# Module 12: Evading IDS, Firewalls, and Honeypots - Practical Guide

This guide details the specialized tools and step-by-step procedures for the hands-on lab sessions required to master the art of bypassing security controls and identifying defensive traps.

## 1. Comprehensive Evasion Toolset

### IDS/IPS Tools & Evasion

* **Snort:** The industry-standard open-source IDS. Used in labs to understand how signatures are triggered.
* **Fragroute:** A specialized tool that intercepts, modifies, and rewrites egress traffic. It is the primary tool for testing IDS evasion via fragmentation and overlapping packets.
* **Fragtest:** Used to test which types of ICMP, UDP, and TCP fragments a network or IDS allows.
* **Inundator:** An IDS evasion tool designed to flood an IDS with false positives to mask a real attack.

### Firewall Evasion & Anonymity

* **Proxychains:** A tool that forces any TCP connection made by any given application to follow through proxy like TOR or any other SOCKS4, SOCKS5 or HTTP(S) proxy.
* **Anonsurf:** A Parrot OS-specific tool that routes all system traffic through the TOR network with a single command.
* **HTTPLingual / Super-UDP:** Tools used for tunneling protocols over HTTP or UDP to bypass port-specific firewall restrictions.
* **Nmap:** Features advanced flags for evasion (MTU manipulation, fragmentation, decoys, and source port spoofing).

### Honeypots & Detection Tools

* **KFSensor:** A Windows-based host-based IDS and honeypot that acts as a decoy to lure and monitor attackers.
* **Honeyd:** A small daemon that creates virtual honeypots on a network. It can simulate thousands of different OS personalities.
* **SendSafe Honeypot Hunter:** A specialized scanner used by attackers to check if a proxy or server is actually a honeypot.
* **Specter:** A high-interaction honeypot that simulates various vulnerabilities and OS types.

## 2. Hands-On Lab Sessions

### Lab 1: Evading IDS using Nmap (Fragmentation & MTU)

**Goal:** Bypass a signature-based IDS by splitting the TCP header and payload across multiple packets.

1. **Preparation:** Identify the target IP.
2. Basic Fragmentation: ```bash  
   sudo nmap -sS -f [Target\_IP]  
   \*Note: The `-f` flag splits the 20-byte header into 8-byte fragments.\*
3. **Manual MTU Adjustment:** To bypass more sensitive IDS systems, manually set a tiny Maximum Transmission Unit (MTU):  
   sudo nmap -sS --mtu 8 [Target\_IP]  
     
   *Note: MTU must be a multiple of 8.*
4. **Verification:** Monitor the traffic in Wireshark on the target side to see the fragmented "reassembly" process.

### Lab 2: Hiding Scans with Decoys and Source Port Spoofing

**Goal:** Mask your true IP address in the firewall logs of the target.

1. **Decoy Scan:**  
   sudo nmap -sS -D RND:10 [Target\_IP]  
     
   *Note: This generates 10 random "Decoy" IP addresses that appear to be scanning the target simultaneously with you.*
2. **Source Port Spoofing:** Many firewalls allow all traffic coming from port 53 (DNS) or port 80 (HTTP). Trick the firewall into thinking your scan is legitimate traffic:  
   sudo nmap -sS -g 53 [Target\_IP]  
     
   *Note: The -g (or --source-port) flag forces the scan to originate from the specified port.*

### Lab 3: Global Anonymity with Proxychains

**Goal:** Route an entire scanning session through multiple geographic nodes to evade IP-based blocking.

1. **Configure:** Edit the configuration file: sudo nano /etc/proxychains.conf.
2. **Set Chain Type:** Ensure dynamic\_chain is enabled and strict\_chain is commented out.
3. **Add Proxies:** Scroll to the bottom and add your list of SOCKS5 or HTTP proxies.
4. **Execute:**  
   proxychains nmap -sT -Pn [Target\_IP]  
     
   *Note: You must use -sT (TCP Connect) because raw sockets (-sS) cannot be routed through standard SOCKS proxies.*

### Lab 4: Using Fragroute for Advanced Evasion

**Goal:** Automatically fragment all outgoing traffic from your Parrot OS machine.

1. **Configure Rules:** Edit /etc/fragroute.conf to include specific evasion rules:  
   tcp\_seg 8  
   ip\_frag 8  
   order random
2. **Launch:**  
   sudo fragroute [Target\_IP]
3. **Result:** Now, any attack tool you run against that specific Target IP (like a Metasploit exploit or Nmap scan) will be automatically fragmented according to the rules in the config file.

### Lab 5: Honeypot Detection with Nmap

**Goal:** Identify if a target is a decoy system.

1. **Action:** Run a service version scan:  
   sudo nmap -sV --script banner [Target\_IP]
2. **Analysis:** Look for "unusual" banners. For example, if a system claims to be a Windows IIS server but responds to Linux-specific pings, or if the banner looks "too perfect," it is likely a honeypot (e.g., KFSensor).
3. **Time Delay Check:** Use Nmap's timing to check for unusual delays. Honeypots often introduce artificial latency while logging attacker actions.

## 3. CEH Practical Tips for Module 12

* **The Fragmentation Limit:** If an IDS uses "Packet Reassembly" before inspection, simple fragmentation will fail. You must then use **Overlapping Fragments**.
* **Encryption Evasion:** Remember that an IDS cannot see what is inside an **HTTPS (TLS)** packet. Using encrypted tunnels is the most effective way to evade deep packet inspection (DPI).
* **Honeypot Risk:** In a real engagement, never "fully compromise" a honeypot, as it is designed to trap you and log your keystrokes for forensic evidence.