EC-Council

VULNERABILITY SCANNING: OPEN SOURCE WEB APPLICATION VULNERABILITY SCANNING TOOLS

This white paper is to encourage those organizations that have an insufficient budget, to purchase web application vulnerability scanner tools license or conduct penetration testing from third-party organizations. It is additionally beneficial to those organizations or penetration testers to help them pick out the proper tool for web application vulnerability scanning.

- By: Mujahid Shah
C|EH

EC-Council Cyber Research

TABLE OF CONTENTS

INTRODUCTION

No enterprise is simply too small to avoid a cyber attack or information breach. Unfortunately, smaller organizations might not have the finances and in-house expertise to harden their systems and networks towards cyber threats.

Most companies are already implementing vulnerability scans in their enterprise, understanding the importance of doing so before reaching out to the public. The obvious advantage to using an open source tool of any kind is that it usually lacks any type of price tag. The free nature of the tools makes open source an easy choice for those who have no budget to spare or those with a minimal budget. There are other financial and resource considerations to be considered while implementing the tool in their specific environment, but overall, the lack of expenditure makes open source tools the most sought-after option for the cash-strapped.

Some organizations choose open source tools because of the ability to alter the tool to their specific needs, as they possess the source code. Once they have obtained the open source tool code, the organization is free to modify it for their organization's needs.

This white paper examines three open source web application software vulnerability scanning tools (Vega, ZEB proxy, and Paros) and one commercial web application software vulnerability scanning tool (Netsparker). This has been done to compare and demonstrate the vulnerability detection functionality and effectiveness of the various tools.

VULNERABILITY ASSESSMENT

Vulnerability scanning is a security technique used by organizations to find the flaws in a targeted system. This means that the organization can discover any holes in the web application and system before the malicious user does. This activity is generally executed before deploying web applications on the internet . Web application security is the method of defending websites and online services against different security threats that exploit vulnerabilities in an application's code. Nowadays web applications are more attractive for cyber attacks as the complexity and integration of different software with web applications provide a great attack surface for attackers. Integrally web applications are much harder to protect versus traditional applications that have the advantage from the security infrastructure that has already been deployed. To detect and appropriately protect against web application threats, organizations must first have the capacity to identify these vulnerabilities. This includes performing web application vulnerability assessment scanning.

TYPES OF VULNERABILITY ASSESSMENTS

A vulnerability assessment is the process of defining, identifying, classifying and prioritizing vulnerabilities in computer systems, applications and network infrastructures and providing the organization doing the assessment with the necessary knowledge, awareness and risk background to understand the threats to its environment and react appropriately.

Some of the vulnerability assessment scans consist of the following:

- Network-based vulnerability scanning can help an organization identify weaknesses in their network security before the bad guys can mount an attack. The goal of running a vulnerability scanner or conducting external vulnerability assessments is to identify devices on your network that are open to known vulnerabilities without actually compromising your systems.
- Host-based scans are secondary to understand the vulnerabilities in servers, workstations, and different network hosts. It scans the host or system in order to diagnose the security weaknesses in the wireless network. The wireless network scans of an enterprise's wifi networks are required to bring to attention the points of attack in the wireless network infrastructure. Apart from discovering rogue access points, a wireless network scan can also validate that an organization's network is securely configured.
- Application scans are imperative to web sites to discover recognized software vulnerabilities and unwarranted configurations in the network or web application.
- Database scans can detect the susceptible factors in a database, that can cause malicious attacks, such as a SQL injection attack.

WHY PERFORM A VULNERABILITY ASSESSMENT?

A vulnerability assessment informs companies of the weaknesses in their digital infrastructure and points them in the direction to reduce the threat that the weaknesses can cause/have caused. Vulnerability scanning enables an organization to reduce the chances of an attacker breaching the network/system. For businesses looking to decrease their security threat, a VA is a process to identify and quantify the security vulnerabilities in an organization's environment. A comprehensive vulnerability assessment program provides organizations with the knowledge, awareness, and risk background necessary to understand threats to their environment and react accordingly.

OPEN SOURCE WEB APPLICATION VULNERABILITY SCANNERS

An plethora of tools is available to software testers to help detect software vulnerabilities. However, some tools are more powerful than others.

