Document d'installation et de reproduction du projet

Installation du système

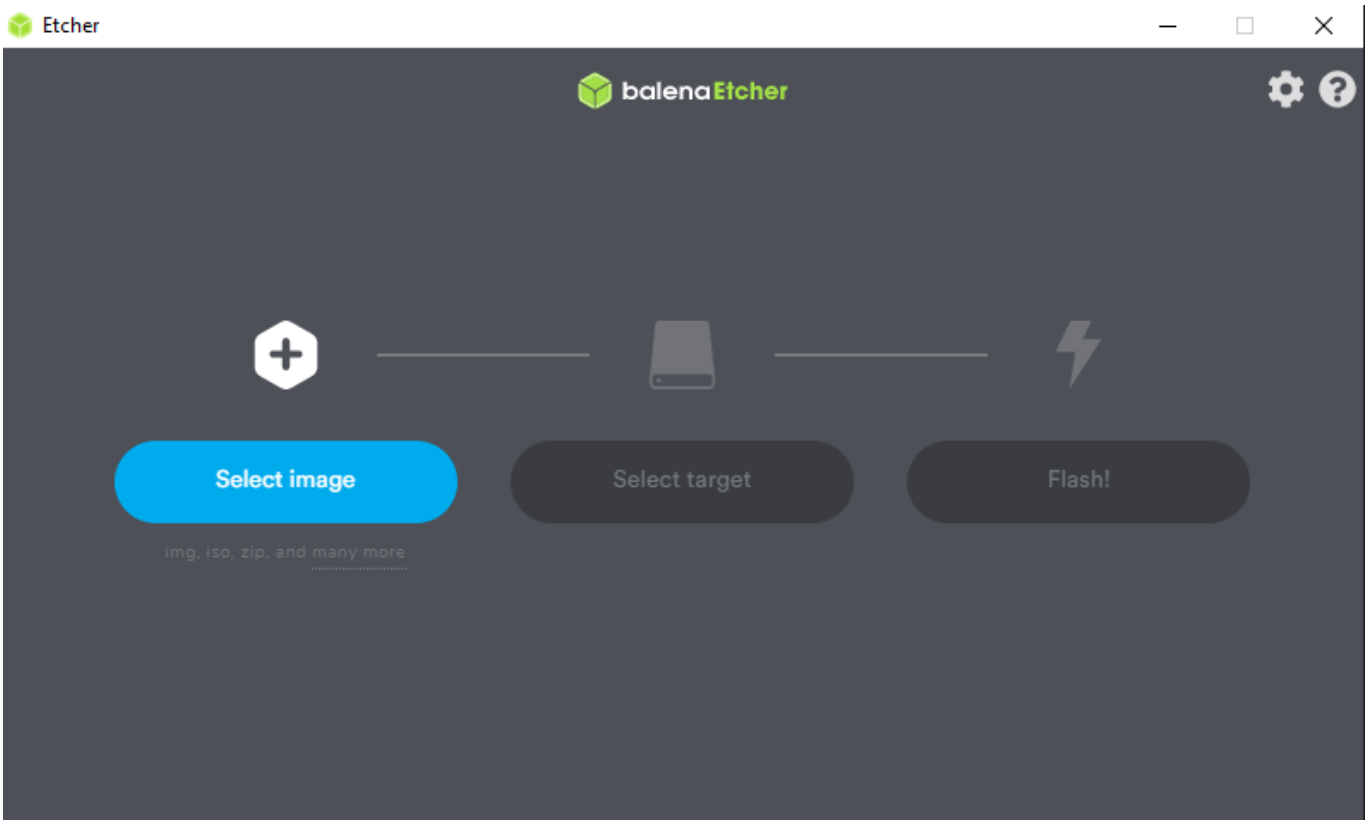
Téléchargement de l'OS

Download - https://www.offensive-security.com/kali-linux-arm-images/

```
Version utilisée : Kali Linux 2020.1a rpi3-nexmon-64
Dernière version en date : Kali Linux 2020.2
```

Flash de la carte sd

Download - https://www.balena.io/etcher/



Configuration du système

Paramètres de langage et du clavier

```
setxkbmap be
dpkg-reconfigure tzdata
dpkg-reconfigure locales
```

