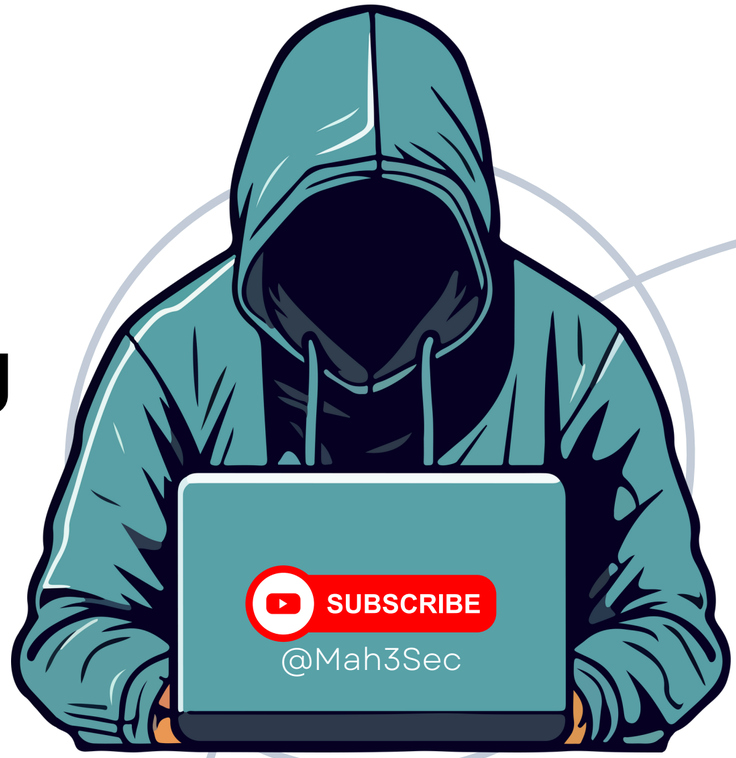
HackLab 101:
The Quick Guide to Setting Up Your Pentest Space



How to setup VM

Step 1: Download and Install Virtualization Software

- For Windows, download and install either VirtualBox or VMware Workstation. You can find VirtualBox at virtualbox.org and VMware Workstation at vmware.com.

Step 2: Download Pre-built Kali Linux Virtual Machine

- Visit the official Kali Linux website at kali.org.
- Download the pre-built Kali Linux Virtual Machine image specifically designed for VMware or VirtualBox.

Note: Pre-built images come with default credentials. The username is "kali," and the password is also "kali."

Step 3: Launch Virtualization Software

- Open VirtualBox or VMware Workstation on your Windows machine.

Step 4: Import Kali Linux VM Image

- In VirtualBox, click on "File" > "Import Appliance" and select the downloaded Kali Linux OVA file.
- In VMware Workstation, click on "File" > "Open" and choose the Kali Linux VMX file.

Step 5: Start the Kali Linux VM

- Power on the imported Kali Linux virtual machine.

Step 6: Update and Upgrade

- Once Kali Linux is running, open a terminal and run sudo apt update && sudo apt upgrade to ensure your system is up to date.

Step 7: Run PimpMyKali Script (Optional)

- Check and run the PimpMyKali script from its GitHub repository to enhance your Kali Linux environment. You can find the script at github.com/Dewalt-arch/pimpmykali.
- Follow the instructions provided with the script for setup or issue resolution.

Subdomain Enumeration Tools

Subfinder

Installation:

1. Install Go on your system if you haven't already. Follow the official Go installation guide.
2. Clone the Subfinder repository and build it:

go get -v github.com/projectdiscovery/subfinder/v2/cmd/subfinder

Usage:

1. To enumerate subdomains for a target domain (e.g., example.com):

subfinder -d example.com

Amass:

Installation:

1. Install Go on your system if you haven't already. Follow the official Go installation guide.
2. Clone the Amass repository and build it:

go get -v github.com/OWASP/Amass/v3/...

Usage:

1. To enumerate subdomains for a target domain (e.g., example.com):

amass enum -d example.com

Subdomain Enumeration Tools

Assetfinder

Installation:

1. Install Node.js on your system if you haven't already. Follow the official Node.js installation guide.
2. Install Assetfinder using npm:

npm install -g assetfinder

Usage:

To enumerate subdomains for a target domain (e.g., example.com):

assetfinder example.com

Additional Tips:

- **Wordlists:** You can enhance subdomain discovery by using custom wordlists with these tools. Both tools allow you to specify a wordlist using flags.
- **Output:** Amass and Assetfinder provide options to save the results to a file for further analysis.

Subdomain Enumeration Tools

httpx:

Description:

httpx is a powerful reconnaissance tool designed for probing and interacting with web applications. It helps identify live hosts, collect information about web servers, and discover potential vulnerabilities or misconfigurations.

Installation:

- Using pip: **pip3 install httpx**
- Using apt (for Debian/Ubuntu): **sudo apt-get install python3-httpx**
- Using git clone

Using httpx with Subfinder:

1. Run Subfinder to Enumerate Subdomains: subfinder -d example.com -o subfinder_output.txt
2. Use httpx to Probe Live Hosts: cat subfinder_output.txt | httpx -title -status-code -content-length

Subdomain Enumeration Tools

Using httpx with Amass:

1. Run Amass to Enumerate Subdomains: **amass enum -d example.com -o amass_output.txt**
2. Use httpx to Probe Live Hosts: **cat amass_output.txt | httpx -title -status-code -content-length**

Using httpx with Assetfinder:

1. Run Assetfinder to Enumerate Subdomains: **assetfinder example.com > assetfinder_output.txt**
2. Use httpx to Probe Live Hosts: **cat assetfinder_output.txt | httpx -title -status-code -content-length**

Additional Tips:

- Customizing httpx Output:
  - You can customize the httpx command to include specific information. For example, -title displays the page title, -status-code shows the HTTP status code, and -content-length displays the content length.
- Combining Tools:
  - You can chain these commands together to create powerful reconnaissance pipelines. For instance, combining subdomain enumeration with live host probing using httpx provides a more comprehensive view of the target's web infrastructure.