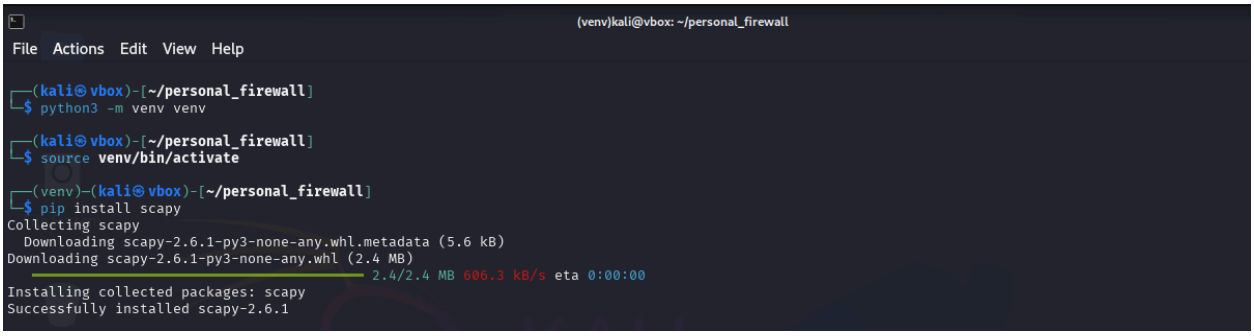
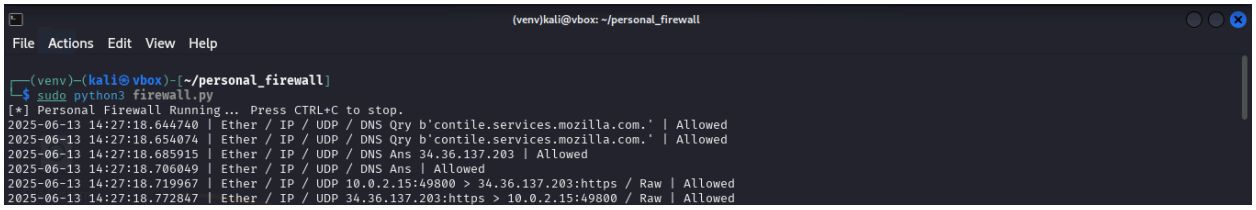
Personal Firewall Project

Image-1: Personal Firewall Script Execution



- Shows the Python-based firewall script running in a terminal.
- Displays filtering logic for blocking/allowing packets based on predefined rules.
- Demonstrates the real-time packet inspection process.

Image 2: Live Packet Logging



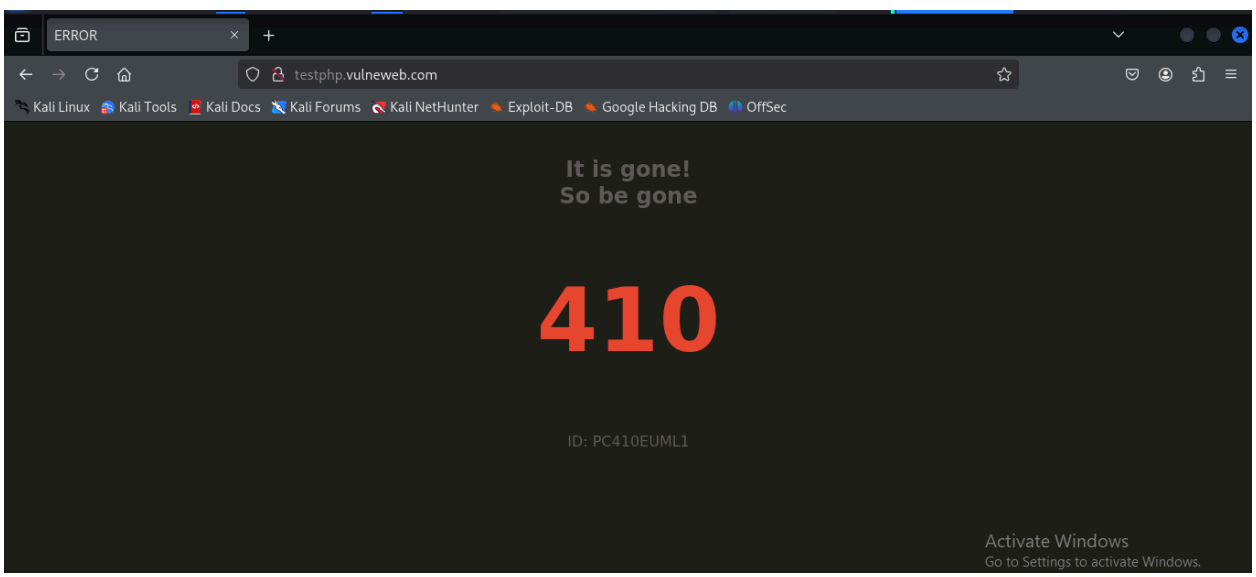
- Captures ongoing network traffic analysis with logged packets.
- Highlights allowed TCP/UDP connections, including DNS queries.
- Confirms correct firewall rule application and filtering efficiency.

