GOING BEYOND AUTOMATED SCANNING

SUPERIOR VULNERABILITY ASSESSMENT AND PENETRATION TESTING WITH PERATON LABS' TAILORED, HOLISTIC 4-QUADRANT™ APPROACH

Penetration testing is a form of ethical hacking that simulates attacks on an organization's networks, systems, data, and other assets to find exploitable vulnerabilities in the environment. Many organizations focus their penetration testing on only one or two types of assets, such as applications or network components, and rely primarily, if not exclusively, on automated scanning tools for those types of assets. This approach fails to acknowledge the interconnected nature of enterprise assets and the sophisticated capabilities of attackers, at the risk of missing critical, exploitable vulnerabilities. Peraton Labs offers superior penetration testing leveraging our tailored, holistic 4-Quadrant™ Assessment Methodology. Our approach addresses embedded hardware and wireless domains in addition to networks and applications, and in a unified manner to expose the true risk and potential for damage that may not be apparent when looking at one domain at a time.

Peraton | LABS

THE CHALLENGE

Today's business environments are highly interconnected, interdependent systems with a growing variety of remote access capabilities and an increasing number of security controls. Your process, people, technology, and data are always changing. And as the threat landscape rapidly evolves and attack surfaces expand, so do your physical and cybersecurity vulnerabilities. Attack tactics and procedures that were once only used by nation-states are now commonplace in the cybercrime domain.

A properly planned and executed vulnerability assessment and penetration testing (VA/PT) strategy provides valuable information to validate design-driven controls, discover unexpected weaknesses and vulnerabilities, understand your risk profile, evaluate technical performance, and assess system maturity. Additionally, it helps determine whether systems are operationally effective, suitable, and survivable—by identifying exposures so you can target and eliminate risks that threaten the confidentiality, integrity and availability of mission critical services.

EVALUATING FOR VULNERABILITIES

While many vendors commonly rely only on running automated tool scans, Peraton Labs adds a systematic process, which includes targeted manual assessments of policies, processes, and procedures to address the all-important and often overlooked human element and the multitude of environmental factors. With our tailored approach, the vulnerability assessment is conducted within the context of the threats defined for your unique environment and the value of your organization's assets at risk. As part of our process, we consult with industry and U.S. government databases and vendor-published information; we conduct our own leading-edge cybersecurity research; we interview business owners and stakeholders; and we analyze each component for vulnerabilities to each threat, to assign a vulnerability rating based on criteria established for your organization. Ultimately, we synchronize risks to your identified critical processes so you can focus and prioritize your limited resources on what matters most — mitigating or eliminating the most critical vulnerabilities.

PENETRATION TESTING CUSTOMIZED FOR YOUR NEEDS

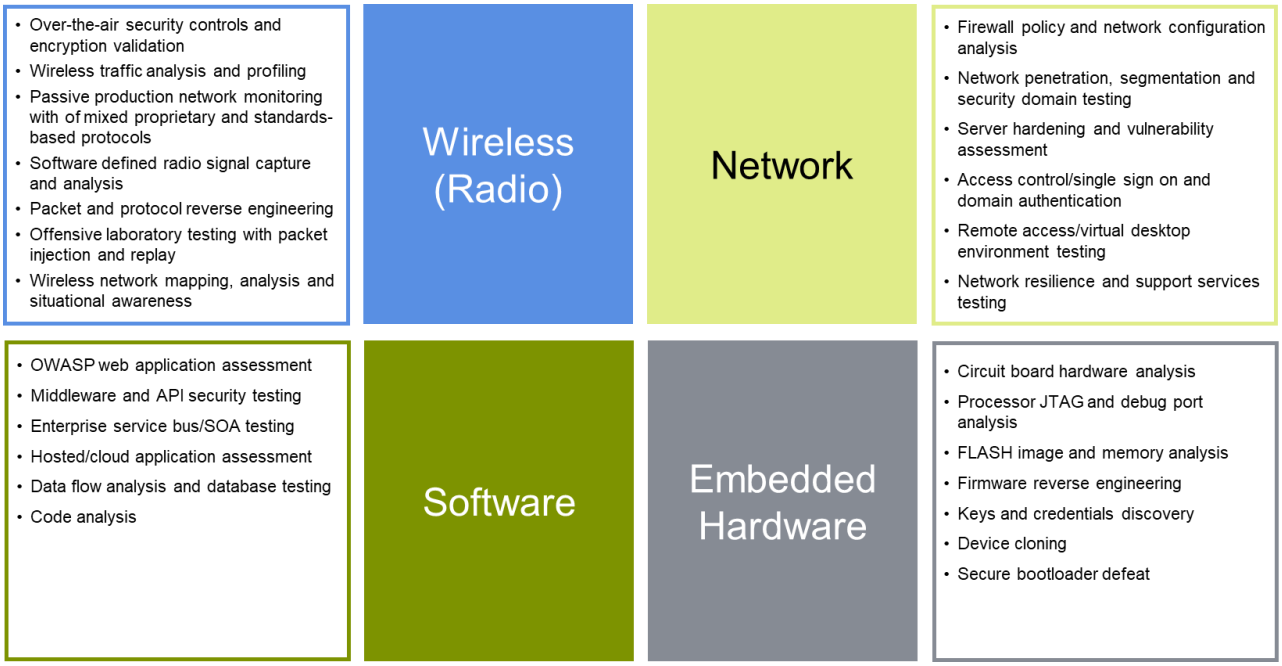
Penetration testing (i.e., pen testing or ethical hacker testing) simulates a real-world attack on your networks, systems, and data to evaluate the actual risk profile of your environment. This includes understanding the level of skill required and time needed for an attacker to exploit each vulnerability and the level of impact to your organization if the attack is successful. Peraton Labs works with you to clearly define pen testing goals and to identify the boundaries, limitations, and acceptable testing activities. We develop a pen testing strategy based on your objectives that define test sources, how assets are targeted, how much information is provided to the testers (e.g., black box vs. white box), test measurements, and types of tests. A well-planned pen test will validate the efficacy of your current defensive controls and the implementation of your organization's policies and procedures.