Création de l'utilisateur non privilégié

```
adduser <NOM>
```

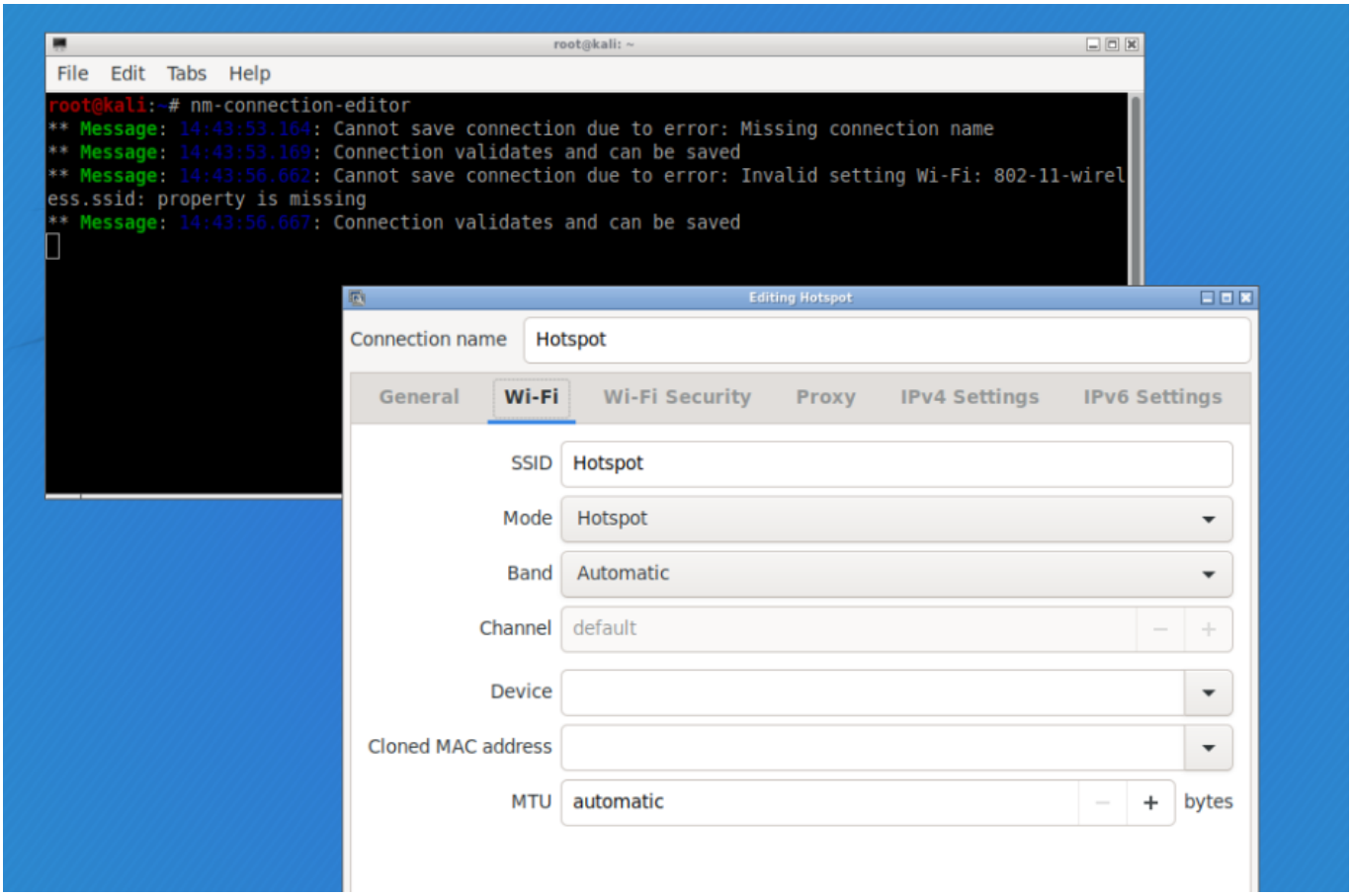
Configuration de l'auto-login

```
nano /etc/lightdm/lightdm.config

uncomment
    autologin-user=<NOM>
    autologin-timeout=0
```

