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

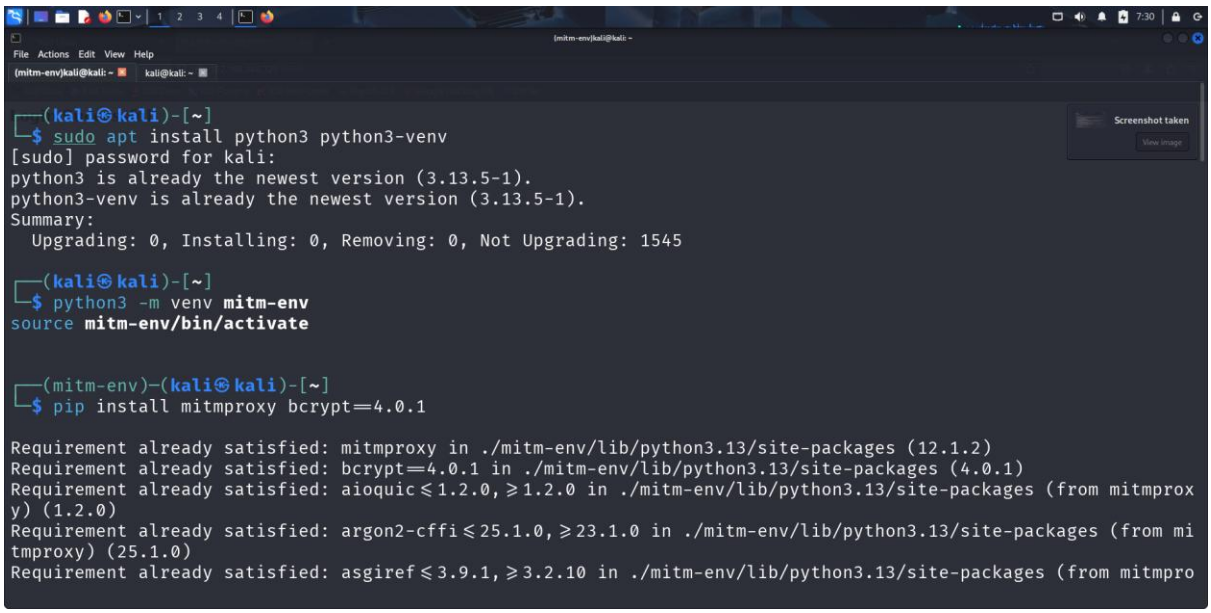
Step 3 – Create Virtual Environment

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:

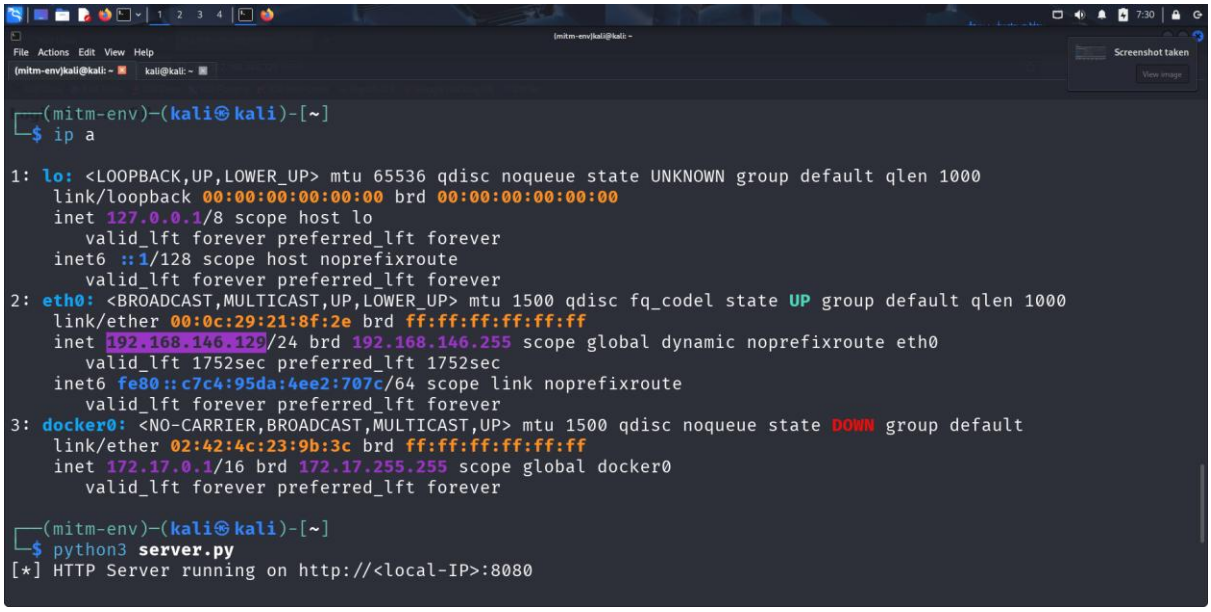
ip a

Example result:

