

- Filename: eccouncil-ceh31250-v10-6-1-2-password_attacks_pt2.md
- Show Name: CEHv10 (312-50)
- Topic Name: Attacks and Exploits
- Episode Name: Password Attacks Pt.2
- Description: In this episode, Daniel and Zach get into some system hacking by exploring ways to attack password-based authentication. Here they will demonstrate online password attacks using tools such as Medusa and Hydra. They also show you how to grab passwords that are passing through the network, utilizing packet sniffing tools like Wireshark.

=====

Password Attacks Pt.2

- **So now that we are aware of the different types of password attacks, can you demonstrate a password attack in action?**
 - Differentiate Online vs Offline attacks
 - Online attacks network service authentication
 - Offline attacks stolen password hashes
 - Online cracking tools
 - Medusa
 - Network remote access audit tool
 - Dump all medusa modules: `medusa -d`
 - Bruteforce SSH: `medusa -h 10.0.0.165 -u msfadmin -P passwords.txt -M ssh`
 - Hydra
 - Network remote access audit tool
 - Bruteforce FTP: `hydra -L users.txt -P passwords.txt 10.0.0.165 ftp`
 - Captured
 - Use Wireshark to view telnet creds