A white paper from The Net Effect, L.L.C.

Assessing Cyber Security Risk:

1 - Security Assessment

2 - Vulnerability Scan

3 - Penetration Testing

What's the Difference?

by Glenda R. Snodgrass
(grs@theneteffect.com)
www.theneteffect.com
(251) 433-0196

Assessing Cyber Security Risk:

Security Assessment, Vulnerability Scan, Penetration Testing

What's the Difference?

. . . . . .

Security Assessment, Vulnerability Scan, Penetration Testing -- these three terms are often used interchangeably and yet are not at all the same, creating confusion for the organization seeking assistance. Let's examine these three very different things to understand the differences between them.

✯ *A Security Assessment is a process*

Typically a security assessment will involve a physical investigation of your computer network and the work environment overall, as well as your business policies and processes.

Telecommunication systems, video/security systems, building automation systems and other "smart" devices would fall within the scope of review. Automated tools may be used to identify hardware and software on the network, and employee interviews can provide additional, valuable information. Documentation review would include any written security policies as well as asset lists, network diagrams and prior compliance audits. Your current security posture will be evaluated based on a standard list of controls (such as the CIS 20 Controls from the Center for Internet Security[1]) and compared to any regulatory or other compliance requirements your organization has.

Depending on the size and scope of your information system, a security assessment could require a few hours, days, weeks or even months to complete.

1 http://www.cisecurity.org/controls/

✯ *A Vulnerability Scan is a tool*

This is used to identify assets and to report vulnerabilities which could be exploited to compromise your systems. The scans may be run internally or externally, lasting only a few seconds or a few minutes, and can be performed automatically on a schedule. Vulnerability scans may be included in the security assessment process, as part of a penetration testing program, or on a standalone basis.

✯ *Penetration Testing is a task*

The CIS 20 Controls are numbered 1-20 and grouped in numeric order as Basic, Foundational and Organizational. Penetration testing (pentesting) is #20, the last of the CIS 20 controls, as it is designed to identify deficiencies in the implementation of the first 19 controls.

Pentesting will use automated tools to identify vulnerabilities, with manual verification and possibly attempted exploitation. Depending on the scope of the engagement, pentesting can include social engineering, physical security exploits and sample data exfiltration, and will typically last days or even weeks.

✯ *Which one is right for you?*

If you haven't had a security assessment performed by an independent third party (*i.e.*, an individual or entity who is not responsible for installing, configuring and/or maintaining your information system), **that is the place to start.**

Vulnerability scans are less costly, but may be of limited usefulness to the business owner. They typically deliver a lengthy and detailed report with specific technical information which may require interpretation by an expert in the field.

Penetration testing can be very expensive, and isn't worth the money if your organization hasn't already developed and implemented a strong security program.

A basic security assessment will identify gaps in your security program and provide a roadmap for improvement.

Contact us to get started today!

The Net Effect, LLC
Your security is our business

Post Office Box 885
Mobile, Alabama 36601-0885 (US)
phone: +1 (251) 433-0196
https://www.theneteffect.com

The Net Effect, L.L.C. is a consortium of consultants experienced in providing technology consulting services to commercial, non-profit and governmental organizations. The company was founded in Mobile, Alabama in 1996 and has worked with businesses across the US, in Canada and in Europe.

Glenda R. Snodgrass, President and lead consultant for The Net Effect, specializes in information security training and compliance. She has extensive experience teaching and training security awareness and compliance requirements. She has conducted numerous workshops covering PCI DSS, GLBA, FAR 52.204-21, DFARS 252.204-7012, NIST 800-171, NIST CSF and CMMC. Her public speaking includes regional conferences of multiple organizations for security professionals. Glenda holds a B.A. from the University of South Alabama (1986) and a maîtrise from Université de Paris I - Panthéon-Sorbonne in Paris, France (1989).