A purple triangle with a white tree and a red circle

Description automatically generated

**UNIVERSITI MALAYSIA TERENGGANU**

**SEMESTER 1 2023/2024**

**CYBER SECURITY CSF3233**

**LAB 7**

**PREPARED FOR:**

**MUHAMMAD ABDUL AALIM AHMAD ROSLI**

**PREPARED BY:**

**ARUN MUGILAN A/L SARGUNAN S63746**

REFLECTION QUESTIONS

1. Why do we need to information gathering before we can proceed with testing a website?

* To understand the website's structure and components.
* Identify specific elements for testing.
* Assess risks and weaknesses.
* Customize testing approaches.

1. What are the common vulnerabilities of a website?

* SQL Injection
* Cross-Site Scripting (XSS)
* Security Misconfigurations
* Broken Authentication
* Insecure Direct Object References (IDOR)
* Server-Side Request Forgery (SSRF)

1. List tools that we can use for information gathering of a website.

* Whois
* Nslookup/Dig
* Sublist3r
* TheHarvester
* Shodan
* Maltego
* Google Dorks
* Wayback Machine

1. Why does some whois information is not available to the public?

* Privacy Protection Services
* Legal and Policy Restrictions

1. What tools we can use to scan a subdomain of a website domain?

* Sublist3r
* Amass
* DNSDumpster
* Subfinder
* OWASP Amass
* Nmap

**Task 1 : Exploring Vulnerable Websites in Metasploitable**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

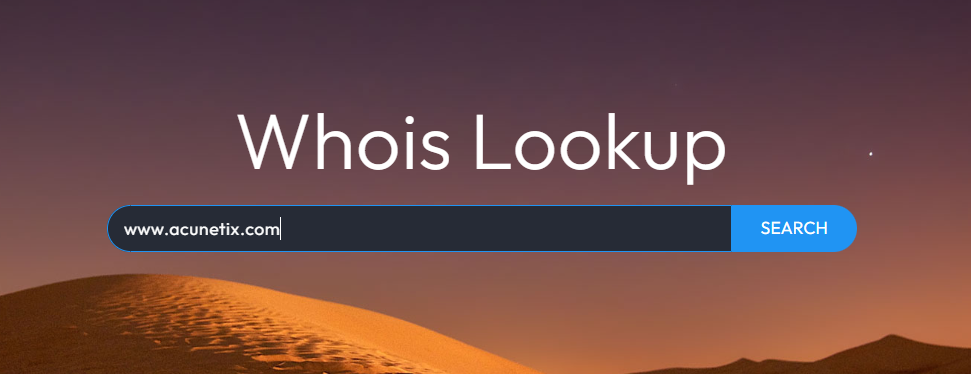
A screenshot of a computer

Description automatically generated

A screenshot of a security system

Description automatically generated

**Task 2 : Information Gathering of a Website**



A screenshot of a computer

Description automatically generated

www.netflix.com

A screenshot of a computer

Description automatically generated

Couldn’t find 3 websites sir the free trial ran out.

A screenshot of a web page

Description automatically generated

Acunetix in Netcraft

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

**Name.com**

A screenshot of a computer

Description automatically generatedA screenshot of a graph

Description automatically generated

**Domain.com**

A screenshot of a computer

Description automatically generatedA screenshot of a web page

Description automatically generated

**Hostinger.com**

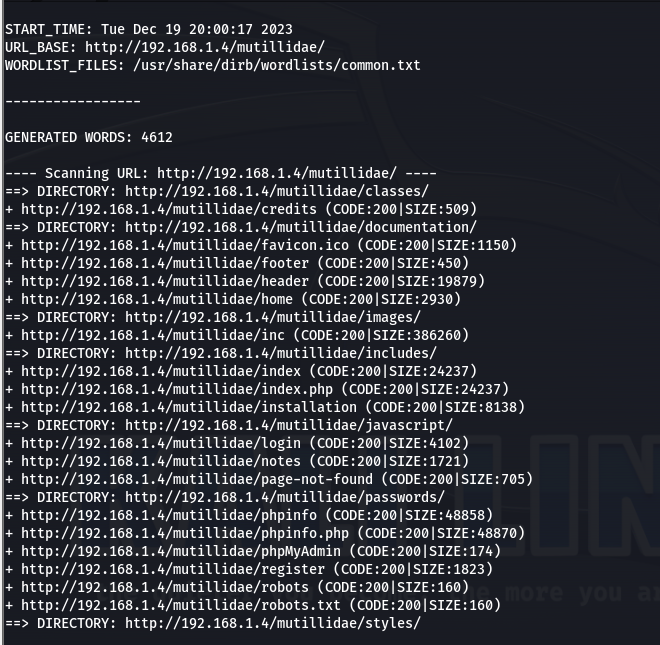
A screenshot of a computer

Description automatically generated

A screenshot of a graph

Description automatically generated

**Task 3 : Scanning Content of a Website**



4. a) When is the built date? **Jan 6 2010**

b) What is the version of PHP used by the Mutillidae wesite? **PHP version 5.2.4-2ubuntu5.10**

c) What is the database server used by the Mutillidae website?

Robots.txt

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated