# CEH Module 12 - IDS, Firewall, and Honeypot Evasion Tools & Commands Cheat Sheet

## Nmap

Use: Port scanning, firewall rule detection, packet fragmentation for evasion

Basic Commands:

* nmap -f <target> # Fragment packets
* nmap -Pn <target> # Disable host discovery
* nmap --source-port <port> <target> # Send traffic from specific port
* nmap -D RND:10 <target> # Decoy scanning

## Hping3

Use: Custom packet crafting, firewall testing, IDS evasion

Basic Commands:

* hping3 -S <target> -p <port> # SYN scan
* hping3 -f <target> # Fragment packets
* hping3 --spoof <IP> <target> # Spoof source IP
* hping3 --source-port <port> <target>

## Netcat (nc)

Use: Port redirection, tunneling, backdoor creation

Basic Commands:

* nc -lvp <port> # Listen on a port
* nc <target> <port> # Connect to target
* nc -L -p <port> -e /bin/bash # Bind shell

## Proxychains

Use: Routing traffic through proxies for anonymity

Basic Commands:

* proxychains nmap <target>
* proxychains firefox <URL>

## Metasploit

Use: Exploitation framework with evasion modules

Basic Commands:

* use auxiliary/scanner/portscan/tcp
* set RHOSTS <target>
* exploit
* use evasion/windows/windows\_defender\_exe

## Scapy

Use: Custom packet crafting and sending

Basic Commands:

* from scapy.all import \*
* pkt = IP(dst='target')/TCP(dport=80,flags='S')
* send(pkt)