

Experiment No. 4

Aim: Performing reconnaissance and information gathering on a web application.

Learning Objective: To perform reconnaissance and gather information on a web application.

Theory:

Reconnaissance (or "recon") is the foundational, information-gathering phase of any security assessment or attack. The goal is to collect as much data as possible about a target to understand its structure, technology, and potential weaknesses. This phase is analogous to a military scout surveying the landscape before planning an operation; the more you know, the higher your chances of success.

- **Types of Reconnaissance**

- **Passive Reconnaissance:** This involves gathering information from publicly available sources without directly interacting with the target's systems. It's stealthy and legally safe, as it uses resources like search engines, public records, and social media.
- **Active Reconnaissance:** This involves directly probing the target's systems to get a response. This method yields more detailed technical information (like open ports and running services) but is "louder" and can be detected by firewalls and Intrusion Detection Systems (IDS).

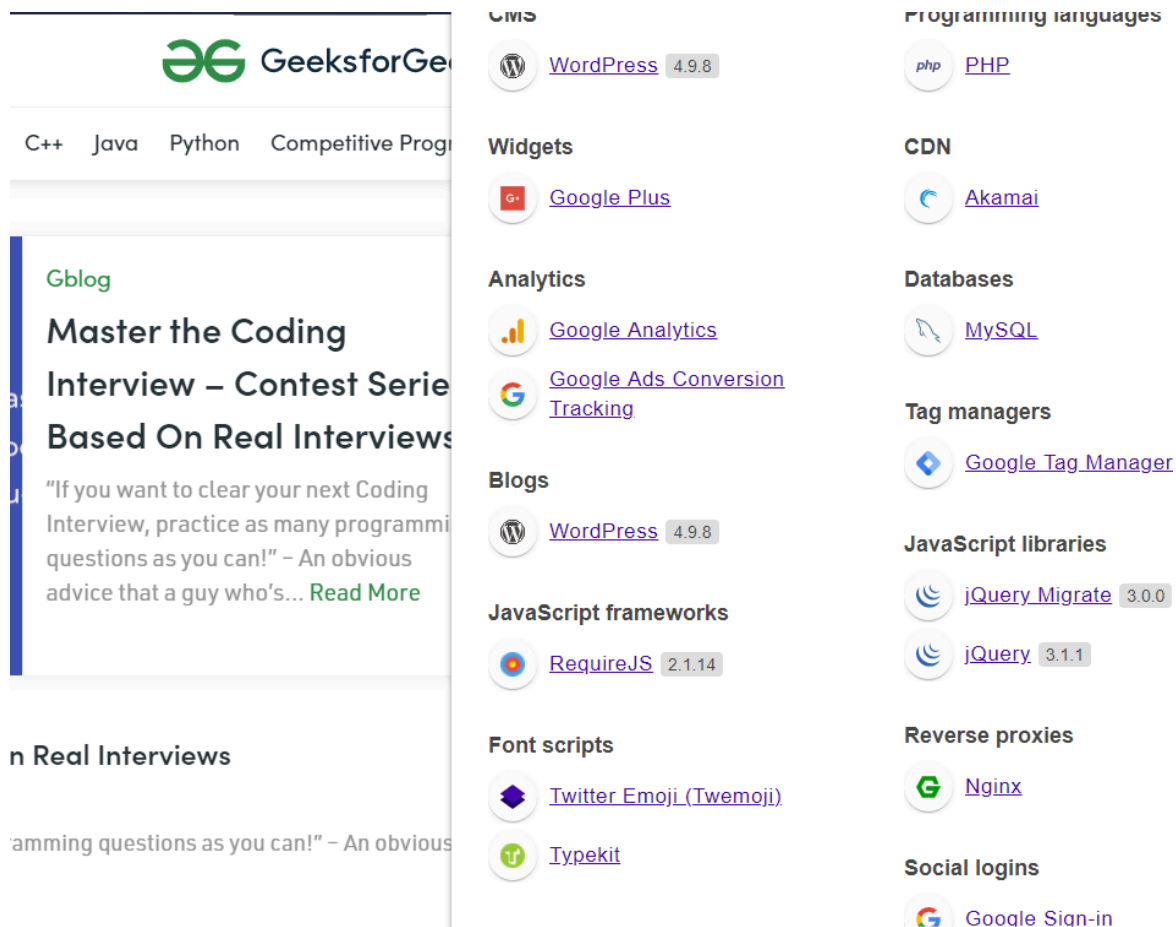
- **Key Information to Gather** The objective is to build a complete profile of the target, including:

- IP addresses and domain ranges.
- Domain registration details ([whois](#)).
- DNS records (MX for mail servers, A for addresses).
- Subdomains (e.g., [api.example.com](#), [dev.example.com](#)).
- Technologies in use (web server, backend language, CMS, frameworks).
- Open ports and running services.

