CEH Module 8 - Sniffing Tools Practical Cheatsheet

# Wireshark

Purpose: Capture and inspect network packets.

Example Commands:

* wireshark
* # Apply display filter for HTTP traffic
* http
* # Filter for specific IP
* ip.addr == 192.168.1.10

# tcpdump

Purpose: CLI tool to capture network packets.

Example Commands:

* sudo tcpdump -i eth0
* sudo tcpdump -i eth0 tcp port 80
* sudo tcpdump -i eth0 -w capture.pcap

# macof

Purpose: Overflow switch MAC table to force fail-open mode.

Example Commands:

* sudo macof -i eth0

# arpspoof

Purpose: Redirect victim traffic to attacker machine via ARP poisoning.

Example Commands:

* sudo arpspoof -i eth0 -t 192.168.1.5 192.168.1.1
* sudo arpspoof -i eth0 -t 192.168.1.1 192.168.1.5

# Ettercap

Purpose: Perform MITM attacks with GUI/CLI.

Example Commands:

* ettercap -G
* sudo ettercap -T -M arp:remote /192.168.1.5/ /192.168.1.1/

# Bettercap

Purpose: Advanced replacement for Ettercap with HTTPS stripping.

Example Commands:

* sudo bettercap -iface eth0
* net.probe on
* set arp.spoof.targets 192.168.1.5
* arp.spoof on
* net.sniff on

# dsniff

Purpose: Extract credentials from network traffic.

Example Commands:

* sudo dsniff -i eth0

# Aircrack-ng Suite

Purpose: Wireless sniffing and cracking.

Example Commands:

* sudo airmon-ng start wlan0
* sudo airodump-ng wlan0mon
* sudo airodump-ng -c 6 --bssid 00:11:22:33:44:55 -w capture wlan0mon
* sudo aircrack-ng capture-01.cap -w /path/to/wordlist.txt

# mitmproxy

Purpose: Intercept and inspect HTTP/HTTPS traffic.

Example Commands:

* mitmproxy -p 8080

# XArp

Purpose: Detect ARP spoofing attempts. (GUI tool, no CLI commands)

# Netresec NetworkMiner (Windows)

Purpose: Passive network sniffer & forensic tool for Windows.

# Capsa Free (Windows)

Purpose: Packet analyzer for network monitoring and troubleshooting.

# Microsoft Message Analyzer (Windows)

Purpose: Advanced network protocol analyzer from Microsoft.

# CommView (Windows)

Purpose: Network monitoring & packet capture for Windows.