Image 3: Outbound Traffic Blocking

```
2025-06-13 14:30:11.535482 | Ether / IP / TCP 34.107.221.82:http > 10.0.2.15:42122 A / Padding | Allowed
2025-06-13 14:30:14.266394 | Ether / IP / ICMP 10.0.2.15 > 8.8.8.8 echo-request 0 / Raw | Blocked Outbound IP: 8.8.8.8
2025-06-13 14:30:14.294787 | Ether / IP / ICMP 8.8.8.8 > 10.0.2.15 echo-reply 0 / Raw | Allowed
2025-06-13 14:30:14.862998 | Ether / IP / TCP 10.0.2.15:57092 > 104.104.138.107:http A | Allowed
2025-06-13 14:30:14.866696 | Ether / IP / TCP 104.104.138.107:http > 10.0.2.15:57092 A / Padding | Allowed
2025-06-13 14:30:15.268795 | Ether / IP / ICMP 10.0.2.15 > 8.8.8.8 echo-request 0 / Raw | Blocked Outbound IP: 8.8.8.8
2025-06-13 14:30:15.298110 | Ether / IP / ICMP 8.8.8.8 > 10.0.2.15 echo-reply 0 / Raw | Allowed
2025-06-13 14:30:16.269658 | Ether / IP / ICMP 10.0.2.15 > 8.8.8.8 echo-request 0 / Raw | Blocked Outbound IP: 8.8.8.8
2025-06-13 14:30:16.298180 | Ether / IP / ICMP 8.8.8.8 > 10.0.2.15 echo-reply 0 / Raw | Allowed
2025-06-13 14:30:17.270646 | Ether / IP / ICMP 10.0.2.15 > 8.8.8.8 echo-request 0 / Raw | Blocked Outbound IP: 8.8.8.8
2025-06-13 14:30:17.298778 | Ether / IP / ICMP 8.8.8.8 > 10.0.2.15 echo-reply 0 / Raw | Allowed
2025-06-13 14:30:18.272091 | Ether / IP / ICMP 10.0.2.15 > 8.8.8.8 echo-request 0 / Raw | Blocked Outbound IP: 8.8.8.8
2025-06-13 14:30:18.303543 | Ether / IP / ICMP 8.8.8.8 > 10.0.2.15 echo-reply 0 / Raw | Allowed
2025-06-13 14:30:18.957517 | Ether / IP / TCP 10.0.2.15:57368 > 104.104.138.106:http A | Allowed
2025-06-13 14:30:18.959400 | Ether / IP / TCP 104.104.138.106:http > 10.0.2.15:57368 A / Padding | Allowed
2025-06-13 14:30:19.275889 | Ether / IP / ICMP 10.0.2.15 > 8.8.8.8 echo-request 0 / Raw | Blocked Outbound IP: 8.8.8.8
2025-06-13 14:30:19.305585 | Ether / IP / ICMP 8.8.8.8 > 10.0.2.15 echo-reply 0 / Raw | Allowed
2025-06-13 14:30:21.773443 | Ether / IP / TCP 10.0.2.15:42122 > 34.107.221.82:http A | Allowed
```

- Logs of blocked ICMP echo requests to `8.8.8.8`, demonstrating outbound traffic control.
- Shows structured timestamps, IPs, ports, and action statuses.
- Verifies the firewall's enforcement of outbound rules.

Image 4: DNS Query Blocking



- Displays a blocked DNS request to "testphp.vulnweb.com", preventing access to vulnerable domains.
- Browser error message (410 Gone) confirms successful filtering.
- Demonstrates DNS-based security enforcement within the firewall.