DENAIL OF SERVICE
&
DISTRIBUTED DENAIL OF SERVICE

DOS (Denial of Service) and DDOS (Distributed Denial of Service) attacks are malicious attempts to disrupt the normal functioning of a network, service, or website by overwhelming it with a flood of illegitimate traffic. These attacks can lead to service downtime, loss of functionality, and potential financial or reputational damage.

Denial of Service (DOS) Attacks:

Definition:

A DOS attack aims to make a computer, network, or service unavailable to its intended users by flooding it with a large volume of traffic or by exploiting vulnerabilities to consume system resources.

Types of DOS Attacks:

Flooding Attacks:

UDP Flood:

Overwhelms the target with a flood of User Datagram Protocol (UDP) packets.

ICMP Flood:

Floods the target with Internet Control Message Protocol (ICMP) packets.

SYN/ACK Flood:

Exploits the TCP handshake process, overwhelming the target with incomplete connection requests.

Logic Attacks:

Exploits vulnerabilities in the target system or application to cause it to crash or become unresponsive.

Resource Depletion Attacks:

Exhausts system resources, such as CPU, memory, or disk space, rendering the target inaccessible.

Distributed Denial of Service (DDOS) Attacks:

Definition:

A DDOS attack involves multiple compromised computers (often a botnet) that work together to launch a coordinated assault on a target, amplifying the impact compared to a single DOS attack.

Characteristics of DDOS Attacks:

Botnets:

Networks of compromised computers controlled by an attacker to carry out the attack.

Amplification:

Exploits vulnerabilities to magnify the volume of attack traffic.

Spoofing:

Uses fake or manipulated IP addresses to make tracing and blocking the attack more challenging.

DDOS Attack Vectors:

Volumetric Attacks:

Floods the target with a massive volume of traffic, overwhelming its bandwidth.

Protocol Attacks:

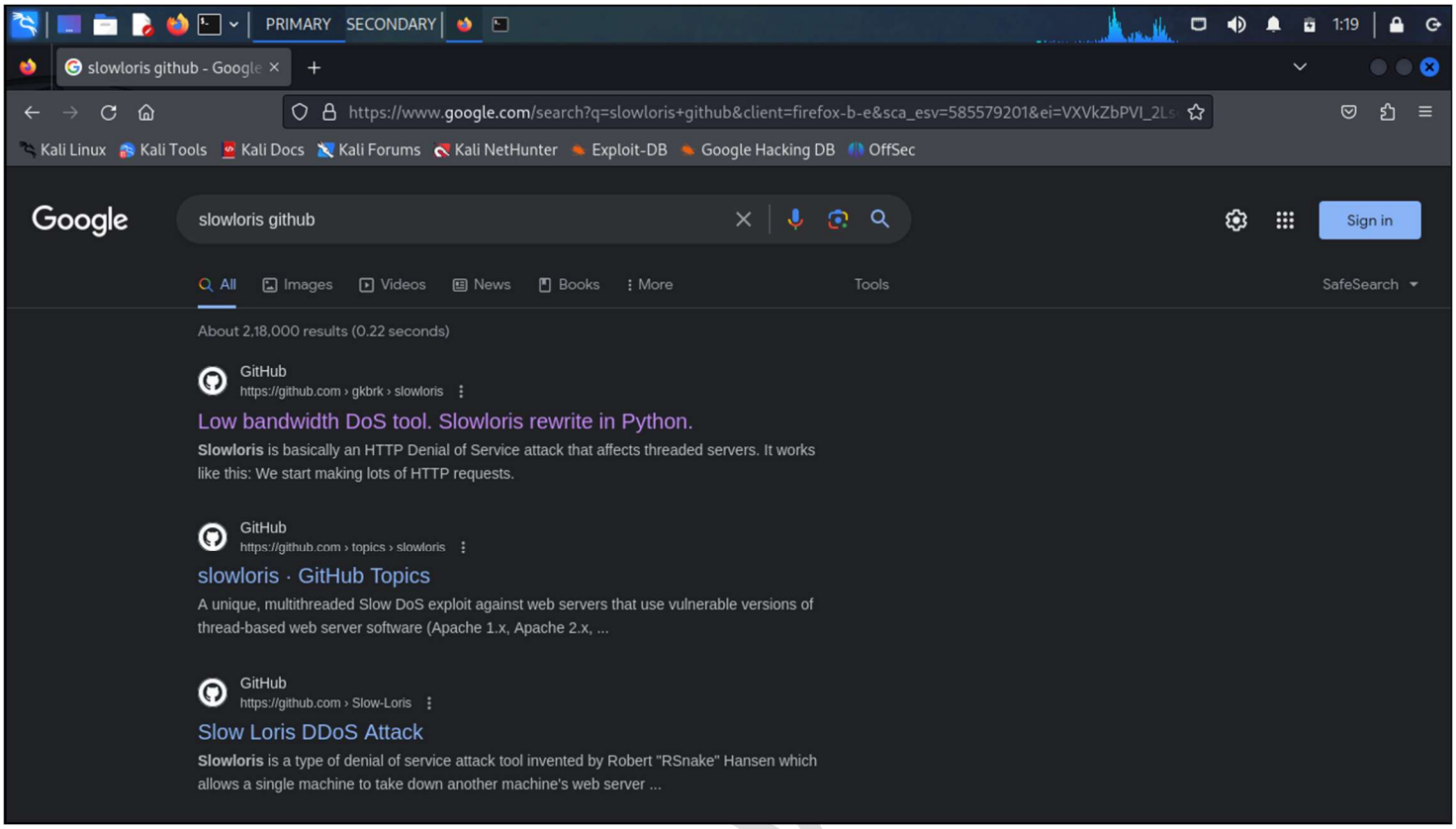
Exploits weaknesses in network protocols.

