultants.com/pentestingTierComparison.

Other unique aspects to how we operate: https://penconsultants.com/whyPENConsultants

We would be honored to serve your organization and assist with your information and cybersecurity testing needs. Reach out to start the conversation! https://penconsultants.com/contactus

	Automated Testing	Penetration Testing (Basic)	Penetration testing (Standard & Premium)	Red Teaming Technique Simulation	Red Teaming Adversary Simulation	Social Engineering	"Security Testing" Custom Approach
OVERVIEW / TOP QUESTIONS							
Description	Our most simplistic testing service that utilizes industry standard automated vulnerability scanners	Sub Option #1: Partially Automated / Partially Manual: The same as "Vulnerability Scanning", with each potential finding penetrated to verify risk Sub Option #2: Mostly Manual - This is a "see what the tester can find/do" / "just like an attacker" approach Pentest Tier Comparisons: https://penconsultants.com/PentestingTierComparison.pdf	Comprehensive, automated, semi-manual, and manual testing performed to industry penetration testing standards Pentest Tier Comparisons: https://penconsultants.com/PentestingTierComparison.pdf	Isolated mitigation and detection verification against a custom risk-tailored and prioritized list of trending attacker techniques	Testing of blue team staff, while attempting stealthy recon and action on pre-defined objectives "just like an attacker would operate" or as training via a more overt/controlled purple team tabletop or full-blown incident response exercise (IRE)	Phishing (email-based), SMS (smishing), phone (vishing), in-person impersonation (physical SE), baiting (ex. USB drops), social media, mailed letters/packages, etc.	If our standards based service offerings do not exactly fit your need, we can take just about any approach you request, and simply call it "Security Testing" or similar
Testing Goal(s)	Identify common technical vulns, misconfigurations, & weaknesses	Identify common technical vulns, misconfigurations, & weaknesses	Identify as many vulns as possible, beyond what an automated scanner can find	Identify as many individual gaps in security solutions, controls, and detections as budgeted time allows	Identify gaps in detection and response, as well as possible in analysis, containment, eradication, and recovery.	Gauge your user's ability to distinguish between legitimate and varying sophistication levels of social engineering	Varies
Common Scope	Corporate network (internal, external, cloud), web apps/APIs	Corporate network (internal, external, cloud), web apps/APIs	Corporate network (internal, external, cloud), web apps/APIs, mobile and thick apps, hardware/IoT, wireless	Monitoring of corporate network (internal, external, cloud), web apps/APIs, wireless, physical	All the things	Users of corporate networks, hardware/IoT, wireless, physical, etc.	Varies
Coverage	Limits of scanner	Sub Option #1: Limits of scanner Sub Option #2: Limits of budgeted testing time	*Varies** NOTE: Our Premium level leaves "no stone is left unturned", whereas our Standard level prioritizes focus	*Focused** NOTE: Focus is restricted to the prioritized testing list, and by budgeted hours	*Laser focused** NOTE: As in, ~99% of the authorized scope will be ignored to focus on the ~1% that may lead to AOO	*Focused** NOTE: For example: email only if phishing is requested	Varies
Meets Compliance Testing Requirements **NOTE: PCI DSS*, SOC 2, HIPAA, NCUA, HITRUST, GDPR, FFIEC, CIS Controls, RBI, etc.**	Maybe	Checks the box	Yes* NOTE: Standard meets all known compliance standards and requirements; Premium far exceeds the same	N/A	Likely Not	N/A	Varies
