

# Step 1: Set Up Environment

- **Install necessary software on Kali Linux:**

Ensure your Kali Linux environment is ready by installing essential tools such as Nmap, Gobuster, Hydra, and Metasploit.

- **Commands to Install:** ```bash sudo apt update  
sudo apt install -y nmap gobuster hydra  
metasploit-framework ```



Photo by Michael Geiger on Unsplash

## Step 2: Network Scanning

- **Objective:** Identify the target's open ports and services.
- **Tools: Nmap:** Utilize Nmap to scan the target for open ports and services.
- **Commands:** ```bash nmap -sS -sV -O 192.168.1.226 ```

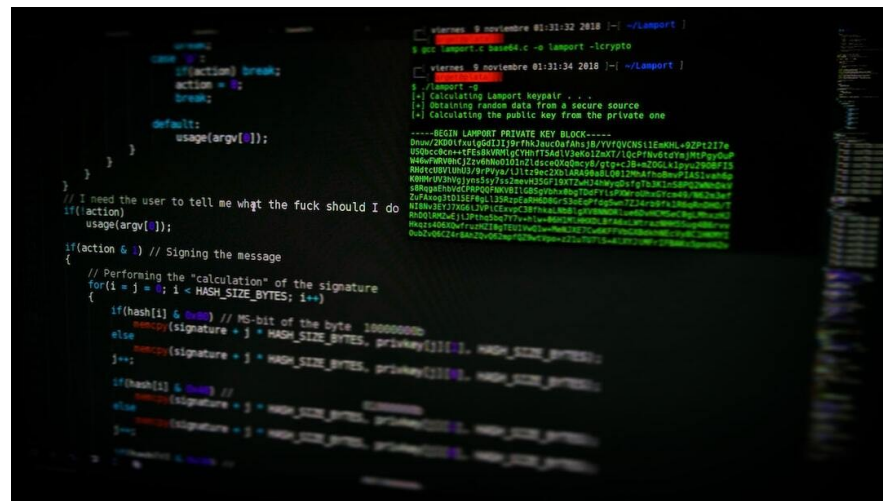


Photo by Arget on Unsplash

# Step 3: Enumeration

- **Objective:** Gather detailed information about the target's web applications and technologies.
- **Tools: Gobuster, Wappalyzer:** Utilize Gobuster and Wappalyzer for directory enumeration and identifying web technologies.
- **Commands:** `bash gobuster dir -u http://192.168.1.226 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt`
- **Wappalyzer:** Use Wappalyzer browser extension to identify web technologies used by the target site.

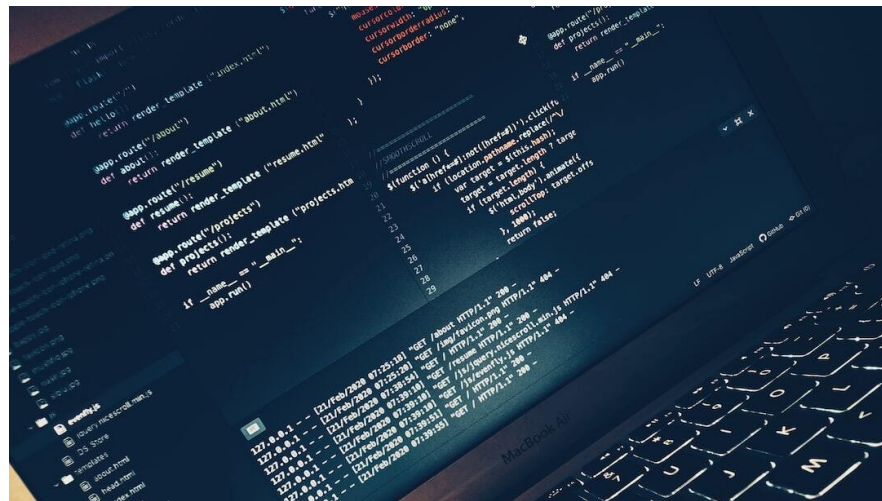


Photo by Muhammed suhail ek on Unsplash

## Step 4: Vulnerabilities

- **Objective:** Identify vulnerabilities in the target's web applications and services.
- **Tools: Nmap, Nikto:** Utilize Nmap and Nikto for vulnerability scanning.
- **Commands:** `bash nmap --script vuln 192.168.1.226 nikto -h http://192.168.1.226`



