Professional Manual: Medusa Tool in Kali Linux

Medusa is a fast, parallel, and modular login brute-forcing tool available in Kali Linux. It is commonly used by penetration testers and security researchers to perform dictionary-based and brute-force attacks on various services like SSH, FTP, HTTP, SMB, RDP, and more. Medusa is designed for speed and supports parallel threads, making it effective for testing large sets of credentials quickly.

# 1. Purpose of the Tool

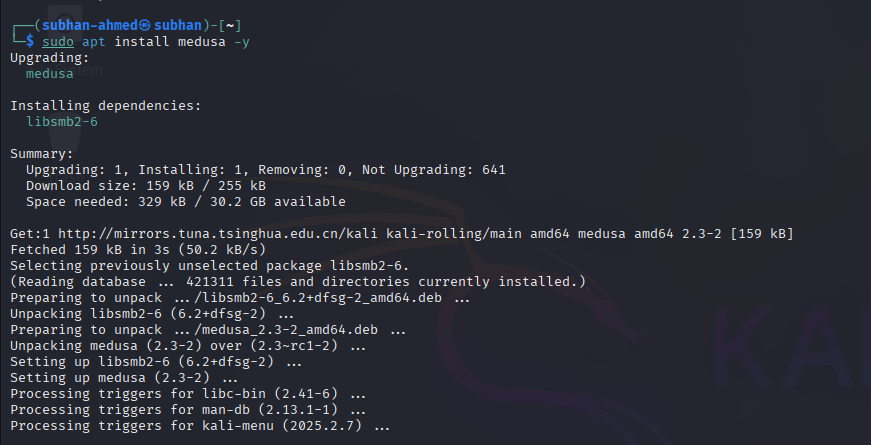
• Medusa is primarily used to test authentication services by performing brute-force or dictionary attacks.  
• It helps penetration testers identify weak or default credentials.  
• Supports multiple protocols including SSH, FTP, HTTP, MySQL, SMB, RDP, VNC, and others.  
• Modular design allows adding new protocols easily.

# 2. Installation in Kali Linux

Medusa comes pre-installed in Kali Linux. If it is not available, it can be installed with the following commands:

sudo apt install medusa -y # Install Medusa

medusa -h # Verify installation



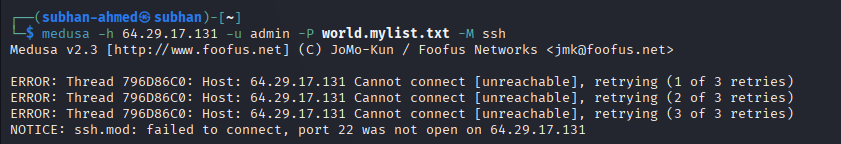
# 3. Usage in Kali Linux

The general syntax of Medusa is:

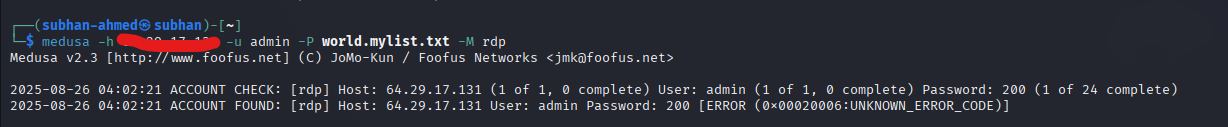
medusa -h <target> -u <username> -P <password\_file> -M <module>

Examples:

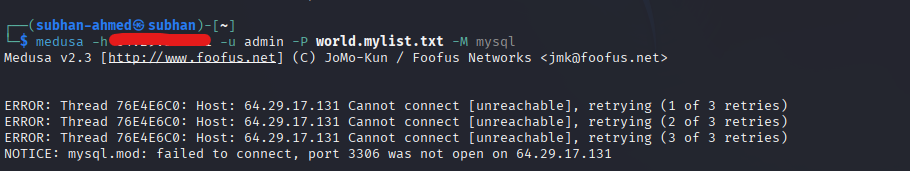
medusa -h 192.168.1.10 -u admin -P /usr/share/wordlists/rockyou.txt -M ssh # Brute force SSH login



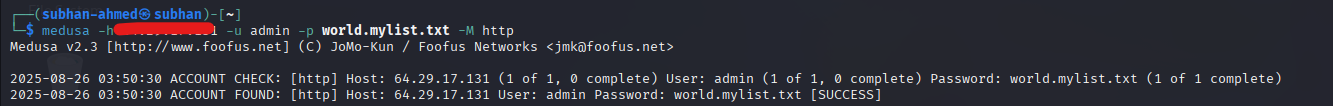
medusa -h 192.168.1.10 -u administrator -P passwords.txt -M rdp # Brute force RDP login



medusa -h 192.168.1.10 -u root -P passlist.txt -M mysql # Brute force MySQL login



medusa -h 192.168.1.10 -P list.txt -M http

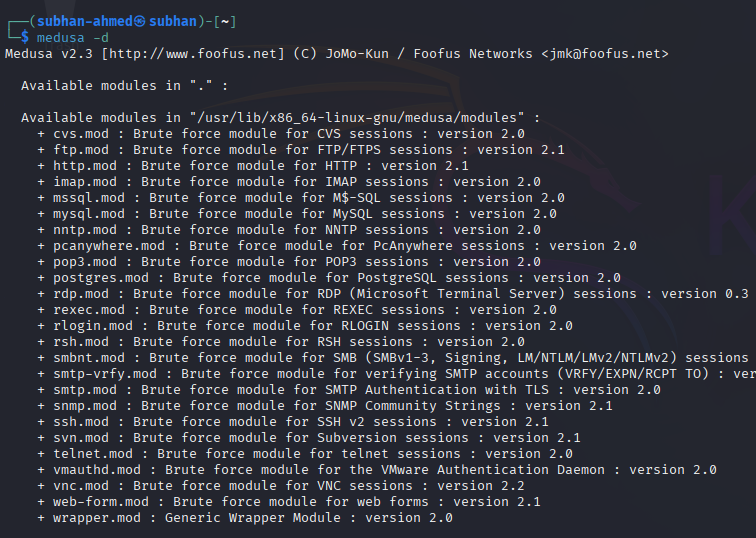


# 4. Workflow Example

1. Identify the target service and IP address (e.g., SSH on 192.168.1.10).  
2. Select a username or a file containing usernames.  
3. Choose a password list (e.g., rockyou.txt).  
4. Run Medusa with the appropriate module:  
 medusa -h 192.168.1.10 -u admin -P /usr/share/wordlists/rockyou.txt -M ssh  
  
5. Medusa will attempt to login using all combinations and display valid credentials.

# 5. Practical Commands Overview

medusa -d # Debug mode for detailed output



medusa -q 5 # Stop after 5 successful logins

# 6. Conclusion

Medusa is a powerful and versatile brute-force tool in Kali Linux. With support for a wide range of protocols and its high-speed parallel execution, it is an essential tool for penetration testers performing password auditing and security assessments. However, it should only be used in legal and authorized testing environments.