Industry testing standards our proprietary methodology incorporates	N/A	N/A	Network, Wireless: PTES, NIST SP 800-115, OSSTMM, etc. Web, Mobile: OWASP	MITRE ATT&CK framework, and others as needed	MITRE ATT&CK framework, and aspects of PTES, NIST SP 800-115, OSSTMM, and OWASP	Varies	Varies
Start Date (from client ready date) NOTE: The 'client ready date' is when all deliverables are verified and ready for testing. Our testers are usually engaged in other projects, which must be completed first.	*0-8 weeks out**	*0-8 weeks out**	*0-8 weeks out**	*0-8 weeks out**	*0-8 weeks out**	*0-8 weeks out**	*0-8 weeks out**
Testing Timeframe (from start date) NOTE: If another firm claims to complete testing faster, they are likely not being as thorough as we are. Certain tests cannot be rushed without risking account locks, resource strain, missed findings, etc.	*1-2 weeks**	*2-3 weeks**	*3-6 weeks**	*Starts at 2 weeks** NOTE: This is for a minimally viable engagement, but more hours/time is generally recommended	*2-6 months* adv sim; 1-3 months IRE or tabletop* *NOTE: This is for a minimally viable engagement, but more hours/time is generally recommended*	*1-2 weeks**	Varies
Typical number of findings	Varies	Sub Option #1: 12 (std dev of 5) - typically 7 - 16 Sub Option #2: There are often less findings from this approach	Premium: 26 (std dev of 8) - typically 23 - 35 Standard: 17 (std dev of 7) - typically 14 - 26	Varies	Varies	Varies	Varies
False Positives (FP)	~94% Info, ~2% FP	100% actionable findings	100% actionable findings	100% actionable findings	100% actionable findings	100% actionable findings	Varies
Usage of our testing platform for internal testing (AKA our "dropbox") and provisioning of VDI/Workstation NOTE: See details below	*Required / Highly Recommended**	*Sub Option #1: Required for Internal* *Sub Option #2: Highly Recommended*	*Required / Highly Recommended**	*Required / TBD**	*Varies**	*Rare / Highly Recommended**	Varies
Exceptions/whitelisting in firewalls, WAFs, IPSs, etc. - prevent interference NOTE: See details below	*Required**	*Sub Option #1: Required** *Sub Option #2: Highly Recommended*	*Required**	*Partial**	*Varies**	*Highly Recommended**	Varies
Whitebox, full access and knowledge NOTE: See details below	*Highly Recommended**	*Highly Recommended**	*Highly Recommended**	*Highly Recommended**	*Highly Recommended**	*Highly Recommended**	*Highly Recommended**
Testing Credentials - user, admin, domain admin NOTE: See details below	*Net: Highly Recommended** *Web: Required**	*Net: Highly Recommended** *Web: Required**	*Net, wireless: Highly Recommended** *Web, mobile, thick: Required**	*Highly Recommended / TBD**	*Varies**	*Partial / Highly Recommended**	Varies
Purple Teaming NOTE: See details below	Available	Available	*Recommended**	*Required**	*Required / Varies**	Recommended	Available

	Automated Testing	Penetration Testing (Basic)	Penetration testing (Standard & Premium)	Red Teaming Technique Simulation	Red Teaming Adversary Simulation	Social Engineering	"Security Testing" Custom Approach
Pre-coordination of mitigation - testing activity treated friendly, not hostile NOTE: See details below	*Required**	*Required**	*Required**	*Required / Varies**	*Varies**	*Required**	Varies
Other client deliverables NOTE: See details below	Scoping questionnaire, 2-3 hrs prep	Scoping questionnaire, 3-5 hrs prep	Scoping call and questionnaire, 5-8 hrs prep	Scoping call and questionnaire, 8+ hrs prep, 1-2 hrs/day during testing	Scoping call and questionnaire, 24+ hrs prep, 1-2 hrs/day during testing	Scoping questionnaire, 2-3 hrs prep, 1-2 hrs/day during testing	Scoping call and questionnaire, prep time, ongoing support,