Application Layer Attacks:

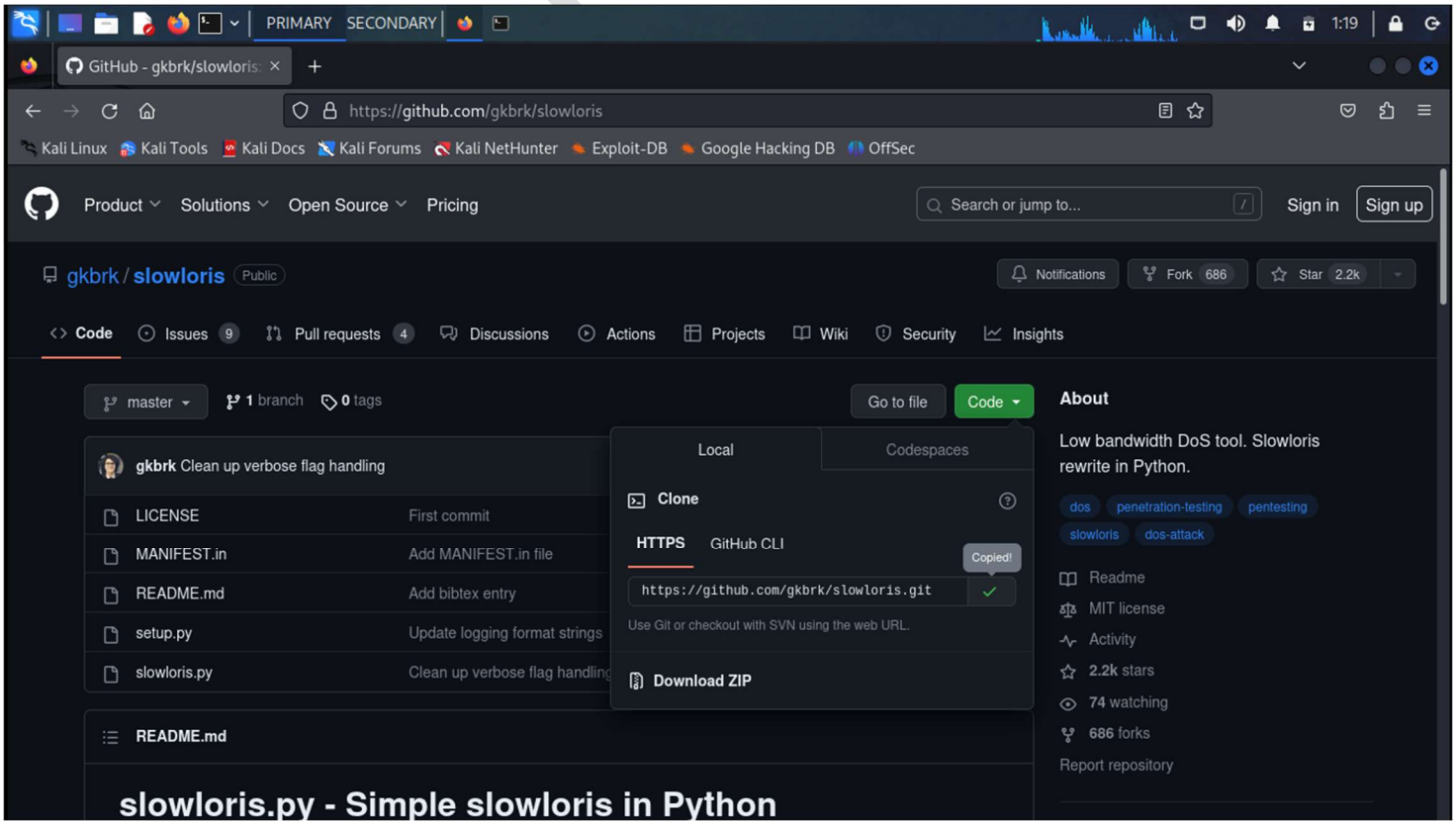
Targets vulnerabilities in web applications or services.

