**Day 5 –**

**Subdomain Enumeration & Identifying Firewalls**

**Subdomain Enumeration**

**What is a Subdomain?**

A subdomain is a subset of a larger domain that is used to organize or navigate to different sections of a website. For example, in 'blog.example.com', 'blog' is the subdomain of 'example.com'. Subdomains can host separate services such as mail servers, apps, or admin panels. They can also reveal hidden or less-secure parts of a website.

**Definition of Subdomain Enumeration**

Subdomain enumeration is the process of identifying valid subdomains associated with a main domain. It is a crucial step in the reconnaissance phase of ethical hacking and penetration testing. Finding subdomains can uncover additional attack surfaces that are not visible on the main site, such as development environments, old versions of websites, or admin interfaces.

**Tools for Subdomain Enumeration**

**Subfinder**

Subfinder is a fast and reliable subdomain discovery tool written in Go. It uses passive online sources to find subdomains for a given domain.  
Example command:  
`subfinder -d org.com`

**Subdomain Finder (Web Tool)**

An alternative tool is the web-based subdomain finder available at:  
https://subdomainfinder.c99.nl  
This tool allows users to perform subdomain lookups directly through a browser interface without needing command-line tools.

**Identifying Firewalls**

**What is a Firewall?**

A firewall is a network security system that monitors and controls incoming and outgoing network traffic. It acts as a barrier between a trusted internal network and untrusted external networks (like the internet). Firewalls are used to prevent unauthorized access and filter harmful traffic based on predefined security rules.

**Tool for Firewall Detection**

**wafw00f**

wafw00f is a tool used to detect and fingerprint Web Application Firewalls (WAFs) protecting web applications. It helps penetration testers understand the defenses in place.  
  
Basic usage:  
`wafw00f https://org.com`  
  
If the above command doesn’t work, try running with elevated privileges:  
`sudo wafw00f https://org.com`  
  
Note: This tool may work effectively for some organizations but not for all, as WAF configurations vary widely.

**Conclusion**

Subdomain enumeration is essential in reconnaissance to uncover hidden web assets. Tools like Subfinder and online lookup platforms help streamline the process. Identifying firewalls using wafw00f can reveal the presence and type of protective layers on a domain, although detection may not be universal due to different configurations. Both techniques are foundational in ethical hacking for mapping the target surface effectively.