**Using NMAP to Exploit the FTP service On Metasploitable2: A Case Study**

As a network security enthusiast, one of my primary responsibilities is identifying vulnerabilities in network infrastructure before malicious actors exploit them.**NMAP** is aopen-source tool for network discovery and security auditing. NMAP allows to perform tasks such as identifying live hosts, open ports, services, and even potential vulnerabilities on a network. Its versatility makes it a go-to solution for penetration testers, system administrators, and network engineers.

**Metasploitable 2** is a deliberately vulnerable virtual machine (VM) designed for testing, learning, and practicing penetration testing and security assessments. Created by Rapid7, the company behind the Metasploit Framework, it provides a safe environment for users to explore and experiment with various cybersecurity tools and techniques without affecting real-world systems.

**Introduction**

In the realm of network security, gaining hands-on experience is invaluable. One of the best ways to learn is by practicing in controlled environments like Metasploitable 2, a deliberately vulnerable virtual machine. In this case study, I demonstrate how I used **NMAP (Network Mapper)** to identify and exploit an insecure FTP service running on Metasploitable 2. The objective was to simulate a real-world penetration testing scenario and practice responsible vulnerability management.

**Scenario Overview**

**Environment:**

* Target Machine: Metasploitable 2 (IP Address: 192.168.220.128)
* Attacker Machine: Kali Linux (IP Address: 172.17.122.42)

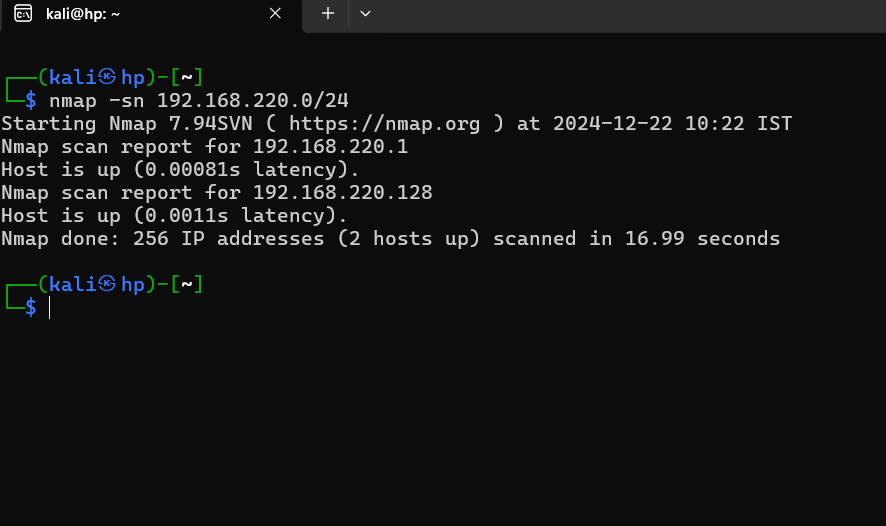
**Objective:**

* Discover and analyze the FTP service running on Metasploitable 2.
* Exploit vulnerabilities to gain unauthorized access to the system.
* Knowing the services and versions running.

**Step 1: Initial Reconnaissance**

Before diving into detailed scans, I identified the live host (Metasploitable 2) on the network.

**Command:** nmap -sn 192.168.220.0/24

****

**Explanation:**

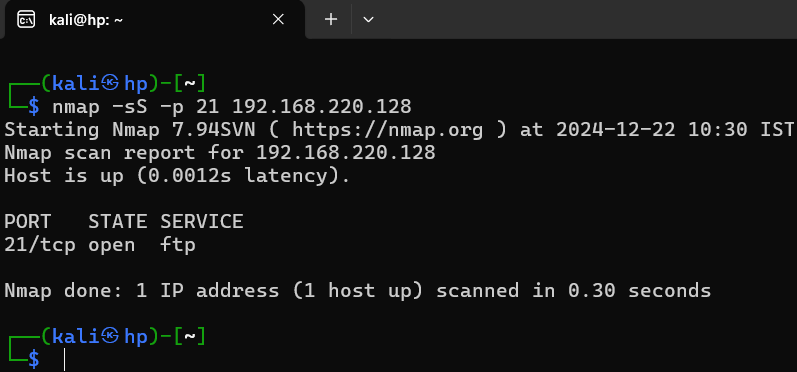
* **-sn**: Performs a ping scan to check for live hosts without port scanning.
* **192.168.220.0/24**: The subnet where Metasploitable 2 resides.

**Result:** NMAP identified a live host at **192.168.220.128**. This confirmed the target machine was active and ready for scanning.

**Step 2: Port Scanning**

Next, I scanned the target for open ports to understand the attack surface.