IMPLEMENTATION:

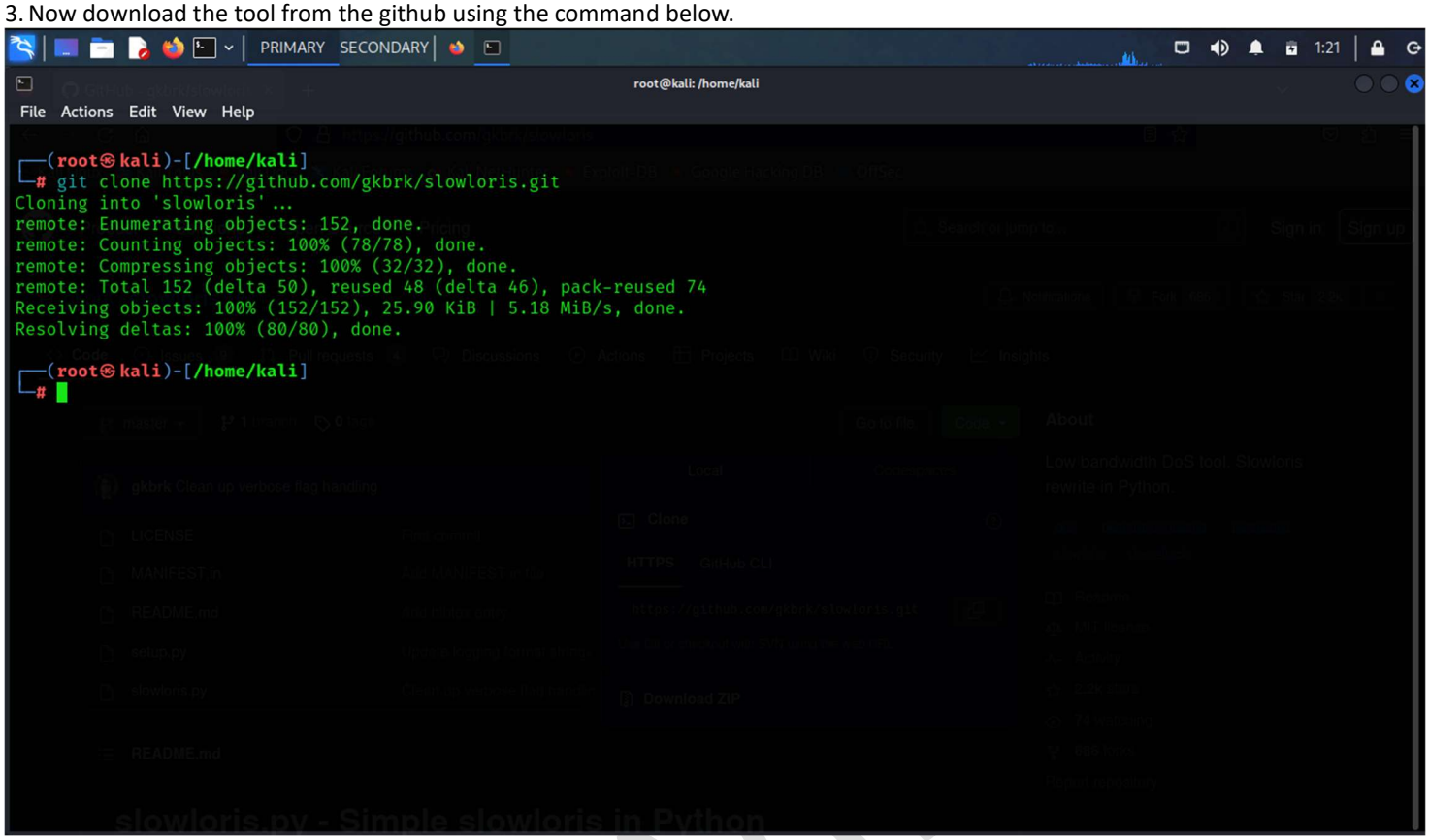
1. Search for a tool called **slowloris** which is available in GitHub.