LightDM config - https://wiki.ubuntu.com/LightDM

Création du réseau hotspot

```
nm-connection-editor
```



man page - nm-connection-editor

Setup des accès à distance

Config SSH

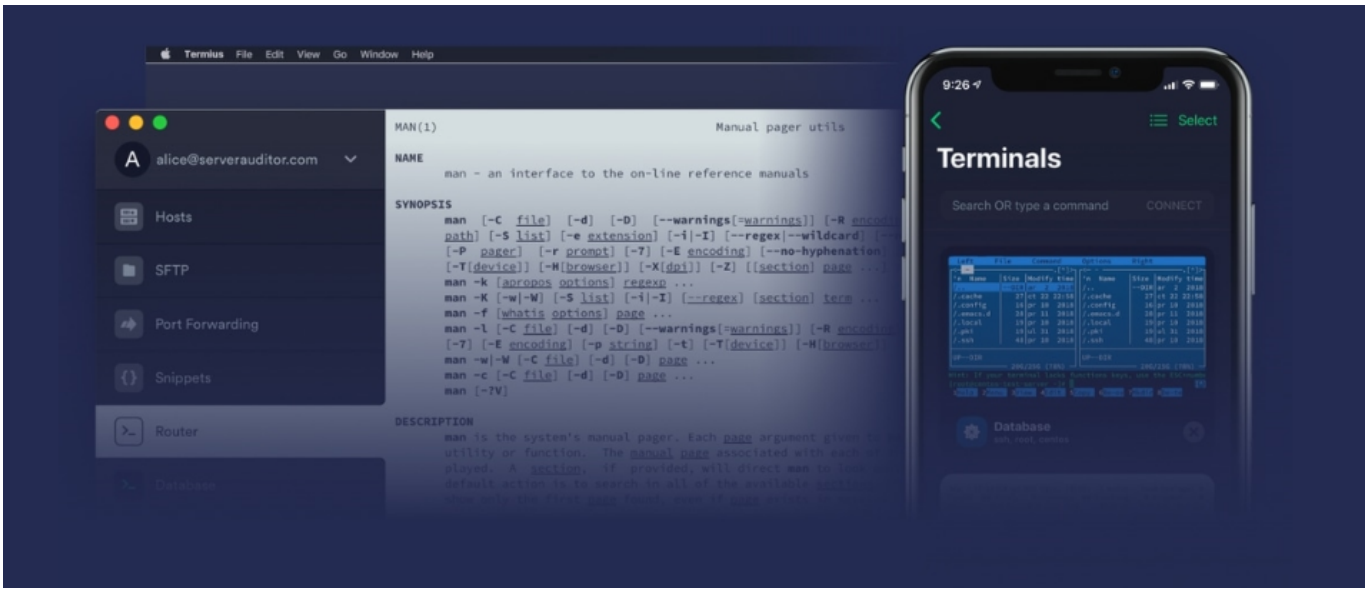
```
root@kali:~# ssh -V
OpenSSH_8.1p1 Debian-1, OpenSSL 1.1.1d  10 Sep 2019
```

```
sudo nano /etc/ssh/sshd_config

    PermitRootLogin no
    Port 2222
    ListenAddress <NETWORK>
    ClientAliveInterval 360
    ClientAliveCountMax 0
    PermitEmptyPasswords no
    MaxAuthTries 3
```

```
apt-get install fail2ban

nano /etc/fail2ban/jail.local

    # [sshd]
    enabled = true

    # "bantime" is the number of seconds that a host is banned.
    bantime  = <NUMBER_IN_SECONDS>

    # A host is banned if it has generated "maxretry" during the last
"findtime"
    # seconds.
    findtime = <NUMBER_IN_SECONDS>
    maxretry = 3
```

Config - fail2ban

Download Terminus Client - https://termius.com/



Config VNC

```
sudo apt-get install tightvncserver
sudo apt-get install lxde
```

```
cd /home/user/.vnc
nano xstartup

    + /usr/bin/startlxde
```

