OpenVAS

Zoë Medina, Aida Gaston, Pelumi Akande, Randall Seymore

Professor Hoffman

CYBR-501 Intro Cyber Concepts and Tools

Shiley-Marcos School of Engineering (SMSE), University of San Diego

Table Of Content

Abstract

This essay explores OpenVAS history and development, as well as its various features, capabilities, and uses for a small business. It also covers use cases, such as network scanning and vulnerability management. OpenVAS is an open-source vulnerability scanner that can help security professionals identify and address security gaps in digital systems. It has become a valuable tool in the fight against cybercrime due to its ability to quickly identify and close gaps that can be exploited by malicious actors. In addition to identifying and addressing security gaps, OpenVAS also has a wide range of features that make it an excellent tool for managing and reporting vulnerabilities. Its web-based interface makes it easy for users to configure and manage scans. It includes a detailed reporting feature that allows users to monitor and track their exposure to vulnerabilities over time. Finally, this essay talks about the importance of conducting vulnerability assessments and how they can be integrated into a small business structure. This paper aims to introduce OpenVAS to the reader and provide an overview of its capabilities.

Introduction

OpenVAS is a Kali vulnerability scanner tool that can detect vulnerabilities in any server or network appliance. It is a free and open-source vulnerability scanning framework that may be used to detect security risks and vulnerabilities in a network or computer system. It may scan for and report on a variety of vulnerabilities, such as software exploits, misconfigurations, and missing security patches ("Open Vulnerability Assessment Scanner," n.d.). Security specialists, network administrators, and IT departments all utilize OpenVAS to examine the security of their systems and ensure that they are protected against known threats. OpenVAS identifies potential risks using a comprehensive database of known vulnerabilities and exploits and delivers a

complete report that enables users to prioritize the most serious vulnerabilities and concentrate their efforts on resolving them. In addition to vulnerability scanning, the tool offers vulnerability management tools such as tracking vulnerabilities over time and collaboration features that allow several users to resolve the same scan at the same time.

OpenVAS is frequently used as part of a comprehensive security plan. It has a simple online interface for controlling scans and can be set to run frequent scans automatically to keep your systems up to date. The framework is extremely flexible, allowing users to select the categories of vulnerabilities to scan for, the frequency with which scans are performed, and the exact targets to be examined ("OpenVAS Vulnerability Scan," n.d.). It also comes with a number of plugins and extensions that may be used to expand its capabilities, making it a very versatile tool.

Custom scans are supported by OpenVAS, allowing administrators to develop bespoke scans that are targeted on specific targets, services, and vulnerabilities. Customized scans can be used to execute focused services on certain systems or applications, as well as to exclude specific systems or services from being scanned. With the capacity to execute scans across numerous systems and scan vast networks in parallel, OpenVAS is built to scale to meet the needs of growing companies. This makes it an ideal tool for enterprises with large or complex networks or small networks with the intent of growing. Several security tools, security information and event management (SIEM) systems, intrusion detection systems (IDS), and vulnerability management platforms are compatible with OpenVAS ("Cybersecurity Risks and Business Context," n.d.). This enables firms to streamline their security operations and more efficiently manage security risks.

What it does for security

The Open Vulnerability Assessment System, or OpenVAS, was created by Greenbone Networks as a competing vulnerability scanner to Nessus. In 2005, the developers of Nessus decided to no longer offer the scanner under open-source licenses, instead moving to a proprietary business model. By the following year, many forks of Nessus were developed to continue the open-source model that many customers were looking for. Of these, OpenVAS is the only one to maintain development and remain operational. When creating OpenVAS, the developers wanted it to be "an all-in-one vulnerability scanner with a variety of built-in tests…to make setting up and running vulnerability scans fast and easy" (Poston, 2018).

Vulnerability scanners are a powerful security tool to keep track of and monitor devices on a network. First they scan the network for all connected devices and gather important information on them such as their operating system and any open ports. The inventory list created by the scan makes it easier for security professionals to see which devices should and should not be using their network. OpenVAS accomplishes this by "closely inspecting areas such as firewalls, applications, and services to gain unauthorized access to organizational networks and assets" (Bugcrowd, 2022). OpenVAS also includes the option to run authorized or unauthorized scans. This allows for different views of the system, one from the perspective of an external malicious actor and one from the perspective of an internal actor. By knowing what an external actor can see and access, it gives security professionals an idea of which devices need to be hardened.

