🛡 Network Penetration Testing with Realistic Exploits and Mitigation Techniques

This project demonstrates practical network attack and defense scenarios using Kali Linux as the attacker and Metasploitable 2 as the victim system. It covers stages like scanning, information gathering, exploiting vulnerabilities, cracking passwords, and applying security fixes — all done within a secure lab setting for ethical cybersecurity training.

🎯 Goals

Learn how real-world network breaches occur

Use tools like Nmap and Metasploit for reconnaissance and exploitation

Break Linux password hashes via John the Ripper

Spot outdated and weak services and provide appropriate security solutions

---

💻 Lab Configuration

🖥️ Operating Systems

Kali Linux – Used as the attacker's platform

Metasploitable 2 – Set as the vulnerable machine

🛠️ Tools Employed

nmap – For port scanning, OS and service version detection

Metasploit – To exploit discovered vulnerabilities

John the Ripper – For password hash decryption

Linux CLI tools – For user and system inspection

🚀 Activities Performed

🔍 Network Reconnaissance

nmap -v IP – Standard scan

nmap -v -p- IP – Full range port check

nmap -sV IP – To find software versions

nmap -O IP – Identifying the OS

🔐 Uncommon Ports Detected

Found ports such as 6697, 3632, and 44553 using exhaustive scanning

---

📡 Information Gathering

Operating System Identified: Linux 2.6.x

Active services: vsftpd, SSH, Apache, MySQL, Samba, etc.

At-risk ports: 21 (FTP), 445 (SMB), 512–514 (Remote services)

💥 Attacks Launched

Used known backdoor in vsftpd 2.3.4

Exploited Samba vulnerability via Metasploit

Leveraged flaws in Rexec, Rlogin, and Rsh for unauthorized access

---

👤 Privilege Escalation

Created user "shwetank" with superuser rights

Retrieved password hashes and cracked them using John the Ripper

---

🔧 Mitigation Recommendations

Service	Risk	Solution
vsftpd	Backdoor vulnerability (CVE-2011-2523)	Update to version 3.0.5 or switch to SFTP
SMB	Remote Code Execution & Null Sessions	Upgrade to Samba version 4.20.1
R Services	Sends passwords in plain text (CVE-1999-0651)	Disable and replace with SSH

📚 Key Takeaways

This exercise taught me user and privilege management in Linux, working with system logs, cracking hashed passwords, and recognizing vulnerable services using tools like Nmap and John. I gained practical knowledge on how legacy services such as FTP, SMB, and R services can be security threats and learned how to mitigate them with modern alternatives.

⚠ Ethical Notice

All testing was conducted strictly in a controlled, isolated environment for educational reasons only. Do not attempt these activities on live systems or networks without legal authorization.

📎 Resources

CVE-2011-2523

Metasploit Documentation

John the Ripper Manual

Apache Security Advisories

https://youtu.be/x9cEaiApTWg?si=3Di5d5dVgXqxluT0