Grey Screen comes on connecting to VNC server - Youtube

```
vncserver :1 -geometry 1920x1080
netstat -tulpn ( debug )
```

Download VNCviewer Client - https://www.realvnc.com/en/connect/download/viewer/

Installation et configuration des services

Installation

```
apt-get install mariadb-server mariadb-client
apt-get install mysql-server
apt-get install apache2
apt-get install phpmyadmin

systemctl enable apache2 mariadb phpmyadmin
```

```
root@kali:~# mysql --version
mysql  Ver 15.1 Distrib 10.3.22-MariaDB, for debian-linux-gnu (aarch64)
using readline 5.2
```

```
Apache/2.4.41
```

```
root@kali:/etc/ssh# php --version
PHP 7.3.15-3 (cli) (built: Feb 23 2020 07:15:44) ( NTS )
Copyright (c) 1997-2018 The PHP Group
Zend Engine v3.3.15, Copyright (c) 1998-2018 Zend Technologies
    with Zend OPcache v7.3.15-3, Copyright (c) 1999-2018, by Zend
Technologies
```

Configuration de la base de données

```
mariadb-secure-installation ( commande pour la sécurisation du service )
```

```
MariaDB [(none)]> CREATE DATABASE <DB_NAME>;
MariaDB [(none)]> CREATE USER '<USER>'@'%' IDENTIFIED BY 'password';
MariaDB [(none)]> GRANT ALL PRIVILEGES ON <DB_NAME>.* TO '<USER>'@'%';
MariaDB [(none)]> FLUSH PRIVILEGES;

[CHECK]
MariaDB [(none)]> SELECT user, host FROM mysql.user;
```

```
nano /etc/mysql/mariadb.conf.d/50-server.cnf
```

```
    port 30306 ( custom port )
    bind-address = <NETWORK> ( ici 10.42.0.1 )
```

```
[Création des certificats]

$ mkdir /etc/mysql/ssl & cd /etc/mysql/ssl

$ sudo openssl genrsa 2048 > ca-key.pem
$ sudo openssl req -new -x509 -nodes -days 365000 -key ca-key.pem -out ca-
cert.pem
$ sudo openssl req -newkey rsa:2048 -days 365000 -nodes -keyout server-
key.pem -out server-req.pem
$ sudo openssl rsa -in server-key.pem -out server-key.pem
$ sudo openssl x509 -req -in server-req.pem -days 365000 -CA ca-cert.pem -
CAkey ca-key.pem -set_serial 01 -out server-cert.pem
$ sudo openssl req -newkey rsa:2048 -days 365000 -nodes -keyout client-
key.pem -out client-req.pem
$ sudo openssl rsa -in client-key.pem -out client-key.pem

$ openssl verify -CAfile ca-cert.pem server-cert.pem client-cert.pem
```

```
[SERVER]

$ sudo vi /etc/mysql/mariadb.conf.d/50-server.cnf
    ssl-ca=/etc/mysql/ssl/ca-cert.pem
    ssl-cert=/etc/mysql/ssl/server-cert.pem
    ssl-key=/etc/mysql/ssl/server-key.pem
    tls_version = TLSv1.2

chown mysql:root /etc/mysql/ssl/
systemctl restart mysql
```

```
L'envoit des fichiers peut être effectué par FTP ou grâce à la commande
suivante (dans le dir contenant les fichiers) :
    python3 -m http.server
```

```
[CLIENT]

$ sudo vi /etc/mysql/mariadb.conf.d/50-mysql-clients.cnf
    ssl-ca=/etc/mysql/ssl/ca-cert.pem
    ssl-cert=/etc/mysql/ssl/client-cert.pem
    ssl-key=/etc/mysql/ssl/client-key.pem
```

```
[Verification]

$ mysql -u root -h 192.168.0.30
MariaDB [(none)]> SHOW VARIABLES LIKE '%ssl%'; ( have_openssl & have_ssl
enabled )
MariaDB [(none)]> status;
```