Once the list is created, the scanner runs each item on the inventory list against a Common Vulnerabilities and Exposures, or CVE, database. These databases are curated by different companies to keep up to date information about found vulnerabilities. Ideally,

vulnerability scans should be run against more than one database since a found vulnerability might be recorded in one database but not another. If the scanner finds a known vulnerability with a device on the network, it will highlight it in the report and give it a severity rating. The severity rating makes it easier for security professionals to quickly see which devices need to be patched quickly. Vulnerability scanners are only the first line of defense when it comes to cybersecurity. These scans allow for "early detection of known security problems but by itself it isn't the perfect solution for the protection of the network" (Chalvatzis et al., 2019). Vulnerability scanners only report back the state of the devices at the time of the scan, meaning that vulnerabilities created after a scan will not be listed in the report. Therefore, it is important to run scans often enough to catch new vulnerabilities quickly.

OpenVAS also offers the option of continuous monitoring, where it will continue to run a new scan after the prior one has concluded. Furthermore, Vulnerabilities scanner might not always flag a true vulnerability. False positives occur when the scan thinks there is vulnerability where there isn't one. Therefore, a security professional will still be required to review the results after a scan has completed to verify the validity of each found vulnerability. Because OpenVAS is an open-source software, it relies on its community to report false positives to improve its CVE database. Once the user has identified the cause of the vulnerability and sends "a false positive to the OpenVAS mailing list, the feedback is usually prompt and knowledgeable. In this way, false positives may be remediated within hours" (Bugcrowd, 2022), which improves the software as a whole. It is also important to keep in mind that vulnerability scanners work based on known vulnerabilities. Therefore, zero-days will not be caught in one of these scans. Pairing vulnerability scanners with another security tool such as penetration testing is essential to fill in these gaps.

Security Features

OpenVAS is a tool popularly used by security professionals to assess the security of systems and to identify potential vulnerabilities that may be exploited by attackers. To do this, the security tool comes with a variety of features for security professionals to utilize.

Firstly, OpenVAS is equipped with Comprehensive Vulnerability Scanning. Its vulnerability scanner can find a wide range of security issues, such as web application and network vulnerabilities. It utilizes active and passive scanning methods to identify potential threats. An active scan is used to simulate an attack on the system. It sends packets to nodes on the network and then investigates the replies it receives. This allows security professionals to analyze what information is given to malicious actors when they are communicating with their network. The downside of an active scan would be the potential of overwhelming the network with unnecessary packets, especially if the network is currently being used by employees or customers as well. A passive scan is used to monitor the flow of traffic within the network without directly interacting with any of the devices. It is responsible for viewing the details of packets being sent and received, and then reporting any vulnerabilities it witnesses. The downside of a passive scan would be that it is not as thorough as an active scan. A passive scan can only see vulnerabilities from packets sent and received. This means that even though there are no devices triggering a vulnerability, a vulnerability could still exist in the system and the network is simply not sending the correct trigger to see it at that time.

Another feature of this tool is Deep Scanning. The OpenVAS vulnerability scanner performs deep scanning to find hidden and difficult-to-detect flaws in various applications and services. It scans for open ports and services that are running on them. False Positive Reduction

is another feature of the OpenVAS security tool. It provides a way to filter results by severity level, which can help prevent users from getting false positives. Next, the OpenVAS tool has the ability to integrate with other tools, such as Nmap and Metasploit, and therefore, OpenVAS can be used by security professionals to perform a more thorough and automated assessment of their target system by data automatically being shared amongst the different tools.

User Management is another security feature within OpenVAS where the administrators can easily set up user accounts with varying access levels. This ensures that only authorized individuals can modify or access the scans. Additionally, the security tool offers reporting features. These are reports generated by OpenVAS that contain detailed information about the identified vulnerabilities, such as their severity level and recommendations for addressing them. It makes it easier for security experts to prioritize their work. Finally, OpenVAS is an open source software, meaning that anyone can use and modify it. This makes it easier for experts to contribute to its development and customize it for their specific needs.

OpenVAS is a powerful tool that can help security experts identify and address security vulnerabilities in web and network applications. It can perform deep scanning and provide a false positive reduction, which makes it an ideal tool for organizations that want to improve their systems' security.

Recommendations For Use

To implement OpenVAS into the customer’s network it is recommended that the tool first be tested in a sandbox environment. To do so, the environment should first be built to simulate the actual information system that is intended for end use. This should be done by cloning the images of a computer currently in production. This image will include all current security

settings and policy settings currently implemented within the customer's network. An image of each operating system type will be included in the sandbox. This testing environment will allow the company to see how OpenVAS will perform in the real-world system without disrupting any of the current process flows that the customer relies on for day-to-day business.

