Network Vulnerability & Penetration Scanning

TPx is a leader in cybersecurity for small and medium businesses and public-sector organizations. Our depth of expertise enables us to offer standards-based security consulting services developed from our experiences in solving strategic and operational challenges for customers.

TPx consultants are subject matter experts in their field and thought leaders in security. All of our offerings are based on best practices derived from Information Security Standards (CISSP Domains, NIST, ISO 27000 series, etc.) and our extensive experience deploying, architecting, operating, and securing environments nationwide.

Proactively maintaining and protecting a computing network requires continuous effort. Vendors are continually releasing patches and updates, access and permissions requirements are always evolving, and most importantly, the threat landscape is continuously expanding and becoming more dangerous. Preparing ahead of time for the inevitable attack by thinking like a hacker and understanding the way they will attack is critical and leaves you and your organization better protected against hackers and malware than a "just-in-time" approach.

Regular Vulnerability and Penetration Scanning are two of the best tools you can use to understand where your weaknesses are and how likely it is that a hacker will be able to exploit them.

Get answers to these questions…

- What vulnerabilities currently exist in my network? How do I know which ones pose the greatest threat?
- How do I best prioritize my patching and updating activities?
- Am I susceptible to attack from employees and others inside my organization?
- Based on my network infrastructure, are there threats that I do not need to worry about?
- How do I stay current on the threat landscape and defend my organization against emerging threats?

57% of data breaches are attributed to poor patch management. The average time to apply, test, and fully deploy a patch is 102 days.

Ponemon Institute

Overview

TPx's Vulnerability and Penetration Scanning Service (VPS) consists of two components: a Vulnerability Scan and a Penetration Scan. For further visibility into the strength of your overall Vulnerability Management Program, we also offer an optional Vulnerability Management Plan Review as part of this engagement.

The **Vulnerability Scan** evaluates devices that are connected to the network for the purpose of identifying vulnerabilities that may be present on those devices due to open ports, exposed services, lack of current patches, etc. The TPx Vulnerability Scan:

- Uses manually written signatures to detect known vulnerabilities
- Leads to discovery of new vulnerabilities or validates the presence (or remediation) of vulnerabilities that had been previously identified

The **Penetration Scan** shows how exploiting a vulnerability could result in a significant impact to the environment. By demonstrating this impact, it is possible to get organizations to reconsider the priority of remediating vulnerabilities that Vulnerability Scanners may have reported as non-urgent. The TPx Penetration Scan mirrors the behavior of bad actors by:

- Performing exploits against identified network vulnerabilities (shell file uploads, hash cracking, password dumping)
- Executing multiple authentication-based attacks (POP3, Telnet, SMB, AD, FTP)
- Conducting man-in-the-middle (MitM) attacks (SMB relay, DNS poisoning, ARP poisoning)
- Attempting privilege escalations on the network using AD group and share enumeration
- Impersonating users to find sensitive data

Regular Penetration Scanning is one of the best tools you can use to understand where your weaknesses are and how likely it is that a hacker will be able to exploit them and gain access to other systems and/or confidential information on the network.

Although both Vulnerability and Penetration scans can be run independently, there is tremendous added value in running them together. The additional discovered details can be used in strengthening the security posture of your business. The Vulnerability Scan looks for known vulnerabilities on the network but will not exploit them. In addition to testing each of the vulnerabilities that are found in the Vulnerability Scan (which lowers the number of false positives), the Penetration Scan probes various parts of the network, potentially uncovering unpublicized weaknesses and running further testing to discover the extent of those weaknesses.

During the optional **Vulnerability Management Plan Review**, we will evaluate your organization's security program through interviews, policy review, validation and investigation of processes to generate an assessment of your Vulnerability Management (VM) program. TPx will detail the results of the assessment of each aspect of the program, any deviation from best practice, and the resulting risk to the business.

Scheduling and Reporting

TPx can schedule a scan as frequently as needed and keep track of your risk profile in near real time. Our reports will show your trending data, allowing your team to see improvements from one month to the next.

The post-scan reports will speak to two distinct levels of resources: the security practitioner and the leadership. For the security practitioner, we'll deliver the results of the scans — annotated to highlight the most important findings — and recommend how to mitigate those vulnerabilities. An additional Best Practices report presents assessment results and observations related to your organization's current level of exposure.

TPx will also generate an executive-level document containing a summary of our findings. From our insights, you will be able to build or enhance a VM program based on controls with the greatest impact to your risk posture, ensuring that you utilize your limited resources most effectively.

74% of IT security pros believe their orgs would test systems more frequently if the penetration testing process was more efficient or required less management.

VentureBeat, Nov. 2021