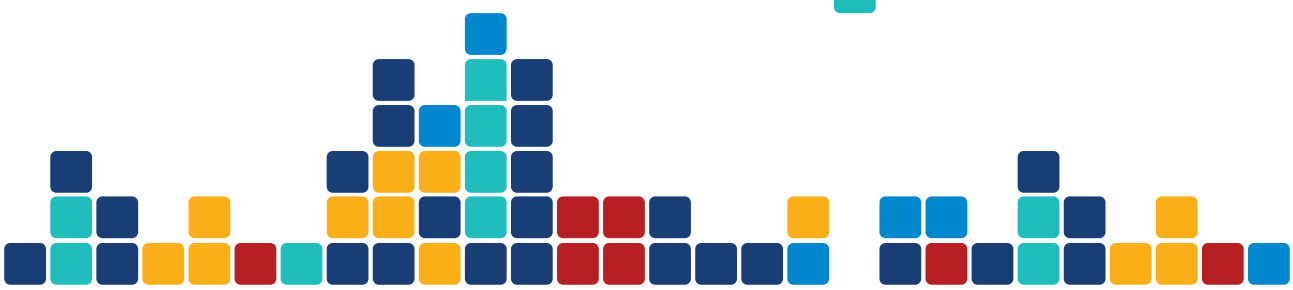
VULCAN

mind the gap

Best Free Vulnerability Management Tools And Repositories

A Vulcan Whitepaper • November 2018



Introduction

Vulnerability management is an increasingly complex challenge. Risk factors are greater than ever. With more types of technologies come more vulnerabilities, and more things to patch. These increased risks lead to higher labor and licenses costs, which add to the pressure on CISOs and security teams.

A prevalent issue across many organizations is that there is a large number of technologies to assess - new types of infrastructures (containers, cloud-based, and so on) and new programming languages to consider, such as Python and Go. Another common pain point is the difficulty in prioritizing, which is why data repositories are important. The number of difficult decisions that need to be made can be overwhelming, even for the most prepared infosec staff.

So before you spend valuable resources investigating, piloting, assessing, and investing in any enterprise-grade technology, we recommend that you use these free open-source tools. They are specifically designed to enable you to assess your risk and understand how you should manage scanning and activities in every field. Using your experience with these tools, you will be in a better position to select permanent, enterprise-grade technology wisely.

Here are the tools we recommend that you try out before locking yourself into an enterprise-grade solution:

- Static code scanner testing tools (such as Bandit and Dependency Check)
- DAST tools (such as Archery, Arachni Scanner, and OWASP ZAP)
- Infrastructure scanners (such as OpenVAS, CoreOS Clair, Vulners, and BelSecure)
- Vulnerability Repositories (such as CVE Details, WPScan, CERT-EU, Zero Day Initiative, Vulners, and Rubysec)

Read on for more information about each of these tools and repositories.

One of the primary functions of IT departments is to make sure that the infrastructure and information that it controls is safe. Just like a soldier inspecting the walls of a fort for weak spots, IT is charged with identifying and mitigating vulnerabilities in the organization's cyber defences. Vulnerability management - a segment of risk management - asks where the risks are in an organization's cyber security defenses that might appear as a result of, say, flawed security systems, outdated processes, or ineffective IT security strategies. While vulnerability management in its broadest sense is not a new concept, its application in cyber security is relatively new. Over time, CIOs and IT managers have to continuously develop new vulnerability management strategies as cyber attacks become increasingly sophisticated. This has lead to the rise of the vulnerability management market in which a number of tools are now available to detect vulnerabilities and mitigate the risks of cyber attacks and breaches. This paper discusses some of those tools and how they can help you keep your enterprise's defenses strong and intact.

Vulnerability Management Tools

Static Code Scanner Testing

Static Code Scanners (also known as "security linters") are tools that scan source code for security vulnerabilities or errors. This is a very important part of the app development process because these scanners compare the code to libraries of known vulnerabilities and report on their findings. Examples of Static Code Scanners include Bandit (managed by the Python Code Quality Authority) which specifically analyzes Python code, and Dependency-Check, similar to Bandit, but that supports Java and .NET (with experimental support for Ruby, Node.js, Python, and limited support for C/C++). These tools keep your users safe by enabling you to test your code in situ, before it is run, to find weak spots that need to be hardened.

