**Cyber Security – Assessment # 7**

**Part 1: Conceptual**

**Q1.** – Briefly explain different techniques for system hacking like password cracking, vulnerability exploitation and using payload.

**Q2**. – Summarize important differences between John the Ripper, Hydra and Hash cat password cracking techniques.

**Part 2: Lab**

**Q3.** John the Ripper (JtR) is a powerful password-cracking tool that supports multiple modes for different attack strategies. Single Crack Mode uses known user information to intelligently generate password guesses, making it effective in targeted scenarios. Wordlist Mode relies on a predefined list of potential passwords, testing each against the hashed password. Incremental Mode performs a brute-force attack by systematically trying all possible character combinations, ensuring comprehensive coverage. For advanced customization, External Mode allows users to define their own cracking algorithms or rules. Additionally, if enabled, Markov Mode prioritizes guesses based on statistical probabilities of character sequences, improving efficiency for common patterns. Perform following tasks:-

1. **John the Ripper ( Single Crack Mode )**

* Designate a short string (topgun) as a username and variations on its capitalization as the password (such as Topgun).
* Show the output of the SHA-256-hashed password:

echo -n 'Topgun' | sha256sum

* Create a new text file (simple.txt) to store the username and the password hash value from prior steps:

echo -n 'topgun:4558ce5abe3b1e70bbadc3b95f2ff84f54d0a5c30fb524ceebfd401f8233fda7' > simple.txt

* Run simple.txt through John the Ripper’s Single Crack Mode (change the --format argument as you see fit):

john --single --format=raw-sha256 simple.txt

* Get results.

1. **John the Ripper (Wordlist Mode)**

* Pipe a hash based on one or more dictionary words (optionally with numbers) to SHA-256:

echo -n 'password1234' | sha256sum

* Write your username, a colon (:), and the hash as a single long string into a new text file (crack.txt):

echo user01:b9c950640e1b3740e98acb93e669c65766f6670dd1609ba91ff41052ba48c6f3>>crack.txt

* Repeat Steps 1 and 2 to generate as many username-password pairs as desired and append them to crack.txt.
* Run crack.txt through John the Ripper’s Wordlist Mode:

john --wordlist=rockyou --format=raw-sha256 crack.txt

* Get results.

1. **John the Ripper (Incremental Mode)**

* Pipe a hash on a simple alphanumeric password to SHA-256:

echo -n 'passw0rd' | sha256sum

* Write your username, a colon (:), and the hash as a single long string into a new text file (inc.txt):

echo user02:8f0e2f76e22b43e2855189877e7dc1e1e7d98c226c95db247cd1d547928334a9>>inc.txt

* Run inc.txt through John the Ripper’s Wordlist Mode:

john --incremental --format=raw-sha256 inc.txt

* Get results.

**Answer Part 1**

**Techniques for System Hacking:**

1. **Password Cracking**:

* This technique involves decoding or recovering passwords to gain unauthorized access to a system.
* Common methods include brute force (trying every combination), dictionary attacks (using precompiled wordlists), and rainbow tables (precomputed hash values).
* Tools: John the Ripper, Hydra, Hashcat, etc.

1. **Vulnerability Exploitation**:

* This involves identifying and exploiting weaknesses or flaws in software or systems (e.g., outdated software, unpatched systems).
* Attackers use tools and scripts to exploit these vulnerabilities and gain control of the target system.
* Tools: Metasploit Framework, OpenVAS, Nessus.

1. **Payloads**:

* A payload is a piece of malicious code delivered to a system to perform specific actions like creating a backdoor or escalating privileges.
* Payloads can be delivered using exploits, social engineering, or malicious files.
* Tools: Metasploit (e.g., Meterpreter payloads), custom payload generators Like Crunch, CeWl etc.

