# 🛡️ Day 7 – Ethical Hacking Journey

## 📂 Topic: Directory Bruteforcing

## 🔍 What is a Directory in Web Applications?

In web applications, a directory is a logical folder on a server that stores files, scripts, or other folders. Just like folders on your computer, directories can hold:  
- Configuration files  
- Web pages (e.g., index.html)  
- Admin panels  
- Sensitive backups  
  
Sometimes these directories are hidden or unlinked from the main website, meaning they cannot be discovered just by navigating through the UI. These hidden directories might contain sensitive or exploitable data, so discovering them can be crucial during penetration testing.

## 🛠️ Practical: Directory Bruteforcing

✅ Step 1: Launching the Target

We used TryHackMe and started the "Vulnversity" machine, which is a beginner-friendly vulnerable box.  
Once started, we copied the IP address of the target machine, e.g., http://10.10.188.89

## 🚀 Tool 1: Gobuster for HTTP URLs

Gobuster is a tool for brute-forcing directories on websites. It’s fast and simple to use.

🔹 Command:

gobuster dir -u http://10.10.188.89 -w /usr/share/seclists/Discovery/Web-Content/common.txt

⚠️ Note: If the path does not work, use:

ls /usr/share/seclists/Discovery/Web-Content/  
or install via:  
sudo apt install seclists

🔍 Explanation of Command Flags:

|  |  |
| --- | --- |
| Flag | Description |
| dir | Directory brute-force mode |
| -u | Target URL |
| -w | Path to the wordlist |

## 📄 Interpreting Gobuster Output

Example Output:

/.htaccess (Status: 403)  
/.hta (Status: 403)  
/admin (Status: 301)  
/uploads (Status: 301)

📘 Explanation of Status Codes:

|  |  |
| --- | --- |
| Status Code | Meaning |
| 403 | Forbidden – Exists but access denied |
| 301 | Moved Permanently – Exists and is accessible |

## 🔐 Gobuster HTTPS Limitation

Gobuster may not work well with HTTPS URLs. It can fail due to SSL/TLS handling issues.

## 🚀 Tool 2: Feroxbuster for HTTPS Support

Feroxbuster handles HTTPS effectively and provides deeper scanning.

🔹 Command:

feroxbuster --url https://10.10.188.89 -w /usr/share/seclists/Discovery/Web-Content/common.txt

✅ Why Feroxbuster:

• Supports HTTPS without issues

• Handles recursion and redirects

• Faster and multithreaded

## 📂 Finding the Wordlist Path

Commands to locate wordlist:

ls /usr/share/wordlists/  
ls /usr/share/seclists/Discovery/Web-Content/  
sudo find / -name "common.txt" 2>/dev/null

## 🧠 Summary: Key Tool Differences

|  |  |  |  |
| --- | --- | --- | --- |
| Tool | Protocol | Usage Purpose | Wordlist Example |
| Gobuster | HTTP | Fast directory brute-forcing | /usr/share/seclists/Discovery/Web-Content/common.txt |
| Feroxbuster | HTTPS | TLS-supported and recursive scan | /usr/share/seclists/Discovery/Web-Content/common.txt |

## 📁 Example Valid Paths Found

/admin (Status: 301)  
/backup (Status: 301)  
/css (Status: 301)  
/.htaccess (Status: 403)  
/.hta (Status: 403)

Visit:  
http://10.10.188.89/admin  
http://10.10.188.89/backup