IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⫘ Vol. 11, Issue 2, February 2022

DOI: 10.17148/IJARCCE.2022.11206

NMAPAGUI [Network Mapper Advance Graphical User Interface]

K.S. Shimpale[1], Amey Barbate[2], Akshay Chavan[3], Aditya Nawale[4]

Prof, Department of Computer Engineering, SKN Sinhgad Institute of Technology and Science, Lonavala, India[1]

Student, Department of Computer Engineering, SKN Sinhgad Institute of Technology and Science, Lonavala, India[2,3,4]

Abstract: Network scanning is the process of discovering active hosts on the network and information about the hosts, such as operating systems, active ports, services, and applications. In addition to these basic techniques, advanced network s canners can perform other techniques such as masking the origin of the scanning, enabling timing features for stealth y scans, evading perimeter defenses such as firewalls, and providing reporting options. Nmap is used to perform the above task, but Nmap is a cmd line tool and for beginners, it is daunting to use the cmd line tool. Sometimes while te sting, organizations do not allow our toolset to perform the test. They offer their environment. So we build the GUI interface which is easy to use because of the graphical user interface and also we host this as a website so the tester can access it from anywhere .

Keywords: Network Mapper, GUI, Nmap, port scanning.

I.INTRODUCTION

Nmap was first published in September 1997, as an article in Phrack Magazine with source-code included. It is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service up time. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (N diff), and a packet generation and response analysis tool (Nping)..

II.LITERATURE SURVEY

"Penetration Testing Active Reconnaissance Phase– Optimized Port Scanning With Nmap Tool" , Mujahid Shah, Sheeraz Ahmed, Khalid Saeed, Muhammad Junaid, Hamayun Khan, Ata-ur-rehman. Reconnaissance might be the longest phase, sometimes take weeks or months. The black hat makes use of passive information gathering techniques. Once the attacker has sufficient statistics, then the attacker starts the technique of scanning perimeter and internal network devices seeking out open ports and related services. In this paper we are showing traffic accountability
and time to complete the specific task during reconnaissance phase active scanning with nmap tool and proposed strategies that how to deal with large volumes of hosts and conserve network traffic as well as time of the specific task.

There are many different tools and online resources available that allow a user to perform their own port scans or to retrieve port scan data from open sources. Nmap is an example of a tool that can be used to source scans and the University of Michigan's Zmap and John Matherly's Shodan are examples of open source data. One of the benefits of using scan data from a third party is that the researcher never directly accesses the ports and machines being scanned. There are situations in which institutions performing scanning have received threats from some of their targets as a result of their port scanning efforts. A team at the University of Arizona has combined the results of third party sources with anonymous scanning methods to collect data first-hand without leaking any university IP addresses to the targets. The biggest challenge in first hand data collection was the performance impact that Tor has on scans. By increasing scan performance through parallelization, the team was able to perform data gathering in a large scale fashion by generating focused target areas based on third party scan data and then anonymously scanning the targeted areas of interest with Nmap.

In another paper,the scanning of the target host is the first stage of an attack and the quality of the scan results almost determines whether the attack will succeed or not. The scanning will not destroy the visible assets of the attacking target but usually the purpose is to steal information and assist in the subsequent attack. Inthe scanning stage, Nmap (Network