- Open Source tools are easily available
- They identify almost all vulnerabilities
- Automated for scanning
- Easy to run on a regular basis

RESEARCH MOTIVATION

Picking a vulnerability discovery tool for those organizations that have no security expert may be a crucial downside. There is some disadvantage of automatic vulnerability scanning tools have false positive and false negative results. Thus, exploiting the system using the wrong tool can lead to the preparation of web application/services with unseen vulnerabilities.

TESTING THE TOOLS

A. OWASP ZEB Attack Proxy

The OWASP zed attack proxy (zap) is one of the globe's most famous free security tool and is actively used by masses around the world. It helps find security vulnerabilities on applications. It is used by penetration testers while conducting manual tests.

HTTPS://WWW.OWASP.ORG/INDEX.PHP/OWASP_ZED_ATTACK_PROXY_PROJECT

B. Paros Web Proxy Tool

Paros is a free of cost web proxy tool that is written solely in Java. Through Paros' proxy nature, all http and https data among server and client, along with cookies and form fields, can be intercepted and modified.

HTTP://SECTOOLS.ORG/TOOL/PAROS/

C. Vega Tool

Vega is a platform for testing the security of web applications. It is GUI based, written in Java, and runs on Linux, OS X, and Windows. It can be easily extended with modules written in Javascript.

HTTPS://SUBGRAPH.COM/VEGA/

D. Netsparker Web Security Scanner

Netsparker Desktop is an easy-to-use, yet powerful web application security scanner that scans websites, web applications, and web services automatically identifying vulnerabilities and security flaws in them.

HTTPS://WWW.NETSPARKER.COM/

EXPERIMENT

In this white paper, we selected web based applications that handle various types of loan disbursements (house loan, car loan etc) processes. We conducted two different scanning policies: Default Scanning Policy and Custom Scanning Policy.

Scanning Conducted

- Scan web application using three open source web security scanners and one commercial web security scanner.
- Scan different scanning policy.
- Compare the vulnerability scanning results.

ANALYSIS

Default Scan Policy:

On analyzing the first experiment, it was found that Vega detected five high and zero medium vulnerabilities (Figure 1), ZEB attack proxy detected one high and two medium vulnerabilities (Figure 2), and Paro detected two high and four medium vulnerabilities (Figure 3).

