Automated Vulnerability Scanning – Your Powerful Weapon against Cyber Crime

A bluedog Whitepaper

bluedog
SECURITY MONITORING

Contents

Executive Summary

2020 has been a rough year for everyone and cyber security is no different. We were met with new threats and the existing ones multiplied to such an extent that specialists deemed 2020 the year of the cyber pandemic[1], on top of the COVID-19 crisis.

Videoconference and teleconference hijackings became the norm and data breaches also grew exponentially[2]. In short, cyber-attacks had an 800% surge, so we saw no less than 4,000 a day, every day[3].

To add salt to the wound, there is a worldwide shortage in cyber security skills and it doesn't look like it's going to get sorted any time soon. 74% of cyber security professionals say that this shortage has affected their organization in one way or another[4]. This is a complex topic, with significant ramifications. We covered it in a stand-alone whitepaper that you can download completely free using this link.

In this murky landscape, it's obvious that we need different solutions. In fact, even before the rise in cyber-attacks and the onset of the dire skills shortage, hiring costly teams of cyber security professionals was far from being ideal (or affordable) for SMEs.

This whitepaper offers an in-depth approach on one of the most affordable and easy to use solutions: automated vulnerability scanning. This is, in fact, the solution that seasoned professionals use, too. It's not a compromise for not having the funds to hire a top-tier security team.

It's the smart solution to keep a close eye on your internet-facing digital assets, irrespective of your company's size or your cyber security budget.

The whitepaper is a comprehensive intro to automated vulnerability scanning. You will find out what this solution entails, what are its benefits and its shortcomings, as well as how to leverage it to the fullest.

[1] https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-brought-a-cyber-pandemic.html, retrieved January 2021

[2] https://www.bizjournals.com/cincinnati/news/2020/06/01/cyberattacks-on-the-rise-during-covid-19.html, retrieved January 2021

[3] https://www.prnewswire.com/news-releases/top-cyber-security-experts-report-4-000-cyber-attacks-a-day-since-covid-19-pandemic-301110157.html, retrieved January 2021

[4] https://www.esg-global.com/data-point-of-the-week-05-13-19, retrieved January 2021

What Is Automated Vulnerability Scanning?

Automated vulnerability scanning refers to the use of software/computer programs to identify weaknesses in devices, networks, or applications. Vulnerability scanning relies on databases of known vulnerabilities (like CVE/NVD, for instance[5]). This means that the software compares the findings in your devices, network, or applications to know exploits or known issues. When such a vulnerability is identified, the user is automatically notified.

The best vendors of vulnerability scanners are those that use several vulnerability databases – this makes for a more comprehensive scan. It's important to note that vulnerability scans don't solve the issues they find. Some tools will suggest solutions or rank the issues they found in order of their importance or urgency, but they will not do the actual patching.

Regular vulnerability scans are common practices for enterprise networks. More importantly, in some industry, they are mandated by government regulations and industry standards as a means to keep the organization's vulnerabilities in check.

[5] https://nvd.nist.gov/, retrieved January 2021

Automated vs Manual Vulnerability Scanning

The introduction of this whitepaper mentioned the cyber security skills shortage and the astounding budget you need to hire a team of cyber security professionals. Does this mean that performing manual scans is better than letting an automated solution do this job for you?

Not really.

In fact, we would argue that this is a waste of resources. For starters, vulnerability scanning and management requires a lot of diverse skills and demands a lot of time for:

- Project scoping
- Gathering information
- Doing the actual scanning
- Identifying and validating vulnerabilities
- Creating and discussing reports
- Fixing the issues detected

All of the above would require a fairly large number of people with complementary skills: QA analysts, developers, networks administrators, application developers, auditors, security offices, project managers, and, of course, top management.

Aside from having to cough up a large budget for all these high-paying individuals, there is another big problem with manual scanning. Most companies rely on a lot of web applications, plus various networks and types of devices. When the digital asset pool is large, you always run the risk of duplicating your efforts senselessly.

Plus, it will take a lot of time. By the time manual scanning is done, you will have to restart the whole project because new vulnerabilities have been identified. An automated security scanner, on the other hand, allows you to scan all your applications simultaneously.

Let’s look at a real-life example, a custom-made ERP. These solutions typically have hundreds or even thousands of attack entry points – SQL injections and cross-site scripting being the most common of them.

If a *good* ERP only has 400 entry points that require verifications against no less than 100 vulnerability variants, the time needed to perform this is astounding. Assuming that it takes only five minutes for a test to be completed by a manual tester and that he’d need to perform a minimum of 40,000 security tests, this means that it would take more than 400 business days (that’s almost two years!) to complete the tests on a single web application.

Plus, manual scanning means that you are limited to the tester’s vulnerability knowledge. No matter how good the expert is, they can’t compete with an automated solution that is updated constantly by a large team of experts in cyber security.