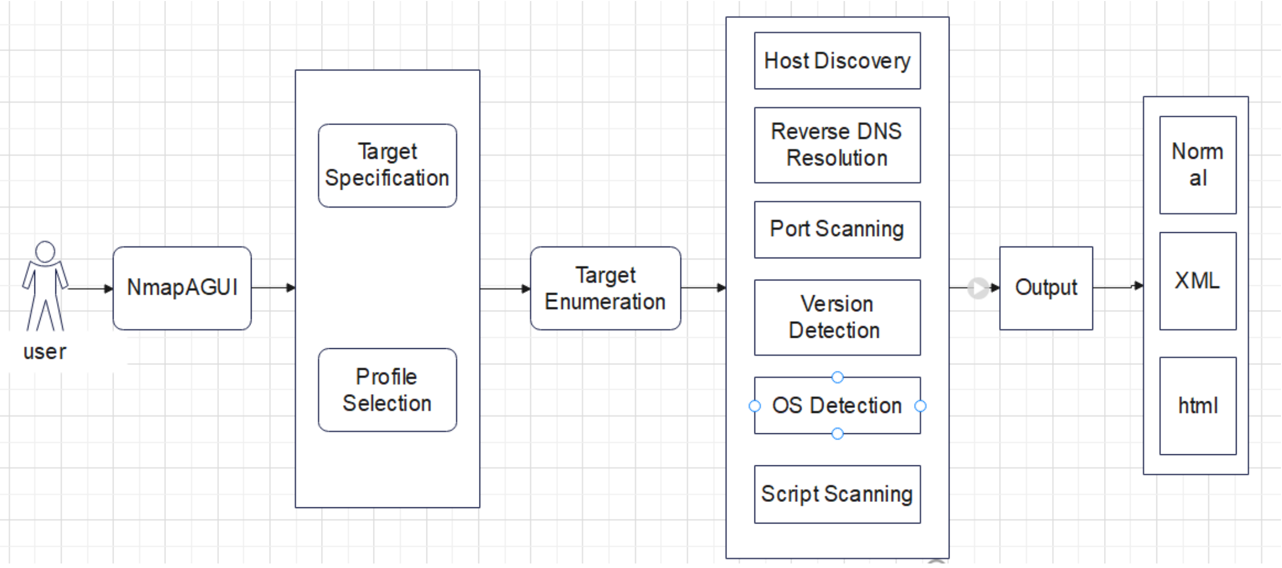
DOI: 10.17148/IJARCCE.2022.11206

Mapper) is one of the most widely used tools for scanning the states of the target host . Compared with other scan tools such as Hping or Scanner, Nmap provides more comprehensive scan types and firewall evasion methods. Traditional defense methods such as the firewall can not effectively detect the scanning flow when facing Nmap, but the Intrusion Detection System (IDS) such as Snort and Suricata will monitor security events in the network space and alert when abnormalities appear. So far, some scholars have carried out research on the usage and detection of Nmap. Among them, using Snort to detect Nmap can achieve better results. The authors in have made certain improvements to Snort's rules and achieved better detection of Nmap. But they only give the Nmap command that can be detected, no improvement comparison is made. The author mention that approximately 96% of alerts generated are asserted as false positives in Snort, while less than 1% of the total alerts are affirmed to be irrelevant positives. So Snort's rules have great potential for improvement.

III.EASE OF USE

The Nmap AGUI tool allows to extend and ease the typical usage of NMap by providing a visual and fast interface with the application. The idea behind this is to make the use of tool easy to beginners. After user run the GUI it will run on webserver locally. If user wanted he can host the tool on VPS system and access it like normal website from anywhere. Then User can perform all the task which is performed by CMD line tool using GUI. Scan output can be save as xml, html or normal format. The input of target systems, scanning and output is the main flow of the system.
Network scanning is comprised of the following four basic techniques:
- Network Mapping Sending messages to a host that will generate a response if the host is active
- Port Scanning Sending messages to a specified port to determine if it is active
- Service and Version Detection Sending specially crafted messages to active ports to generate responses that will indicate the type and version of service running
- OS Detection Sending specially crafted messages to an active host to generate certain responses that will indicate the type of operating system running on the host