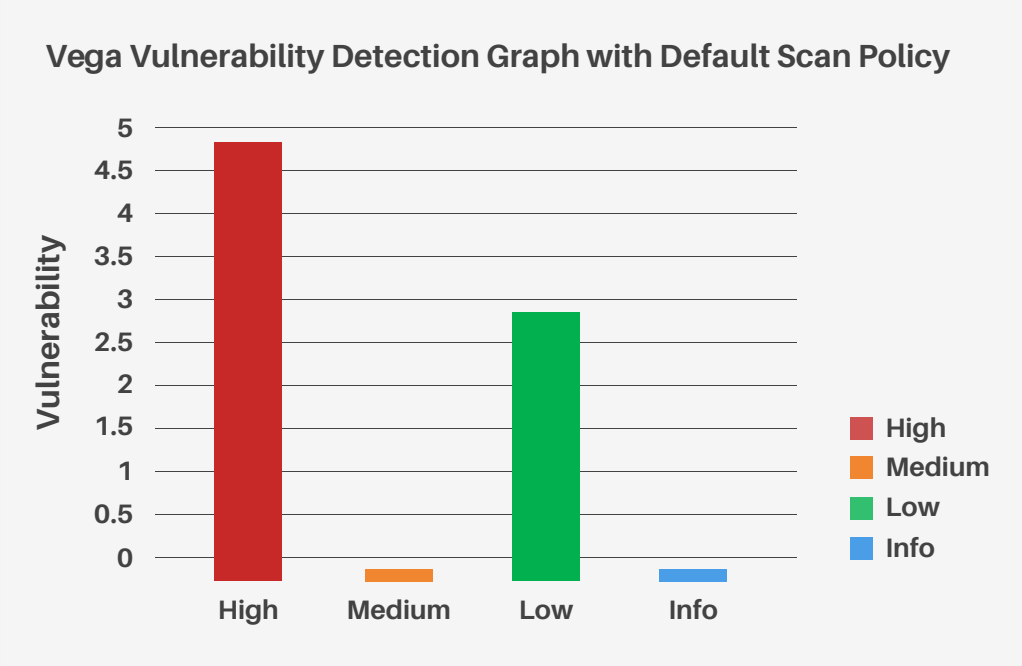

Figure 1: Vega Scan Result

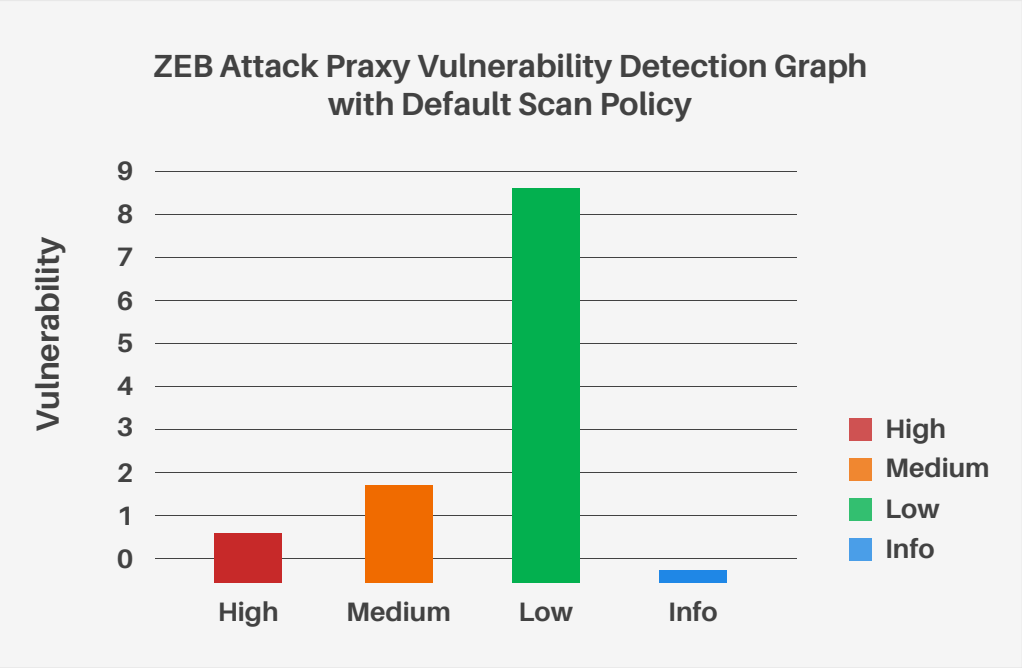

Figure 2: ZEB Attack Proxy Scan Result

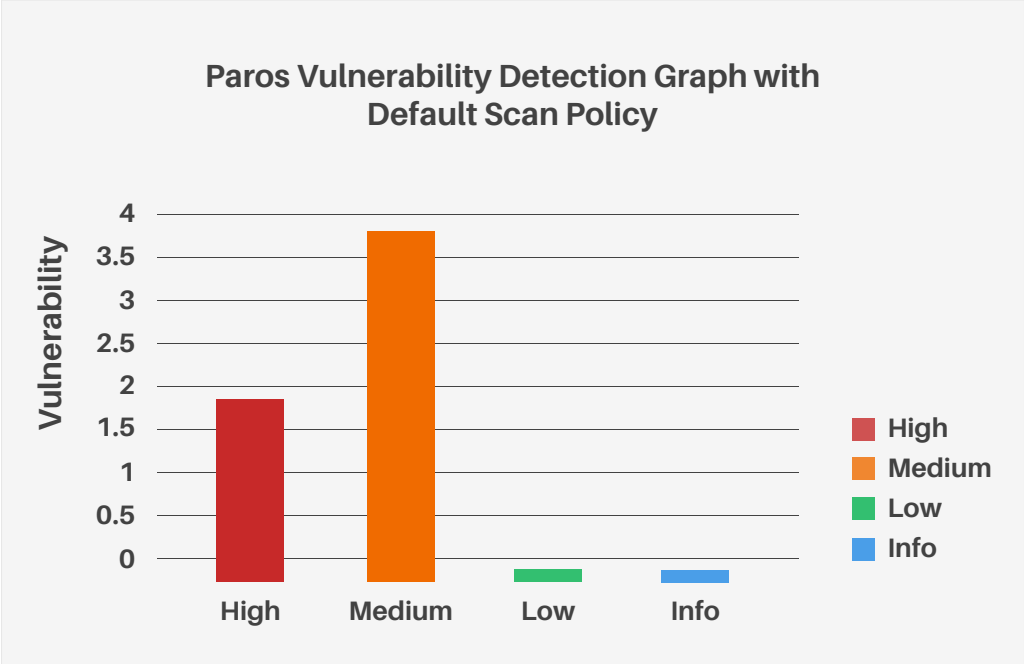

Figure 3: Paros Scan Result

Custom Scan Policy:

