International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 12 | Dec - 2021 ISSN: 2582-3930

DOMAIN ANALYSIS SYSTEM

NEHA, ANNANYA SHIROMANI, UDIT OBERAI

B. TECH STUDENTS

Computer Science Department, Manav Rachna International Institute of Research and science, Sector-43, Suraj Kund road Faridabad, Haryana, India

ABSTRACT: This project "Domain Analysis System" works for any domain name and port number is the process that identifies the relevant objects of an application domain. The goal of Domain Analysis is software system utilize. the upper is that the level of the life-cycle object to utilize, the larger ar the advantages coming back from its utilize, the more durable is that the definition of a practicable method. This project offers intelligence part is followed by the scanning and enumeration part wherever the data collected from intelligence part is employed to look at the target or target network any for obtaining specific details like pc names, informatics addresses, open ports, user accounts, running services, OS details, system design, vulnerabilities, etc. This project collects the data from network mistreatment the tools like Whois, Geoip, DNS, shodan, data etc. These tools scan any domain given by the user and so it fetch the data of that domain provided by the user to gather the data for any vulnerability analysis. This project introduces totally different scanning and enumeration tools utilized in the scanning part of the moral hacking method very well. One might use scanning and enumeration tools and techniques involving packet analyzers, port scanners, network clerk, and vulnerability scanners throughout this part. The chapter introduces tools like, NMAP security scanner, scapy scanning, banner grabbing mistreatment ID serve. This project solely collects the data of given name and port variety and eventually scan the vulnerabilities of the given name and port variety no malicious activity done throughout the operating of this project. the data is employed to enhance the safety system of any domain and maintaining privacy whereas effecting such scanning.

KEYWORDS: Domain name System, Python, Network Mapper, Metadata, Shodan, Scapy, Banner Grabbing, Geographic location Internet protocol, , Port scanner.

INTRODUCTION: Given the ever present nature of software system and also the growing complexness of technology and interconnected systems, exaggerated by adversarial techniques like social engineering, the idea of keeping systems secure looks a foreign goal. Risk assessments ar a necessity to make sure that call manufacturers understand the vulnerabilities on their systems and also the potential impacts of Associate in Nursing adversarial event. For this reason, it's vital that network security testers have at their disposal tools and techniques that leave economical testing; as time and price ar precious resources. The network technology house is extremely dynamic; new devices ar perpetually developed and allowed on networks that access and ar accessible across the world. the net of Things (IoT), and within the military world, systems ar smart examples. whereas a number of these use and trust vetted and familiar network protocols; most tough to check ar the nuances that ar specific to the devices. As Associate in Nursing example, many times, devices use the standard Transport management Protocol/Internet Protocol (TCP/IP) network stack to handle packet fragmentation, reordering, transmission management, and OS sockets and ports. For a network security analyst ar vital for testing and uncovering vulnerabilities in these systems. Keeping these things in mind we tend to introduce domain analysis system as our project that derives protocol info from real information from real applications. we tend to use the data assortment tools like WHOIS, Shodan, data etc. additionally we tend to ar about to use vulnerability scanning tools like NMAP scan, Scapy Scan and Banner grabbing scan.

EXISTING SYSTEM: Previous studies, like those expressed below, have examined into existing domain analysis strategies. Propose many needs for a site analysis tool, concentrating on functions like traceability, consistency checking, and power integration that a tool ought to have so as to possess a uniform atmosphere. They later on get into however existing domain analysis tools fulfill these wants. Present a collection of criteria for effective product variability reduction. These views outline specific functionalities like feature model, metamodel, consistency checking, and products derivation. They additionally

propose a product repository and a multiple product read. Their needs apply to the whole domain and application engineering processes, not solely the domain study part. These needs, on the opposite hand, ar extremely solely tested on their image and not on different tools. These studies, however, need change and ar restricted to examining a pre-defined set of needs. additionally, many studies have centered on specific elements of the method, like variability modelling. These studies ar mentioned a lot of below. define and examine several existing strategies supported a collection of ideas for variability modelling and management. As a result, they known the present limits of tool support for processes, in addition as what to expect from subsequent generation of tools. outline comparison criteria for variability modelling notations and methodologies, in addition as different criteria for examining the tools. These were chosen supported the method they motor-assisted. However, the outcomes ar centered on the procedures instead of the tool support.