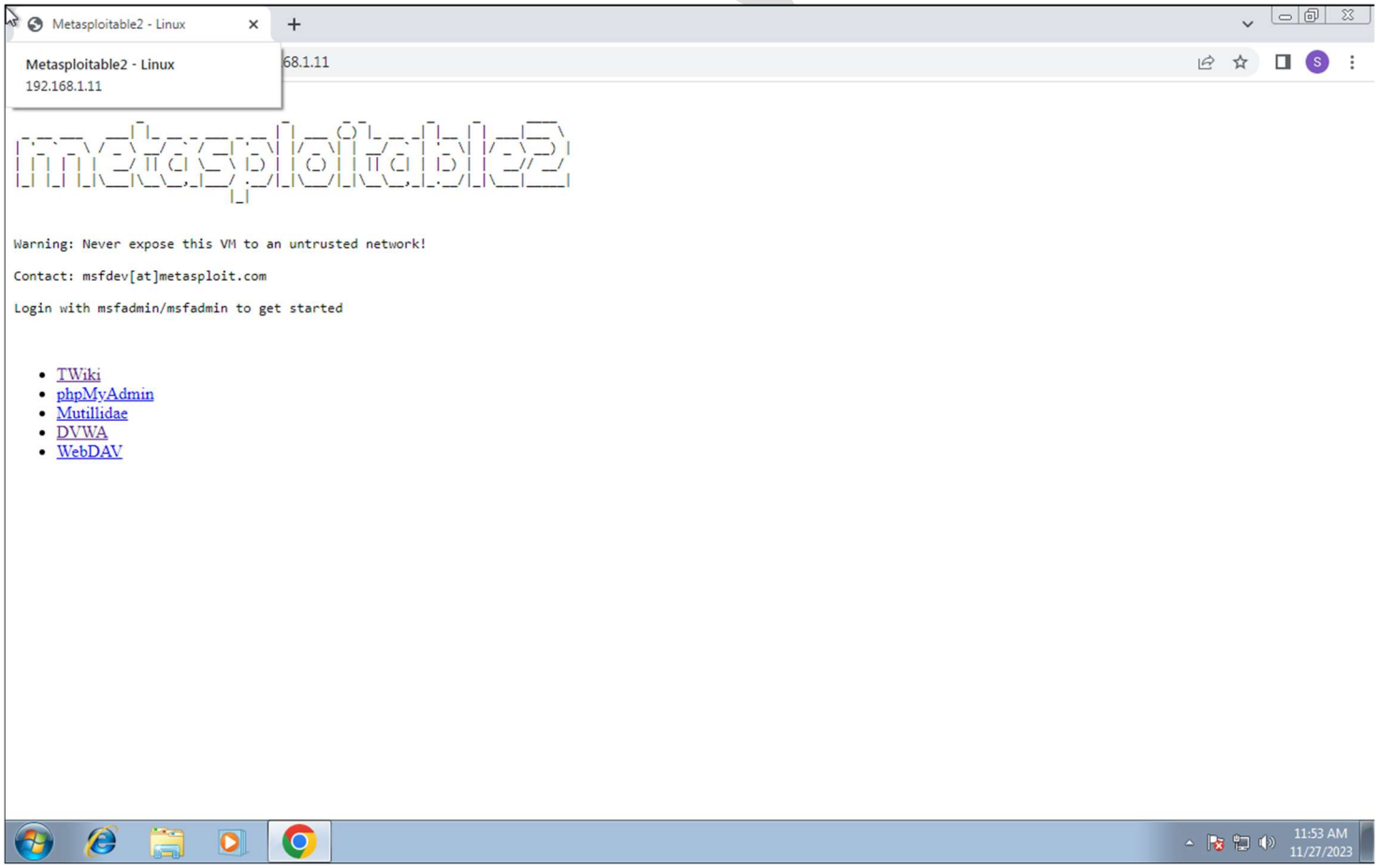
2. Copy the link of the repository to download the tool into our machine.