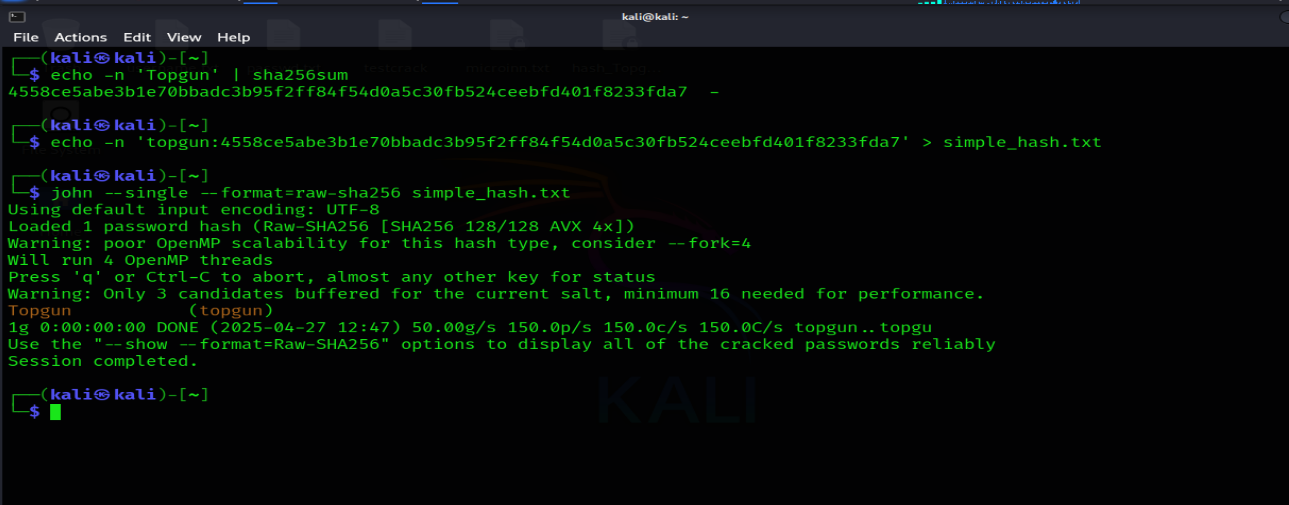
**Differences between John the Ripper, Hydra, and Hashcat**

|  |  |  |
| --- | --- | --- |
| **Tool** | **Purpose** | **Cracking Technique** |
| **John the Ripper** | Password cracking for multiple formats. | Brute force, dictionary attacks, and rule-based attacks. |
| **Hydra** | Brute-forcing login credentials on services. | Focuses on network protocols like SSH, FTP, etc. |
| **Hashcat** | Advanced hash cracking tool. | Utilizes GPUs for brute force, dictionary, and hybrid attacks. |

**Answer Part 2**

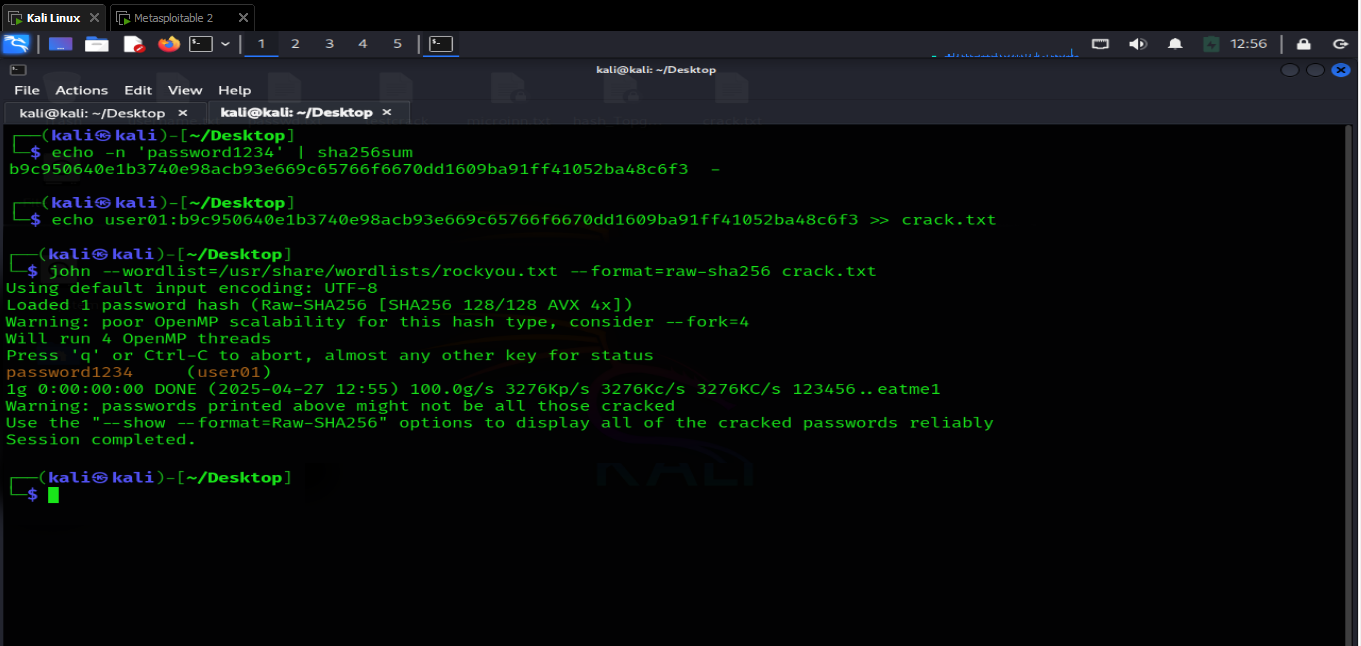
1. **Single Crack Mode**

* Purpose: Uses known user information to intelligently guess passwords.
* Steps:
  1. Create a username (topgun) and a password (Topgun).
  2. Generate the SHA-256 hash of the password:
     + **Command:** echo -n 'Topgun' | sha256sum
  3. Store the username and hash in a file (simple.txt):
     + echo 'topgun:4558ce5abe3b1e70bbadc3b95f2ff84f54d0a5c30fb524ceebfd401f8233fda7' > simple.txt
  4. Run John the Ripper in Single Crack Mode:
     + john --single --format=raw-sha256 simple.txt



