GreyCastle security

# VULNERABILITY ASSESSMENT VS. PENETRATION TESTING:

# 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.**

A **VULNERABILITY ASSESSMENT** is the process of identifying vulnerabilities and weaknesses within a business environment and where they are located in the network. An organization's infrastructure may be scanned for technical vulnerabilities using automated tools. Vulnerability scanning tools are unable to distinguish between flaws that can be exploited by attackers and those that can't.

**Some reasons to perform a vulnerability assessment include:**

- Matching up critical vulnerabilities with critical assets
- Generating a list of patches or other remediation that need to be applied
- Identifying all of the false positives and false negatives that exist
- Satisfying PCI, HIPAA and NERC-CIP regulatory requirements

A **PENETRATION TEST** (or "pen test") is used to simulate a real-world cyberattack on an organization's targeted assets. A pen test will use the same techniques that modern cybercriminals use. Penetration testing is designed to simulate as closely as possible the effect these threats would have on your business, and is accomplished by understanding your threats, their capabilities, motivations, and targets.

**Some reasons to perform penetration testing include:**

- Testing your cybersecurity controls after they have matured
- Identifying exploitable vulnerabilities in critical assets, including money, intellectual property, credit card applications, critical infrastructure, etc.
- Satisfying PCI, NERC and other compliance requirements
- After significant changes to your business or infrastructure

## The GreyCastle Difference

Both vulnerability assessments and penetration testing are critical to maintaining a strong security posture. Here are more ways the function of a vulnerability assessment differs from that of a penetration test:

| FUNCTION | VULNERABILITY ASSESSMENT | PENETRATION TESTING |
|---|---|---|
| Identification of ALL Technology Vulnerabilities | ✓ | |
| Analysis of False-Positives and False-Positives | ✓ | |
| Vulnerability Scanning | ✓ | OPTIONAL |
| Full Interaction with Client Team | ✓ | |
| Limited or No Interaction with Client Team | | ✓ |
| Social Engineering (Phishing, Vishing, Smishing) | | ✓ |
| Targeting of Critical Assets | | ✓ |
| Exploitation of People, Process and Technology | | ✓ |

**TIP:** A penetration test should be conducted by a third party rather than an internal team. This helps to avoid conflicts of interest and provides a more objective view of the environment.

## Should I do a vulnerability assessment or a penetration test?

The answer is probably both. It depends on the business problems your organization is trying to solve, the maturity of your cybersecurity program, and the compliance requirements you need to satisfy.

## Not sure where to start?

**GreyCastle Security can help you find the right solution for identifying and assessing your security weaknesses.**

**Email us at intel@greycastlesecurity.com or give us a call: (518) 274-7233.**