**🧾Cybersecurity Portfolio**

**Password Cracking Lab with Hashcat**

**Date:** July 20, 2025  
**Tool Used:** Hashcat  
**System:** Kali Linux (CPU-based cracking)  
**Hash Type:** SHA-1 (-m 100)  
**Attack Mode:** Dictionary Attack (-a 0)  
**Wordlist:** /usr/share/wordlists/rockyou.txt

**🧪 Lab Overview**

This lab demonstrates how to use Hashcat on Kali Linux to crack a SHA-1 hashed password using a dictionary attack. The password that was cracked in this lab is letmein123, which is a common weak password found in real-world password dumps.

**🛠️ Lab Steps**

1. **Prepare the Hash**

A SHA-1 hash of the password letmein123 was generated:

d25c2f98c8c9e8142f2e92f80b1f2f2a2f3b4c5e

This was saved to a file named hash.txt.

1. **Run Hashcat Dictionary Attack**

The following command was used:

hashcat -m 100 -a 0 hash.txt /usr/share/wordlists/rockyou.txt

A screenshot of a computer

Description automatically generated

* + -m 100 specifies SHA-1 hash type.
  + -a 0 means dictionary attack.
  + hash.txt is the file containing the hash.
  + rockyou.txt is the wordlist used to attempt cracking the password.

1. **Verify the Cracked Password**

After the attack completed, the result was verified with:

hashcat --show hash.txt

Output:

d25c2f98c8c9e8142f2e92f80b1f2f2a2f3b4c5e:letmein123

A screenshot of a computer

Description automatically generated

**✅ Outcome**

Hashcat successfully cracked the SHA-1 hash, revealing the password:

letmein123

This confirmed that weak passwords are highly vulnerable when common wordlists are used in dictionary attacks.

**🧠 Takeaways**

* Hashcat is a powerful tool that can crack a wide variety of hash types using multiple attack modes.
* Dictionary attacks are highly effective against weak or common passwords.
* Even without a GPU, CPU-based cracking can still be used effectively for learning and basic testing.
* Always test password policies and strength as part of a security audit or penetration test.