Budget / Cost NOTE: we guarantee the best value, but we will NOT be the "cheapest"	External Net: $2,500+ Internal Net: $4,250+ Web: $4,000+	External Net: $4,500+ Internal Net: $7,000+ Web: $6,000+	External Net: $9,000+ Internal Net: $12,000+ Web: $9,000+ Mobile: $11,000+ Thick: $7,000+ Wireless: $5,000+	$12,000+	$24,000+	Phishing/email: $2,750+ Vishing/voice: $3,000+ Smishing/SMS: $3,000+ Baiting/USB: $3,250+ Physical: $2,250+ plus travel	Varies
Primary cost drivers (in addition to graybox balance, testing accounts, interference, deadlines)	Net: Active IPs Web: Major functions (pages/API endpoints), number of user roles	Net: Active IPs Web: Major functions (pages/API endpoints), number of user roles	Net: Active IPs Web, mobile, thick: Major functions (pages/API endpoints), number of user roles Wireless: APs, SSIDs, clients, travel (if needed), sqft	Desired number of techniques	Goals and objectives	Users targeted, types of SE requested, travel (if needed)	Varies
TYPICAL SCOPE (separate quotes)							
External Network	Available	Available	Available	Available	Partial, all-in-one	Available	Available
Internal Network	Available	Available	Available	Available	Partial, all-in-one	Rare	Available
Cloud	Available	Available	Available	Available	Partial, all-in-one	Available	Available
Web Apps/APIs	Available	Available	Available	Available	Partial, all-in-one	Rare	Available
Mobile Applications	N/A	N/A	Available	Rare	Partial, all-in-one	Rare	Available
Software/Thick Apps	N/A	N/A	Available	Rare	Partial, all-in-one	Rare	Available
Hardware/IoT	N/A	N/A	Available	Rare	Partial, all-in-one	Available	Available
Wireless	N/A	N/A	Available	Available	Partial, all-in-one	Available	Available
Physical	N/A	N/A	N/A	Available	Available	Available	Available
Multiple services performed in parallel NOTE: Multiple requested testing services are usually performed in parallel. Sequential or staged testing incurs additional fees.	*Highly Recommended**	*Highly Recommended**	*Highly Recommended**	*Highly Recommended**	Varies	*Highly Recommended**	Varies
VULNERABILITIES & WEAKNESSES IDENTIFIED							
"Low hanging fruit"	Yes	Yes	Yes	Yes	Limited	Yes	Varies
Misconfigurations	Partial	Partial	Yes	Partial	Limited	Partial	Varies
Control Gaps	Limited	Limited	Yes	Yes	Limited	Partial	Varies
Detection Gaps	Limited	Limited	*Partial** NOTE: Our penetration testing service does not have a core focus on detection testing, but should "light up" your detections	Yes	Yes	Partial	Varies
Process Gaps	N/A	N/A	*Partial** NOTE: As with detection gaps, there are some checks, but it is not a core focus	Varies	Yes	Partial	Varies
IT/Security Staff	N/A	N/A	Rare	Rare	Yes	*Yes** NOTE: Assuming this staff is included in targeted testing	Varies
End Users	N/A	N/A	*Limited** NOTE: Testing against weak user passwords, unsolicited MFA pushes and bombing, etc. but generally NOT "attacking the user"	N/A	Varies	Yes	Varies
CLIENT MUST-HAVES							

	Automated Testing	**Penetration Testing (Basic)**	**Penetration testing (Standard & Premium)**	**Red Teaming Technique Simulation**	**Red Teaming Adversary Simulation**	**Social Engineering**	**"Security Testing" Custom Approach**
Detection Capability	N/A	N/A	Recommended	*Required** NOTE: One of the primary goals of this service is to test detections	*Required** NOTE: One of the primary goals of this service is to test detections and the follow-on incident response	N/A	Varies
SOC	N/A	N/A	N/A	*3rd party SOC at min** NOTE: Requires close coordination w/detection team/MSSP to validate alerts	*In-house SOC required** NOTE: A primary goal is to test YOUR incident response process, not that of a 3rd party	N/A	Varies
Incident Response Capability	N/A	N/A	N/A	N/A	Required	N/A	Varies
CLIENT DELIVERABLES (before testing)							
Call / Conversation	Recommended	Recommended	Required	Required	Required	Recommended	Required