Photo by Mar Linares on Unsplash

## Step 5: Brute-force

- **Objective:** Gain access to the target by brute-forcing login credentials.
- **Tools: Hydra:** Utilize Hydra for brute-force attacks.
- **Commands:** ```bash hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.1.226 http-post-form "/wp-login.php:log=^USER^&pwd=^PASS^:Invalid username" ```

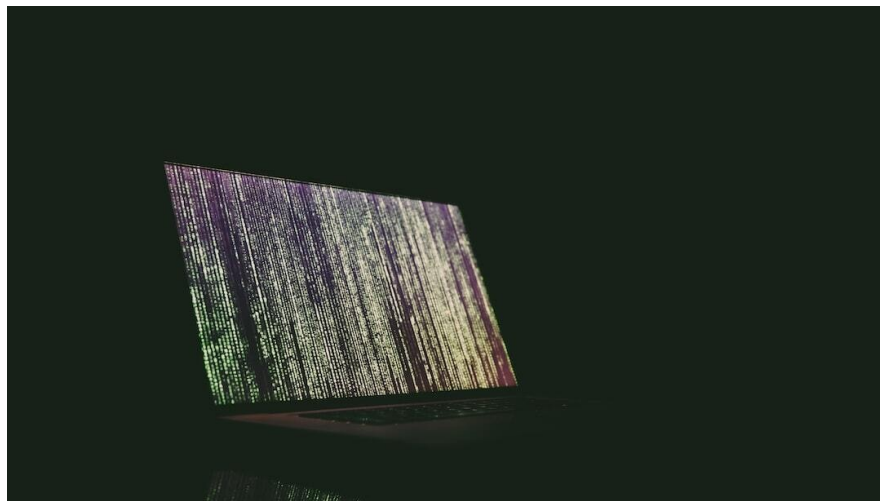


Photo by Markus Spiske on Unsplash

# Step 6: Reverse Shell

- **Objective:** Gain remote access to the target system.
- **Tools: PHP Reverse Shell, Metasploit:** Utilize a crafted PHP reverse shell and Metasploit to exploit vulnerabilities and gain access.
- **Techniques and Commands:** - Crafting a PHP reverse shell - Using Metasploit to exploit vulnerabilities and gain access

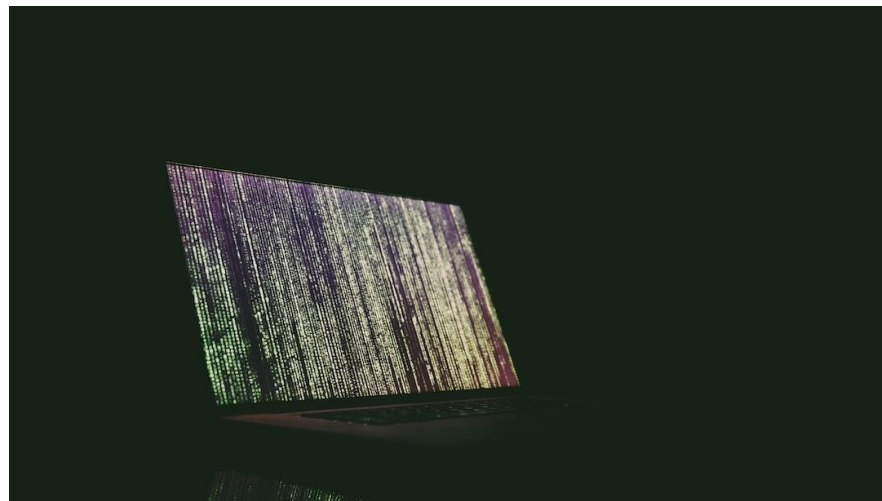


Photo by Markus Spiske on Unsplash

# Conclusion

- **Recap:** Reviewed the steps: Setup, Scanning, Enumeration, Identifying Vulnerabilities, Bruteforce, and Reverse Shell.
- **Importance of Ethical Hacking:** Emphasizes the significance of ethical hacking in improving security and protecting systems.
- **Practice Responsibly:** Encourages responsible practice and continuous learning in the field of cybersecurity.



Photo by Hacker Noon on Unsplash