Penetration Testing Program Best Practices

Step One: The Plan

ELEMENTS OF SUCCESS

Develop a plan that puts structure and strength around cyber security to include continuous vulnerability testing and patching, incident response plans, and training and security awareness programs. The ultimate goal? Decrease time to remediation and to close security gaps in your network.

Clearly define the scope, objectives, identification of testing, and the order in which they are to be performed.

Build a vulnerability management team. This could include both in-house talent as well as industry analysts or consultants. When choosing a pentesting service provider, ask about the credentials of their pentesting team, beyond technical competencies. Will your team be comprised of a dedicated work group or an outsourced group who haven't previously worked together, for example. Team structure has implications on streamlined communications and in knowing who is inside your network.

Augment with careful preliminary risk planning with contingency plans should any services be unintentionally disrupted.

Resources:

- Cloud penetration testing
- Application penetration testing
- Host-based penetration testing
- Network penetration testing

REQUIREMENTS

- ☐ Develop a high-level vulnerability management plan – be sure to include non-negotiables such as scalability and continuous testing
- ☐ Present your case to business leadership; gain agreement on budget
- ☐ Refine plan and define ownership and scope of your program to include personnel and their roles and responsibilities
- ☐ Develop policies, standards, and procedures
- ☐ Determine merchandising strategy – to bring visibility to the program's successes

Step Two: Scanning and Assessment

ELEMENTS OF SUCCESS

Layer in automated scanning functions that deliver results that can be easily sorted and acted upon with human capital to find and fix vulnerabilities.

Create an enumeration (list and count) of suspected vulnerabilities that are enumerated only after using multiple automated tools over time, not just one single tool.

Build in further analysis of suspected vulnerabilities using specialized tools and manual techniques as required.

REQUIREMENTS

- ☐ Identify all assets you want to scan
- ☐ Define vulnerability landscape:
  - Common vulnerabilities and exposures (CVEs)
  - Common configuration and enumeration (CCEs)
  - Architecture
  - Design
- ☐ Define actionable reporting structure of vulnerabilities
- ☐ Deploy automated vulnerability scanning, use authenticated mode to scan high-value resources
- ☐ Prioritize pentesting cadence, beginning with an external network penetration test followed by internal network testing
- ☐ Commence manual pentesting

Step Three: Preparing for Risk-Based Remediation

ELEMENTS OF SUCCESS

Develop a risk-based remediation plan commensurate with your program's maturity level and appetite for business risk.

Employ a comprehensive verification of high-risk vulnerabilities including but not limited to safe exploitation of these vulnerabilities using both automated and manual processes, including the injection of malicious code when called for.

REQUIREMENTS

- ☐ Rank vulnerabilities through an established remediation timeline. For example:
  - Critical = 7 days
  - High = 2 weeks
  - Medium = 1 month
  - Low = Patch driven updates
- ☐ Assign application and system remediation owner
- ☐ Build in business leadership approvals for long lead remediations

Step Four: Ongoing Reporting and Improvement

ELEMENTS OF SUCCESS

Automate your vulnerability management program as much as possible: spreadsheets, emails, and document sharing portals are insufficient for most organizations, large ones in particular. Automation enables 24/7 visibility with business leadership and continuous improvement.

Find a reporting platform that is engaging and customizable to showcase what is most important to your business, one that can track and compare data over time.

REQUIREMENTS

- ☐ Build a reporting framework – for the pentesting team and for business leadership
- ☐ Identify continual improvement opportunities
- ☐ Use comparison data to showcase progress over time and highlight successes

All organizations should aspire to have the people, processes, and tools necessary to effectively execute an ongoing vulnerability management program. Failure to do so may result in poor tool selections, testing mistakes, and faulty interpretation of results that often lead to a false sense of security and could put the enterprise at risk. By building out a vulnerability management plan, as depicted above, you can dramatically increase the security of your enterprise and can be better assured to reach your ultimate goal: to decrease time to remediation and close any security gaps in your network.

About NetSPI

NetSPI is the leader in enterprise security testing and vulnerability management. We are proud to partner with seven of the top 10 U.S. banks, the largest global cloud providers, and many of the Fortune® 500. Our experts perform deep dive manual penetration testing of application, network, and cloud attack surfaces. We uniquely deliver Penetration Testing as a Service (PTaaS) through our Resolve platform. Clients love PTaaS for the simplicity of scoping new engagements, viewing their testing results in real-time, orchestrating remediation, and the ability to perform always-on continuous testing. We find vulnerabilities that others miss and deliver clear, actionable guidance allowing our customers to find, track, and fix their vulnerabilities faster. Follow us on LinkedIn, Twitter, and Facebook.