Vulnerability Report on Metasploitable1 Machine

Overview:

This report highlights two critical vulnerabilities discovered during a penetration test of a virtual machine. Using network scanning tools and exploitation frameworks, I was able to gain unauthorized access to the system via open services, including FTP and Samba. The following steps were taken to identify and exploit the vulnerabilities:

---

1. Vulnerability on Port 21 (FTP - ProFTPD 1.3.1):

- **Discovery Process:** Initially, I conducted a network scan using **nmap** to identify the machine's IP address. I then ran **nmap -A** to scan for open ports and services, discovering that port 21 was running **ProFTPD 1.3.1**, an FTP service.
- **Exploit:** Using **msfconsole**, I searched for exploits targeting **ProFTPD 1.3.1**. After identifying an available exploit, I executed it, which successfully provided me with the FTP login credentials. I then used the **ftp <IP>** command and entered the credentials to log in to the FTP server.
- **Impact:** This vulnerability allowed unauthorized access to the FTP service, potentially enabling an attacker to upload, modify, or delete files. It presents a significant risk as attackers could leverage this access to upload malicious software or escalate their privileges within the system.
- **Recommendation:** It is recommended to update **ProFTPD** to a newer, secure version. Additionally, secure the FTP service with strong, non-default credentials, or consider disabling FTP if it is not essential.

---

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

- **Discovery Process:** The **nmap -A** scan also revealed that port 139 was open, running **Samba**, a service used for file and printer sharing. I used **msfconsole** to search for an exploit for the Samba version in use.
- **Exploit:** I found an exploit for this version of Samba and executed it. The exploit provided me with a reverse shell, allowing me to gain **root** access to the machine.
- **Impact:** Gaining root access through the Samba service represents a critical vulnerability. With full administrative control, an attacker can execute commands,

steal sensitive information, and potentially launch attacks on other connected systems.

- **Recommendation:** Update Samba to the latest secure version, restrict access to port 139, and implement stronger network security measures to prevent unauthorized access. Additionally, configure the firewall to block unnecessary connections to this port.

Conclusion:

The two vulnerabilities identified in this report, FTP on port 21 and Samba on port 139, present significant risks to the virtual machine. Both services allowed unauthorized access, with one leading to root privileges. Immediate action should be taken to patch the vulnerabilities, strengthen authentication methods, and limit access to these services to prevent exploitation in the future.