inet 192.168.43.10/24

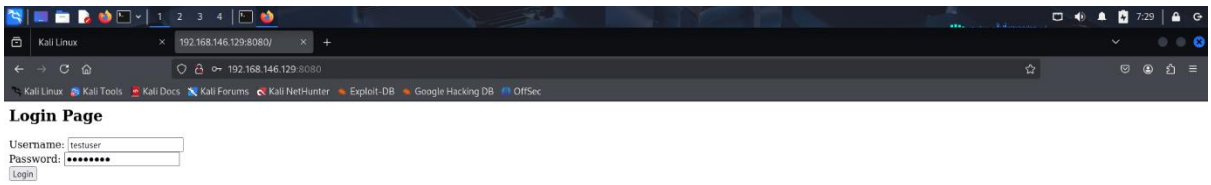
Use this IP when opening the browser:

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

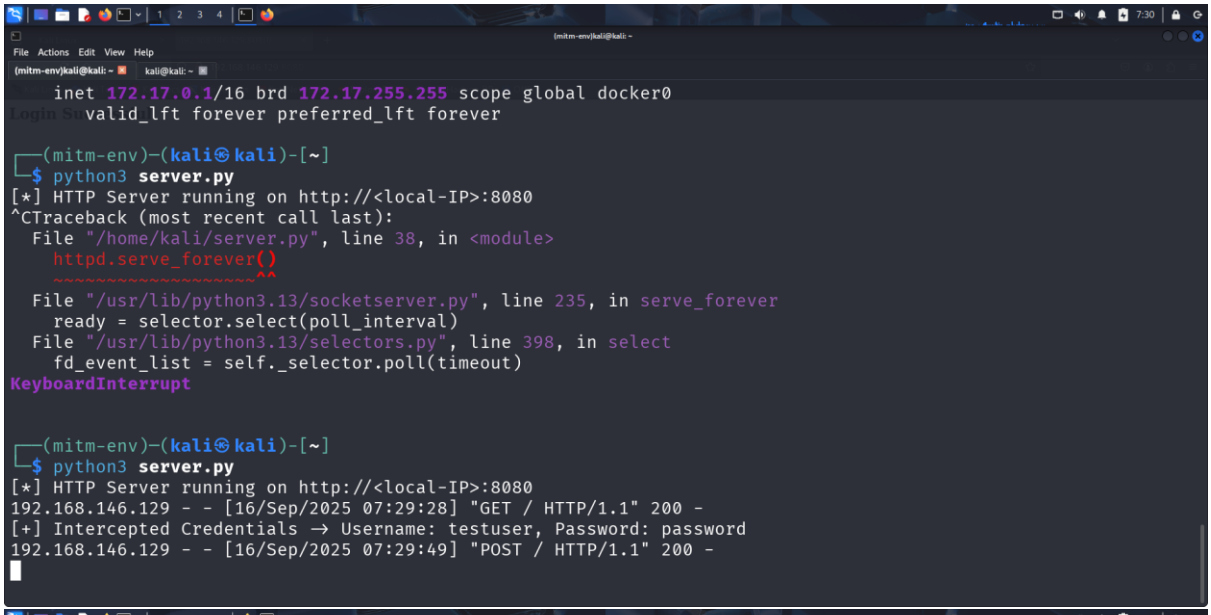
- Stop HTTP Server:
- Ctrl + C
- Stop mitmproxy:

- Ctrl + C
- Deactivate virtual environment:
- deactivate

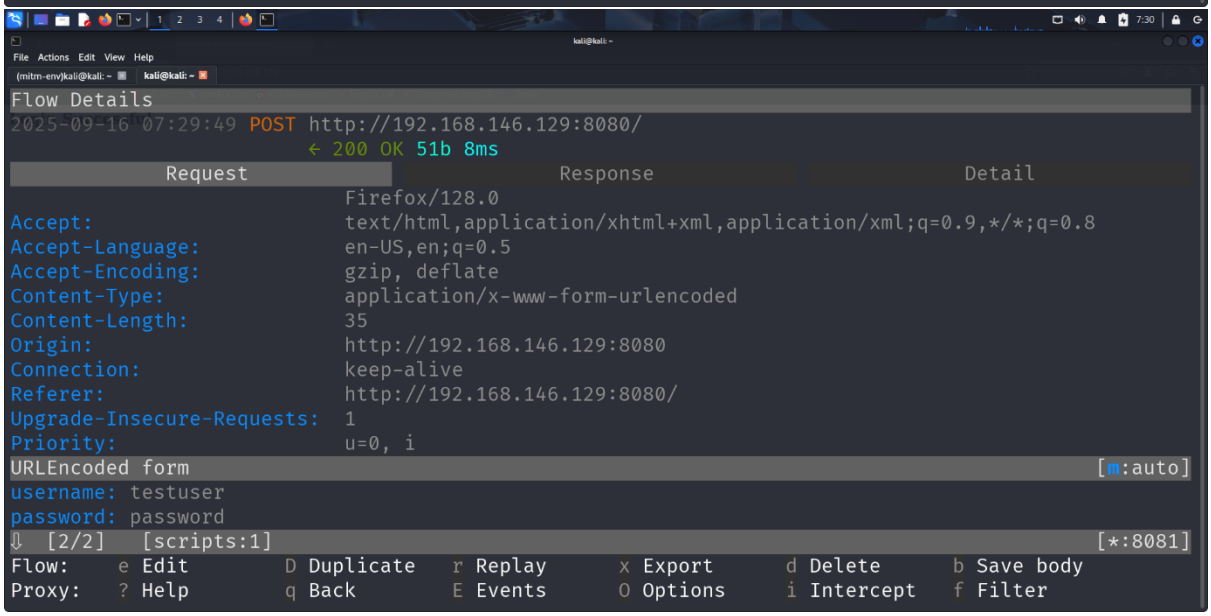
Full Command Summary

```
# 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
```

OUTPUT



```
File Actions Edit View Help
(mitm-env)kali@kali: ~  kali@kali: ~
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever

┌──(mitm-env)─(kali㉿kali)-[~]
└─$ python3 server.py
[*] HTTP Server running on http://<local-IP>:8080
^CTraceback (most recent call last):
  File "/home/kali/server.py", line 38, in <module>
    httpd.serve_forever()
    ~~~~~~~~~~~~~~~~~~~^^
  File "/usr/lib/python3.13/socketserver.py", line 235, in serve_forever
    ready = selector.select(poll_interval)
  File "/usr/lib/python3.13/selectors.py", line 398, in select
    fd_event_list = self._selector.poll(timeout)
KeyboardInterrupt


┌──(mitm-env)─(kali㉿kali)-[~]
└─$ python3 server.py
[*] HTTP Server running on http://<local-IP>:8080
192.168.146.129 - - [16/Sep/2025 07:29:28] "GET / HTTP/1.1" 200 -
[+] Intercepted Credentials → Username: testuser, Password: password
192.168.146.129 - - [16/Sep/2025 07:29:49] "POST / HTTP/1.1" 200 -
```



```
File Actions Edit View Help
(mitm-env)kali@kali: ~  kali@kali: ~
Flow Details
2025-09-16 07:29:49 POST http://192.168.146.129:8080/
                    ← 200 OK 51b 8ms
          Request                    Response                   Detail
                          Firefox/128.0
Accept:                   text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language:          en-US,en;q=0.5
Accept-Encoding:          gzip, deflate
Content-Type:             application/x-www-form-urlencoded
Content-Length:           35
Origin:                   http://192.168.146.129:8080
Connection:               keep-alive
Referer:                  http://192.168.146.129:8080/
Upgrade-Insecure-Requests: 1
Priority:                 u=0, i
URLEncoded form                                                    [m:auto]
username: testuser
password: password
⇩  [2/2]   [scripts:1]                                             [*:8081]
Flow:    e Edit       D Duplicate   r Replay      x Export      d Delete      b Save body
Proxy:   ? Help       q Back        E Events      O Options     i Intercept   f Filter
```