# CEH Module 11 - Session Hijacking Tools & Commands Cheat Sheet

|  |  |  |  |
| --- | --- | --- | --- |
| Tool | Purpose (Practical Use) | Launch Command | Common Commands / Notes |
| Bettercap | MITM attacks (ARP/DNS spoofing), sniffing cookies, credentials. | bettercap -iface eth0 | net.probe on – discover hosts arp.spoof.targets <IP> – set victim arp.spoof on – start MITM net.sniff on – sniff traffic |
| Ettercap | MITM for sniffing & packet manipulation. | ettercap -T -M arp /<victim>/ /<gateway>/ | -T → text mode -M arp → ARP spoof mode |
| Wireshark | Capture & inspect packets to extract cookies/session IDs. | wireshark | Filter: http.cookie or tcp.port == 80 |
| tcpdump | CLI packet capture for later analysis. | tcpdump -i eth0 | Save: tcpdump -i eth0 tcp port 80 -w cap.pcap Read: tcpdump -r cap.pcap |
| Burp Suite | Intercept & modify HTTP/S requests, replay session IDs. | GUI app | Proxy → capture request Send to Repeater → edit Cookie header |
| OWASP ZAP | Open-source HTTP/S interception, fuzzing, scanning. | owasp-zap | Proxy setup → Manual Request Editor → edit cookies |
| Hunt | LAN session sniffing/takeover (older). | hunt | Modes: watch sessions, takeover TCP streams |
| Ferret | Sniffs cookies/credentials from traffic. | ferret -i eth0 | Works with Hamster to replay sessions |
| Hamster | Replays stolen cookies in browser. | hamster | Visit http://127.0.0.1:1234 to load stolen cookies |
| NetWitness | Forensic analysis of packet captures. | GUI app | Import .pcap, search Set-Cookie or Authorization |
| SSLstrip | Downgrade HTTPS → HTTP for sniffing. | sslstrip -l 8080 | Combine with ARP spoofing to capture creds |
| arpspoof | Redirect victim traffic via ARP poisoning. | arpspoof -i eth0 -t <victim> <gateway> | Run reverse for gateway to victim |
| mitmproxy | Intercept & modify HTTP/S traffic via CLI/TUI. | mitmproxy | Interactive session editing of requests/responses |