Vulnerability Report on Kioptrix Machine

Overview:

This report details two critical vulnerabilities discovered during a security assessment of a virtual machine. By leveraging network scanning and exploitation tools, I was able to gain unauthorized access through two services running on the machine: Apache HTTP on port 80 and Samba on port 139. Below is a step-by-step account of how the vulnerabilities were identified and exploited.

---

1. Vulnerability on Port 80 (HTTP - Apache HTTPD 2.2.8):

- **Discovery Process:** I began by scanning the network using **nmap** to identify the virtual machine's IP address. Following that, I executed **nmap -A** to determine the open ports, services, and their versions. The scan revealed that port 80 was open and running **Apache HTTPD 2.2.8**, an older version of the popular web server.
- **Exploit:** Using the **searchsploit** tool, I searched for known exploits targeting **Apache HTTPD 2.2.8**. I discovered a known vulnerability, ran the exploit, and successfully obtained a shell on the machine, gaining access to one of the user accounts.
- **Impact:** Exploiting this vulnerability allowed unauthorized access to the web server, which could potentially lead to further escalation of privileges or manipulation of web application data. This access compromises the confidentiality, integrity, and availability of the server.
- **Recommendation:** Immediate action should be taken to update Apache HTTPD to the latest secure version. It is also recommended to review the web server configuration for security misconfigurations and restrict public access where not necessary.

---

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

- **Discovery Process:** During the **nmap -A** scan, I also found that port 139 was open and running **Samba**, a service often used for file sharing. I used the **msfconsole** tool to search for an exploit targeting the specific version of Samba in use.

- **Exploit:** I found an exploit for this version of **Samba** and executed it. The exploit provided me with a reverse shell, granting **root** access to the virtual machine.
- **Impact:** Gaining **root** access through Samba is a severe vulnerability, as it allows complete control over the machine. With administrative privileges, an attacker can access sensitive data, install malicious software, or cause significant damage to the system.
- **Recommendation:** Update **Samba** to the latest secure version and restrict access to port 139 by implementing proper firewall rules. Additionally, ensure that strong authentication mechanisms are in place and limit access to trusted sources only.

Conclusion:

Both vulnerabilities discovered in this assessment, the Apache HTTPD 2.2.8 on port 80 and Samba on port 139, pose significant security risks. The Apache vulnerability led to unauthorized user access, while the Samba vulnerability resulted in root privileges. Immediate patching and strengthening of network security measures are essential to protect the system from potential exploitation.