■■■■ CTF Mega Cheat Sheet (100+ Commands)

Recon & Enumeration (20 commands)

```
nmap -sC -sV -p- target.com
nmap -A target.com
nmap --top-ports 100 target.com
gobuster dir -u http://target.com -w wordlist.txt
dirb http://target.com /usr/share/wordlists/dirb/common.txt
feroxbuster -u http://target.com -w wordlist.txt
sublist3r -d target.com
amass enum -d target.com
dnsenum target.com
whois target.com
dig target.com ANY
dig axfr target.com @ns1.target.com
theHarvester -d target.com -l 500 -b google
wafw00f http://target.com
whatweb http://target.com
nikto -h http://target.com
wpscan --url http://target.com
curl -I http://target.com
wget -r http://target.com
```

Password Cracking & Hashes (15 commands)

```
john --wordlist=rockyou.txt hash.txt
john --format=raw-md5 hash.txt
hashcat -m 0 -a 0 hash.txt rockyou.txt
hashcat -m 100 hash.txt rockyou.txt
hashid hash.txt
md5sum file.txt
sha1sum file.txt
strings binary | grep password
fcrackzip -u -D -p rockyou.txt file.zip
zip2john file.zip > hash.txt
rar2john file.rar > hash.txt
gpg2john file.gpg > hash.txt
hydra -l admin -P rockyou.txt ftp://target.com
hydra -L users.txt -P pass.txt ssh://target.com
cewl http://target.com -w custom.txt
```

Steganography (10 commands)

```
steghide extract -sf image.jpg
steghide info image.jpg
exiftool secret.jpg
binwalk -e secret.png
zsteg secret.png
foremost -i secret.jpg -o output
strings secret.wav | less
xxd secret.png | head
outguess -r secret.jpg output.txt
pngcheck -v secret.png
```

Forensics (10 commands)

```
binwalk -e file.png
foremost -i file.raw -o output
volatility -f memdump.raw imageinfo
volatility -f memdump.raw pslist
volatility -f memdump.raw filescan
wireshark capture.pcap
tshark -r capture.pcap
tcpdump -r capture.pcap
```

```
grep 'flag' file.txt
xxd -p file.bin | tr -d '\n'
```

Cryptography (10 commands)

```
echo "c2VjcmV0" | base64 -d
echo "secret" | base64
echo "uryyb" | tr 'A-Za-z' 'N-ZA-Mn-za-m'
openssl enc -aes-256-cbc -d -in file.enc -out file.txt
openssl rsa -in private.pem -pubout
openssl dgst -sha256 file.txt
gpg --decrypt secret.gpg
python3 -c "print(2**128)"
xxd -p file.bin | tr -d '\n' | xxd -r -p
hashcat -m 1800 hash.txt rockyou.txt
```

Exploitation (15 commands)

```
sqlmap -u "http://target.com/page.php?id=1" --dbs
sqlmap -u "http://target.com/page.php?id=1" --dump
nc -lvnp 4444
nc target.com 1337
rlwrap nc -lvnp 4444
python3 -c 'import pty;pty.spawn("/bin/bash")'
socat TCP-L:4444 FILE:`tty`,raw,echo=0
msfconsole
searchsploit wordpress 5.0
searchsploit apache
metasploit-framework
exploit-db
hydra -l admin -P pass.txt ssh://target.com
ssh user@target.com
scp file.txt user@target.com:/tmp
```

Reverse Engineering (10 commands)

```
file binary
strings binary | less
ltrace ./binary
strace ./binary
gdb ./binary
objdump -d binary | less
radare2 binary
ghidra binary
checksec --file=binary
ldd binary
```

Miscellaneous (10 commands)

```
echo "... --- ..." | morse -d
zbarimg qr.png
xxd file.bin | head
base32 -d encoded.txt
uudecode file.txt
xxd -r -p hex.txt > out.bin
curl ifconfig.me
tar -xvf file.tar
7z x archive.7z
file unknown.bin
```