VM Installation, Linux, and Browser Extensions Usage Guide

Virtual Machine (VM) Installation & Linux

Need: A VM provides an isolated environment for testing tools and penetration activities without harming the host system.
Usage: Run Linux distributions such as Kali/Ubuntu inside VirtualBox or VMware.
Steps: 1. Download and install VirtualBox or VMware Workstation. 2. Download a Linux ISO (Kali Linux recommended for pentesting). 3. Create a new VM and allocate RAM (2–4GB) and disk space (20GB+). 4. Attach ISO and start the VM. 5. Complete Linux installation and update system packages.

FoxyProxy Standard

Need: Easily switch between multiple proxy servers for anonymity and testing.
Usage: Manage and configure proxy settings in browsers.
Steps: 1. Install FoxyProxy Standard from Chrome/Firefox Web Store. 2. Add new proxy details (IP, port, protocol). 3. Enable the proxy for browsing through it. 4. Toggle between proxies quickly.

Wappalyzer

Need: Identify technologies used by a website (CMS, frameworks, databases).
Usage: Helpful in reconnaissance for ethical hacking.
Steps: 1. Install Wappalyzer extension. 2. Visit any website and click on the Wappalyzer icon. 3. View detected technologies (e.g., WordPress, Apache, jQuery).

DotGit

Need: Checks if a website has exposed .git repositories.
Usage: Find sensitive source code leaks.
Steps: 1. Install DotGit extension. 2. Visit a target website. 3. Extension automatically detects exposed .git directories.

Gopher

Need: Convert text into URL-encoded payloads for testing vulnerabilities.
Usage: Useful in SSRF and injection attacks.
Steps: 1. Install Gopher extension. 2. Input text or payload. 3. Copy generated encoded URL for testing.

Knoxss

Need: Automated XSS vulnerability scanner.
Usage: Detects XSS payload injection points.
Steps: 1. Install Knoxss browser extension. 2. Open the target website. 3. Run Knoxss scan to detect potential XSS vulnerabilities.

Cookie-Editor

Need: View, edit, add, or delete browser cookies.
Usage: Test cookie-based authentication/session management.
Steps: 1. Install Cookie-Editor. 2. Open it on any site to view cookies. 3. Modify cookies for session hijacking tests.

JsonWebView

Need: Beautify and view JSON responses.
Usage: Useful for API response analysis.
Steps: 1. Install JsonWebView. 2. Open JSON endpoints in browser. 3. View formatted JSON for analysis.

HackBar

Need: Manual testing of SQLi, XSS, and other web attacks.
Usage: Inject payloads into requests directly from browser.
Steps: 1. Install HackBar extension. 2. Enable HackBar on target site. 3. Test payloads (SQLi, XSS, LFI, etc.).

Hunter.io

Need: Find email addresses associated with domains.
Usage: Email OSINT for penetration testing.
Steps: 1. Sign up on Hunter.io. 2. Install extension. 3. Visit domain → extension shows email addresses.

Trufflehog

Need: Detects secrets (API keys, credentials) in repositories.
Usage: Prevent secret leaks in codebases.
Steps: 1. Clone repository or visit site with extension. 2. Run Trufflehog scan. 3. Identify exposed keys/secrets.

Shodan

Need: Search engine for internet-connected devices.
Usage: Identify open ports, services, and vulnerabilities.
Steps: 1. Create Shodan account. 2. Install Shodan extension. 3. Search for IP, domain, or service.

TouchVPN

Need: Secure browsing with VPN tunneling.
Usage: Hide IP and bypass geo-restrictions.
Steps: 1. Install TouchVPN. 2. Connect to desired country server. 3. Browse securely.

User-Agent Switcher

Need: Change browser User-Agent headers.

Usage: Evade restrictions, test web app responses.
Steps: 1. Install User-Agent Switcher. 2. Select desired browser/device agent. 3. Reload site to see changes.

Live HTTP Headers

Need: View live HTTP/HTTPS request headers.
Usage: Analyze request/response details for security testing.
Steps: 1. Install Live HTTP Headers. 2. Open site and capture requests. 3. Inspect headers for sensitive info.

Retire.js

Need: Detect vulnerable JavaScript libraries.
Usage: Helps in identifying outdated libraries in web apps.
Steps: 1. Install Retire.js extension. 2. Visit target site. 3. Extension highlights vulnerable JS libraries.

BuiltWith

Need: Provides detailed insights about website technologies.
Usage: Used for reconnaissance and competitive analysis.
Steps: 1. Install BuiltWith extension. 2. Visit any site and click extension icon. 3. View full technology stack details.

Managing Extensions in Kali Linux VM

Need: Running security-related extensions inside a Kali Linux virtual machine ensures that your main host system stays safe and isolated from potentially malicious web activity. Extensions can interact with network traffic and browser storage, so isolation is crucial.
Usage: Install, enable, disable, and configure penetration testing browser extensions inside the VM without affecting the host operating system.
Steps: 1. Open Firefox/Chromium inside your Kali VM. 2. Navigate to the Add-ons Manager (Menu → Add-ons and Themes → Extensions). 3. Search for the extension (e.g., Wappalyzer, FoxyProxy) and install it. 4. After installation, manage permissions and enable/disable extensions as required. 5. Use the extensions sidebar (puzzle icon in the browser toolbar) to quickly access installed tools. 6. Keep your extensions updated for security patches. 7. Use them only within the VM to minimize risks to your host system.