|  |  |
| --- | --- |
| Une image contenant capture d’écran, Graphique, cercle, technologie  Le contenu généré par l’IA peut être incorrect. | Fiche n° 1  Installation de l’environnement cyber |

* Machine virtuelle : Ubuntu 24.04 (with Rosetta)
  1. Clavier et langue
  2. Activer le compte root
  3. Mise à jour
  4. Modifier l’espace disque 300 go
  5. Installer gparter pour la gestion des partitions du disque
  6. Modifier sudo visudo pour ne plus saisir le mot de passe
     1. Dans le terminal

sudo visudo

à la igne %sudo mettre ALL=(ALL:ALL) NOPASSWD: ALL

* Installation de Docker
  1. Site : <https://docs.docker.com/engine/install/ubuntu/>
  2. Donnée les droits sudo à docker
     1. Commande à saisir dans le terminal

curl -fsSL "https://get.docker.com/" | sh

sudo usermod -aG docker $(id -u -n)

newgrp docker

* Installation de DVWA
  1. Commande à saisir dans le terminal
     1. git clone <https://github.com/digininja/DVWA.git>
     2. cd DVWA
     3. docker compose up -d
* Installation de EXEGOL
  1. Site : <https://exegol.readthedocs.io/en/latest/getting-started/install.html>
* Installation des Addons pour FireFox
  1. FoxyProxy
  2. Cookie-Editor
  3. Multi-Account containers
* Matériels à installer
  1. Clé bluetooth UD100
  2. Clé Wifi BrosTrend AC1200
     1. Dans le terminal

sh -c 'wget deb.trendtechcn.com/install -O /tmp/install && sh /tmp/install'

* Logiciels cyber
  1. Sublime texte : sudo snap install sublime-text --classic
  2. Nmap : sudo apt-get install nmap
  3. Wireshark : sudo apt-get install wireshark
  4. Hydra : sudo apt-get install hydra
  5. Burp Suite :
     1. Site : <https://portswigger.net/burp/documentation/desktop/getting-started/download-and-install>
     2. Configuration de FoxyProxy
        1. Nom : BurpSuite
        2. Type : HTTP
        3. Hostname : 127.0.0.1
        4. Port : 8080
  6. Spiderfoot

Dans le terminal

git clone <https://github.com/smicallef/spiderfoot.git>

cd spiderfoot/

docker compose up -d

* 1. Nessus (voir fiche pour installation) pour lancer dans Firefox : <https://ubuntu-linux-2404:8834/>
  2. SQLMap : sudo apt-get install sqlmap
  3. MySQL : sudo apt-get install mysql-server
  4. Metasploit : script ./metasploit.ssh
  5. DRADIS

Site : <https://docs.vultr.com/how-to-install-ruby-on-ubuntu-24-04>

Site : <https://dradis.com/ce/documentation/install_git.html>

* 1. SYSREPTOR

Site : <https://docs.sysreptor.com/setup/installation/>

Dans le terminal

sudo apt update

sudo apt install -y sed curl openssl uuid-runtime coreutils

bash <(curl -s <https://docs.sysreptor.com/install.sh>)

répondre aux questions dans l’ordre :

* Enter, y, y, y, y, enter, localhost, y, y,
* Copier le username et le password
* Dans le navigateur : <https://localhost:443>
* Saisir username et password et faire skip pour passer la double authentification
  1. Setoolkit

Site : <https://trustedsec.com/resources/tools/the-social-engineer-toolkit-set>

Télécharger le dossier et le dézipper

Dans le terminal

cd social-engineer-toolkit-master

sudo apt install python3-pip

pip3 install -r requirements.txt

sudo python setup.py

passer sous root et taper setoolkit

* 1. Footprinting
     1. Recon-ng

Site : <https://securitytrails.com/blog/recon-ng>

Installation dans exegol

* + 1. TheHarvester

Site : <https://cipherssecurity.com/how-to-install-theharvester-tool/>

Installation dans exegol

* + 1. Reconftw

Site : <https://github.com/six2dez/reconftw>

Installation dans exegol

* + 1. sudo apt install geoip-bin (localisation ip)
    2. sudo apt install sublist3r (scanner les sous-domaines)
    3. sudo apt install nikto (recherche vulnérabilité sur les serveurs web
  1. Spoofing
     1. sudo apt install dsniff (arpspoof)
     2. sudo apt install hping3 (ip)
     3. sudo apt install macchanger (mac adress)