Scoping Questionnaire NOTE: Vulnerability scanning/assessments and social engineering are fairly cookie cutter, with limited info needed. We encourage you to perform these on your own where possible (we can consult). Penetration testing is customized, requiring an understanding of your environment and risks to ensure proper scope and approach. Technical simulation involves coordinating prioritized tests and monitoring their execution. Advanced simulation is highly tailored and requires ongoing conversation with our "trusted insider" throughout the engagement.	*~8-10 questions**	*~8-10 questions**	*~15-20 questions**	*~15-20 questions**	*~20+ questions**	*~6-8 questions**	Varies
Prep Time NOTE: setting up accesses and sending needed information	2-3 hrs over a week	3-5 hrs over a week	5-8 hrs over ~2 weeks	~8 hrs over ~3 weeks	~24 hrs over a month	2-3 hrs over a week	Varies
Usage of our testing platform (AKA our "dropbox") NOTE: Internal network testing requires an internal testing platform. Costs will be significantly higher if we need to build our toolset on another platform.	*Required / Highly Recommended**	*Sub Option #1: Required for Internal* *Sub Option #2: Highly Recommended*	*Required / Highly Recommended**	*Required / TBD**	*Varies**	Rare	Varies
Provisioning of VDI/Workstation NOTE: This is required for whitebox network testing and is highly recommended otherwise. Many tests cannot be performed efficiently, safely, or perhaps at all without it.	*Required / Highly Recommended**	*Sub Option #1: Required for Internal* *Sub Option #2: Highly Recommended*	*Required / Highly Recommended**	*Required / TBD**	*Varies**	*Highly Recommended**	Varies
Exceptions/whitelisting in firewalls, WAFs, IPSs, etc. - prevent interference NOTE: Reputable testing standards mandate whitelisting of tester IPs, domains, testing platforms, etc. for all but red teaming. Without it, testing will take months instead of weeks, costs may double, ROI will be minimal, and the report will include a Critical-level finding (in accordance with industry standards). https://penconsultants.com/shields	*Required**	*Sub Option #1: Required** *Sub Option #2: Highly Recommended*	*Required**	*Partial** NOTE: it is often necessary to temporarily whitelist layers of security in order to test the desired scope	*Varies** NOTE: generally there would NOT be whitelisting, but some situations do still warrant it	*Highly Recommended**	Varies
Whitebox, full access and knowledge NOTE: Blackbox testing costs significantly more (up to double), sacrifices ROI, and is discouraged by compliance standards. It should be avoided, as it leads to extreme value loss without full knowledge and access. https://penconsultants.com/whiteboxApproach	*Highly Recommended**	*Highly Recommended**	*Highly Recommended**	*Highly Recommended**	*Highly Recommended**	*Highly Recommended**	*Highly Recommended**
Testing Credentials - user, admin, domain admin NOTE: There are numerous tests and checks that cannot be run without various levels of authentication. Testing costs are much lower (~half), ROI higher, and testing thoroughness is increased twentyfold when administrative access is given to all in-scope systems. Some compliance and testing standards require authentication (ex. FedRAMP RA-5(5)) Web app testing requires at least user level credentials, otherwise we'd just be testing the "login screen".	*Net: Highly Recommended** *Web: Required**	*Net: Highly Recommended** *Web: Required**	*Net, wireless: Highly Recommended** *Web, mobile, thick: Required**	*Highly Recommended / TBD**	*Varies** NOTE: Depends on the goals and objectives	*Partial / Highly Recommended**	Varies

	Automated Testing	Penetration Testing (Basic)	Penetration testing (Standard & Premium)	Red Teaming Technique Simulation	Red Teaming Adversary Simulation	Social Engineering	"Security Testing" Custom Approach
CLIENT REQUIREMENTS (during testing)							
