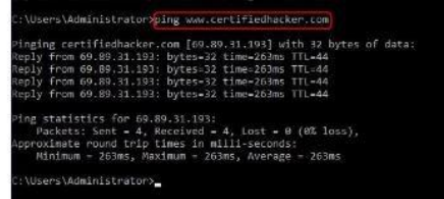
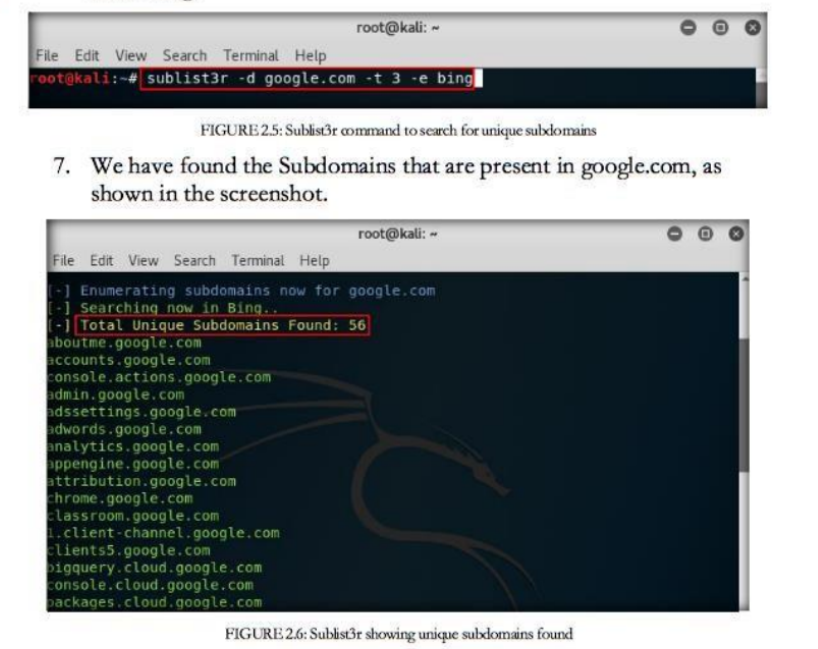
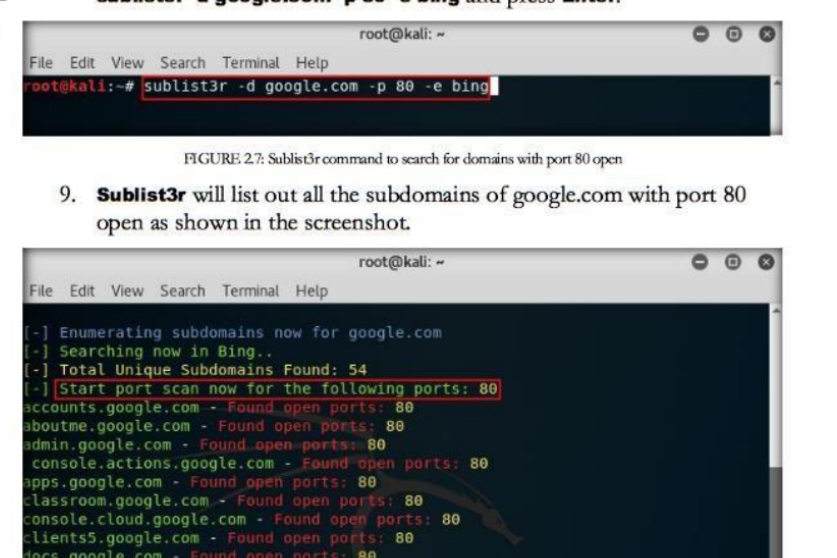
Scanning tool  
**ping**  
**Ping is a network scanning tool that sends an ICMP (Internet Control Message Protocol) echo request to a device and waits for an ICMP echo reply. If a reply is received, it indicates that the device is active and reachable on the network.**

**  
  
Reconasince tool**

**Sublist3r**

**Use for subdomain and check which subdomain is open on specific port no:**

****

****

**Footprinting tool**

**Whois**

**Extract ip address and hostname of the company DNS server.It queries the WHOIS databases.**

**Scanning Tools**

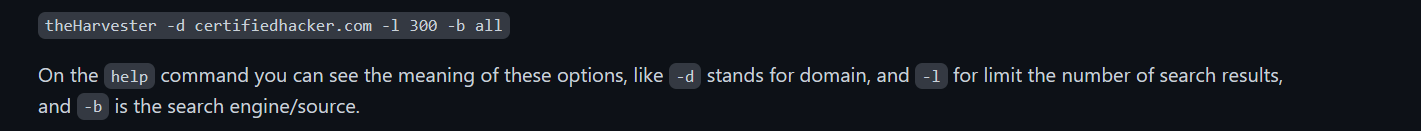
**Nmap**

**nmap is a powerful command-line tool used for network exploration, management, and security auditing. It is widely used by network administrators, security professionals, and system administrators to scan networks, identify hosts, discover services running on those hosts, and detect vulnerabilities.**

**Reconisance tool**

**theHarvester**

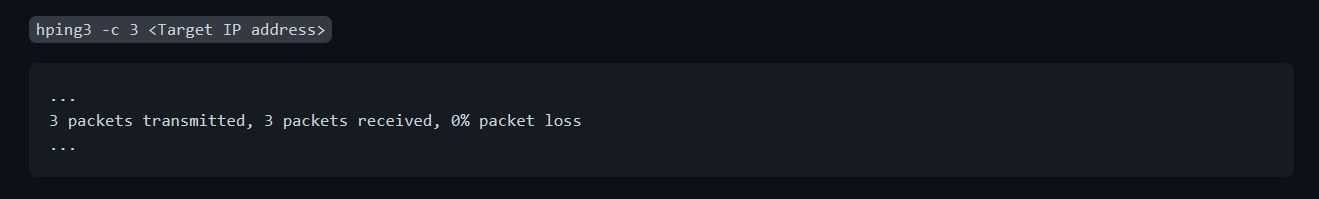
**theHarvester gathers emails, subdomains, hosts, employee names, open ports and banners from different public sources like search engines,**

****

**Scanning Tool**

**Hping3**

**determine all possible open ports, live hosts, and running services.**

****

**Nslookup**

**nslookup can be used to perform a variety of DNS queries, including querying for the IP address of a given domain name, querying for the domain name associated with a given IP address, and querying for information about a specific DNS record type (such as MX records for email servers).**