PROBLEMS IN EXISTING SYSTEM:

- Administrators need to put lot of efforts to identify the port.
- longer consumption.
- No risk of automatic network management.

PROBLEM DEFINITION: To develop a totally purposeful and user interactive on- line tool which may enhance and facilitate numerous hacking system users to manage and compile their work expeditiously and fruitfully.

PROJECT OVERVIEW/SPECIFICATIONS

PROPOSED SYSTEM: this could provides a clear image of the project. the method of the full software projected, to be developed, ought to be mentioned briefly. To develop a totally purposeful and user interactive on-line tool which may enhance and facilitate numerous info and analysis users system to manage and compile their users system to manage and compile their work expeditiously and fruitfully.

INFORMATION COLLECTION

DNS queries - A DNS query is a demand for information sent from a user's computer (DNS client) to a DNS server.

WHOIS queries - WHOIS is a query and response Communications protocol.

Autonomous system Internet system, but is also used for a wider range of other information. And many more information collection tools used in the project.

VULNERABILITY ANALYSIS:

1. Vulnerability analysis Nmap vulnerability scan using NSE scripts.
2. Vulnerability analysis scanning with Scapy
3. Vulnerability analysis banner grabbing

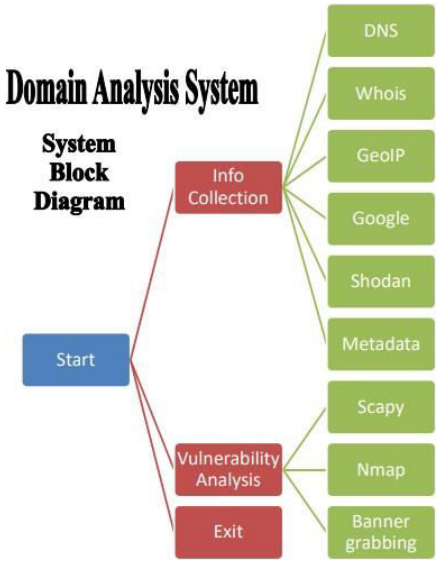

Fig.1.System Block Diagram

ADVANTAGES WITH THE PROPOSED SYSTEM:

- The user can examine the domain name and port number from any location.
- There are fewer security concerns.
- The system's security is enhanced.

SOFTWARE REQUIREMENTS

Operating system: Windows 10 or latest Language: IDLE (Python 3.9) & it's libraries

Packages: Microsoft Office 365 or Others Anti-Virus: Quick Heals Total Security or Other

HARDWARE REQUIREMENTS

Processor: Intel i3 10th Generation or Latest RAM: 8 GB or more

HDD: 1 TB or More UPS: Microtek or Other Keyboard: TVS Gold Mouse: Logitech or Other

