MAN IN THE MIDDLE ATTACK

Step 1 – Setup Environment (Use Internet Initially)

connect your Kali Linux laptop to the internet (only for setup).

Step 2 – Install Dependencies

```
sudo apt update

sudo apt install python3 python3-venv
```

Step 3 – Create Virtual Environment

```
python3 -m venv mitm-env

source mitm-env/bin/activate
```

Step 4 – Install mitmproxy and Fix bcrypt Issue

```
pip install mitmproxy bcrypt==4.0.1
```

Step 5 – Turn OFF Internet

Ensure everything works fully offline.

Step 6 – Create server.py (Simple HTTP Server)

Open a text editor (like nano) and create server.py:

```
nano server.py
```

Paste this code inside server.py:

```
from http.server import BaseHTTPRequestHandler, HTTPServer

import urllib.parse

class SimpleHTTPRequestHandler(BaseHTTPRequestHandler):

    def do_GET(self):

        self.send_response(200)

        self.end_headers()

        self.wfile.write(b"""

            <html>

                <body>

                    <h2>Login Page</h2>

                    <form method="POST">

                        Username: <input type="text" name="username"><br>

                        Password: <input type="password" name="password"><br>

                        <input type="submit" value="Login">
                    </form>
                </body>
            </html>
        """)

    def do_POST(self):
        content_length = int(self.headers['Content-Length'])
        post_data = self.rfile.read(content_length)
        form_data = urllib.parse.parse_qs(post_data.decode('utf-8'))

        username = form_data.get('username')[0]
        password = form_data.get('password')[0]

        print(f"[+] Intercepted Credentials -> Username: {username}, Password: {password}")

        self.send_response(200)
        self.end_headers()
        self.wfile.write(b"<html><body><h2>Login Successful</h2></body></html>")

server_address = ('0.0.0.0', 8080)
httpd = HTTPServer(server_address, SimpleHTTPRequestHandler)
print("[*] HTTP Server running on http://<local-IP>:8080")
httpd.serve_forever()
```

Save & exit (Ctrl + O, Enter, Ctrl + X).

Step 7 – Create intercept.py (mitmproxy Script)

Create the script file:

```
nano intercept.py
```

Paste this code:

```
from mitmproxy import http
```

```
def request(flow: http.HTTPFlow) -> None:
  if flow.request.method == "POST":
    print("\n[+] Intercepted POST Data:")
    print(flow.request.content.decode())
```

Save & exit (Ctrl + O, Enter, Ctrl + X).

Step 8 – Terminal Setup and Commands

Terminal	Action
◆ Terminal 1	Run HTTP Server: python3 server.py
◆ Terminal 2	Run mitmproxy with intercept script: mitmproxy --mode regular -p 8081 --listen-host 0.0.0.0 -s intercept.py
◆ Browser	Configure proxy: HTTP Proxy → 127.0.0.1, Port → 8081 Then visit: http://192.168.X.X:8080 and submit the form

Step 9 – Finding Local IP Address

In any terminal:

```
ip a
```

Example result:

```
inet 192.168.43.10/24
```

Use this IP when opening the browser:

http://192.168.43.10:8080

Step 10 – Run the Demo

1. Open browser → Visit http://192.168.43.10:8080
2. Submit dummy username & password (e.g., testuser / mypassword).
3. Observe:
    - mitmproxy terminal prints intercepted POST data.
    - HTTP server terminal prints credentials.

Step 11 – Cleanup After Demo

- Stop HTTP Server:
- Ctrl + C
- Stop mitmproxy:
- Ctrl + C

- Deactivate virtual environment:
- deactivate

Full Command Summary

```
# Install Dependencies (once)
sudo apt update
sudo apt install python3 python3-venv

# Create Virtual Env
python3 -m venv mitm-env
source mitm-env/bin/activate

# Install mitmproxy
pip install mitmproxy bcrypt==4.0.1
# (Turn OFF Internet)
# Find Local IP
ip a

# Run HTTP Server (Terminal 1)
python3 server.py

# Run mitmproxy with script (Terminal 2)
mitmproxy --mode regular -p 8081 --listen-host 0.0.0.0 -s intercept.py
# Configure Browser Proxy: 127.0.0.1:8081
# Visit in Browser: http://<local-IP>:8080
# Submit dummy credentials
# Stop everything when done:
 Ctrl + C
deactivate
```