**Command:** nmap -sS -p 21 192.168.220.128



**Explanation:**

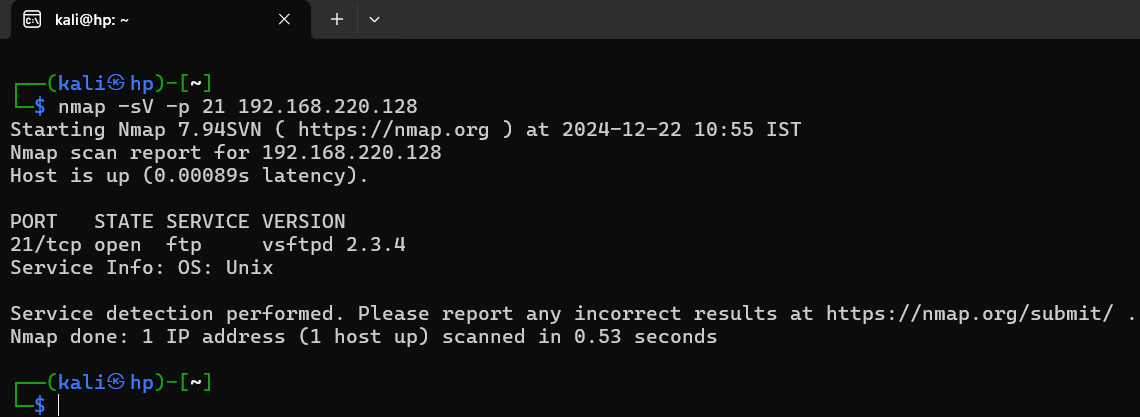
* -sS: Conducts a stealth SYN scan.
* -p 21: Focuses the scan on port 21 (commonly used for FTP).

**Result:** The scan revealed that port 21 was open.

**Step 3: Service and Version Detection**

To know the running service and version, I conducted a detailed scan.

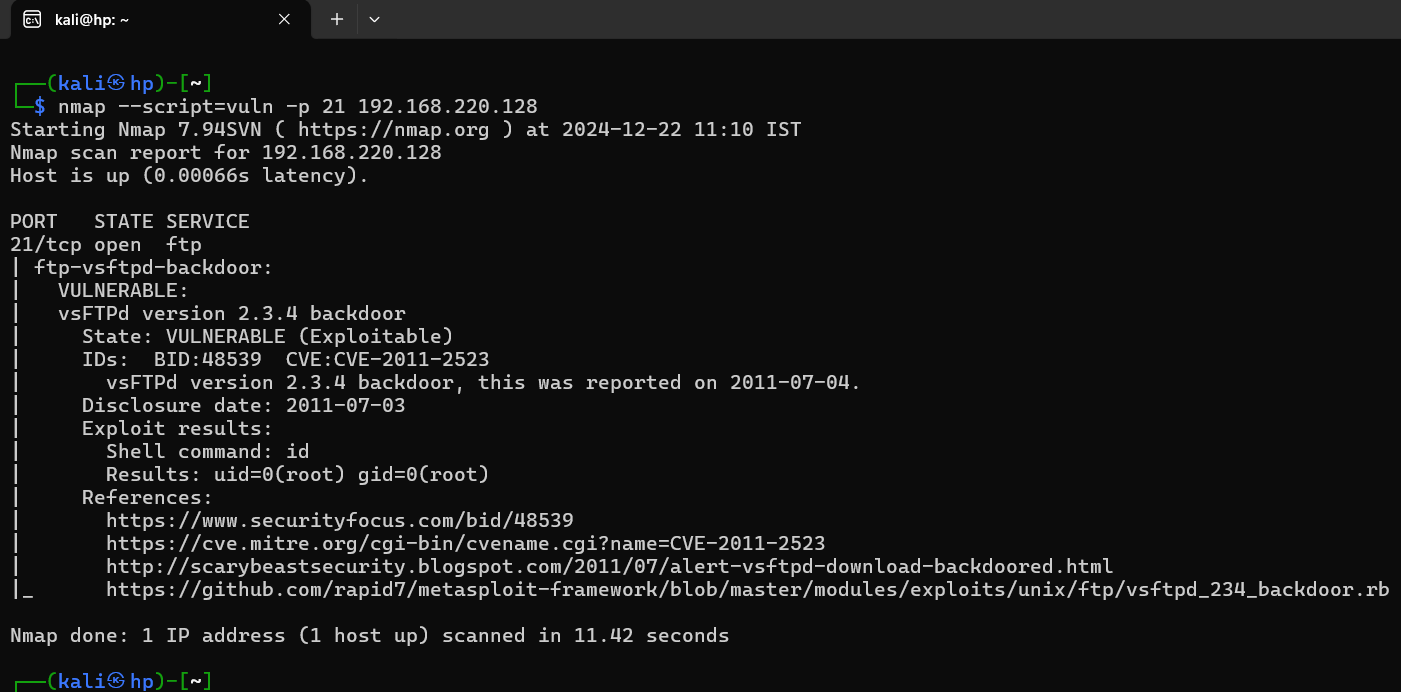
**Command:** nmap -sV -p 21 192.168.220.128



**Explanation:**

* -sV: Enables service and version detection.