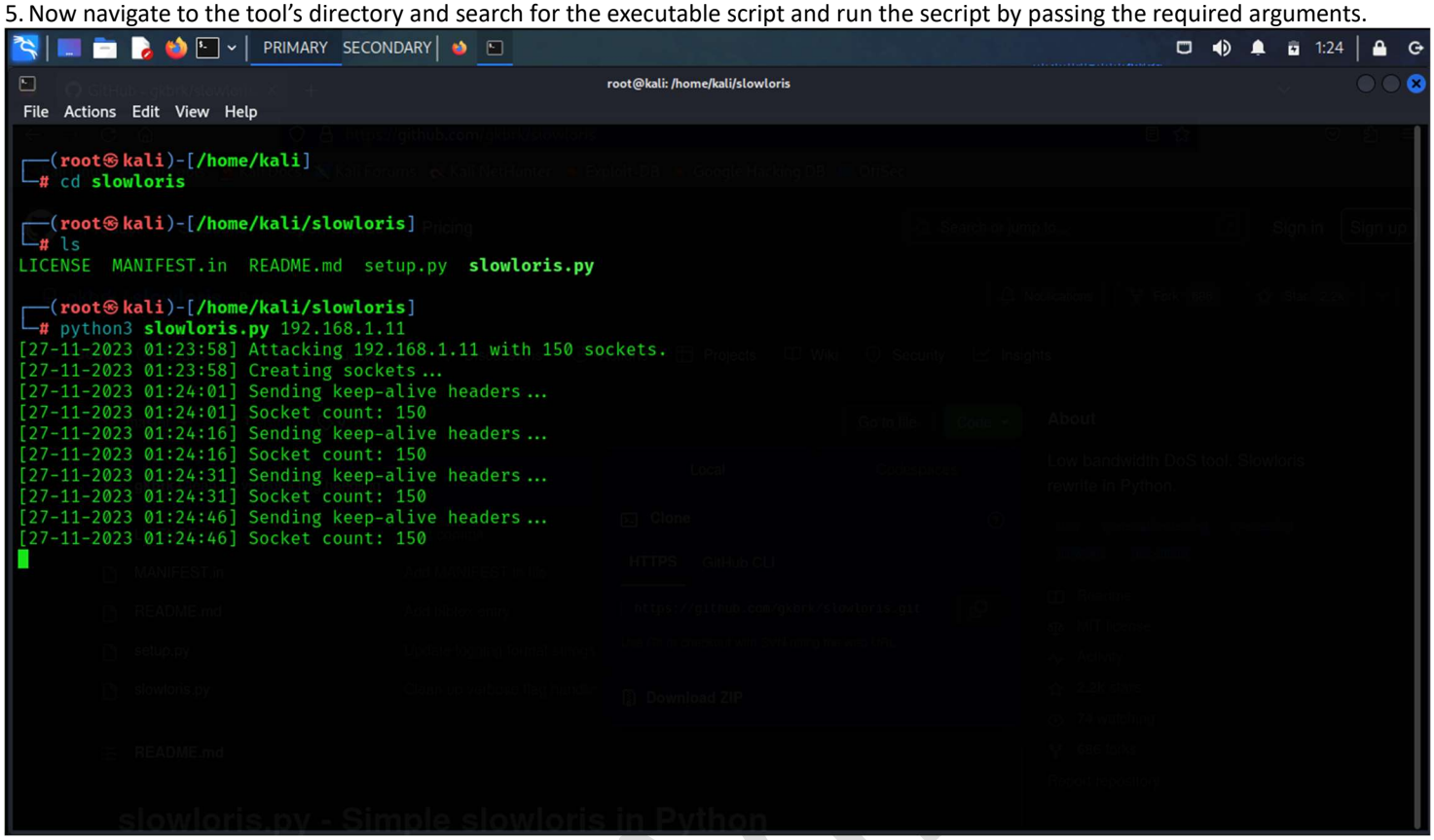
3. Now download the tool from the github using the command below.



