Objective

The objective of this reconnaissance step was to gather domain-related information, including subdomains, emails, and IP addresses, using theHarvester and Nmap. This helps in understanding the attack surface of the target domain by passively collecting publicly available data.

Tools Used

1. **theHarvester -** A powerful OSINT (Open-Source Intelligence) tool used for gathering domain-related information from multiple public data sources.
2. **Nmap -** A network scanning tool used for mapping networks, discovering hosts, and identifying services, including DNS enumeration.

theHarvester Scan

Command Executed

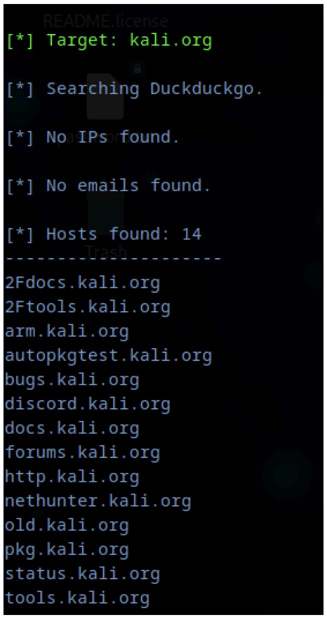
```
theHarvester -d kali.org -l 200 -b duckduckgo
```

Explanation of Parameters

- **`-d kali.org`** → Specifies the target domain (`kali.org`).
- **`-l 200`** → Limits the results to 200 entries.
- **`-b duckduckgo`** → Specifies DuckDuckGo as the search engine for gathering information.

Findings

The scan was successfully executed against `kali.org`, and the following results were obtained:



```
[*] Target: kali.org

[*] Searching Duckduckgo.

[*] No IPs found.

[*] No emails found.

[*] Hosts found: 14
---------------------
2Fdocs.kali.org
2Ftools.kali.org
arm.kali.org
autopkgtest.kali.org
bugs.kali.org
discord.kali.org
docs.kali.org
forums.kali.org
http.kali.org
nethunter.kali.org
old.kali.org
pkg.kali.org
status.kali.org
tools.kali.org
```

Nmap DNS Brute-Force Scan

Command Executed

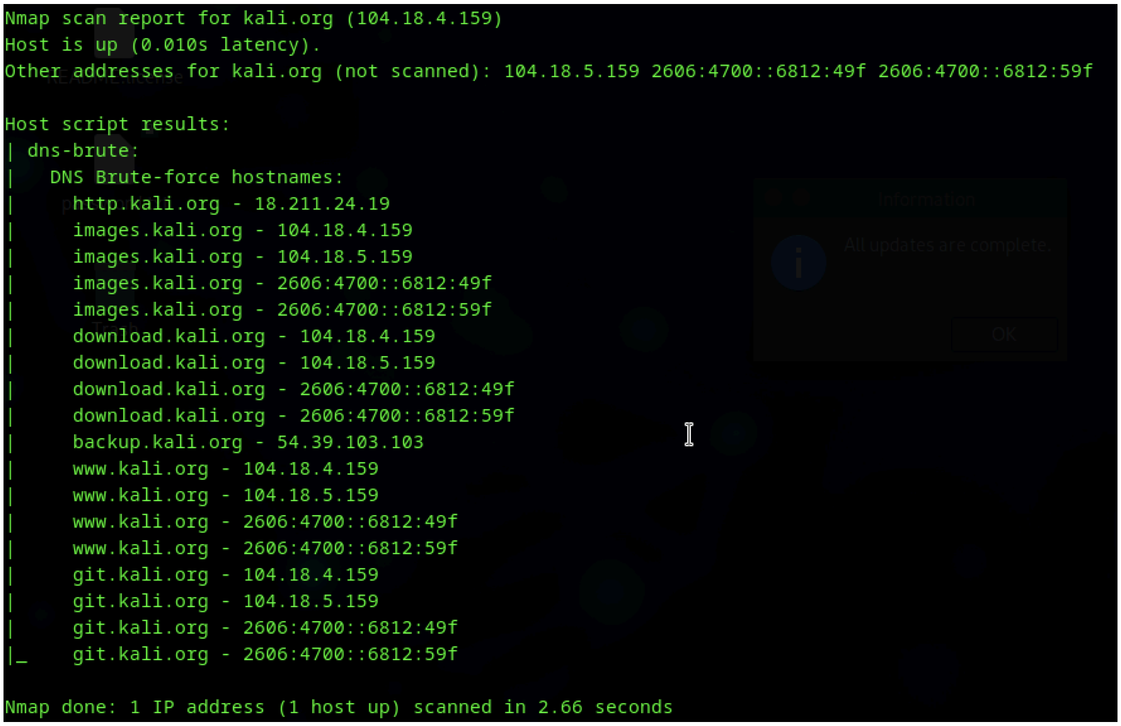
nmap --script=dns-brute -sn kali.org

Explanation of Parameters

- **`--script=dns-brute`** → Uses the `dns-brute` script to brute-force subdomains.
- **`-sn`** → Disables port scanning to focus on host discovery.

Findings

- The scan revealed multiple subdomains associated with `kali.org`:



```
Nmap scan report for kali.org (104.18.4.159)
Host is up (0.010s latency).
Other addresses for kali.org (not scanned): 104.18.5.159 2606:4700::6812:49f 2606:4700::6812:59f

Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|     http.kali.org - 18.211.24.19
|     images.kali.org - 104.18.4.159
|     images.kali.org - 104.18.5.159
|     images.kali.org - 2606:4700::6812:49f
|     images.kali.org - 2606:4700::6812:59f
|     download.kali.org - 104.18.4.159
|     download.kali.org - 104.18.5.159
|     download.kali.org - 2606:4700::6812:49f
|     download.kali.org - 2606:4700::6812:59f
|     backup.kali.org - 54.39.103.103
|     www.kali.org - 104.18.4.159
|     www.kali.org - 104.18.5.159
|     www.kali.org - 2606:4700::6812:49f
|     www.kali.org - 2606:4700::6812:59f
|     git.kali.org - 104.18.4.159
|     git.kali.org - 104.18.5.159
|     git.kali.org - 2606:4700::6812:49f
|_    git.kali.org - 2606:4700::6812:59f

Nmap done: 1 IP address (1 host up) scanned in 2.66 seconds
```

- The scan identified both IPv4 and IPv6 addresses associated with the subdomains.

Analysis

- TheHarvester provided an initial list of subdomains, while the Nmap DNS brute-force scan confirmed and expanded on that list.
- The discovery of multiple subdomains suggests potential attack surfaces that could be further analyzed for vulnerabilities.
- Identifying IP addresses allows for additional reconnaissance steps, such as checking for open ports and running service enumeration scans.

Ethical Considerations

All reconnaissance activities were conducted within ethical boundaries, ensuring compliance with legal and organizational policies. No intrusive scanning or unauthorized access attempts were made during the process.