

## OUTPUT – Penetration Testing Toolkit

- Port Scanning using 27.0.0.1 IP address (safe to test).

```
PS C:\Users\surat\OneDrive\Desktop\TASK 3> cd /TASK 3/main.py"

◆ PENETRATION TESTING TOOLKIT ◆

1. Port Scanner
2. Brute-Force Attacker
3. Packet Sniffer
4. Subdomain Enumeration
5. Vulnerability Scanner
6. Exit

Select an option: 1

Enter the target IP: 127.0.0.1

[*] Scanning 127.0.0.1 for open ports..
[+] Port 135 is open
[+] Port 445 is open
```

- Brute Force on <https://juice-shop.herokuapp.com> ( A website made to test vulnerabilities, brute force, etc.)

[illegible]

- Packet Sniffing on Wi-Fi Interface

```

♦ PENETRATION TESTING TOOLKIT ♦
1. Port Scanner
2. Brute-Force Attacker
3. Packet Sniffer
4. Subdomain Enumeration
5. Vulnerability Scanner
6. Exit
Select an option: 3
Enter network interface (e.g., eth0, wlan0, Wi-Fi): Wi-Fi
[*] Starting packet sniffing on Wi-Fi
Ether / IPv6 / TCP
Ether / IPv6 / TCP
Ether / IPv6 / TCP
Ether / IPv6 / TCP
Ether / ARP who has
Ether / IPv6 / ICMPv6ND_NS /
Ether / ARP is
Ether / IPv6 / ICMPv6 Neighbor Discovery -
Ether / IPv6 / TCP
Ether / IPv6 / TCP
Ether / IPv6 / ICMPv6ND_NS / ICMPv6 Neighbor Discovery Option
Ether / IPv6 / ICMPv6ND_NA / ICMPv6 Neighbor Discovery Option

```

- Subdomain enumeration (example).

```

[+] Enumerating Subdomains for example.com
[*] Found: mail.example.com
[*] Found: shop.example.com
[*] Found: dev.example.com
[✓] Enumeration Completed.

```

- Vulnerability Scan on <https://www.hackthebox.com/> ( A safe website made to test network and web application vulnerabilities and can be used for testing).

```

♦ PENETRATION TESTING TOOLKIT ♦
1. Port Scanner
2. Brute-Force Attacker
3. Packet Sniffer
4. Subdomain Enumeration
5. Vulnerability Scanner
6. Exit
Select an option: 5
Enter target URL: https://www.hackthebox.com/
[*] Scanning https://www.hackthebox.com/ for vulnerabilities...
[+] Possible SQL Injection vulnerability found at https://www.hackthebox.com/

```