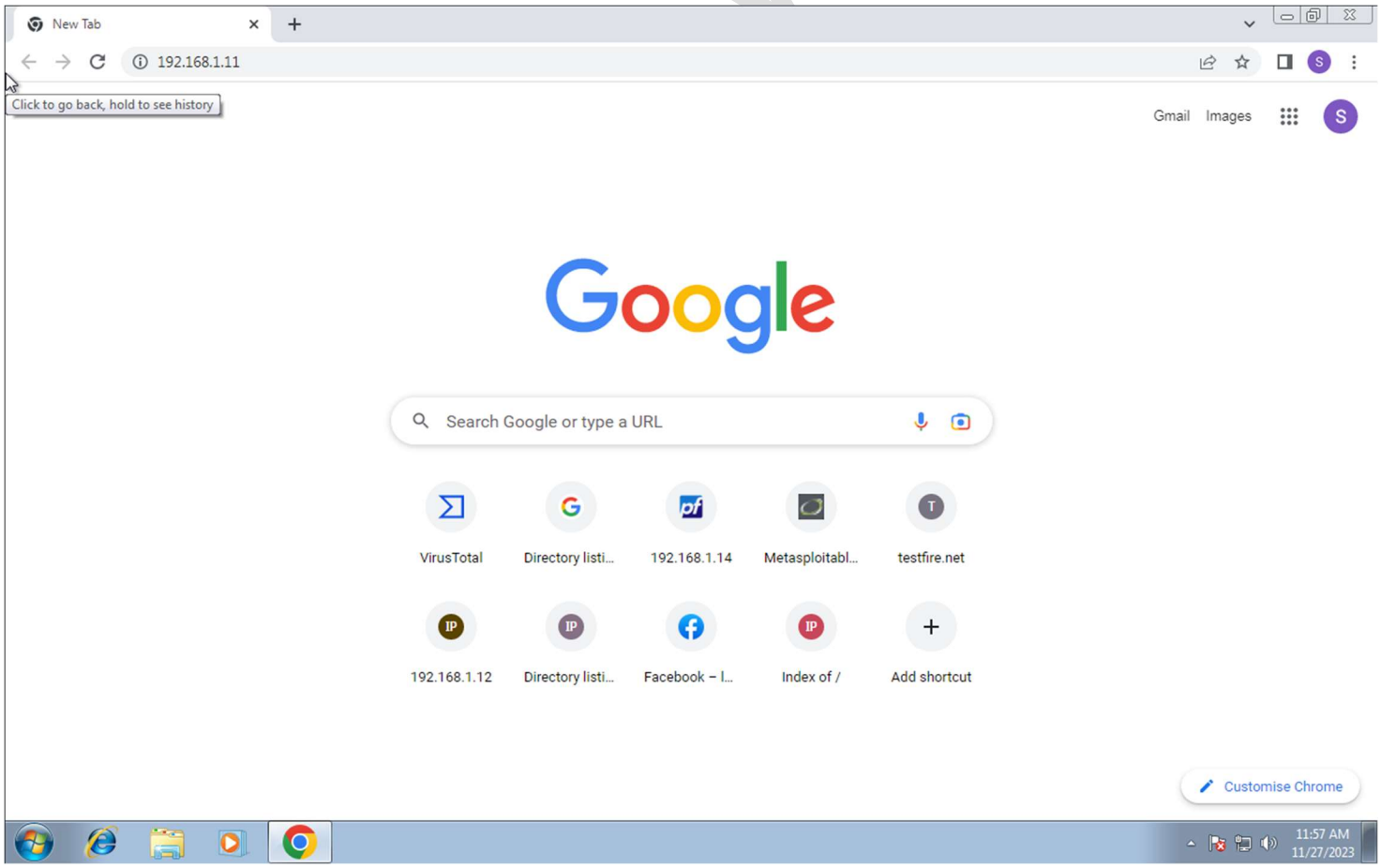
4. Test any website before performing the attack.