On-going Time Commitment	Limited	Limited	Limited	~1 hour per day throughout testing	1-2 hours per day throughout testing	1-2 hours the day of testing	Varies
Purple Teaming NOTE: Not only can your team benefit greatly from this approach, but testing thoroughness can as well. https://penconsultants.com/purpleTeaming	Available	Available	*Recommended**	*Required** NOTE: This testing would not work without it	*Required / Varies** NOTE: At least with our "trusted insider"; with the whole team for IRE and tabletop exercises	Recommended	Available
Pre-coordination of mitigation - testing activity treated friendly, not hostile NOTE: One of the primary difference between red teaming and other testing is being treated as a hostile threat versus authorized testing. NOTE: Except for red teaming, testing is NOT compatible when teams actively mitigate vulnerabilities or block attacks without prior coordination, as testing will be negatively impacted (ex. false negatives) and incur additional fees.	*Required**	*Required**	*Required**	*Required / Varies**	*Varies** NOTE: There is better value when our "trusted insider" provides at least notification this is occuring or if it is a purple team engagement.	*Required**	Varies
TESTING DETAILS							
Client access to real-time progress, findings, notes, etc. https://penconsultants.com/realtimeTransparency	Yes	Yes	Yes	Yes	*Yes** NOTE: At minimum, the "trusted insider" would have full access	Yes	Varies
Highly skilled & experienced tester(s) assigned	Varies	Typical	Yes	Yes	Yes	Yes	Varies
Our testers just "wing it"	Never	Sub Option #1: Never Sub Option #2: Yes, that's what this option is	Never	Never	Never	Never	Varies
Recon	N/A	Sub Option #1: N/A Sub Option #2: Varies	Yes	Rare	Typical	Rare	Varies
Complete Endpoint Discovery (ex. all RFC 1918)	Yes	Sub Option #1: Yes Sub Option #2: Varies	Yes	Rare	Varies	N/A	Varies
Full Service Enumeration (ex. 65k TCP ports)	Yes	Sub Option #1: Yes Sub Option #2: Varies	Yes	Varies	Varies	N/A	Varies
Automated Vulnerability Scanner(s)	Yes	Sub Option #1: Yes Sub Option #2: Varies	Yes	Typical	Varies	N/A	Varies
Manual Vulnerability Testing	N/A	Sub Option #1: N/A Sub Option #2: Yes	Yes	Yes	Yes	N/A	Varies
Vulnerability Verification	N/A	Yes	Yes	Yes	Varies* NOTE: Vuln identification is not a primary goal	Yes	Varies
Penetration	N/A	Sub Option #1: Shallow. Only tests what an automated scanner identifies, penetrates "one layer deep" as compared to penetration testing (for example) Sub Option #2: Varies	Moderate	Varies	Deep	Varies	Varies
Privilege Escalate	N/A	Sub Option #1: Rare Sub Option #2: Varies	Yes	Varies	Typical	Rare	Varies
Laterally Move	N/A	Sub Option #1: Rare Sub Option #2: Varies	Yes	Varies	Typical	Rare	Varies
Completion metric	Scan completes	Sub Option #1: All scan results have been manually tested Sub Option #2: Budgeted time is consumed	Completion of testing guide	Budgeted hours consumed	Action on objectives complete	Social engineering campaign(s) complete	Varies
OUR DELIVERABLES							

	Automated Testing	Penetration Testing (Basic)	Penetration testing (Standard & Premium)	Red Teaming Technique Simulation	Red Teaming Adversary Simulation	Social Engineering	"Security Testing" Custom Approach
Real-time progress, findings, notes, etc. https://penconsultants.com/realtimeTransparency	Yes	Yes	Yes	Yes	Yes* NOTE: At minimum, the "trusted insider" would have full access	Yes	Varies
Raw Scanner Reports	Yes	Yes	Yes	Varies	Varies	N/A	Varies
Mitigation Option(s)	Yes	Yes	Yes	Yes	Yes	Yes	Varies
Detailed Reproducibility	Varies	Yes	Yes	Yes	Yes	Yes	Varies
Quantified & Explained Risks	Varies	Yes	Yes	Yes	Yes	Yes	Varies
Customized Recommendation(s)	N/A	Yes	Yes	Yes	Yes	Yes	Varies
Tailored Findings & Recommendations Report https://penconsultants.com/sampleReport	N/A	Yes	Yes	Yes	Yes	Yes	Varies