SSL/TLS config

Installation des outils

Python & Pip

```
root@kali:~# python3 --version
Python 3.7.7
```

```
root@kali:~# pip3 --version
pip 18.1 from /usr/lib/python3/dist-packages/pip (python 3.7)
```

requirements.txt

```
pip3 install nmap
pip3 install mysql-connector-python
pip3 install getmac
pip3 install netifaces
pip3 install python-nmap
```

Installation des outils

Recursive gobuster - github

```
git clone https://github.com/epi052/recursive-gobuster.git
```

Kerbrute - github

```
git clone https://github.com/ropnop/kerbrute.git

sudo apt-get install golang
```

```
go build
alias kerbrute="<DIR>/kerbrute"
```

Smtp-user-enum - github

```
git clone https://github.com/pentestmonkey/smtp-user-enum.git
```

Enum4Linux - github

```
git clone https://github.com/portcullislabs/enum4linux.git
```

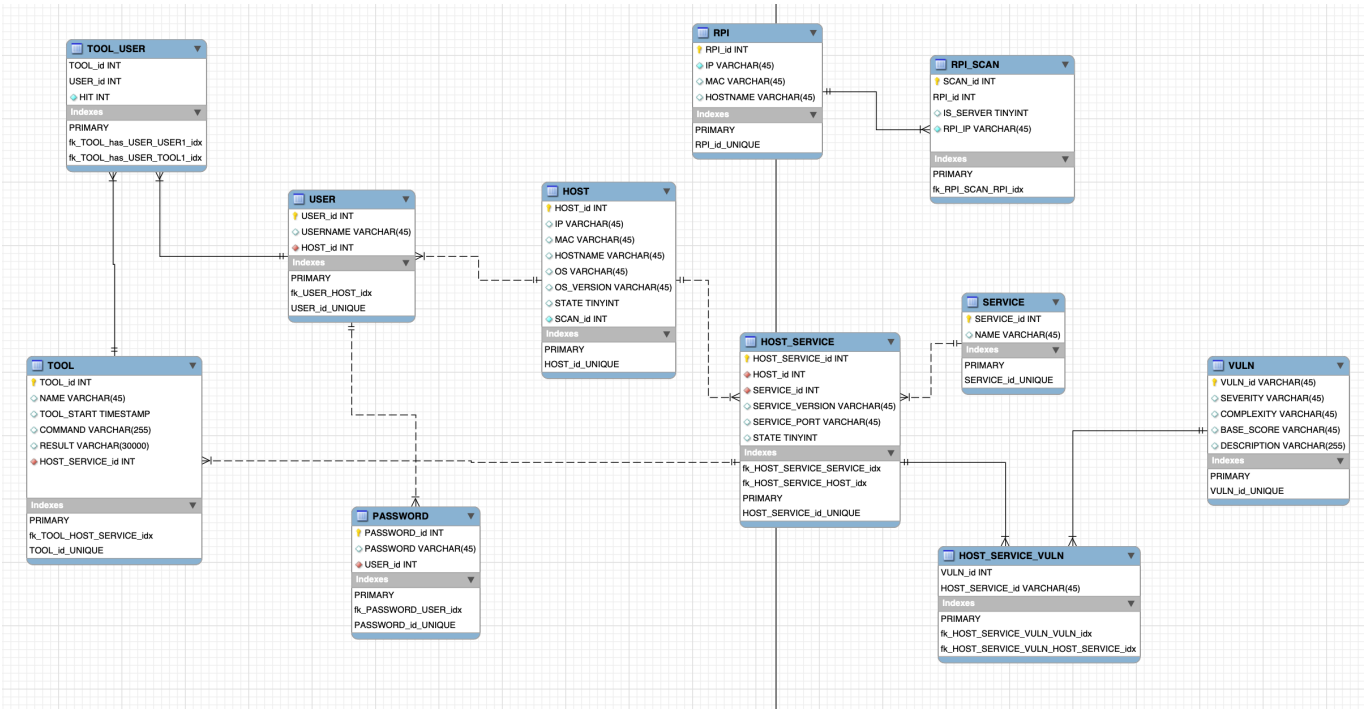
> **Autres outils (déjà présent sur Kali)**

```
dig
nikto
hydra
ldapsearch
nbtscan
rpcclient
nmblookup
smbclient
```