On analysing the second experiment, it was found that Vega detected eight high and three medium vulnerabilities (Figure 4), ZEB attack proxy detected one high, three medium, and 11 low vulnerabilities (Figure 5), and Paro detected two critical, three important, three medium, and nine low vulnerabilities (Figure 6).

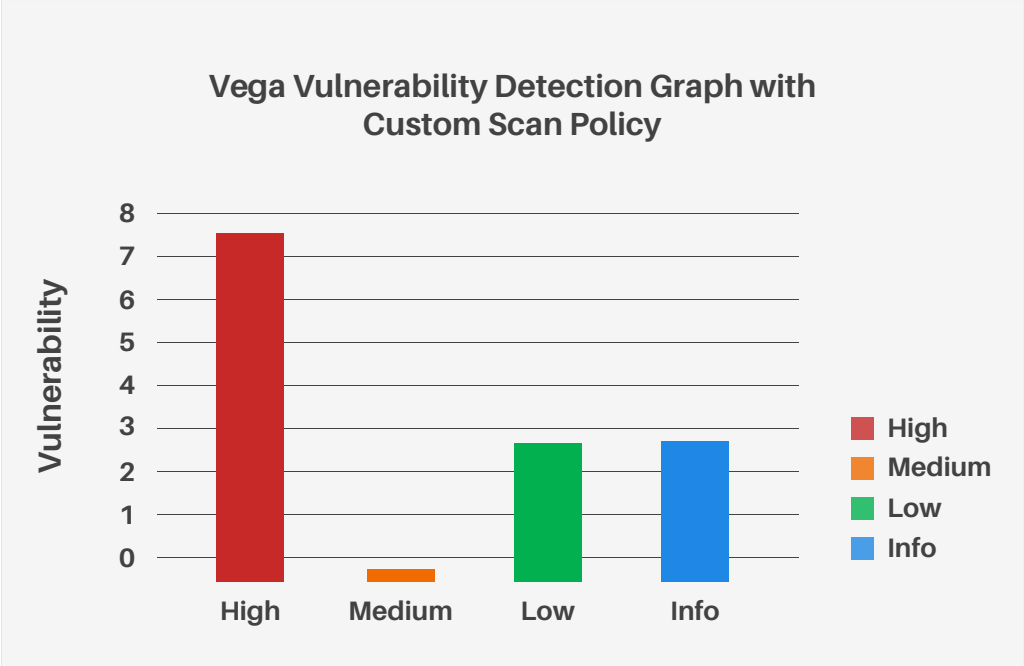

Figure 4: Vega Scan Result

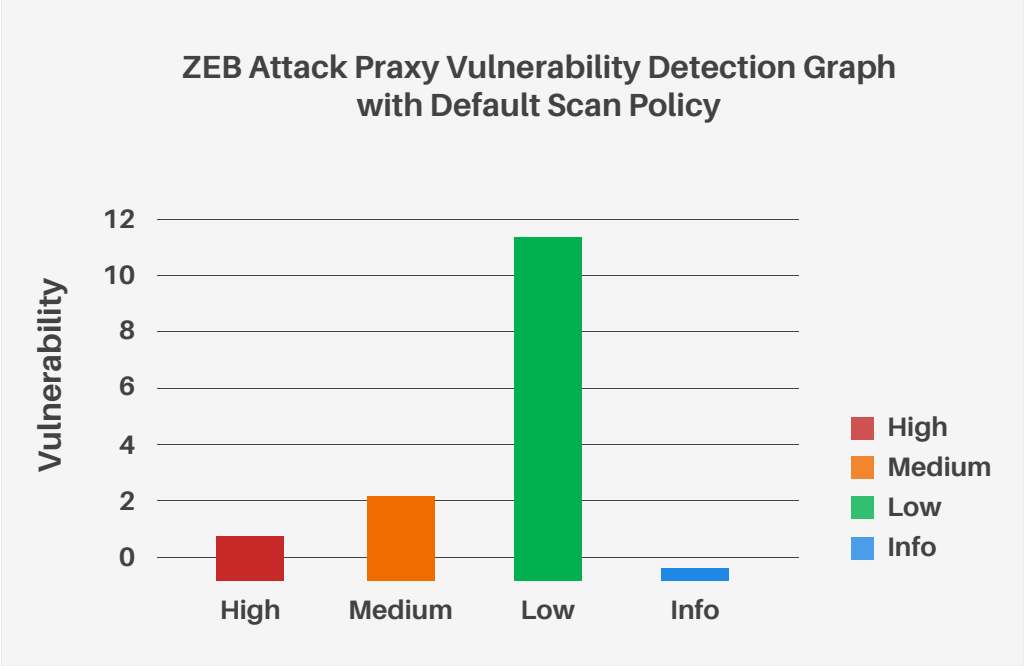