This procedure outlines the steps for conducting both passive and active reconnaissance on a target. **Note: Only perform these steps on applications you have explicit written permission to test.** For this experiment, we'll use [scanme.nmap.org](#) as a safe and legal target.

1. **Perform Initial Passive Reconnaissance** Start by gathering basic domain and DNS information. Use command-line tools like [whois](#) to find registration data and [nslookup](#) or [dig](#) to find the IP address and other DNS records associated with the target domain.
2. **Use Search Engines for Deeper Insights (Google Dorking)** Leverage advanced search engine operators to find information that isn't directly visible on the target's website. Search for specific file types, login pages, or exposed subdomains that may have been indexed by Google.

3. **Discover Subdomains** Expand the attack surface by identifying all subdomains associated with the main domain. Use a combination of online tools like DNSdumpster and command-line tools that automate the discovery process.
4. **Conduct Active Port and Service Scanning** Switch to active reconnaissance by using the network mapping tool **Nmap**. Scan the target's IP address to discover which ports are open and, more importantly, what services and version numbers are running on those ports. ***Image Suggestion:*** A screenshot of the **nmap** command-line output, showing a list of open ports with their corresponding service and version information.
5. **Identify Web Technologies** Analyze the web application itself to identify the technology stack. Use browser extensions like **Wappalyzer** or built-in developer tools (specifically the Network tab) to inspect HTTP headers and source code for clues about the web server, framework, and third-party libraries.



The screenshot displays the Wappalyzer web application interface, which has analyzed the target website (GeeksforGeeks.com) and identified various technologies. The detected technologies are categorized as follows:

- CMS:** WordPress 4.9.8
- Widgets:** Google Plus
- Analytics:** Google Analytics, Google Ads Conversion Tracking
- Blogs:** WordPress 4.9.8
- JavaScript frameworks:** RequireJS 2.1.14
- Font scripts:** Twitter Emoji (Twemoji), Typekit
- Programming languages:** PHP
- CDN:** Akamai
- Databases:** MySQL
- Tag managers:** Google Tag Manager
- JavaScript libraries:** jQuery Migrate 3.0.0, jQuery 3.1.1
- Reverse proxies:** Nginx
- Social logins:** Google Sign-in

Here are the example commands and techniques for the procedure. Replace scanme.nmap.org with your authorized target.

1. Passive Domain and DNS Information

```
1 # Get domain registration information
2 whois scanme.nmap.org
3
4 # Get the IP address and other DNS records
5 nslookup scanme.nmap.org
```

2. Google Dorking Examples

```
1 site:drive.google.com filetype:pdf
2 site:erp.tcetmumbai.in intitle:"admin login"
3 site:erp.tcetmumbai.in inurl:"dashboard"
```

3. Active Port Scanning with Nmap

```
1 # Perform a fast scan for common ports and services
2 nmap -sV -F scanme.nmap.org
```

4. Web Technology Identification

```
1 # Request headers from the server
2 curl -I http://scanme.nmap.org
```

Learning Outcome: Upon completing this experiment, you will understand the principles of reconnaissance and its critical role as the first phase of an ethical hacking engagement. You will also gain practical experience using various tools and techniques to gather technical and infrastructure-related information about a target web application from public and direct sources.

Conclusion:

.....
.....
.....



TCET
BE COMPUTER SCIENCE & ENGINEERING (CYBER SECURITY)
Choice Based Credit Grading System (CBCGS)
Under TCET Autonomy



Name:

Class: BE-CSE

Roll No.:

For Faculty Use

Correction Parameters	Formative Assessment [40%]	Timely completion of Practical [40%]	Attendance / Learning Attitude [20%]	
Marks Obtained				