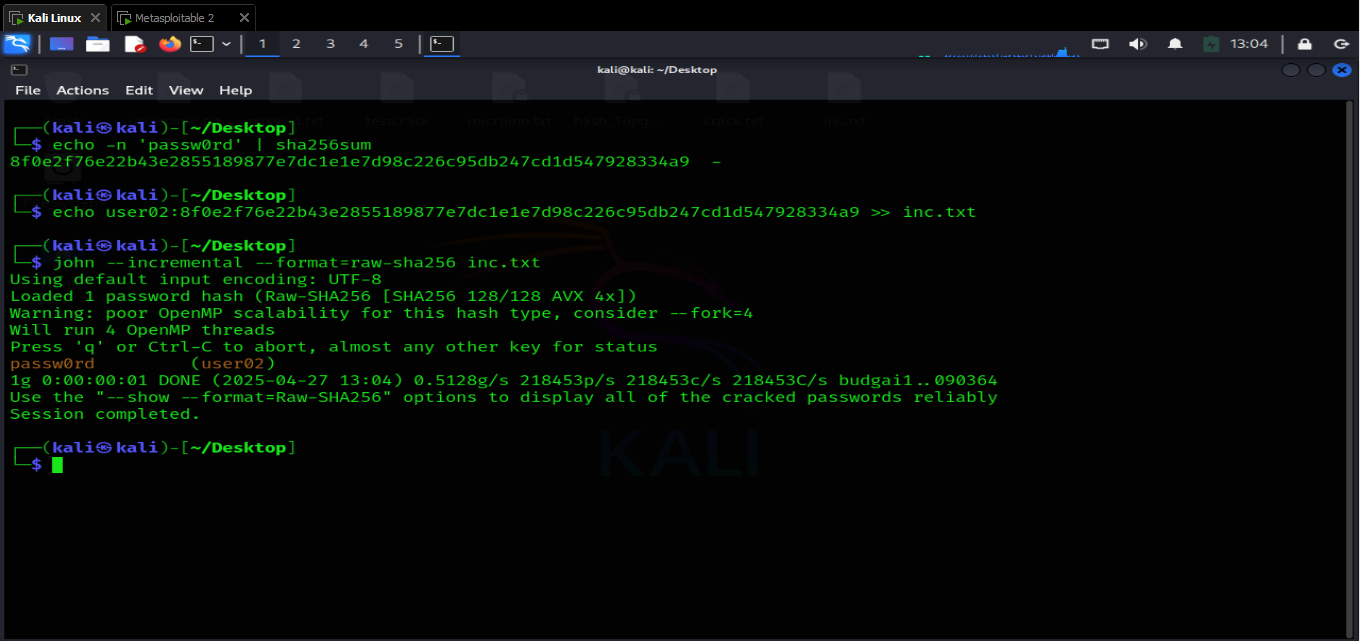
1. **Wordlist Mode**

* **Purpose**: Tests predefined passwords from a wordlist.
* **Steps**:
  1. Generate a hash for a dictionary-based password (password1234):
     + echo -n 'password1234' | sha256sum
  2. Write the username and hash into a file (crack.txt):
     + echo user01:b9c950640e1b3740e98acb93e669c65766f6670dd1609ba91ff41052ba48c6f3 >> crack.txt
  3. Repeat to add more username-password pairs.
  4. Run John the Ripper with the rockyou wordlist:
     + john --wordlist=/usr/share/wordlist/rockyou.txt (first Unzip) --format=raw-sha256 crack.txt



1. **Incremental Mode**

* **Purpose**: Performs brute-force attacks by systematically trying all character combinations.
* **Steps**:
  1. Generate a hash for a simple alphanumeric password (password):
     + echo -n 'passw0rd' | sha256sum
  2. Write the username and hash into a file (inc.txt):
     + echo user02:8f0e2f76e22b43e2855189877e7dc1e1e7d98c226c95db247cd1d547928334a9 >> inc.txt
  3. Run John the Ripper in Incremental Mode:
     + john --incremental --format=raw-sha256 inc.txt



Each mode demonstrates a unique approach to password cracking, showcasing the versatility of John the Ripper.