Penetration testing cheat sheet

Conception de la base de données

Download MySQL workbench - https://www.mysql.com/products/workbench/




```sql
-- phpMyAdmin SQL Dump
-- version 4.9.2deb1
-- https://www.phpmyadmin.net/
--
-- Hôte : localhost:3306
-- Généré le :  mer. 20 mai 2020 à 16:11
-- Version du serveur :  10.3.22-MariaDB-1
-- Version de PHP :  7.3.15-3

SET SQL_MODE = "NO_AUTO_VALUE_ON_ZERO";
SET AUTOCOMMIT = 0;
START TRANSACTION;
SET time_zone = "+00:00";


/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!40101 SET NAMES utf8mb4 */;

--
-- Base de données :  `STAGE`
--

-- --------------------------------------------------------

--
-- Structure de la table `HOST`
--

CREATE TABLE `HOST` (
  `HOST_id` int(11) NOT NULL,
  `SCAN_id` int(11) NOT NULL,
```

```
  `IP` varchar(45) DEFAULT NULL,
  `MAC` varchar(100) DEFAULT NULL,
  `HOSTNAME` varchar(50) DEFAULT NULL,
  `OS` varchar(100) DEFAULT NULL,
  `VENDOR` varchar(100) DEFAULT NULL,
  `LAST_BOOT` varchar(100) DEFAULT NULL,
  `STATE` tinyint(4) NOT NULL DEFAULT 0
) ENGINE=InnoDB DEFAULT CHARSET=utf8;

-- --------------------------------------------------------

--
-- Structure de la table `HOST_SERVICE`
--

CREATE TABLE `HOST_SERVICE` (
  `HOST_SERVICE_id` int(11) NOT NULL,
  `HOST_id` int(11) NOT NULL,
  `SERVICE_NAME` varchar(45) NOT NULL,
  `SERVICE_VERSION` varchar(45) DEFAULT NULL,
  `SERVICE_PORT` varchar(45) DEFAULT NULL
) ENGINE=InnoDB DEFAULT CHARSET=utf8;


-- --------------------------------------------------------

--
-- Structure de la table `HOST_SERVICE_VULN`
--

CREATE TABLE `HOST_SERVICE_VULN` (
  `HOST_SERVICE_id` int(11) NOT NULL,
  `VULN_id` varchar(45) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=utf8;


-- --------------------------------------------------------

--
-- Structure de la table `HOST_USER_PASSWORD`
--

CREATE TABLE `HOST_USER_PASSWORD` (
  `HOST_USER_PASSWORD_id` int(11) NOT NULL,
  `HOST_id` int(11) NOT NULL,
  `USERNAME` varchar(45) NOT NULL,
  `PASSWORD` varchar(45) DEFAULT NULL
) ENGINE=InnoDB DEFAULT CHARSET=utf8;

-- --------------------------------------------------------

--
-- Structure de la table `PASSWORD`
--
```

```
CREATE TABLE `PASSWORD` (
  `PASSWORD` varchar(45) NOT NULL,
  `HIT` int(11) NOT NULL DEFAULT 0
) ENGINE=InnoDB DEFAULT CHARSET=utf8;

-- --------------------------------------------------------

--
-- Structure de la table `RPI`
--

CREATE TABLE `RPI` (
  `RPI_id` int(11) NOT NULL,
  `IP` varchar(45) NOT NULL,
  `MAC` varchar(45) NOT NULL,
  `HOSTNAME` varchar(45) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=utf8;

-- --------------------------------------------------------

--
-- Structure de la table `RPI_SCAN`