Dynamic Application Scanner Testing (DAST)

While Static Code Scanners analyze source code, Gartner comments that Dynamic Application Scanners *"...are designed to detect conditions indicative of a security vulnerability in an application in its running state."* In other words, DAST means running the application to perform functional testing to detect vulnerabilities, such as remote procedure calls, Session Initiation Protocol [SIP], and so on. This is extremely important because some security vulnerabilities only show up when the program is executed.

Archery is a popular example of a DAST solution. The results of vulnerability management testing are displayed in a dashboard that provides a color-coded overall view of the security status of your applications. This kind of information is important for developers and pentesters because it helps them to both catch and patch security vulnerabilities before the application is released to the public.

Arachni Scanner is a free DAST tool that is specifically aimed at testing web applications. While not as slick looking as Archery, its a full-featured platform-agnostic program that can be deployed easily for both small and global-scale projects. Arachni's Crawl Scanner score of 96% puts it at the top of the list for scanning efficiency. According to sectoolsmarket.com, Arachni has near perfect scores when it comes to vulnerability detection.

OWASP ZAP is another free and popular DAST tool used by developers and pen testers specifically for web applications. According to their Getting Started Guide, "ZAP can be used as a "man in the middle," but also can be used as a stand-alone application, and as a daemon process." Conveniently, ZAP supports every major Operating System and Docker. Guru99 listed OWASP ZAP as the 2nd best of 40 pentesting tools of 2018. Part of its appeal is that ZAP is both easy to use and powerful. Those with minimal knowledge can benefit from this tool by running the built-in automated tests, but seasoned and professional security testers can dive deeper into the settings to devise more complex tests for their web applications.

Infrastructure Scanning

Infrastructure scanning is necessary because you get a better picture of the risk levels that your organization is working under, which can help you develop an action plan to prevent hacks and leaks. Neil Roiter from Computerworld.uk says, *"[Infrastructure] Vulnerability management tools scan the network for hosts, enumerate network services and use a variety of techniques to determine possible vulnerabilities…If an open port is discovered, they check the asset status against their database of vulnerability signatures."*

Some prominent players in the infrastructure scanning space include:

OpenVAS: An open source infrastructure vulnerability scanner that includes over 50,000 vulnerability tests. It is secured with SSL and comprises a number of different modules, each of which provides different services that, together, result in a comprehensive analysis of your computer network infrastructure. Cybersecurity journalist, Kim Crawley, shares an information security professional's experience using OpenVAS: *"I'm able to quickly identify systems of interest that might need immediate attention. The reporting is also about to show top ten most vulnerable hosts, along with all open ports on the perimeter. Armed with this information, I can reach out to networking and devops teams to quickly triage any systems or address possible firewall misconfigurations."*

CoreOS Clair: A vulnerability management scanner that is maintained as a GitHub project, CoreOS Clair analyzes vulnerabilities in appc and Docker containers. Serge Dukic of connect.cd puts it succinctly by saying that Clair "allows you to 'scan' Docker images in order to ensure that all patches/upgrades have been applied." The project was named "Clair" for the French word "clear" because the results of the scan are transparent views of the security of your container-based infrastructure.

Vulners Audit Scanner: A free infrastructure scanning tool for Linux, Vulners Audit Scanner is an open source product that can scan infrastructures of any size. With a clean and neat interface, Vulners provides the information you need to keep your network patched and protected. Alexander Leonov, an information security automation expert impressed with the Vulners Audit Scanner, found that its API was the key to making it work in the real world. He also liked that you can sign up for email alerts to be notified about security vulnerabilities as they are discovered and published.

BelSecure: This scanner was developed by the makers of Belarc Advisor, a well known and popular tool for determining the status of installed software and hardware on your personal computer. BelSecure is made for the corporate environment and analyzes your network to find security vulnerabilities. It compares your IT configurations to consensus security benchmarks so that the scores you receive are according to industry standards. According to their website, "BelSecure helps automate security processes such as FISMA, HIPAA and FFIEC."

Leading Vulnerability Repositories and Databases

Vulnerability management tools check your code, applications, and infrastructure for known security vulnerabilities. All of those tools pool their knowledge of known vulnerabilities from repositories and databases that are maintained by different governments and organizations around the world. Daniel Miessler, an Information Security Professional, provides a list of such repositories and databases, including the US Government's NVD, among others. Here is a short list of our own.

