Vulnerability Assessment vs. Penetration Test

? What's the Difference?

There are several key differences between vulnerability assessments and penetration testing. If your organization uses these terms interchangeably, you may unknowingly have a gap within your cybersecurity program that prevents you from effectively protecting your business and its assets. It may also put you at risk of noncompliance with federal, state, or industry regulations.

PENETRATION TEST

A DeepSeas penetration test is a process where we simulate a real-world cyber-attack on your organization's targeted assets. Our penetration testers will use the same tools, techniques, and procedures that modern cybercriminals use. Whereas vulnerability scanning tools are unable to distinguish between flaws that can be exploited by attackers and those that can't, penetration testing is designed to simulate as closely as possible the effect threats would have on your organization. This is accomplished by understanding viable threats with the associated risks, motivations, and targets.

VULNERABILITY ASSESSMENT

A DeepSeas vulnerability assessment is a process where we identify vulnerabilities and weaknesses within your environment. This typically involves assessors scanning your organization's infrastructure using automated tools and providing expert insight on risk and mitigation.

Reasons to Perform a DeepSeas Vulnerability Assessment:

- ✔ Matching up critical vulnerabilities with critical assets

- ✔ Generating a list of prioritized patches or other remediations that need to be applied

- ✔ Identifying all the false positives and reducing occurrence of false negatives

- ✔ Satisfying PCI, HIPAA, and NERC-CIP regulatory requirements

- ✔ Enhancing your risk management program

Reasons to Perform a DeepSeas Penetration Test:

- ✔ Testing your cybersecurity controls after they have matured

- ✔ Modeling real-world attack activities Exploiting weaknesses in configuration that are overlooked within patch management

- ✔ Identifying exploitable vulnerabilities in critical assets, including financial procedures, intellectual property, credit card applications, critical infrastructure, etc.

- ✔ Satisfying PCI, NERC, and other compliance requirements

- ✔ Undergoing significant changes to your organization or infrastructure

Do I need a DeepSeas Vulnerability Assessment or a Penetration Test?

The answer is likely both. It depends on the problems your organization is trying to solve, the maturity of your cybersecurity program, and the compliance requirements you need to satisfy. Both vulnerability assessments and penetration testing are critical to maintaining a strong security posture. Below are ways a vulnerability assessment differs from a penetration test.

	Vulnerability Assessment	Penetration Test
Are you trying to find the weaknesses in your vulnerability management process?	✔	
Do you want to know where the vulnerabilities are in your environment?	✔	
Are you confident in your vulnerability management process?		✔
Do you need to prove potential impact of an exploitation to justify budget or improvements?		✔
Are you protected against common cyber-criminal tactics?		✔
Do you have compliance requirements?	✔	✔
Are you seeking to obtain or retain cyber liability insurance?	✔	✔
Do you need to validate your configuration and patch management functions?	✔	✔

Get a Quote for your offensive security project.