(/)

Curriculum
Interview Preparation - Algorithms
Average: **95.83%**

Passive Reconnaissance

Introduction:

Passive reconnaissance is an essential phase in the field of cybersecurity, where an attacker gathers information about a target without directly interacting with it. By utilizing various tools and techniques, passive reconnaissance aims to obtain valuable insights into a target's network infrastructure, system architecture, and potential vulnerabilities. This information can then be utilized for further analysis and planning of cyber attacks, or in the case of ethical hacking, to identify and strengthen security weaknesses proactively.

`WHOIS`

`WHOIS` is a protocol used to obtain information about domain names and IP addresses. It provides a database of registered domain names and the contact information of the domain registrant. `WHOIS` can be accessed through public WHOIS servers or using specialized tools, enabling users to gather details such as the domain owner's name, email address, phone number, and registration and expiration dates.

Tools for Passive Reconnaissance

Shodan

`Shodan` is a powerful search engine specifically designed for finding internet-connected devices. It allows users to discover various devices, including servers, routers, webcams, and more, by scanning open ports and analyzing banners and other metadata. `Shodan` provides insights into exposed services, vulnerabilities, and misconfigurations, allowing both attackers and defenders to assess potential security risks.

Subfinder

`Subfinder` is a command-line tool used for passive subdomain discovery. It leverages public DNS data sources and search engines to identify subdomains associated with a target domain. By gathering subdomain information, an attacker can expand their attack surface and potentially discover lesser-known or forgotten subdomains that might have weaker security controls. Example of how to use `Subfinder` (command line): To perform a subdomain enumeration using `Subfinder`, you can execute the following command:

Example:

```
subfinder -d example.com
```

Replace “example.com” with the target domain you want to investigate. Subfinder will query multiple data sources and provide a list of subdomains associated with the target domain.

Recon-ng

`Recon-ng` is a powerful framework designed for conducting reconnaissance and information gathering. It offers a wide range of modules and capabilities, allowing users to perform various tasks, including DNS reconnaissance, OSINT (Open-Source Intelligence) gathering, social media analysis, and more. Recon-ng provides a command-line interface for interacting with its modules and conducting comprehensive reconnaissance operations. Example of how to use Recon-ng (command line): To perform DNS reconnaissance with Recon-ng, follow these steps:

Example: Start Recon-ng by executing the following command:

```
recon-ng
```

- Load the DNS reconnaissance module:

```
modules load recon/domains-hosts/bing_domain_web
```

- Set the target domain:

```
options set SOURCE example.com
run
```

- Recon-ng will use Bing search results to discover subdomains associated with the target domain.

theHarvester (/)

`theHarvester` is a command-line tool used for gathering information about a target domain from various public sources, such as search engines, social networks, and PGP key servers. It collects email addresses, subdomains, virtual hosts, and other relevant information to help identify potential attack vectors or security weaknesses.

Example: To gather email addresses related to a target domain using theHarvester, you can execute the following command:

```
theharvester -d example.com -b google
```

Replace **example.com** with the target domain you want to investigate. theHarvester will query Google and provide a list of email addresses associated with the target domain.