TAKING A 4-QUADRANT™ APPROACH

What takes our VA/PT services to the next level is the use of our comprehensive 4-Quadrant Security Assessment Methodology, built on industry standards (e.g., OWASP, NIST 800-115), government guidelines (e.g., FIPS 199), our cross-sector experience, and customized techniques. It is a honed and proven approach that goes beyond traditional IT security assessments. It provides a comprehensive assessment of the security weaknesses across the domains of a customer's environment:

- **Software, including service and management applications and associated databases** – seek to uncover weaknesses and vulnerabilities in head-end management server applications, customer care, customer portal, and business support systems

- **Network infrastructure** – focus on perimeter and compartment defenses; edge routers and gateways; and means to access backend compartments from field networks, internal corporate data networks, and remote access, including by third party contractors or vendors
- **Wireless communications** – seek to uncover low-level vulnerabilities beginning with modulation scheme and coding, media access control, link level properties, network synchronization, routing, and transport security
- **Embedded hardware and firmware** – seek to uncover weaknesses and vulnerabilities related in the embedded system circuitry, hardware interfaces, on-chip debugging functions, bootloaders, and firmware



CONSTRUCTING A VULNERABILITY ATTACK TREE USING 4-QUADRANT RESULTS

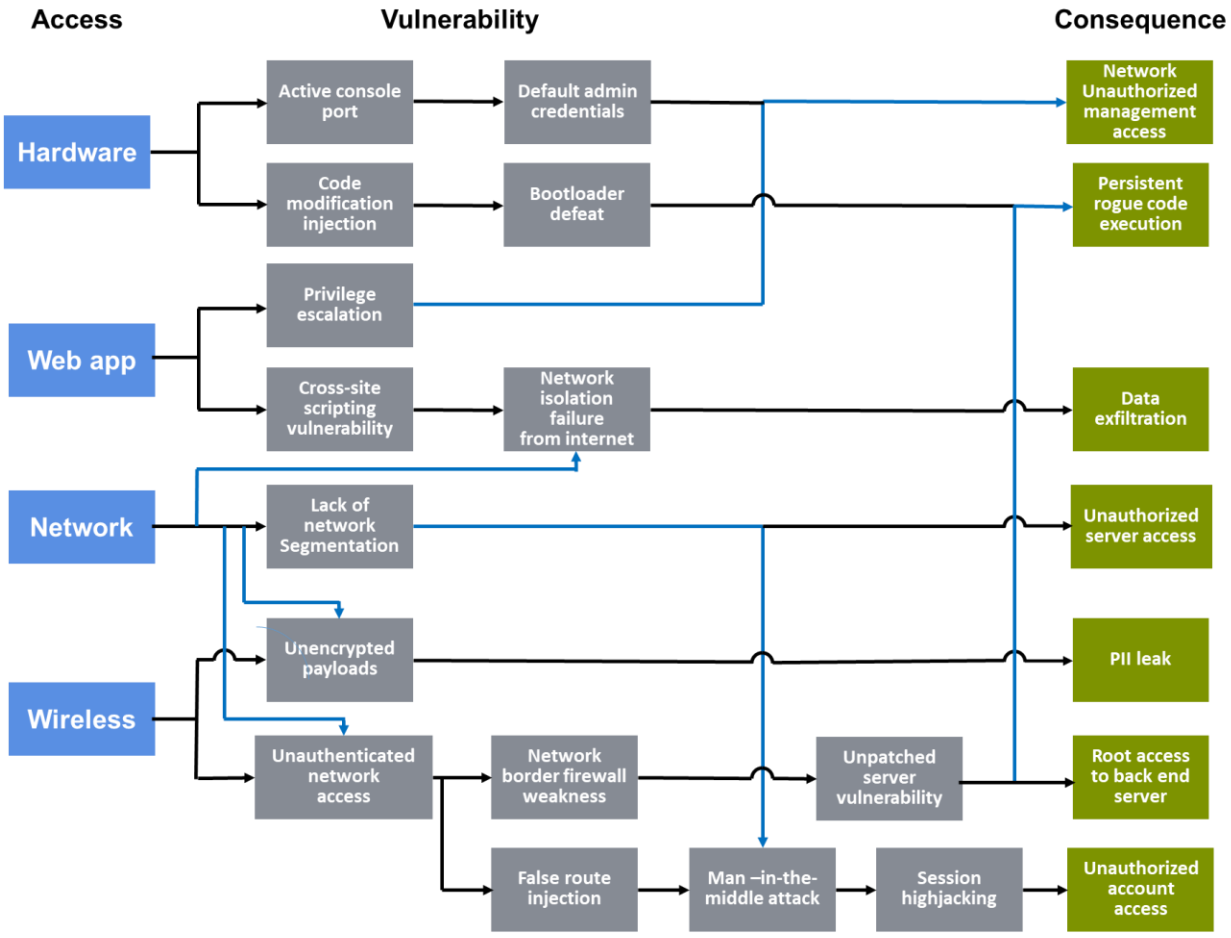
Our 4-Quadrant methodology validates whether the security controls claimed by the system vendor, operator, and owner actually exist and are operational. It then discovers and attempts to exploit design, implementation, and configuration weaknesses. Our methodology is designed to emulate real attacks against targeted systems to determine the potential for malicious actors to perform the same attacks in a production environment. While results from each quadrant individually provide deep insight, Peraton Labs links findings across all quadrants to expose the true risk and potential for damage that is sometimes not apparent when looking at only one quadrant.