CVE Details This is one of the definitive lists of Common Vulnerabilities and Exposures (CVEs) on the Internet – in fact, the CVE Details website tagline is "The ultimate security vulnerability database." The CVE Details website merges information gathered from other websites and databases so that all of the information you need is concentrated in one place. You can search for specific CVEs, view the top 50 vulnerabilities, read reports, and so on. An extensive collection of security vulnerabilities, CVE presents the latest statistics as informative graphs and charts to make the data easily understandable in the fast-moving world of cyber vulnerabilities.

WPScan Vulnerability Database: As of March 2018, approximately 30% of the world's websites run on WordPress, which is why the WPScan Vulnerability Database is so important. An online browsable database of all security vulnerabilities found in WordPress core, themes, and plugins, the WPScan Vulnerability Database is the go-to authority for WordPress website developers. The list of vulnerabilities is compiled by the WPScan team which comprises security testers, pentesters, and Ruby experts. Interestingly, the WPScan database does not seem to use a WordPress theme, which one hopes is not indicative of their confidence in the security of WordPress themes in general.

CERT-EU (Computer Emergency Response Team for EU organizations) comprises small teams of computer security experts in both the public and private sectors. In fact, the CERT-EU website states that the Digital Agenda (2010) calls for "all [EU] Member States to establish their own CERTs, paving the way to an EU-wide network of national and governmental Computer Emergency Response Teams." One of the results of this is a comprehensive and well-documented list of computer security vulnerabilities, including a list of:

- Vulnerabilities found in products (e.g. Microsoft, Linux, Apple, Google, and so on)
- General vulnerabilities (in applications, Operating Systems, networking software, hardware, etc.)
- Cybersecurity threats and incidents (such as cyber crime, economic threats, DDoS attacks, among others)
- Hacking techniques (such as malware, social engineering, and APTs)

Zero Day Initiative: By financially rewarding white-hat hackers who find security vulnerabilities in software, the ZDI project helps to protect users around the world from Zero-Day attacks. In fact, the ZDI website declares that "the ZDI represents the world's largest vendor-agnostic bug bounty program" and will never release Zero-Day vulnerability information until the vendor has been informed and a patch released. Furthermore, even though ZDI is run by TrendMicro (a security software provider), security vulnerabilities are not released to the public until the other security software providers have had a chance to provide security responses for their customers.

Vulners: Vulners makes a free infrastructure scanning tool for Linux and maintain an impressive database of security vulnerabilities which is open to the public. Vulners calls their database "Google for Hackers" because they claim that all security vulnerabilities are listed and defined in their database. As of August 2018, the Vulners Security Database included 979,693 CVE security advisories and bulletins, 117 software vendors, bug bounty programs, and other security sources, and 174,985 known exploits for popular software. The Vulners database is fully searchable and includes tens of links to security blogs and articles by independent security consultants, general software vendors, and security software companies. Dennis Gorchakov, Projects Director of Cyber Security, wrote that Vulners is "...like a metasearch engine, combining info on CVEs, exploits, patches and related information, so you don't need to walk through a dozen of sites (CVEDetails, SecurityFocus, Rapid7 DB, ExploitDB, NIST vulnerability database, multiple vendor pages) to collect all the info you need during vulnerability assessment." In other words, Vulners is a one-stop vulnerability shop.

Rubysec A community-maintained repository of security vulnerabilities that affect Ruby libraries and Virtual Machines. Ruby is an extremely popular programming language that is used for web applications, web servers, system utilities, database work, backups, parsing, even biology and medicine. Because of its popularity and versatility, it became necessary to keep the Ruby community informed of all security vulnerabilities associated with it. The Ruby Advisory Database has advisories dating back to May 2007 and also includes vulnerabilities from the Open Source Vulnerability Database. A simple form enables anyone to submit a vulnerability and an official CVE identifier is automatically allocated to each submission, which are vetted on the GitHub Repository.

Conclusion

Every day new vulnerabilities are discovered in popular software applications and in hardware devices. For example, in March 2018 a new and major "backdoor" vulnerability was discovered in Cisco router firmware, rendering 8.5 million routers open to attack. Finding, patching, reporting, and responding to these security flaws is paramount to keeping a step ahead of hackers who are forever poking at our cyber defences to find a soft spot they can exploit.

However, the only really effective way to manage these kinds of security issues is through continuous remediation. While knowing about a new security vulnerability is important, it doesn't help your organization until something is actually done about it. Enabling automated responses to patch or solve cybersecurity vulnerabilities as they become known is the only answer to ensuring continuous organizational cybersecurity.