Figure 5: ZEB Attack Proxy Scan Result

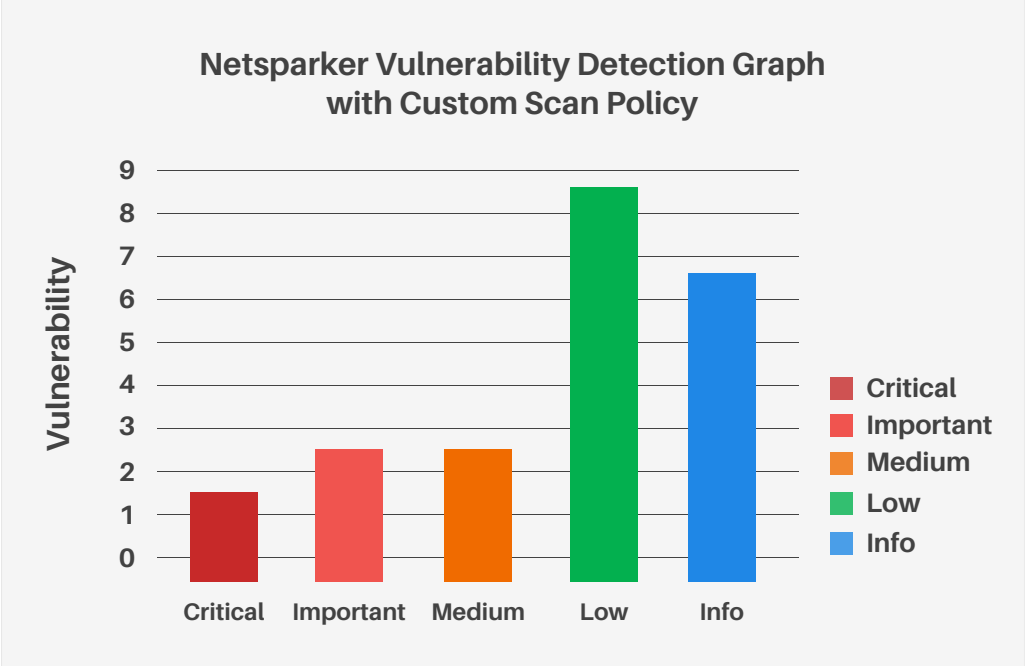

Figure 6: Netsparker scan result

Vulnerability Scanning Results

In the experiment, Vega detected eight high and zero medium vulnerabilities (Figure 7 and 8), ZEB attack proxy detected one high and three medium vulnerabilities (Figure 7 and 8), and Netsparker detected five high and three medium vulnerabilities (Figure 7 and 8).

