Experiment No. 7

Title: Conducting recon with fingerprinting tools

Batch: A2 **Roll No.: 16010421073** **ExperimentNo.:7**

Aim: Conducting recon with fingerprinting tools.

Resources needed: OWASP Fingerprinting Guide, Nmap, Wappalyzer, WhatWeb, HTTPrecon, FingerprintJS, SecurityTube, Stack Exchange - Information Security, Hack The Box (HTB), OverTheWire

---

Pre Lab/ Prior Concepts:

Students should have prior knowledge of understanding Fingerprinting, Types of Fingerprinting, OS Fingerprinting, Application Fingerprinting, Passive Fingerprinting Techniques, Active Fingerprinting Techniques, Tool Selection Criteria, Information Gathering Basics, and Networking Fundamentals.

Theory:

Conducting reconnaissance with fingerprinting tools is a strategic and intricate process in cybersecurity, focusing on identifying and cataloging specific attributes of systems and applications. Fingerprinting tools are crucial in revealing the digital signatures of technology stacks, operating systems, and software versions in a target environment. This descriptive theory explores the key aspects and methodologies of conducting reconnaissance with fingerprinting tools.

Understanding Fingerprinting: Fingerprinting collects and analyzes unique characteristics or fingerprints associated with systems, networks, or applications. In cybersecurity, fingerprinting tools serve as virtual detectives, unveiling the distinct attributes that define the target's digital landscape.

Types of Fingerprinting:

1. **OS Fingerprinting:** OS fingerprinting involves identifying the operating system running on a target system. Tools like Nmap leverage various techniques, such as analyzing network responses, to deduce the underlying OS.
2. **Application Fingerprinting:** Application fingerprinting focuses on identifying specificsoftware and versions on a target system. This includes web servers, content management systems, and other applications—tools like Wappalyzer excel in this domain.
3. **Passive and Active Fingerprinting:** Passive fingerprinting involves collecting information without directly interacting with the target, often by analyzing network traffic patterns. Active fingerprinting, on the other hand, requires intentional interaction with the target to elicit responses and gather data.

Methodologies in Fingerprinting:

1. **Passive Fingerprinting Techniques:** Techniques like analyzing packet timing, size, and sequence numbers in network traffic allow for the passive identification of systems. This method minimizes direct interaction, reducing the risk of detection.
2. **Active Fingerprinting Techniques:** Active techniques involve sending deliberate requests to the target and analyzing responses. This may include sending specific packets or queries to identify open ports, services, and software versions.
3. **Browser Fingerprinting:** In web application reconnaissance, tools like FingerprintJS are used for browser fingerprinting. This involves collecting information about a user's browser and device characteristics to create a unique fingerprint.

Procedure:

Conducting reconnaissance with fingerprinting tools involves systematically gathering and analyzing digital signatures to identify target systems, networks, and applications. The following step-by-step procedure outlines the process for conducting reconnaissance using fingerprinting tools:

Step 1: Define Scope and Objectives: Clearly define the scope and objectives of the reconnaissance. Determine the specific information to be gathered, such as identifying operating systems, software versions, or web applications. Align the scope with the goals of the overall security assessment.
Step 2: Identify Target: Identify the target system, network, or application for reconnaissance. Understanding the target is crucial for tailoring fingerprinting techniques and selecting appropriate tools.
Step 3: Choose Fingerprinting Tools: Select relevant fingerprinting tools based on the type of information sought and the nature of the target. Common tools include:

Nmap: For OS fingerprinting and service version detection.
Wappalyzer: For web application fingerprinting.
FingerprintJS: For browser fingerprinting.

