ISSN No:-2456-2165

Netobile: Network Vulnerability Scanner

[1]Deekshith V. K
Tly19cs021,
Department of Computer Science College of Engineering, Thalassery

[2]Nidhisree P. V
Tly19cs040
Department of Computer Science College of Engineering, Thalassery

[3]Karthika Chandran
Ltly19cs065
Department of Computer Science College of Engineering, Thalassery

[4]Rashma T. V
Professor
Department of Computer Science College of Engineering, Thalassery

Abstract:- Network scanning and vulnerability testing rely on processes and tools to scan your network and its devices for vulnerabilities. It helps improve an organization's security policy by identifying vulnerabilities and ensures that the security measures taken actually provide the protection an organization expects and needs. Administrators should perform regular vulnerability scans to find network vulnerabilities that allow exploits to compromise or destroy data or devices. Different network scanning implementations and tools have different capabilities and different types of results. The heterogeneity of these results usually makes subsequent analysis difficult. In this paper, we consider two basic open-source scanners as NMAP. We show how to integrate these two scanners into a well-structured GUI to provide reliable information. Based on the obstacles of NMAP, another tool was developed that combines the strengths of both devices and overcomes some of their shortcomings. A network scanner developed for this paper scans the network to identify active hosts, remote hosts' operating systems, and programs installed on those hosts. You can find open ports, list services running on a host, and identify active hosts. Further vulnerability scanning is conducted by comparing the information gathered from the network scan to a database of vulnerability signatures to create a group of suspected vulnerabilities that exist on the network. In addition to performing network scans and vulnerability assessments, the new tool also added an automated scanning mechanism to test whether a device has been compromised. This paper examines the capabilities of the new tool. That is, various formats are used to display network maps, vulnerabilities, and configuration errors. Furthermore, a simple methodology is characterized by shortening the output period of weakness.

Keywords: *Nmap, UI, IP, CPE, DHCP, OpenVAS, GUI, NVD, API, HTTP, CEE*

I. INTRODUCTION

As time goes on, the world will become more and more connected through the Internet and new networking technology. The openness of the Internet has made network security a hot topic. With the development of new technol- ogy, the organization is now shifting its business functions to the public networks and the vast amount of personal, business, and organizational information that accompanies them is available on network infrastructures around the world. Therefore, various precautions are taken to ensure data is not compromised or inaccessible to unauthorized persons. Net- work access is unauthorized by outside hackers or disgrun- tled employees and can be intentionally harmful or discard exclusive information that adversely affects or confuses the interests of the organization's ability to survive in intellectual property acquired through the internet with some effort. Net-work security measures include scanning and vulnerability assessment along with penetration tests. Network scanning is fundamental to gathering information about the real state of a computer system or network. It is a system for identifying active hosts on a network with the ultimate goal of network security evaluation. Vulnerability analysis is a systematic analysis of the security status of information systems. For the services like auditing, penetration testing, reporting, and patching organization both techniques are comprehensive. The scope of this dissertation is better understood by the following requirements of the organization. Our goal is fulfill- ing these requirements and giving a well-designed GUI and consistent data structure results: • Check device configuration Vulnerability assessment of the network. The VA can be done internally and externally • Auto-scan. The purpose of Net- work Security in an organization will be more understandable by identifying the reasons for any Corporate Networks being vulnerable:- • Complexity: More imperfections and unin- tended access points in vast, complex networks • Familiarity: Utilizing regular, well-known codes, software, operating systems, and/or hardware builds the likelihood an attacker has or can discover the knowledge and to • old to exploit the flaw. Connectivity: More physical connections, privileges, ports, protocols, and services increment vulnerability. • Password management flaws: The computer user uses weak passwords that can be revealed with brute force. The user saves the password on the computer where a program can access it. Users reuse the

same passwords between many programs and websites. • Fundamental operating system design flaws: The operating system developers choose to apply sub-optimal policies to user/application management. For example, the operating system uses policies such as default permissions to grant all programs and users full access to the entire computer This operating system bug allows viruses and malware to execute commands on behalf of the administrator.

➢ *Problem Statement:*

Identify internal and external threats through vulnerability analysis using a network vulnerability scanner. Developing applications to detect vulnerabilities in computers, computer systems, and networks. Current research recognizes the im- portance of network security, especially current vulnerability scanners. The main purpose is to help improve the vulnera- bility assessment process by combining tools to reduce the administrative burden.

