**Metasploitable Penetration Testing Report: vsftpd 2.3.4 Exploitation**

**Exercise Objective**

I conducted a penetration test against a Metasploitable machine, specifically targeting the vulnerable vsftpd 2.3.4 service. The exercise was performed using **Metasploit Framework** on **Kali Linux**.

**Procedure**

**1.Service Scanning & Vulnerability Identification**

* **Initial Network Scan**
  + Confirmed target availability with:

nmap -sP 192.168.1.149

* + Identified open ports/services using:

nmap -sV 192.168.1.149

*(Revealed vsftpd 2.3.4 running on port 21)*

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

**2.Metasploit Exploitation**

* Launched Metasploit:

msfconsole

Immagine che contiene testo, schermata, Software multimediale, Software per la grafica

Descrizione generata automaticamente

* Searched for and selected the known exploit:

use exploit/unix/ftp/vsftpd\_234\_backdoor

* Configured parameters (RHOSTS: 192.168.1.149) and executed the exploit.
* Result: Gained root shell access on the target machine.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

**2.  Post-Exploitation Actions**

* **Folder Creation**
  + Created a directory /test\_metasploit to verify write access:

mkdir /test\_metasploit

* + Verified creation:

ls /

Immagine che contiene testo, schermata, software, Software multimediale

Descrizione generata automaticamente

* System Reconnaissance
  + Extracted user list (potential attack vectors):

cat /etc/passwd

* + Identified active services/listening ports:

netstat -tuln

Immagine che contiene testo, schermata, menu, Carattere

Descrizione generata automaticamente

Immagine che contiene testo, schermata, menu, design

Descrizione generata automaticamente

**Results**

* **Successful Exploitation**:
  + Achieved **root-level access** via the vsftpd 2.3.4 backdoor vulnerability.
* **System Analysis**:
  + Confirmed insecure configurations (e.g., unnecessary services running).
  + Discovered multiple user accounts (/etc/passwd) and open ports (netstat).

**Security Implications**

* **Critical Risk**: The vsftpd 2.3.4 backdoor allows unauthenticated root access.
* **Remediation**:
  + Immediately patch or replace vsftpd.
  + Restrict FTP service to trusted networks.
  + Disable unused services.

**Conclusion**

This exercise demonstrated how **outdated software** can lead to **full system compromise**. The ease of exploitation underscores the importance of:

* Regular vulnerability scanning.
* Prompt patch management.
* Principle of least privilege.