MVJ COLLEGE OF ENGINEERING, BENGALURU- 560067

(Autonomous Institution Affiliated to VTU, Belagavi)

INTERNSHIP REPORT

on

Foot printing with NMAP

Submitted by

Nagarjun.P

In Partial fulfilment for the award of degree

of

Bachelor of Engineering

in Information Science and Engineering

2023-2024

DECLARATION

I, Nagarjun.P student of Fourth Semester B.E., Department of **Information Science and Engineering** at **MVJ College of Engineering** , Bengaluru - 560067, hereby declare that the Internship Titled “Foot printing with NMAP ” has been carried out by me and submitted in partial fulfilment for the award of the degree of Bachelor of Engineering in **information Science and Engineering** during the year 2023.

Further I declare that the content of the report has not been submitted previously by anybody for the award of any degree or diploma to any other University.

Place: Bengaluru

Date:01-January-2024

Name Signature

Nagarjun.P 1MJ21IS064

ACKNOWLEDGEMENT

I am grateful to “Plasmid Innovation” for their wholehearted support, suggestion and invaluable advice throughout the Internship and also for the help in the preparation of this report.

The videos and PowerPoint presentations provided with the course were very helpful in completing the report and will be useful for future opportunities as well.

I thank all the technical and non-technical staff of PLASMID INNOVATION for their help.

ABSTRACT

In the domain of cybersecurity, Footprinting stands as a crucial first step in understanding and fortifying network defenses. This abstract focuses on the topic of Footprinting with an aim to leverage NMAP, a premier open-source Network Mapper tool. NMAP's versatility and robust feature set makes it an indispensable asset for cybersecurity professionals engaged in network scrutiny.

The abstract begins by emphasizing the significance of Footprinting as the initial phase of ethical hacking, where information gathering becomes paramount. NMAP emerges as beacon in this process, providing a comprehensive suite of scanning techniques to find out essential details about a target network or system. From discovering live hosts and identifying open ports to extracting information about service versions, NMAP reveals the intricate layers of a network's architecture.

The ability of NMAP to do host discovery utilising multiple approaches such as ICMP, TCP, and UDP probing is highlighted. The tool's capability in mapping out network topology and describing the relationships between hosts becomes evident, offering security professionals a holistic view of their digital terrain.

The abstract accentuates NMAP's role in service detection, showcasing how the tool meticulously probes open ports to identify the specific services running on each. Coupled with version detection capabilities, NMAP empowers cybersecurity experts to assess potential vulnerabilities, enabling proactive measures to strengthen the overall security posture.

In conclusion , this abstract serves as a guide to the complex field of Footprinting with NMAP, providing insights into its methodologies, applications, and ethical imperatives. As an indispensable tool for cybersecurity professionals, NMAP's ability in network reconnaissance lays the foundation for robust and strong digital defenses.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1. INTRODUCTION

Footprinting, in the context of cybersecurity, is the initial step in gathering information about a target network, system, or organization. It involves discovering essential details such as IP addresses, network topology, services running, and potential vulnerabilities. The primary goal of footprinting is to assess the security posture of the target and identify potential weaknesses.

The Footprinting ordinarily accumulates network related da-ta, for example, Network ID, space name alongside inside area name, access control instruments, IP address, conventions, VPNs, consents, client and gathering data, directing tables, framework flags, public statements and news stories, distant framework types, web waiter joins and so on.

Assuming the aggressor assembles the touchy data, they might involve the information for extortion, making the phony profiles, and so on. The assailant by get-together more comparable kind of data connected with target interests and exercises, the aggressor can join a few other web-based entertainment and gatherings which further leads further Footprinting.

Footprinting is crucial for several reasons: Identifying potential security weaknesses, Formulating an attack strategy , Reducing the risk of unexpected surprises during penetration testing , Providing valuable insights into the target's network architecture.

Nmap, short for Network Mapper, is a powerful open-source tool used for network discovery and security auditing. Originally developed by Gordon Lyon, also known as Fyodor Vaskevich, Nmap is designed to explore and map networks, identify hosts, discover open ports, and gather information about the services running on those ports.

One of Nmap's key strengths lies in its versatility and flexibility. It can be employed for various purposes, ranging from simple network inventory to more advanced security assessments. Nmap operates by sending packets to target hosts and analyzing the responses to determine the network's topology and identify potential vulnerabilities.

The tool provides a wide array of scanning techniques, including TCP connect scans, SYN scans, UDP scans, and more. Additionally, it supports scripting with Nmap Scripting Engine (NSE), allowing users to create custom scripts to automate tasks or enhance the capabilities of Nmap.

Nmap's popularity stems from its effectiveness in both offensive and defensive security scenarios. Security professionals use it to identify and address vulnerabilities, while malicious actors might use it for reconnaissance before launching an attack. As with any powerful tool, it's crucial to use Nmap responsibly and within legal and ethical boundaries.