➢ *Existing System:*

Network vulnerability scanners are important tools for iden- tifying and mitigating vulnerabilities in a computer network. There are various network vulnerability scanners available, including both open-source and commercial options. These scanners typically work by sending requests to network de- vices and analysing the responses to identify vulnerabilities. There are also lots of desktop applications available that provide network vulnerability scanning capabilities. These applications are typically installed on a local machine and are used to scan the network for vulnerabilities. Some popular desktop applications include Nessus, Nexpose, OpenVAS, and Qualys. These scanners can identify weaknesses in the network's infrastructure including servers, routers, and other devices as well as the software and applications running on those devices. Since most of these applications are built for desktops, it would reduce the ease of using them for users. The DE authentication of any unwanted users is not possible on these tools and it requires other platforms to do so.

➢ *Proposed Systems:*

The proposed is a mobile application that can be used to identify and assess the vulnerabilities that exist within a network. It can scan a network for weaknesses, such as un- hatched software, reconfigured devices, or open ports that could be exploited by attackers. These scanners work by sending requests to the devices on the network and analysing their responses. If a device responds in a way that indicates a vulnerability, the scanner will flag the issue for further review. It is designed to identify vulnerabilities in network infrastructure, such as routers, switches, and firewalls. Port

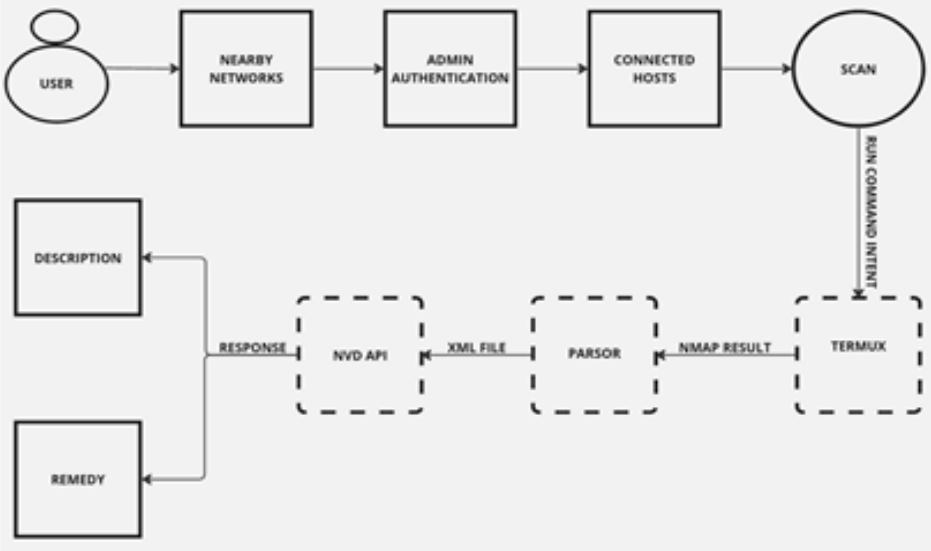

Fig 1 Architecture of the System

scanners are used to identify open ports on devices, which can be exploited by attackers to gain access to the system.It is good practice to explain the significance of the figure in the caption.It will typically provide a report that lists the vulnerabilities it has identified, along with recommendations for how to address them. These recommendations, known as remediations, may include steps such as installing patches or updates, reconfiguring devices or settings or replacing outdated or vulnerable hardware. The specific remediations recommended by a network vulnerability scanner will depend on the vulnerabilities that have been identified and the spe- cific needs of the organization.

➢ *Implementation:*

The project aims to deliver a mobile application which runs on the Android platform. The codebase is written in Dart and Java and uses Flutter for rendering UI. The project has various dependencies, that carry out the core functionalities. The de pendencies are WiFi iot, lan scanner, web driver, NVD API, HTTP client for dart, and Nmap. The package wifi iot helps to scan for nearby wifi access points and helps in handling those wireless connections. he project uses lan scanner which facilitates discovering network devices in the local network via multi-threaded ICMP pings. This library is designed to be used on class C networks. The package web driver is a web scrapping utility for Dart, this package is used for scrapping the management portal of the customer