**Result:** The scan confirmed that the target was running **vsftpd 2.3.4**, a vulnerable FTP service.

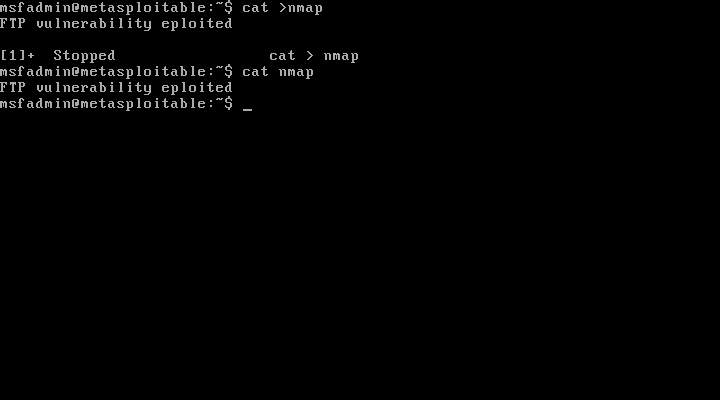


**Step 4: Exploiting the Vulnerability**

**Create a file in Metasploitable 2 using cat command**

**Command:** cat > nmap(in metasploitable 2)

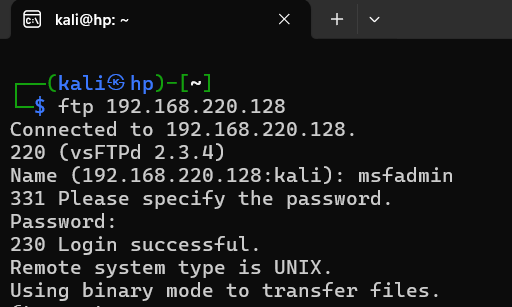
FTP vulnerability exploited

****

Exploit the FTP vulnerability of the target system using kali

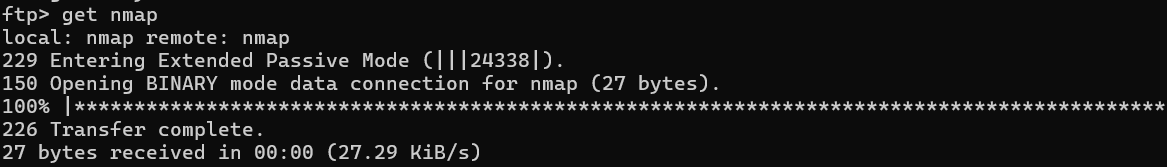
Command: ftp 192.168.220.128(in kali)

This command will give you the ftp access of the target machcine

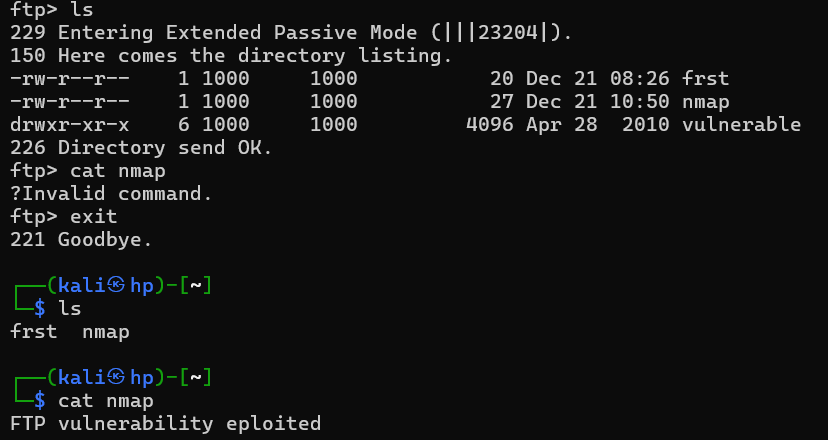


Getting the nmap text file which I created on the target machine using the following command.

ftp>get nmap(in kali)



Use the ls command to access the file in kali



Successfully exploited the vulnerability of FTP service on metasploiatble2.