By footprinting with NMAP, security professionals can assess the potential vulnerabilities of a network, helping organizations strengthen their defenses against potential cyber threats. It's a crucial step in the reconnaissance phase of ethical hacking and penetration testing, allowing security experts to gather valuable insights before diving deeper into assessing and securing a network.

Traceroute is one of the techniques which is used to track the packet information that is moving between different IP addresses. It provides the packet information such as response time to a ping, IP address, and host name. The above two techniques Nmap and traceroute are most widely used tools inorder to gather the network information. In order to protect the data the user need to monitor some countermeasures while using Footprinting.

This report focuses on the use of NMAP (Network Mapper), a popular open-source network scanning tool, for effective footprinting. NMAP's versatility and extensive feature set make it an indispensable tool for ethical hackers and security professionals.The study on the technique of footprinting is conducted and the cloudflare server is utilized for the case study. The ethical hacking tool NMAP available with kali Linux is utilized to perform the task of the footprinting.

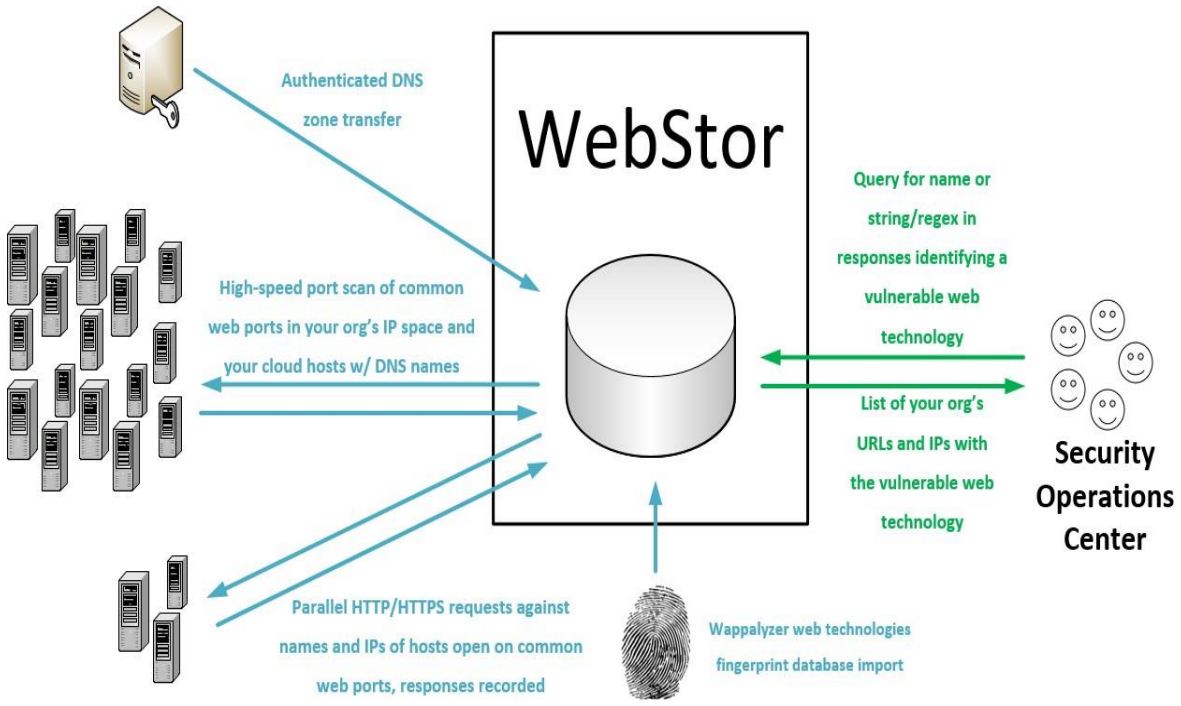
Authenticated DNS
zone transfer
WebStor
Query for name or
string/regex in
responses identifying a
vulnerable web
technology
High-speed port scan of common
web ports in your org's IP space and
your cloud hosts w/ DNS names
List of your org's
URLs and IPs with
the vulnerable web
technology
Security
Operations
Center
Parallel HTTP/HTTPS requests against
names and IPs of hosts open on common
web ports, responses recorded
Wappalyzer web technologies
fingerprint database import

Fig:1.1

2. OBJECTIVES

1. **Network Discovery:**

Identify and document all active hosts on the network.

Map out the network topology, including routers, switches, and interconnected devices.

2. **Port Enumeration:**

Determine open ports on target systems.

Understand the services running on these ports to assess potential vulnerabilities.

3. **Service Version Identification:**

Gather information on the specific versions of services and applications running on open ports.

Use this data to assess the security posture and potential weaknesses associated with outdated software.

4. **Operating System Detection:**

Determine the operating systems of target devices.

This information aids in crafting targeted exploits and understanding the overall security landscape.

5. **Vulnerability Assessment**:

Identify potential vulnerabilities associated with the discovered services and software versions.

Prioritize vulnerabilities based on severity and potential impact.

6. **Security Policy Compliance:**

Assess the network against established security policies and compliance standards.

Identify any deviations from security best practices and policy guidelines.

7. **Risk Analysis**:

Conduct a risk analysis based on the collected information.