With the real-world system belonging to a small office, this testing phase will be able to account for most, if not all hiccups that could possibly occur in the implementation phase. Having the opportunity to test the rollout of the new vulnerability scanner will account for system load issues, issues allowing the software to run under current configurations, and give the administrators the opportunity to become familiar with OpenVAS prior to its implementation into the office's information system.

Once testing is complete and the system administrators are comfortable with the skill sets they have acquired in the testing environment, the introduction of OpenVAS into the operational information system can be completed. Scans will be configured to capture every computer on the domain as well as the networking hardware. To do so, the System Administrator will input the IP addresses of every device on the network.

After scans have been configured and are operational, they will need to be scheduled to run on off-work hours to ensure there is no disruption to the network during the day. Scans will be run and checked at least bi-weekly. With the company being a smaller sized organization, this bi-weekly standard should be easily met.

It is important that OpenVAS is locked down and only accessible to information assurance and information technology personnel. To do so the web application must have a credentialed login that only users with need-to-know will have. Allowing any unauthorized users

or attackers access into OpenVAS would be essentially handing them a list highlighting every aspect of the network that is exploitable. The goal is to avoid this at all costs.

In order to relay and track the progress of the remediation of the vulnerabilities discovered by OpenVAS, the scan results should be exported into excel documents where they can be checked off and marked complete as patches are applied. These excel documents should be saved into a secure folder that only Information Assurance and Information Technology personnel have access to. The focus and main concentration of resources will be directed towards the vulnerabilities with a rating of high. This indicates a higher probability of exploitation. As the vulnerabilities are patched and recorded as fixed, verification scans will be run to ensure the vulnerabilities no longer appear on the OpenVAS scan results.

Once this process is practiced and streamlined, the company will have a very effective method of ensuring that flaw remediation is being conducted on the network. This will not be the only security defense implemented, but it will be one of the most effective. Patching vulnerabilities is a massive piece of the security posture, and having a process such as this will make this small office much more secure than it was prior to OpenVAS's implementation.

Conclusion

Overall, OpenVAS is a robust and adaptable solution that may assist enterprises in ensuring system security and protecting against potential risk. It is widely used by security professionals and routinely updated to stay current with the latest vulnerabilities and exploits. A report is drawn up that includes all of the findings, the specifics on each vulnerability, and any other issues that jumped out. Upon receiving the results, a security professional must determine whether or not a test result is meaningful. To keep your systems secure, you must address any

confirmed vulnerabilities. Monitoring remote servers for security flaws puts you in the shoes of a possible attacker, allowing one to know exactly what information is available to the public on services that are exposed to the rest of the globe. OpenVAS is a fantastic resource for enterprises looking to improve their defense capabilities by detecting and correcting system vulnerabilities. However, in order to give a comprehensive approach to security, it should be used in conjunction with other security measures.

References

Chalvatzis, I., Karras, D. A., & Papademetriou, R. C. (2019, March 31). *Evaluation of Security Vulnerability Scanners for Small and Medium Enterprises Business Networks Resilience towards Risk Assessment*. IEEE Xplore. Retrieved February 24, 2023, from https://ieeexplore-ieee-org.sandiego.idm.oclc.org/document/8873438

Cybersecurity Risks and Business Context. (n.d.). In Cybersecurity Risks and Business Context. https://www.horangi.com/blog/cybersecurity-risks-and-business-context

Green, T. (2018). OpenVAS: A Comprehensive Open-Source Vulnerability Scanning Framework. International Journal of Network Security & Its Applications, 10(4), 107-120.

Monitoring and Analyzing Security Data: A Guide to Setting up a SOC, Monitoring Network Activity for Suspicious Behavior, and Responding to Security Incidents. (2023). TSNC Global: Monitoring and Analyzing Security Data: A Guide to Setting up a SOC, Monitoring Network Activity for Suspicious Behavior, and Responding to Security Incidents. https://www.tsncglobal.com/2023/01/monitoring-and-analyzing-security-data.html

OpenVAS. Bugcrowd. (2022, July 13). Retrieved February 24, 2023, from https://www.bugcrowd.com/glossary/openvas-vulnerability-scanner/

Open Vulnerability Assessment Scanner . (n.d.). In Greenbone OpenVAS. https://www.openvas.org/

OpenVAS Vulnerability Scanner Online | HackerTarget.com. (n.d.). Retrieved from https://hackertarget.com/openvas-scan/

Poston, H. (2018, October 30). *A brief introduction to the openvas Vulnerability Scanner*. Infosec Resources. Retrieved February 24, 2023, from https://resources.infosecinstitute.com/topic/a-brief-introduction-to-the-openvas-vulnerability-scanner/