# Kali Sniffing Toolkit — CEH Practice

## Ettercap

Purpose: Graphical + CLI tool for sniffing, ARP spoofing, and man-in-the-middle (MITM) attacks. Can capture live credentials, modify traffic, and test network vulnerabilities.

Basic Syntax:  
ettercap -T -M arp /TARGET\_IP/ /GATEWAY\_IP/

When to Use: When testing a switched network for ARP poisoning vulnerability or intercepting credentials from protocols like HTTP, FTP, POP3.

Pro Tip: Run with root privileges. Combine with Wireshark for detailed packet analysis.

## arpspoof

Purpose: CLI tool for ARP spoofing to redirect network traffic through your machine.

Basic Syntax:  
arpspoof -i eth0 -t TARGET\_IP GATEWAY\_IP  
arpspoof -i eth0 -t GATEWAY\_IP TARGET\_IP

When to Use: When you need a lightweight MITM setup without extra features. Perfect for quick ARP poisoning tests.

Pro Tip: Disable IP forwarding after testing to restore normal network behavior.

## macof

Purpose: Overloads a network switch with random MAC addresses, forcing it into hub-like mode (fail-open).

Basic Syntax:  
macof -i eth0

When to Use: Before sniffing traffic on a switched network. Often used with tcpdump or Wireshark to capture broadcast traffic.

Pro Tip: Use carefully; can disrupt the entire network.

## dnsspoof

Purpose: Spoofs DNS replies to redirect a target to a malicious IP.

Basic Syntax:  
dnsspoof -i eth0 -f hosts.txt  
  
hosts.txt:  
10.0.0.5 www.example.com

When to Use: For phishing simulations or red team exercises that require redirecting victims to fake sites.

Pro Tip: Edit /etc/hosts carefully. Use in isolated environments to avoid legal issues.

## sslstrip

Purpose: Strips HTTPS encryption, downgrading connections to HTTP for sniffing credentials.

Basic Syntax:  
sslstrip -l 8080

When to Use: When testing sites vulnerable to HTTPS downgrade attacks.

Pro Tip: Pair with ARP spoofing to position yourself between the target and gateway.

## Yersinia

Purpose: Framework for exploiting weaknesses in network protocols like STP, CDP, DTP, HSRP.

Basic Syntax:  
yersinia -I

When to Use: Testing switches, routers, and VLAN hopping vulnerabilities.

Pro Tip: Best run in interactive mode to explore protocol-specific attacks.

## Wireshark

Purpose: Advanced packet analysis tool with GUI, useful for filtering and decoding network traffic.

Basic Syntax:  
wireshark

When to Use: Deep packet inspection after capturing traffic.

Pro Tip: Use filters like 'http', 'ftp', or 'ip.addr == target\_ip' to focus analysis.

## tcpdump

Purpose: CLI packet capture tool for quick traffic recording and filtering.

Basic Syntax:  
tcpdump -i eth0 host TARGET\_IP

When to Use: Quick captures without GUI overhead.

Pro Tip: Save captures using '-w file.pcap' for later analysis in Wireshark.