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.

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:

### Vulnerability Assessment
- Identification of ALL Technology Vulnerabilities
- Analysis of False-Positives and False-Positives
- Vulnerability Scanning
- Full Interaction with Client Team
- Social Engineering (Phishing, Vishing, Smishing)
- Targeting of Critical Assets
- Exploitation of People, Process and Technology

### Penetration Test
- Identification of ALL Technology Vulnerabilities
- Analysis of False-Positives and False-Positives
- Vulnerability Scanning
- Optional
- Full 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.