premise equipment. Nmap is the core utility or the dependency of this project, Nmap scans the network and returns audit data containing limited vulnerabilities and they are further indexed in the app. The HTTP library is used as a client to send HTTP requests to NVD's REST API endpoints to get the vulnerability details associated with a specific CVE. The application starts with an interface showing the nearby available networks, which is done by iot scan, the user on selecting an access point from the screen gets navigated to the next page containing the clients associated with the specific access point, or on a broader case the scan returns the hosts in the accessible subnets with the help of lan scanner. The hosts are listed on the screen. Then the user is prompted to enter the administrator credentials on a login page which on completion initialises the web driver to connect to the IP address of the CPE and access its HTTP server. The script then logs in to the router and stores the session as a state. The script also accesses the DHCP leases generating a client list as a JSON file. After this stage, with the use of run_Command intent the tool nmap is spawned in termux app in the background to scan the subnet for common vulnerabilities. Nmap's output is piped and written to a file, which is then analysed for CVEs and other vulnerability descriptions. After the analysis, the key terms and the CVE ids are sent to NVD's API as HTTP rest requests. The response containing the vulnerability detail is then shown to the user via the app.

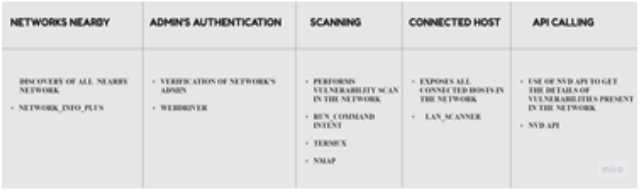

Fig 2 Stages

II. RESULT ANALYSIS

The Application contains four interfaces which is enough for providing the details of vulnerabilities present in the network. The first interface displays all the networks which are nearby the admin. After clicking the admin's respective network, shows an interface for the authentication of network's admin. After the successful login there comes an interface which shows the connected hosts in the network and button for performing vulnerability scan on the network. By pressing the button a new interface is appeared which displays the details of the vulnerabilities present in the network and solutions to resolve them.

➢ *Future Scope:*

Currently the application is working with the support of termux which is an android terminal emulator that has linux environment to run command shell scripts. In future, our app would be able to run the command shell scripts by itself andprocess more efficiently.

III. CONCLUSION

Attackers are becoming more daring in breaking into secure networks, and cyberattacks are on the rise like never before. If the scan finds vulnerabilities, it will succeed. For this reason, every organization, regardless of size, needs a vulnerability scanner, preferably one that runs continuously and automati- cally. Both Nexpose and Nessus Professional are great tools for scanning your IT infrastructure. The results show that the number of vulnerabilities detected by different technologies varies significantly. Comparing vulnerability scanners to an- tivirus programs can be informative. Both are important to security management and improve an organization's security posture. Vulnerability scanners like antivirus software don't find everything malicious. A security professional likes to use Nessus to audit IT systems. Nessus is the natural choice of the two for most organizations funding their best vulnerability scanning experience. In future research, we hope to elaborate on preventative maintenance plans and known approaches to protecting website owners. Each option has the potential to improve an organization's ability to address identified vul- nerabilities, thereby contributing to a more secure society.

REFERENCES

[1]. National Institute of Standards and Technology (September 2008). "Technical Guide to Information Security Testing and Assessment" (PDF). NIST. Retrieved 2017.
[2]. S. Samtani, S. Yu, H. Zhu, M. Patton, and H. Chen, "Iden- tifying SCADA vulnerabilities using passive and active vul- nerability assessment techniques," in Proceedings of the 14th IEEE International Conference on Intelligence and Security Informatics, ISI 2015, pp. 25–30, USA, September 2016.
[3]. M. Evans, L. A. Maglaras, Y. He, and H. Janicke, "Human behaviour as an aspect of cybersecurity assurance," Security and Communication Networks, vol. 9, no. 17, pp. 4667–4679,2016.
[4]. McClure, S., Scambray, J., and Kurtz, G. Hacking Exposed, Seventh Edition (McGraw-Hill Professional, 2012).
[5]. Harris, S. CISSP All-in-One Exam Guide, Fifth Edition (McGraw-Hill Professional, 2010).
[6]. McClure, S., Scambray, J., and Kurtz, G. Hacking Exposed, Sixth Edition (McGraw-Hill Professional, 2009).
[7]. NIST SP 800-27 Rev A, Engineering Principles for Infor- mation Technology Security. NIST SP 800-42, Guidelines on Network Security Testing.
[8]. NIST SP 800-64 Rev. A, Security Considerations in the Information System Development Life Cycle.
[9]. Wood, C. Information Security Policies Made Easy, Version 11 (Information Shield, 2009).