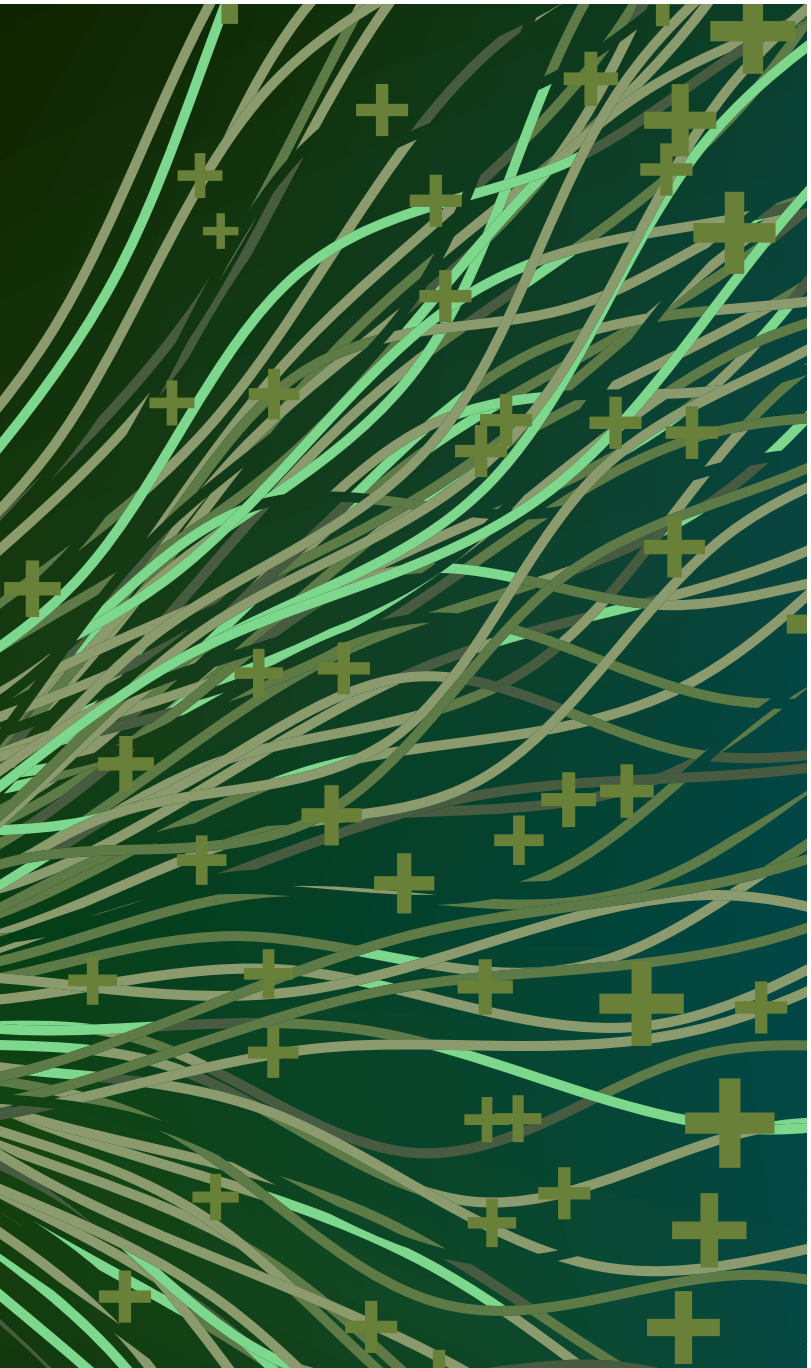

*E-Guide*

# ADDRESSING TODAY'S VULNERABILITIES

TechTarget | SearchSecurity

**EVEN IF YOUR** firm has no legal or contractual obligation to perform them, authenticated scans should be an essential part of your security program. Learn why and what vital information these scans can provide.

# ADDRESSING TODAY'S VULNERABILITIES

*Kevin Beaver*



They say that a picture is worth a thousand words. I haven't been able to confirm that, but I do know that the same can be said about security vulnerability scanner findings. Run a network vulnerability scanner such as Nexpose or LanGuard, or a web vulnerability scanner such as Acunetix Web Vulnerability Scanner or Netsparker, against your systems and applications and you'll certainly uncover a ton of security issues that need to be addressed. This is especially true when performing authenticated—or logged-in—vulnerability scans. Some findings will initially come across as super-urgent but not have any substance, while others will be barely noticeable yet create significant risks.

## THE IMPORTANCE OF AUTHENTICATED SCANS

Interestingly, I find that a lot of people do not perform authenticated vulnerability scans. I'm not sure whether it's by choice or through ignorance of just how valuable this exercise can be. The reality is, if you are going to find most security flaws on your network, you're going to have to look at from the perspective of

authenticated users. In many cases, people assume that generic, unauthenticated vulnerability scans are all that's needed. After all, that's what X, Y, or Z compliance regulation or contract requires. However, there are two key points that are being overlooked:

1. Just because someone is a trusted user of your environment doesn't mean that they don't have malicious intent. They could possess the ability to poke around and fall backwards into some critical security flaws that they can use for ill-gotten gains.

2. Just because legitimate credentials were used to log in to your network or applications doesn't mean that the trusted user is behind the transaction. According to the security research issued each year, one of the most common means of exploitation is compromised user credentials. All it takes is a criminal hacker to guess or crack a user's login credentials—or install malware via phishing or other means to obtain the credentials—and they gain full access to your environment.

## AFTER THE SCAN

In order to minimize your business risks, you need to find out which vulnerabilities are behind the login prompt, so to speak, so you'll know what can be exploited and, of course, what needs to be resolved. Once you find security vulnerabilities in your operating systems or web applications, you must then prioritize them based on various criteria such as the following:

- What privileges the user role has—the higher the level often means higher priority for testing?
- Which system activities are being logged and monitored, and are thus out of sight and out of mind?
- Should multifactor authentication—which can be used to minimize many such risks—be required?
- What is the criticality of the system and the type of information that it houses? That is, why spend time and effort on pursuing flaws on an isolated training network that contains nothing of value?
- How easy it is to "hop" over to other parts of the network? This is a common oversight that simple VLANs or running of services on custom ports cannot solve.

If you are not currently performing authenticated vulnerability scans, you need to. There's simply too much to lose. The good news is that you don't need to perform authenticated scans every time—unless, of course, you're under a contractual or other legal obligation to do so.

Assuming it's not a requirement, I think that performing authenticated vulnerability scans every other time, or even once per year, should suffice as long as the scans are indeed working and you are getting good information. Last but not least, make sure that all parties involved, including system administrators and software developers, are made aware of the results of your authenticated vulnerability scan so something can be done about the findings. There's nothing worse than a known vulnerability that goes unresolved.

**KEVIN BEAVER** is an information security consultant, expert witness, and professional speaker with Atlanta-based Principle Logic, LLC. With over 27 years of experience in the industry, Kevin specializes in performing independent security assessments revolving around information risk management. He has authored/co-authored 12 books on information security including Hacking For Dummies (currently in its 5th edition) and The Practical Guide to HIPAA Privacy and Security Compliance. In addition, he's the creator of the Security On Wheels information security audio books and blog providing security learning for IT professionals on the go. Kevin can be reached at www.principlelogic.com and you can follow him on Twitter, watch him on YouTube, and connect to him on LinkedIn.


## FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

## WHAT MAKES TECHTARGET UNIQUE?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.