Evaluate the potential impact of identified vulnerabilities on the confidentiality, integrity, and availability of the network.

8. **Documentation and Reporting:**

Create detailed documentation of the footprinting process, including methodologies, tools used, and findings.

Generate a comprehensive report highlighting the discovered information and providing actionable recommendations for improving network security.

CHAPTER 2

METHODOLOGY

3. METHODOLOGY

1. **Define Objectives:**

Clearly outline the goals of your NMAP footprinting. Are you focusing on discovering all devices in the network, identifying open ports, or gathering information about the operating systems and services? Defining clear objectives helps in maintaining focus.

2. **Target Selection:**

Specify the target network or range of IP addresses you'll be examining. Ensure you have proper authorization before initiating any scanning activities.

3. **Initial Reconnaissance:**

Start with basic information gathering, like domain names, IP addresses, and network ranges associated with the target. Tools like nslookup or whois can assist in this phase.

4. **Network Discovery (Ping Scanning):**

Use NMAP for basic host discovery to identify live hosts in the target network. Employ techniques like ICMP ping, TCP SYN/ACK, or ARP requests to determine active devices.

5. **Port Scanning:**

Perform port scanning to identify open ports on the live hosts. Utilize various scanning techniques like TCP connect, SYN, and UDP scans to uncover potential entry points.

6. **Service Version Detection:**

Once open ports are identified, use NMAP to determine the versions of services running on those ports. This information is crucial for understanding potential vulnerabilities associated with specific software versions.

7. **Operating System Detection:**

Leverage NMAP's OS detection capabilities to identify the operating systems of the target devices. This information helps in tailoring further exploitation strategies.

8. **Scripting Engine (NSE) Usage:**

Explore NMAP's scripting engine (NSE) to run additional scripts for more in-depth information. Custom or community-contributed scripts can provide valuable insights into specific services or vulnerabilities.

9. **Data Analysis:**

Collect and analyze the results obtained from NMAP scans. Identify patterns, anomalies, or potential security risks based on the discovered information.

10. **Documentation and Reporting:**

Document your findings systematically. Include details about live hosts, open ports, identified services, and operating systems. Provide recommendations for improving security based on your observations.

CHAPTER 3

RESULTS AND DISCUSSIONS

4. RESULTS

1. **Open Ports Identification:**

NMAP has successfully identified the open ports on the target systems. These open ports provide entry points into the network and can be crucial for understanding the services and applications running on those ports.

2. **Operating System Detection:**

The OS detection feature of NMAP has been employed to determine the operating systems running on the target devices. This information is invaluable for understanding the network environment and tailoring further assessments.

3. **Service Version Identification:**

NMAP has provided detailed information about the versions of services running on the open ports. This granularity is essential for pinpointing potential vulnerabilities associated with specific software versions.

5. DISCUSSION

1. **Security Implications:**

The identified open ports serve as potential avenues for attackers. By knowing which ports are open, security measures can be implemented to secure these entry points and mitigate the risk of unauthorized access.

2. **Vulnerability Assessment:**

The detailed service version information allows for a more precise vulnerability assessment. It helps in identifying known vulnerabilities associated with specific software versions, enabling proactive patching and security measures.

3. **Network Architecture Understanding:**

The results provide a comprehensive view of the network architecture, showcasing how devices are connected and what services they are running. This understanding is fundamental for crafting an effective security strategy.

4. **Risk Mitigation Recommendations:**

Based on the findings, recommendations for mitigating potential risks can be outlined. This could include patching vulnerable software, tightening firewall rules, or reconfiguring services to minimize exposure.

5. **Future Security Measures:**

The insights gained from the NMAP footprinting can inform future security measures. This could involve the implementation of intrusion detection systems, regular security audits, or additional layers of authentication to bolster the network's overall security posture.

CHAPTER 4

CONCLUSION

6. CONCLUSION

In conclusion, NMAP footprinting serves as an invaluable asset in the realm of network security. Through its multifaceted capabilities, it enables a thorough understanding of a target network's architecture, devices, and services. The information gathered during thefootprinting process lays the foundation for effective vulnerability assessment and aids incrafting robust security strategies.

By leveraging NMAP's port scanning, OS detection, and service version identification features, security professionals can pinpoint potential weak points in a network's defenses. This proactive approach allows organizations to fortify their security measures,mitigating risks and safeguarding against potential cyber threats.

In the ever-evolving landscape of cybersecurity, where the adversary's tactics become increasingly sophisticated, NMAP footprinting emerges as a crucial ally. Its role in the reconnaissance phase of ethical hacking and penetration testing cannot be overstated, asit empowers security experts to make informed decisions, prioritize vulnerabilities, and ultimately bolster the overall resilience of a network.

In essence, NMAP footprinting transcends mere information gathering; it becomes a strategic cornerstone for building robust cybersecurity frameworks. As organizations strive to stay one step ahead of potential threats, NMAP stands as a reliable companion,providing the insights needed to navigate the complex terrain of network security with confidence and precision.