Monitor: Dell/Samsung 20 Inch or more

SYSTEM ANALYSIS & DESIGN DATA FLOW DIAGRAM

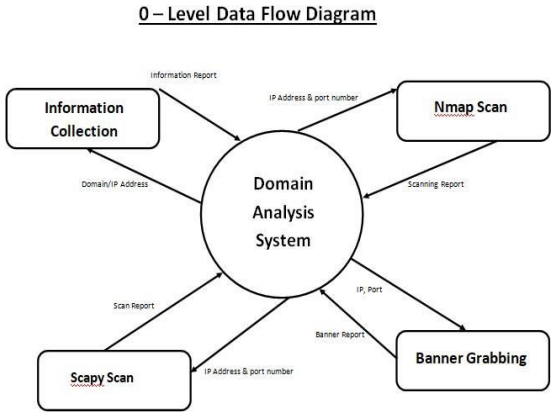

Fig.2.Data Flow Diagram

ARCHITECTURE DIAGRAM

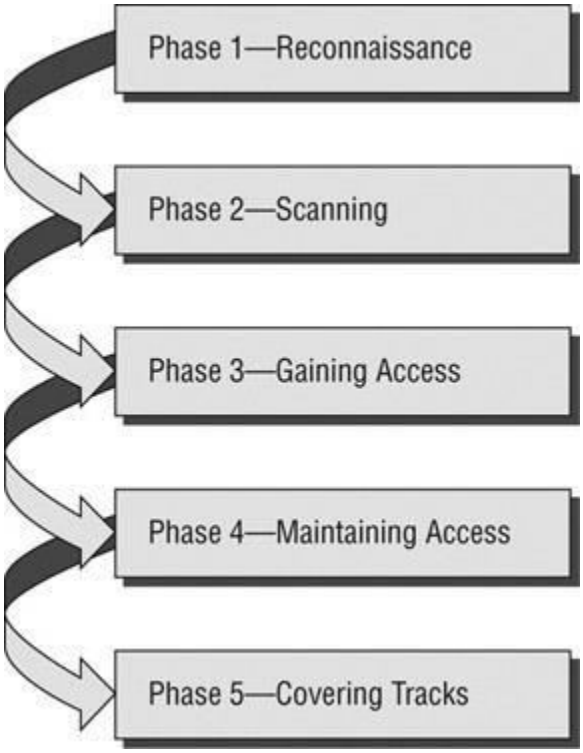

Fig.3. ARCHITECTURE DIAGRAM

ALGORITHMS AND PSEUDO CODE ALGORITHM

STEP 1: Create a new file called start.py and import the module required and choose the option.

STEP 2: Create another file "config_params.py" to define the constant path, variable and menu with color.

STEP 3: Create three utility file " file_utils.py" , "menu_utils.py" and "_int_.py" for execute the functions.

STEP 4: Create a folder "icollection" and files for information collection requirement are "dns_info.py", "geoip_info.py", "google_info.py" , "info_collection.py" , "metadata.py" , " shodan_info.py" and "whois_info.py" .

STEP 5: Create a folder "vanalysis" and files for analysis "vulnerability_analysis_menu.py" , "nmap_scan.py" , "scapy_scan.py" , "banner_grabbing_scan.py".

STEP 6: Install the additional library in command prompt are as follows:-

 Pip install scapy Pip install signal

 Pip install json Pip install shodan

 Pip install PYinstaller Pip install PYPDF2 Pip install socket

 Pip install nmap Pip install itertools Pip install PIL

STEP 7: Program execution start using “start.py”.

STEP 8: END

CONCLUSION AND FUTURE ENHANCEMENTS SUMMARY OF WORK DONE:

Domain Analysis System, information gathered from a searched domain number and port number using various domain analysis tools such as DNS, WHOIS, GOOGLE, and so on.

Following information collection, the system does vulnerability analysis using well-known vulnerability scanning techniques such as NMAP SCAN, SCAPY SCAN, and BANNER GRABBING.

Vulnerability analysis informs us about the flaws that have happened in any system, allowing us to strengthen our security and prevent hacker assaults.

SCOPE OF FUTURE ENHANCEMENT:

This project gives us the understanding to secure our system from these assaults. We learn about the vulnerabilities that occurred during analysis and how we can protect our system from attacks. The more we get into it, the clearer it becomes and the more we learn about these flaws.

In the following phase, by establishing an automated inspection through this unsecured domain, security level issues will be identified and reported.

REFERENCES

1. Scott R. Ellis, in Computer and Information Security Handbook (Third Edition), 2017
2. Jason Andress, Steve Winterfeld, in Cyber Warfare (Second Edition), 2014
3. Eric D. Knapp, Joel Thomas Langill, in Industrial Network Security (Second Edition), 2015
4. L Thévenaz, SF Mafang, J Lin - Optics express, 2013
5. R Prieto-Diaz - ACM SIGSOFT Software Engineering Notes, 1990
6. G Arango - ACM Sigsoft software engineering notes, 1989
7. DN Zmood, DG Holmes, G Bode - Conference Record of the 1999
8. W Frakes, R Prieto, C Fox - Annals of software engineering, 1998

9. YH Gu, MHJ Bollen - IEEE Transactions on Power Delivery, 2000
10. V John, Z Ye, A Kolwalkar – 2003 IEEE Power Engineering
11. Y Wei, Q Luo, A Mantooth – IET Power Electronics, 2020
12. GI Redford, RM Clegg - Journal of fluorescence, 2005
13. U Ahlstrom - Journal of safety research, 2005
14. NJ Mulder, R Apweiler - Current protocols in bioinformatics, 2003
15. V Alves, C Schwanninger, L Barbosa… - 2008
16. A Zavatta, M Bellini, PL Ramazza, F Marin, FT Arecchi - JOSA B, 2002
17. MD Rogge, CAC Leckey - Ultrasonics, 2013
18. Z Tao, P Gao, H Liu - Journal of the American Chemical Society, 2009
19. LB Lisboa, VC Garcia - Information and Vulnerability, 2010
20. N Naikar - 2013