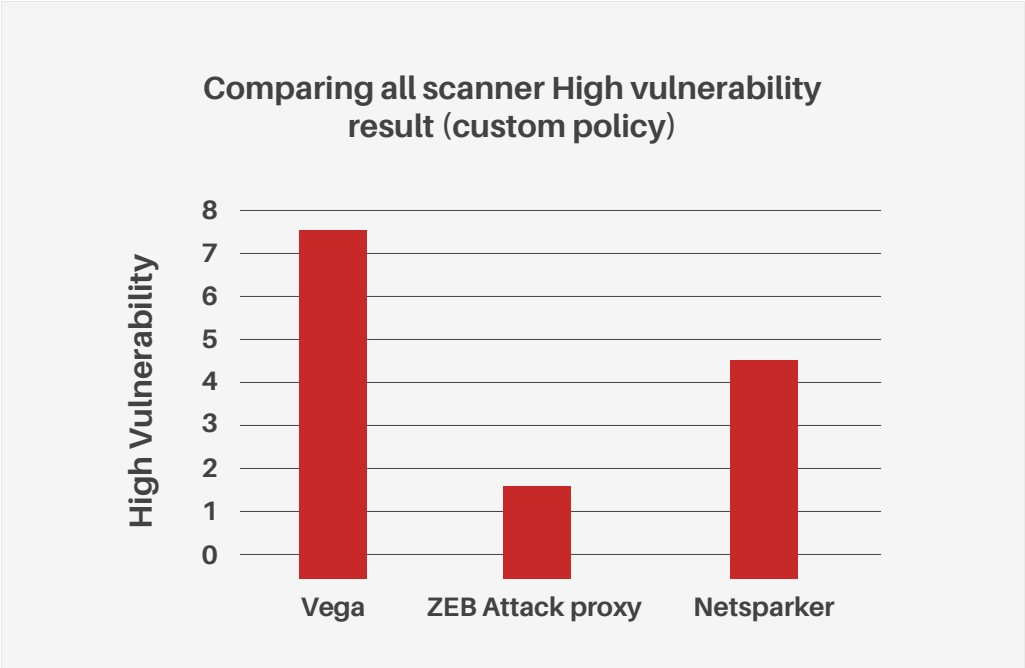

Figure 7: Comparing High Vulnerability Scan Result

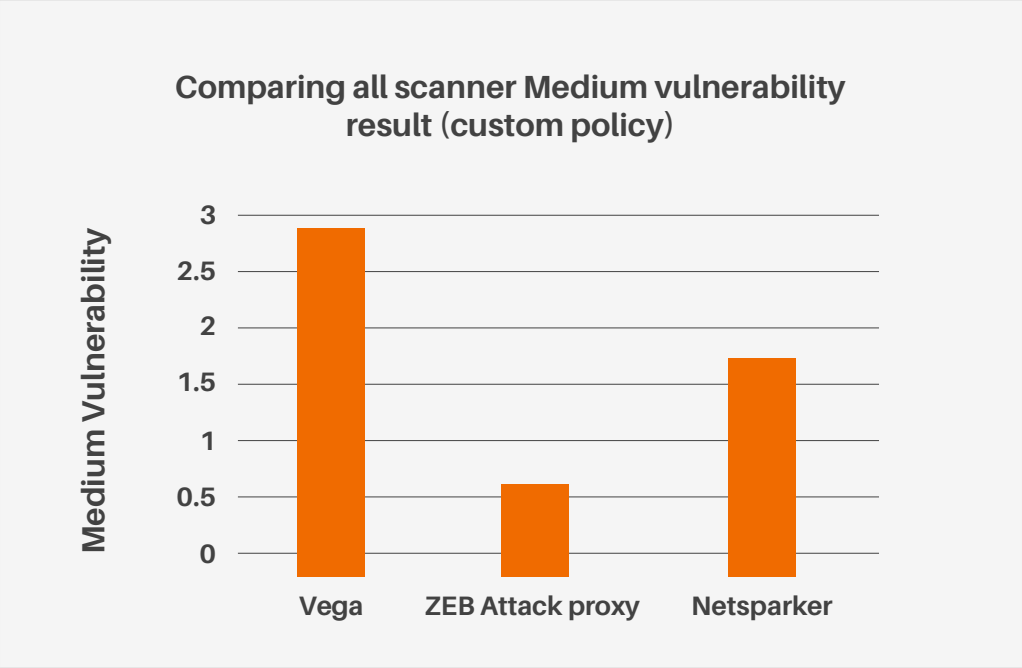

Figure 8: Comparing Medium Vulnerability Scan Results

CONCLUSION

In this white paper, we ran three open source web application security scanners and one commercial web application security scanner with default and custom scanning policies to compare the result. We end with the distinctive coverage result that the custom policy scan came across extra vulnerabilities than the default policy scan.

This shows that the scanners do not show equal results, but that, a combination of two or more scanners can help you detect more vulnerabilities. However, a penetration test is strongly recommended to receive an accurate scan with zero false negative and positive responses.

EC-Council