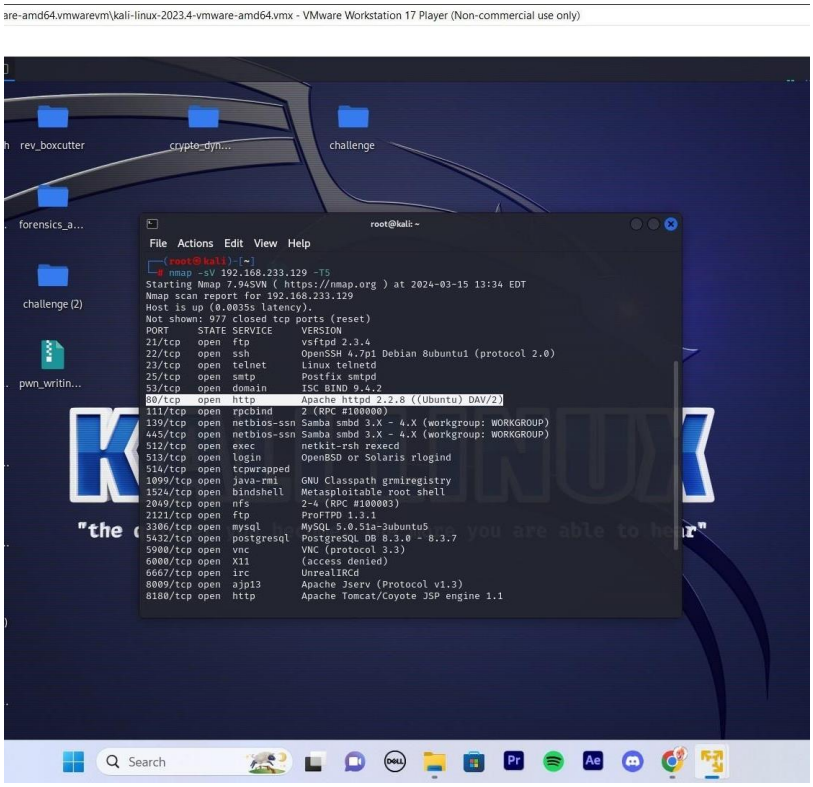
Step 4: Craft Fingerprinting Queries: Craft specific queries or tasks for each selected tool. Customize queries to gather information relevant to the defined objectives. For example, Nmap includes flags for OS fingerprinting and version detection.
Step 5: Execute Fingerprinting Tools: Execute the chosen fingerprinting tools and queries against the target. Monitor and analyze the tool's output for information related to operating systems, applications, and versions. Be mindful of the potential impact on the target and adjust aggressiveness accordingly.
Step 6: Analyze Results: Analyze the results obtained from the fingerprinting tools. Identify patterns, anomalies, and significant information related to the target's technology stack. Correlate data points to comprehensively understand the target's digital footprint.
Step 7: Validate Information: Validate the accuracy of the identified fingerprints by cross-referencing with multiple tools and techniques. Confirm the consistency of results to ensure the reliability of the gathered information.

Output (Code with result Snapshot)

Step 1: Define Scope and Objectives: We will run the fingerprinting tools to run processes on metasploitable.
Step 2: Identify Target: Our target is metasploitable which is running on the same VMWare

Step 3: Choose Fingerprinting Tools: We use Nmap in our application to do fingerprinting on the metasploitablenmap

Step 4: Craft Fingerprinting Queries: -sV 192.168.233.129 -O -T5



Step 5: Execute Fingerprinting Tools: So as per our nmap scan we got the names of open ports present on our metasploitable machine. As Highlighted, port 80 which represents HTTP port can be seen open. So, we searchon our browser about the IP address of the machine and we got this,

Step 6: Analyze Results: Other than port 80, we also can see various of open ports available on this machine which can be easily exploited like ftp, ssh etc and the version of these ports are also mentioned in the nmap scan.

Post Lab Questions: -

1. **Evaluate the effectiveness of the fingerprinting tools used in the reconnaissance. Which tools provided the most valuable insights, and how did they contribute to achieving the defined objectives?**

Ans:

Nmap's comprehensive scanning techniques, accuracy, and speed make it a cornerstone tool for networkreconnaissance.
Its scripting engine enhances functionality, while visualization options aid in data interpretation, contributing to effective assessment of target environments.
Communitysupport and integration capabilities further bolster its utility in diverse cybersecurity contexts.

2. **Assess the potential impact of the fingerprinting activities on the target. Were there any signs of disruption or unintended consequences? How did you mitigate any risks associated with the reconnaissance?**

Ans:

The potential impact of fingerprinting activities on the target can vary depending on factors such as the target'ssecurity posture, network stability, and the techniques employed. While fingerprinting itself is generally non- invasive, extensive scanning or aggressive probing may trigger intrusion detection systems, leading to alert generation or even network slowdowns.
Unintended consequences could include service disruptions, particularly if vulnerable systems are identified but not adequately protected.

To mitigate risks associated with reconnaissance, it's essential to employ techniques that prioritize stealthand minimize disruption. This includes using Nmap's stealth scanning options like SYN scan (-sS) or ACK scan (-sA) to avoid leaving tracesin target logs.
Additionally, scheduling scans during off-peak hours reduces the likelihood of impacting network performance.Utilizing techniques like port knocking or decoy scanning can further obfuscate the origin and intent of reconnaissance activities, reducing the risk of detection and retaliation by the target's security measures.
Regular communication with stakeholders and adherence to rules of engagement also help ensure responsible and ethical conduct during reconnaissance operations.

Outcomes: CO2 Comprehend purpose of Anonymity and Foot printing

Conclusion: (Conclusion to be based on the objectives and outcomes achieved)
We use various fingerprinting tools that allow us to conduct attack on metasploitable

Signature of faculty in charge with date

References:

1. https://securitytrails.com/blog/cybersecurity-fingerprinting
2. https://null-byte.wonderhowto.com/how-to/fingerprint-web-apps-servers-for-better-recon-more - successful-hacks-0302807/
3. https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server