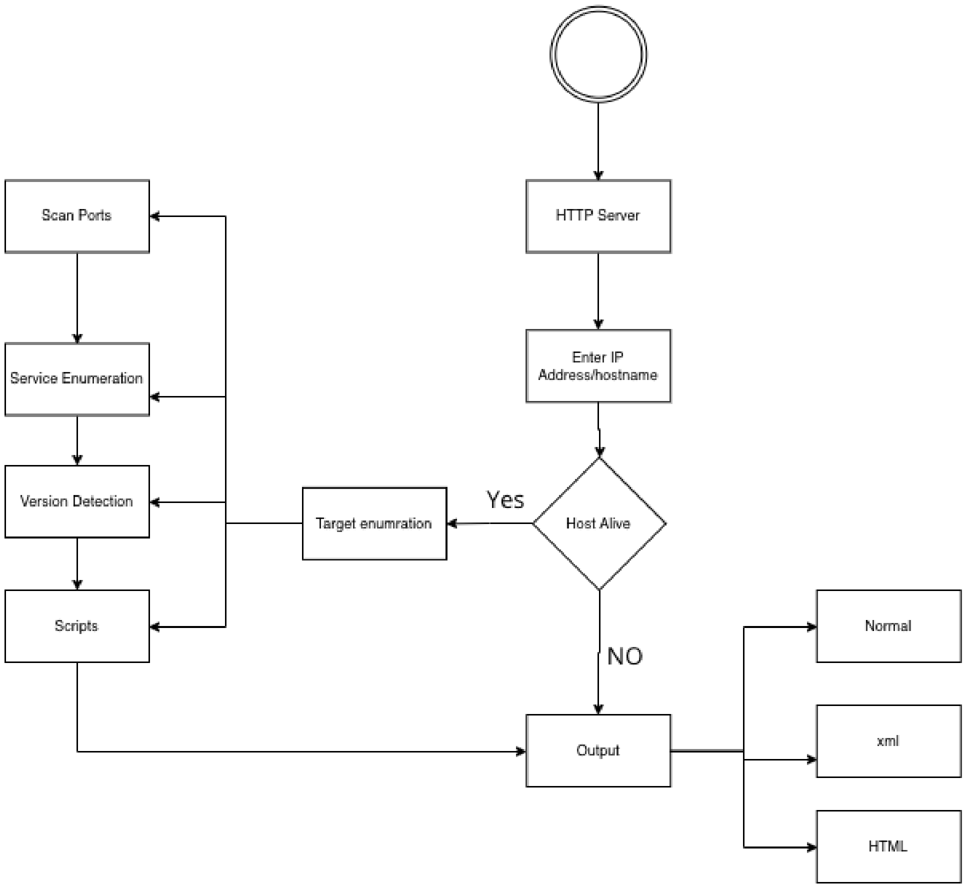
IV.SYSTEM ARCHITECTURE DIAGRAM



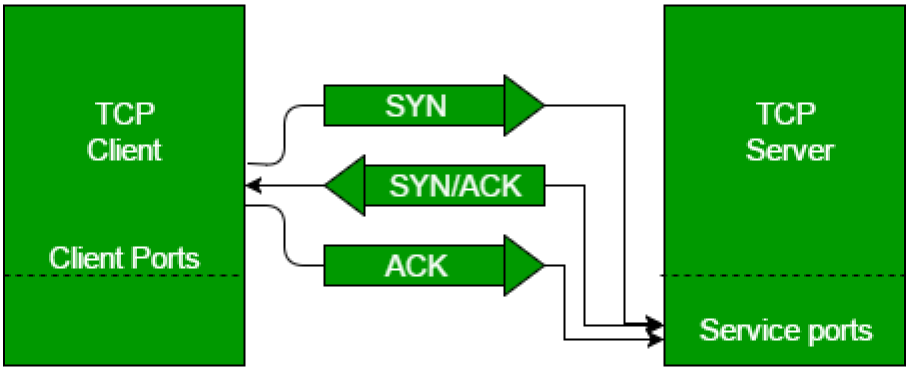
V.UNDERSTANDING THE WORKFLOW

First the user provide target to scan against. target can be IP address, website address or a whole subnet. Nmap GUI perform target enumeration such as it will check if target is live or not. After tool confirmed that target is alive it will perform next scans.

DOI: 10.17148/IJARCCE.2022.11206



If target is alive then it try to scan open port. it will scan the open port using TCP Three-way handshake. First it will send SYN packet to the target port. if port is open, port will reply with SYN-ACK packet. and lastly nmap send the ACK packet to complete handshake. But if port is not open it will not reply the SYN packet.



If port is open nmap try to figure out which service is listening on that port.This is done by sending different request s to the port, and analyzing the replies. This technique is called as fingerprinting. Nmap can perform version detection to assist in gathering more detail on the services and applications running on th e identified open ports. Version detection uses a variety of probes, located in the nmap-services-probes file, to solicit responses from the services and applications. Nmap queries the target host with the probe information and analyzes the response, comparing it against known responses for a variety of services, applications, and versions .

DOI: 10.17148/IJARCCE.2022.11206

VI.FUTURE SCOPE

Looking forward to the future developments and updates include the accuracy of the result with adding some new features that enhance the task and performance of the tool. It also includes the update the menu bar and improment of GUI so that the performance of the can be improved and taken up to the next level.

VII.CONCLUSION

We advanced in developing an NmapAGUI that perform the network mapping task. This GUI based program utilize s an nmap cmd line tool so in order to scan open ports, detect services and version. It can also set up on vpn system s o tester can access it from any machine like a normal website.Output will be saved in three format XML,HTML and normal output.

ACKNOWLEDGMENT

We would like to express our sincere gratitude towards our guide Prof. K S Shimpale for his in-valuable guidance and supervision that helped us in our research. She has always encouraged us to explore new concepts and pursue newer research problems. We credit our project contribution to her. Collectively, we would also like to thank our principal Prof. M. S. Rohokale for their time, suggestions, and for always making themselves available. We cannot thank them enough.

REFERENCES

[1]. Testing for Security Weakness of Web Applications using Ethical Hacking" R. Sri Devi,M. Mohan Kumarn 2020.

[2]. . "A Comprehensive Detection Approach of Nmap:Principles, Rules and Experiments" Si Liao, Chenming Zhou, Y onghui Zhao, Zhiyu Zhang, Chengwei Zhang, Yayu Gao and Guohui Zhong 2020.

[3]. "Penetration Testing Active Reconnaissance Phase – Optimized Port Scanning With Nmap Tool." Mujahid Shah, Sheeraz Ahmed, Khalid Saeed, Muhammad Junaid, Ata-ur-rehman, and Hamayun Khan 2019.

[4]. "Large Scale Port Scanning Through TorUsing Parallel Nmap Scans to Scan Large Portions of the IPv4 Range." Rodney R RohrmannVincet J Ercolani and Dr. Mark W Patton 2017.

[5]. "Network Vulnerability Analysis on Brain Signal/Image Databases using Nmap and Wireshark Tools" G. Bagyala kshmi1,G. Rajkumarl,N. Arunkumar1, M. Easwaran1,K. Narasimhan1,V. Elamaran1 2017