Module 3

Assignment Solution:

Here's a step-by-step guide for completing Mini Project 1: Reconnaissance and Information Gathering:

Objective: Perform passive footprinting and advanced information gathering on a target website.

Skills Developed: Digital footprint analysis, website reconnaissance, information gathering.

Step 1: Choose a Target Website:

1. Select a website that you have permission to analyze. It could be your own website or a publicly available website. Ensure that you are acting within ethical boundaries.

Step 2: Passive Footprinting:

1. DNS Information:
    - Use the nslookup command in your command prompt to find the target website's DNS information. Run: nslookup targetwebsite.com
    - Note down the IP address and the authoritative DNS servers.
2. Whois Lookup:
    - Perform a Whois lookup using online tools or command-line utilities to gather information about the domain registration. Note down details like domain owner, registration date, and contact information.
3. Web Archive Search:

    - Use tools like the Wayback Machine (archive.org) to view historical snapshots of the website. This might reveal past content, design changes, or information that's no longer available.

Step 3: Advanced Information Gathering:

1. Subdomain Enumeration:
    - Use tools like Sublist3r, Amass, or Subfinder to discover subdomains of the target website. These tools might uncover additional web services or resources.
2. Reverse IP Lookup:
    - Perform a reverse IP lookup using tools like ipinfo.io or online services. This might reveal other websites hosted on the same IP address.
3. SSL Certificate Analysis:
    - Use online SSL certificate analysis tools to gather information about the target website's certificate. Identify the certificate authority, expiration date, and sometimes subdomains.
4. Social Media Analysis:
    - Search social media platforms for official accounts associated with the target website. This can provide insights into the website's branding, updates, and potentially employees associated with it.
5. Google Hacking (Dorking):
    - Use Google advanced search operators ("dorks") to find sensitive information or hidden content on the target website. For example, try searching for site:targetwebsite.com filetype:pdf to find PDF files on the site.
6. Email Harvesting:
    - Search for email addresses associated with the target website. These can be found in contact pages, "About Us" sections, or using tools designed for email harvesting.

Step 4: Compile and Document Findings:

1. Organize the gathered information into categories such as DNS information, Whois data, subdomains, SSL certificate details, etc.
2. Create a report that documents the findings, including screenshots, relevant URLs, and any noteworthy observations.

Step 5: Reflect and Review:

1. Reflect on the information you've gathered and consider the implications. What insights can you gain from this information? How could this information be potentially misused?

Step 6: Ethical Considerations:

1. Ensure that you've only performed these activities on websites for which you have proper authorization.
2. Always respect privacy and data protection laws while gathering information.

Step 7: Presentation (Optional):

1. If required, prepare a presentation or summary of your findings to share with your peers or instructor.