--

CREATE TABLE `RPI_SCAN` (
  `RPI_id` int(11) NOT NULL,
  `SCAN_id` int(11) NOT NULL,
  `IS_CONNECTED` tinyint(4) NOT NULL DEFAULT 0
) ENGINE=InnoDB DEFAULT CHARSET=utf8;

-- --------------------------------------------------------

--
-- Structure de la table `SCAN`
--

CREATE TABLE `SCAN` (
  `SCAN_id` int(11) NOT NULL,
  `SCAN_START` timestamp NULL DEFAULT NULL,
  `SCAN_END` timestamp NULL DEFAULT NULL,
  `SUBNET` varchar(45) DEFAULT NULL,
  `STATE` tinyint(4) NOT NULL DEFAULT 0,
  `RECON_STATE` tinyint(4) NOT NULL DEFAULT 0,
  `EXPLOIT_STATE` tinyint(4) NOT NULL DEFAULT 0,
  `VULN_STATE` tinyint(4) NOT NULL DEFAULT 0
) ENGINE=InnoDB DEFAULT CHARSET=utf8;

-- --------------------------------------------------------

--
-- Structure de la table `SERVICE`
--
```

```
CREATE TABLE `SERVICE` (
  `NAME` varchar(45) NOT NULL,
  `HIT` int(11) NOT NULL DEFAULT 0
) ENGINE=InnoDB DEFAULT CHARSET=utf8;

-- --------------------------------------------------------

--
-- Structure de la table `TOOL`
--

CREATE TABLE `TOOL` (
  `TOOL_id` int(11) NOT NULL,
  `HOST_id` int(11) NOT NULL,
  `NAME` varchar(100) NOT NULL,
  `COMMAND` varchar(500) NOT NULL,
  `RESULT` text DEFAULT NULL,
  `TOOL_START` timestamp NULL DEFAULT NULL
) ENGINE=InnoDB DEFAULT CHARSET=utf8;

-- --------------------------------------------------------

--
-- Structure de la table `USER`
--

CREATE TABLE `USER` (
  `USERNAME` varchar(45) NOT NULL,
  `HIT` int(11) NOT NULL DEFAULT 0
) ENGINE=InnoDB DEFAULT CHARSET=utf8;

-- --------------------------------------------------------

--
-- Structure de la table `VULN`
--

CREATE TABLE `VULN` (
  `VULN_id` varchar(45) NOT NULL,
  `SEVERITY` varchar(45) NOT NULL DEFAULT 'UNKNOWN',
  `COMPLEXITY` varchar(45) NOT NULL DEFAULT 'UNKNOWN',
  `BASE_SCORE` varchar(45) NOT NULL DEFAULT 'UNKNOWN',
  `DESCRIPTION` varchar(10000) NOT NULL DEFAULT 'UNKNOWN'
) ENGINE=InnoDB DEFAULT CHARSET=utf8;


--
-- Index pour les tables déchargées
--

--
-- Index pour la table `HOST`
--
ALTER TABLE `HOST`
```

```
  ADD PRIMARY KEY (`HOST_id`),
  ADD KEY `fk_HOST_SCAN2` (`SCAN_id`);

--
-- Index pour la table `HOST_SERVICE`
--
ALTER TABLE `HOST_SERVICE`
  ADD PRIMARY KEY (`HOST_SERVICE_id`),
  ADD KEY `fk_HOST_has_SERVICE_HOST2` (`HOST_id`),
  ADD KEY `fk_HOST_SERVICE_SERVICE1` (`SERVICE_NAME`);

--
-- Index pour la table `HOST_SERVICE_VULN`
--
ALTER TABLE `HOST_SERVICE_VULN`
  ADD PRIMARY KEY (`HOST_SERVICE_id`,`VULN_id`),
  ADD KEY `fk_HOST_SERVICE_has_VULN_VULN1` (`VULN_id`);

--
-- Index pour la table `HOST_USER_PASSWORD`
--
ALTER TABLE `HOST_USER_PASSWORD`
  ADD PRIMARY KEY (`HOST_USER_PASSWORD_id`),
  ADD KEY `fk_HOST_USER_PASSWORD_HOST1` (`HOST_id`),
