# Vulnerability Report on Metasploitable2 Machine

## Overview:

In this assessment, two critical vulnerabilities were identified in the virtual machine. The vulnerabilities were discovered using network scanning and exploitation techniques targeting specific open ports. Below are the details of each vulnerability, along with the steps followed to identify and exploit them.

---

## 1. Vulnerability on Port 21 (FTP - vsFTPd 2.3.4):

- **Discovery Process:** Initially, I scanned the network using the **Kali Linux tool nmap** to identify the machine's IP address. Afterward, I conducted a detailed scan using nmap -A to reveal the open ports, services, and their versions. This scan revealed that port 21 was open and running the **FTP service vsFTPd version 2.3.4**.
- **Exploit:** I then used **msfconsole** to search for known vulnerabilities related to this version of vsFTPd. A well-documented vulnerability in **vsFTPd 2.3.4** allowed me to run an exploit, which successfully opened a reverse shell and provided **root** access to the machine.
- **Impact:** Exploiting this vulnerability provided full administrative privileges, giving an attacker the ability to control the system entirely, access sensitive files, and execute commands as root.
- **Recommendation:** Immediate action should be taken to either update vsFTPd to a more secure version or disable the FTP service entirely if not in use. Additionally, consider limiting access to port 21 and enforcing stronger authentication.

---

## 2. Vulnerability on Port 139 (SMB - Samba):

- **Discovery Process:** The nmap -A scan also identified port 139 as open, running the **Samba** service, which is used for file sharing across networks. Using **msfconsole**, I searched for exploits targeting the specific version of Samba running on the machine.
- **Exploit:** I found an exploit designed to target the identified version of Samba. Running the exploit successfully provided a reverse shell, allowing me to log in as **root**.

- **Impact:** Similar to the first vulnerability, this exploit gave an attacker full root-level access to the system. With this access, the attacker can control the system, steal or manipulate data, and potentially pivot to other systems on the network.
- **Recommendation:** To mitigate this vulnerability, the Samba service should be updated to a secure version. Restricting access to port 139 and ensuring proper authentication for file-sharing services is crucial.

---

## Conclusion:

The vulnerabilities discovered on port 21 (vsFTPd) and port 139 (Samba) are serious security risks, both of which provide attackers with root access to the virtual machine. Immediate remediation steps include updating or disabling the vulnerable services and implementing stronger security measures.