October 11, 2019

Vulnerability Scanning versus Penetration Testing

CYBERSECURITY
BY SEAN THOMAS

SHARE WITH A COLLEAGUE | DOWNLOAD PDF

When organizations look to assess the resiliency of their information systems, there tends to be some confusion around what exactly vulnerability scanning and penetration testing each provide. The truth is that both paint part of the larger picture necessary to spot the key gaps in existing controls. Schneider Downs recommends that organizations perform internal vulnerability scanning at least monthly and external penetration testing annually. When implementing these activities, organizations should understand the basics of each.

Vulnerability Scanning

Continuous vulnerability management practices form one of the cornerstones of any cybersecurity strategy. Scanning tools provide valuable insight into the current health of network-attached devices, and can identify critical gaps in patch management and change control. Vulnerabilities can be prioritized, patches deployed, and device configurations updated. But there are some key areas that vulnerability scanners often miss.

Common issues with vulnerability scanners include:

- **Lack of visibility across all devices.** Scanning across a subset of devices or using a non-authenticated mode for scanning can result in high-risk vulnerabilities going unnoticed.
- **No consideration for system criticality.** Automated scanners assign a baseline risk rating to vulnerabilities, but overlooking the criticality of the underlying systems can lead to incorrect prioritization or even cause important fixes to be skipped entirely.
- **Unable to assess architectural controls.** While scanning will capture known weaknesses in software and configuration at a device level, automated tools cannot account for the impact or lack of compensating controls, resulting in false positives, or worse…

Penetration Testing

While vulnerability scanning uses a set of predefined rules to identify gaps in software patching and system configuration, penetration testing relies on human analysis of systems and leverages many of the same tools that actual hackers use. Some examples of targets and attack techniques used in a high-quality penetration test:

- **Social Engineering –** Phishing and “vishing” (voice phishing via phone). These are common real-world techniques that penetration testers will employ to gain unauthorized access.
- **Web Application –** A skilled team will not only look for common misconfigurations, but also will test file upload interfaces, data entry forms, and authentication/session management components of a website to identify

potential weaknesses.

- **Physical Security –** Testers may use a combination of special tools to bypass traditional and electronic locks, or leverage social engineering to gain physical access to restricted areas.
- **Network Services –** A detailed penetration test will demonstrate how an attacker can use unnecessary or unsecured network services to traverse an organization's network.
- **Wireless Network –** Wi-Fi networks must be assessed for proper logical access controls as well as the opportunity that their physical footprint may present to would-be attackers.

Comprehensive penetration testing requires a diverse set of skills, and while organizations with large security teams may be able to dedicate staff to an internal **red team (attackers)** – a group focused on performing penetration tests – smaller organizations will primarily allocate security staff to their **blue team (defenders)**, which focuses on maintaining technical security controls. For these smaller organizations, **red team** exercises are commonly outsourced to an expert firm. A growing practice is for organizations of all sizes to combine red and blue team efforts in regular **purple team** exercises, which allow the defenders to see attack techniques used in real time and actively tune security controls for prevention, detection and response.

How can Schneider Downs help?

The Schneider Downs cybersecurity practice consists of experts in multiple technical domains. The team's mix of skills and experiences in real-world cyberattack scenarios enables us to provide your organization with a comprehensive look at external vulnerabilities ranging from susceptibility to social engineering to critical weaknesses in external web applications. Our whitepaper outlining the advantages of external penetration testing is available at www.schneiderdowns.com/maximize-value-penetration-testing.

You've heard our thoughts... We'd like to hear yours

The Schneider Downs Our Thoughts On blog exists to create a dialogue on issues that are important to organizations and individuals. While we enjoy sharing our ideas and insights, we're especially interested in what you may have to say. If you have a question or a comment about this article – or any article from the Our Thoughts On blog – we hope you'll share it with us. After all, a dialogue is an exchange of ideas, and we'd like to hear from you. Email us at contactSD@schneiderdowns.com.

