EyeQ Dot Net Pvt. Ltd.

LEARN FROM REAL HACKERS

TASK 3: INFORMATION GATHERING TOOLS

Tools to get the information about the target:

1. Maltego
2. OSINT Framework
3. Recon FTW
4. Recon Ng
5. Spiderfoot
6. Aquatone

Tools Description:

1. Maltego

Maltego is a powerful data mining and link analysis tool used primarily for mapping and analyzing relationships between people, organizations, websites, and social networks. It's popular in cybersecurity and OSINT (Open Source Intelligence) for visually uncovering connections between entities through "transforms"—automated scripts that pull data from sources like social media, DNS records, or WHOIS data. Maltego is highly customizable and supports visual mapping, making it ideal for users who need to explore complex data relationships intuitively.

2. OSINT Framework

The OSINT Framework is a structured collection of resources and tools for gathering publicly accessible information across the internet. It organizes various links and databases for different OSINT categories like social media, geolocation, and domain information, streamlining the process of gathering intelligence. Users benefit from its extensive and categorized layout, which helps them access the most relevant sources efficiently for passive reconnaissance.

3. Recon FTW

Recon FTW is a fully automated reconnaissance tool that uses a variety of open-source tools to collect information on a target. This script automates the process of gathering data by running multiple recon tools and techniques, saving time and improving coverage. Recon FTW is often used for gathering data about domain names, DNS information, and potential vulnerabilities,

making it a valuable tool for penetration testers who want comprehensive reconnaissance with minimal manual effort.

4. Recon-ng

Recon-ng is a web reconnaissance tool designed to gather information from various sources in a modular, scriptable format. Built similarly to the Metasploit Framework, Recon-ng has modules that can be easily added to perform specific data collection tasks, such as retrieving information on IP addresses, domain names, and WHOIS data. Its modular design and automation features make it a favorite among security analysts for detailed data gathering and analysis.

5. SpiderFoot

SpiderFoot is an open-source tool designed for automated OSINT gathering, specifically focused on identifying information related to threat intelligence and security risks. It pulls data from a wide variety of sources, including DNS records, IP addresses, social media, and dark web databases. SpiderFoot's user-friendly interface and customizability make it useful for gathering in-depth insights on potential vulnerabilities and risk factors, valuable for threat intelligence and cybersecurity research.

6. Aquatone

Aquatone is a tool for visually inspecting a website's surface and gathering screenshots of various web applications linked to a target domain. It uses techniques like HTTP probing and screenshot capturing to map subdomains and services, helping to identify potentially vulnerable services visually. Security professionals commonly use Aquatone to quickly assess the attack surface and identify assets needing further analysis, especially in web application security assessments.

Features and Uses:

1. Maltego

Features: Offers data mining and visualization with customizable transforms for mapping complex relationships.

Uses: Ideal for uncovering connections between entities, such as people, organizations, and networks, in investigations.

2. OSINT Framework

Features: A categorized resource of OSINT tools and links across multiple data categories.

Uses: Simplifies public data gathering by providing quick access to resources like social media, geolocation, and web info.

3. Recon FTW

Features: Automated recon tool that integrates multiple data-gathering techniques and tools.

Uses: Performs comprehensive reconnaissance on domains and networks with minimal user input, ideal for quick scans.

4. Recon-ng

Features: Modular and scriptable framework for web-based reconnaissance, similar to Metasploit.

Uses: Gathers data on IPs, domains, and more, making it useful for detailed, customizable web intelligence gathering.

5. SpiderFoot

Features: Automates OSINT collection from diverse sources, focusing on security risks and threat intelligence.

Uses: Useful for uncovering potential vulnerabilities and risk indicators in networks, domains, and IPs.

6. Aquatone

Features: Captures screenshots of websites and services linked to target domains for visual reconnaissance.

Uses: Assesses web application attack surfaces by identifying and mapping subdomains and services visually.

Installation Steps and Commands:

1. Maltego

Installation Steps and Commands:

- Download Maltego from Maltego's official website based on your operating system (Windows, macOS, Linux).
- Run the downloaded installer file and follow the on-screen instructions.
- Linux Command:

```
sudo dpkg -i maltego.deb  # Replace 'maltego.deb' with the actual file name
```

2. OSINT Framework

Installation Steps and Commands:

- OSINT Framework is web-based and does not require installation.
- Access it directly by visiting https://osintframework.com.
- For offline usage, clone the repository using:

```
git clone https://github.com/lockfale/osint-framework.git
```


3. Recon FTW

Installation Steps and Commands:

- Clone the Recon FTW GitHub repository:

```
git clone https://github.com/six2dez/reconftw.git
```

- Move into the `reconftw` directory and execute the installer:

```
cd reconftw
sudo ./install.sh
```

4. Recon-ng

Installation Steps and Commands:

- Install Recon-ng by cloning its GitHub repository:

```
git clone https://github.com/lanmaster53/recon-ng.git
```

- Move into the directory and run the setup:

```
cd recon-ng
sudo pip3 install -r REQUIREMENTS
```

5. SpiderFoot

Installation Steps and Commands:

- Install SpiderFoot by cloning the repository and installing dependencies:

```
git clone https://github.com/smicallef/spiderfoot.git
```

- Navigate into the `spiderfoot` directory and run:

```
cd spiderfoot
sudo pip3 install -r requirements.txt
python3 sf.py
```


6. Aquatone

Installation Steps and Commands:

- Download Aquatone from its GitHub releases page.
- Unzip the downloaded file and move it to a location in your PATH:

```
unzip aquatone_linux_amd64_1.7.0.zip
sudo mv aquatone /usr/local/bin
```

References:

https://chatgpt.com

https://osintframework.com.

https://github.com

https://www.maltego.com

https://www.google.co.in