CODTECH Cybersecurity Internship

Task 3 - Penetration Testing Toolkit

Name: Kodali Harshith

Objective:

To develop a simple penetration testing toolkit in Python with modules like Port Scanner and Brute Force Simulation to understand how basic ethical hacking tools operate.

Modules in Toolkit:

1. Port Scanner - Scans common open ports on a target IP or domain.
2. Brute Force Simulation - Simulates password guessing using a predefined wordlist.

Complete Python Code:

```
import socket

def port_scanner(target):
    print(f"\n[+] Starting Port Scan on {target}...\n")
     common_ports = [21, 22, 23, 25, 53, 80, 110, 135, 139, 143, 443, 445, 993, 995, 1723, 3306,
3389, 8080]
    for port in common_ports:
        try:
            sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
            sock.settimeout(1)
            result = sock.connect_ex((target, port))
            if result == 0:
                print(f"[OPEN] Port {port}")
            sock.close()
        except socket.error:
            print(f"[ERROR] Couldn't connect to port {port}")

def brute_force_simulation():
    print("\n[+] Starting Brute Force Simulation...\n")
    username = input("Enter username: ")
    correct_password = "admin123"
    passwords = ["1234", "admin", "letmein", "password", "admin123"]
    for password in passwords:
        print(f"Trying password: {password}")
        if password == correct_password:
            print(f"\n[SUCCESS] Password found: {password}")
```

CODTECH Cybersecurity Internship

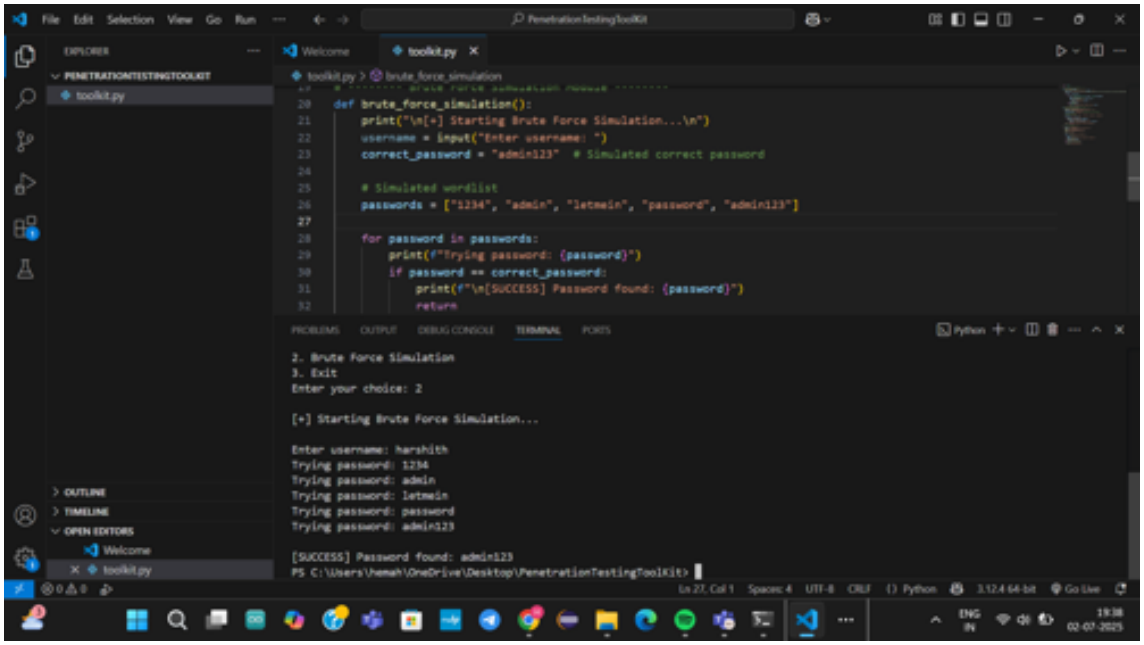
Task 3 - Penetration Testing Toolkit

```
            return
    print("\n[FAILED] Password not found in wordlist.")

if __name__ == "__main__":
    print("=== Penetration Testing Toolkit ===")
    print("1. Port Scanner")
    print("2. Brute Force Simulation")
    print("3. Exit")

    choice = input("Enter your choice: ")
    if choice == "1":
        target = input("Enter the target IP or domain: ")
        port_scanner(target)
    elif choice == "2":
        brute_force_simulation()
    else:
        print("Exiting Toolkit.")
```

Screenshot of Output:



Conclusion:

The toolkit successfully demonstrated basic penetration testing techniques. It scanned open ports and simulated password guessing using a simple brute force loop. This task helped in understanding how basic network attacks are structured in cybersecurity.