Register to receive our weekly newsletter with our most recent columns and insights.

SUBSCRIBE FOR UPDATES

MOST RECENT

Russian Hackers Indicted in Pittsburgh

CYBERSECURITY
BY MATTHEW CREEL | 12.6.2019

Two Russian nationals, Maksim Yakubets and Igor Turashev, were indicted in Pittsburgh on December 5th, for involvement in international multimillion-dollar ...

READ MORE

MOST POPULAR

Tax Treatment of Deferred Revenue in a Taxable Stock Acquisition

MERGERS AND ACQUISITIONS, TAX
BY GARY SLIMAN | 6.1.2016

The general rule under Internal Revenue Code §451 is that an item of income shall be included in gross income for the taxable year or receipt unless ...

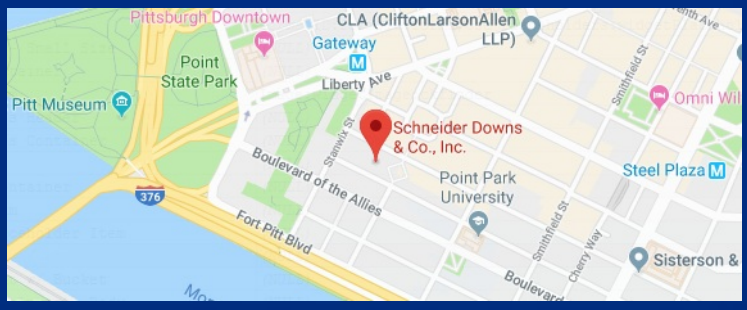
READ MORE

Have a question? Ask us!

We'd love to hear from you. Drop us a note, and we'll respond to you as quickly as possible.

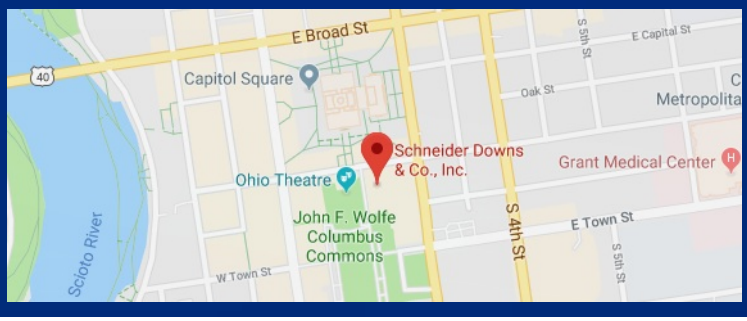
ASK US

CONTACT US



PITTSBURGH
One PPG Place, Suite 1700
Pittsburgh, PA 15222

contactsd@schneiderdowns.com
p:412.261.3644 f:412.261.4876



COLUMBUS

65 East State Street, Suite 2000
Columbus, OH 43215

contactsd@schneiderdowns.com
p:614.621.4060 f:614.621.4062

WASHINGTON, D.C.

1660 International Drive, Suite 600
McLean, VA 22102

contactsd@schneiderdowns.com
p:571.380.9003

PrimeGlobal
An Association of Independent Accounting Firms

FOLLOW US

CLIENT PORTAL

SUBSCRIBE FOR UPDATES

E-mail SUBMIT

INSIDE PUBLIC ACCOUNTING TOP 100 FIRMS 2018

Schneider Downs is a Top 60 independent Certified Public Accounting (CPA) firm providing accounting, tax, audit and business advisory services to public and private companies, not-for-profit organizations and global companies. We also offer Internal Audit; Technology Consulting; Software Solutions; Personal Financial Services; Retirement Plan Solutions and Corporate Finance Services. Schneider Downs is the 13th largest accounting firm in the Mid-Atlantic region and serves individuals and companies in Pennsylvania (PA), Ohio (OH), West Virginia (WV), New York (NY), Maryland (MD), and additional states in the United States with offices in Pittsburgh, PA and Columbus, OH.