The bottom line: don’t waste your team’s time on a Sisyphean endeavor. It will not only be endless, but also very costly and error-prone. You can, instead, run automated vulnerability tests and complement them with other human-led cyber security solutions. We’ll take a look at that below.

Internal vs External Vulnerability Scanning

Vulnerability scans can be conducted from both inside the network that's being evaluated and from outside of it. Why bother with both?

Because they fulfill different roles. An external scan is designed to determine the vulnerabilities of the organization's servers and/or applications that are accessible straight from the internet. On the other hand, internal vulnerability scanning helps to identify the vulnerabilities that attackers can exploit if they move laterally through various servers and systems in the even they gain access to the local network.

Gaining access to the local network can be fairly easy or very complicated, depending on how the network is configured and, above all, segmented. This is why a vulnerability scans always starts (or should always start) with mapping and inventory. This process entails itemizing every asset an organization has and classifying them based on the value of the data they hold and the access they provide.

There are certain industry standards (like PCI-DSS, the Payment Card Industry Data Security Standard) that require both internal and vulnerability scans to be performed quarterly. On top of that, extra internal and external scans should be performed in various other instances that affect a network's topology:

- When the firewall rules are modified.
- When certain software solutions are upgraded.
- When a new system or a new component is installed in the network.

While both internal and external scanning are important, the accelerated adoption of cloud solutions worldwide[6] has created more need for external scanning. Misconfigured (and, consequently, insecure) deployments in the cloud are quite common. External vulnerability scans can help identify them before they become real risks.

Vulnerability scanning has its limits. This is why we always recommend complementing it with penetration testing[7], the process that includes human-led probing and attack simulations to determine which threats should be tackled first.

[6] https://www.flexera.com/blog/industry-trends/trend-of-cloud-computing-2020/, retrieved January 2021

[7] https://bluedog-security.com/penetration-testing/, retrieved January 2021

Authenticated vs Unauthenticated Vulnerability Scanning

You will also encounter this distinction in a different parlance: credentialed or non-credentialed scanning. The terms are interchangeable.

Unauthenticated scans are designed to uncover certain services on a computer or a network that are open. In this context, “open” means that they send packets on their own open ports. These packets are typically used to find information that is available without authentication, such as software versions, open file shares, operating system versions and others. When these details are found, the scanner searches for vulnerabilities in those databases.

Credentialed scans, on the other hand, use login information to collect information about the operating system and the software installed on the scanned assets. Since it uses the login info, the information such a scan can find is usually more accurate and more detailed.

For example, even though some programs are not accessible over the network but they can still have certain vulnerabilities that could be exposed to various attacks. The most common of these attacks are malicious files open by unsuspecting users inside the network or accessing malicious web pages.

It is important to note that, even though authenticated vulnerability scans can collect accurate and detailed information (more so than their unauthenticated counterparts), they are still prone to false positives. This happens because certain vulnerabilities could have been mitigated though workarounds that don’t necessarily entail patch installation or updating the version of the affected application.

What Happens after a Vulnerability Scan

Vulnerability scans usually take place outside of business hours, especially when there are a lot of assets to be scanned. That happens because they can congest the system, slow them down, or cause disruption. Thus, whenever possible, they will be conducted at a time when users are not affected.

When the vulnerability scan ends, the user gets a detailed findings report. Some solutions also categorize the findings based on the severity of the threat. Either way, this report should be reviewed by a security team. Triage and investigation are ideally conducted by human teams. Vulnerability scans are just a part of bigger cyber security solutions.

After the report is analyzed, pen testing is conducted to determine the actual risk score of every vulnerability identified by the scan and to validate flaws. More importantly, pen testing can also test (using real-life scenarios) the effectiveness of the organization’s existing defenses and assess the need to upgrade or change them.

These are some of the questions that security teams need to answer after the vulnerability scan is complete:

- Which vulnerabilities are true and which are false positives?
- How long has a certain vulnerability been on the application/network/device?
- Is this vulnerability exploitable via the internet?
- Do we already have security measures in place to reduce the impact or likelihood of happening of this vulnerability?
- How easy is it to exploit this vulnerability?
- How would the business be affected if this vulnerability was exploited?

If you’re looking for a comprehensive vulnerability scanning solution, you have come to the right place. bluedog Security Management checks all the boxes above and more. Head on to our contact page and let’s talk about how our automated vulnerability scanning solution[8] can help you!

[8] https://bluedog-security.com/vulnerability-scanning/, retrieved January 2021

About bluedog Security Monitoring

Our goal is to provide businesses with a level of network protection typically only afforded by large corporations. We aim to bring high-quality technology, support, and service to the small to medium business, helping protect their business from cyber threats.

Our company is growing quickly, through our simple and affordable end-to-end network monitoring solution. Recently voted one of the Top 10 cybersecurity start-ups of 2019 by Enterprise Security Magazine. Whether you are a small business, or an MSP or IT services reseller or distributor, get in touch and have a chat with us.

20-22 Wenlock Road, London, N1 7GU

info@bluedogsec.com

+44 20 8819 6254