Penetration Testing & Vulnerability Scans

TBI Battlecard

What to Look for in the Field/What you should know

- Customers with regulatory compliance requirements have prerequisites for testing and employing security policies.
- Any customer who has been attacked or scared of being attacked.
- Customers looking to do a firewall/security refresh, and want a baseline on their environment
  - > This can apply to customers who recently upgraded/updated and want to ensure they have minimized any security risks.
- Customers with small IT staffs or lacking security skills to effectively identify vulnerabilities.

Overview

A **penetration test**—typically referred to as pen test—evaluates IT infrastructure security by safely identifying and exploiting vulnerabilities found in appliances, operating systems, services and applications. Vulnerabilities may exist within the environments themselves or from improper configurations or risky end-user behavior.

Penetration testing assessments are also useful in validating the efficacy of defensive mechanisms and determining how well end-users adhere to security policies.

Note: Best practice would be to change up the provider each time a test is run for maximum effectiveness.

Vulnerability scanning detects and classifies system weaknesses in computers, networks and communications equipment and predicts the effectiveness of countermeasures. Vulnerability scanning lets you take a proactive approach to close any gaps and maintain strong security for your systems, data, employees, and customers. Vulnerability Scans are typically an ongoing service.

There are distinct differences between the two. A vulnerability scan searches a system for known vulnerabilities via a passive process where a device or collector is placed on your network to perform a scan.

A penetration test attempts to actively exploit weaknesses in an environment via an individual or group of white-hat hackers attempting to gain entry into the network. Both are critical components in a comprehensive network security protocol and cybercrime prevention.

Data breaches are often the result of unpatched vulnerabilities, so identifying and eliminating these security gaps, removes that attack route.

Discovery Questions

- Do you have regulatory or compliance requirements you are obligated to meet?
- How confident are you of your ability to demonstrate compliance?
- Do you have a clear picture of your overall security posture and of how it relates to industry best practices?
- Do you currently conduct security assessments, such as penetration tests on a bi-annual basis?
- How realistic is your plan to address the security gaps that you might have today?
- Do you have an established process to address computer security breaches?
- When was the last time you tested your security polices? How did you do it?

Add-ons to DDoS

Penetration testing is typically a one-time engagement that will lead to additional services; by uncovering issues or holes in the security a customer has deployed, you can then sell the solutions to migrate the issues and create a more secure environment. Similarly, with vulnerability scanning, you can also sell additional security products and solutions that help a customer with sound security posture.

- Managed Firewall
  - > On-prem or Cloud
- Endpoint Security
- End user Security Training
- SIEM
- DDoS Mitigation

Top Providers

AT&T | CenturyLink | Coeo | Masergy

Synoptek | Verizon | Zayo