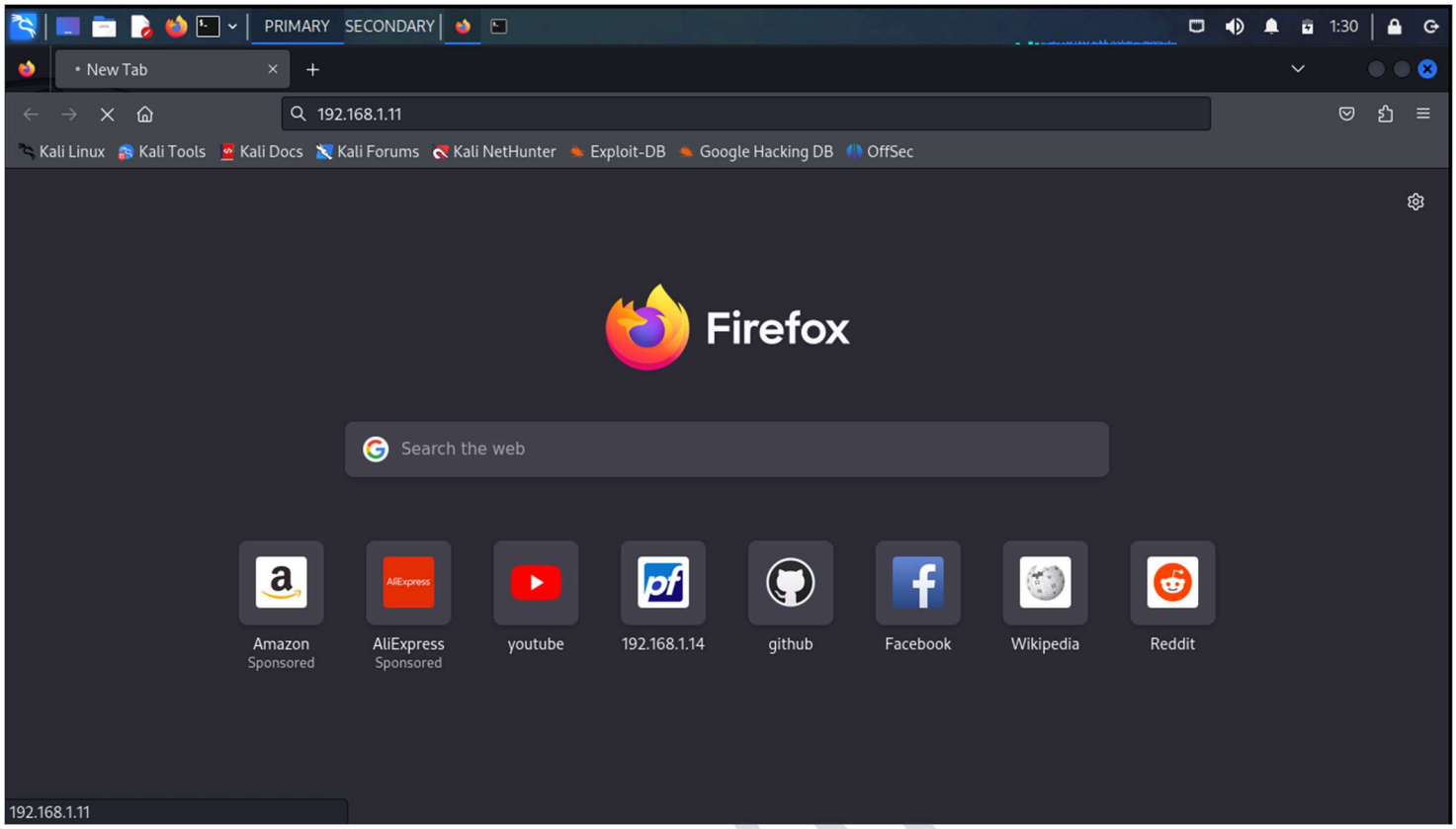


5. Now navigate to the tool's directory and search for the executable script and run the secript by passing the required arguments.



6. Now again test the website after performing the attack and observe the availability of website.





Mitigation and Prevention:

- **Firewalls and Intrusion Prevention Systems (IPS):**
  Filter and monitor traffic to block malicious requests.
- **Content Delivery Networks (CDNs):**
  Distribute website content across multiple servers, dispersing the impact of an attack.
- **Rate Limiting:**
  Imposes restrictions on the number of requests from a single IP address to prevent abuse.
- **Traffic Scrubbing Services:**
  Analyze incoming traffic and filter out malicious packets before reaching the target.
- **Anycast DNS:**
  Distributes DNS requests across multiple servers, improving resilience against attacks.
- **Network Monitoring:**
  Continuous monitoring helps identify abnormal traffic patterns and facilitates early detection.
- **Incident Response Planning:**
  Develop plans to respond quickly to mitigate the impact of an ongoing attack.