To assist in selecting methods of migration to “break the chain,” Peraton Labs creates attack trees to illustrate vulnerabilities, exploit paths, and dependencies. Attack trees can be Interpreted from different perspectives. When read left-to-right, they highlight primary branches that need to be pruned to thwart attacks. When read right-to-left, they show the various ways to achieve a particular goal. While a single “break” in the attack chain may be sufficient to prevent a set of exploitations, it is often best to create multiple “breaks.”

Peraton Labs’ comprehensive VA/PT services provide an in-depth and focused evaluation of your vulnerabilities based on your organization’s industry, business goals and exposure to risk, which includes:

- Infrastructure segmentation – access, core and operations network segments, service layers and supporting systems
- Authentication mechanism validation – hardware security modules and tokens, soft-certificates, user IDs and passwords to provide access
- Authorization mechanism validation – mechanisms and rate limiters used to restrict access to application and network functionality
- Design-driven security control validation – the presence, proper operation and consistent use of these controls and the remediation of their known weaknesses
- Mobile application assessment – accessing the applications from Wi-Fi and mobile devices, such as iPhone and Android devices
- Cloud services security validation – efficacy of deterrent, preventive, detective, corrective controls, cloud access security brokers, data security, encryption, and compliance
- Access and pivot analysis – allowing attackers access to backend infrastructure and exploit weaknesses to attack and pivot across support systems, databases, time services, crypto functions and third-party services
- Server and application configuration analysis – server and application configuration that can be exploited by attackers to compromise the application, web server or underlying operating system

At the conclusion of testing, Peraton Labs provides you with a hierarchical risk level rating with actionable information and practical recommendations to develop an effective remedial plan to allow you to intelligently mitigate vulnerabilities, avoid the cost of network downtime, meet industry regulatory compliance requirements and avoid fines, and preserve reputation and hard-earned customer loyalty.



SUMMARY

Built on more than 30 years of cybersecurity experience in public and commercial sectors spanning defense, communications, energy, transportation, health care, finance, and entertainment, Peraton Labs has an unequaled security perspective, with deep knowledge and exposure to the best practices across industries. Our VA/PT services concentrate on your critical business processes to help you better manage and target your resources and avoid costs due to breaches. Peraton Labs differentiates itself by:

- Applying our comprehensive 4-Quadrant assessment methodology for a holistic view
- Employing an end-to-end process to first understand your environment, resources, and business priorities and articulate the vulnerabilities and risks discovered in context
- Leveraging our multi-industry commercial, government, federal and military experience, and deep understanding of operational risks
- Applying more than 30 years of experience in cybersecurity assessments

For more information:

- Visit Vulnerability and risk analysis - Peraton Labs
- Contact info@peratonlabs.com

LEARN MORE AT

PERATONLABS.COM

150 Mount Airy Road
Basking Ridge, NJ 07920