  ADD KEY `fk_HOST_USER_PASSWORD_USER1` (`USERNAME`),
  ADD KEY `fk_HOST_USER_PASSWORD_PASSWORD1` (`PASSWORD`);

--
-- Index pour la table `PASSWORD`
--
ALTER TABLE `PASSWORD`
  ADD PRIMARY KEY (`PASSWORD`);

--
-- Index pour la table `RPI`
--
ALTER TABLE `RPI`
  ADD PRIMARY KEY (`RPI_id`);

--
-- Index pour la table `RPI_SCAN`
--
ALTER TABLE `RPI_SCAN`
  ADD PRIMARY KEY (`RPI_id`,`SCAN_id`),
  ADD KEY `fk_RPI_has_SCAN_SCAN2` (`SCAN_id`);

--
-- Index pour la table `SCAN`
--
ALTER TABLE `SCAN`
  ADD PRIMARY KEY (`SCAN_id`);

--
-- Index pour la table `SERVICE`
```

```
--
ALTER TABLE `SERVICE`
  ADD PRIMARY KEY (`NAME`);

--
-- Index pour la table `TOOL`
--
ALTER TABLE `TOOL`
  ADD PRIMARY KEY (`TOOL_id`),
  ADD KEY `fk_TOOL_HOST1` (`HOST_id`);

--
-- Index pour la table `USER`
--
ALTER TABLE `USER`
  ADD PRIMARY KEY (`USERNAME`);

--
-- Index pour la table `VULN`
--
ALTER TABLE `VULN`
  ADD PRIMARY KEY (`VULN_id`);

--
-- AUTO_INCREMENT pour les tables déchargées
--


--
-- AUTO_INCREMENT pour la table `HOST`
--
ALTER TABLE `HOST`
  MODIFY `HOST_id` int(11) NOT NULL AUTO_INCREMENT, AUTO_INCREMENT=101;

--
-- AUTO_INCREMENT pour la table `HOST_SERVICE`
--
ALTER TABLE `HOST_SERVICE`
  MODIFY `HOST_SERVICE_id` int(11) NOT NULL AUTO_INCREMENT,
AUTO_INCREMENT=419;

--
-- AUTO_INCREMENT pour la table `HOST_USER_PASSWORD`
--
ALTER TABLE `HOST_USER_PASSWORD`
  MODIFY `HOST_USER_PASSWORD_id` int(11) NOT NULL AUTO_INCREMENT,
AUTO_INCREMENT=169;

--
-- AUTO_INCREMENT pour la table `RPI`
--
ALTER TABLE `RPI`
  MODIFY `RPI_id` int(11) NOT NULL AUTO_INCREMENT, AUTO_INCREMENT=4;

--
```

```
-- AUTO_INCREMENT pour la table `SCAN`
--
ALTER TABLE `SCAN`
  MODIFY `SCAN_id` int(11) NOT NULL AUTO_INCREMENT, AUTO_INCREMENT=29;

--
-- AUTO_INCREMENT pour la table `TOOL`
--
ALTER TABLE `TOOL`
  MODIFY `TOOL_id` int(11) NOT NULL AUTO_INCREMENT, AUTO_INCREMENT=357;

--
-- Contraintes pour les tables déchargées
--


--
-- Contraintes pour la table `HOST`
--
ALTER TABLE `HOST`
  ADD CONSTRAINT `fk_HOST_SCAN2` FOREIGN KEY (`SCAN_id`) REFERENCES `SCAN`
(`SCAN_id`) ON DELETE NO ACTION ON UPDATE NO ACTION;

--
-- Contraintes pour la table `HOST_SERVICE`
--
ALTER TABLE `HOST_SERVICE`
  ADD CONSTRAINT `fk_HOST_SERVICE_SERVICE1` FOREIGN KEY (`SERVICE_NAME`)
REFERENCES `SERVICE` (`NAME`) ON DELETE NO ACTION ON UPDATE NO ACTION,
  ADD CONSTRAINT `fk_HOST_has_SERVICE_HOST2` FOREIGN KEY (`HOST_id`)
REFERENCES `HOST` (`HOST_id`) ON DELETE NO ACTION ON UPDATE NO ACTION;

--
-- Contraintes pour la table `HOST_SERVICE_VULN`
--
ALTER TABLE `HOST_SERVICE_VULN`
  ADD CONSTRAINT `fk_HOST_SERVICE_has_VULN_HOST_SERVICE1` FOREIGN KEY
(`HOST_SERVICE_id`) REFERENCES `HOST_SERVICE` (`HOST_SERVICE_id`) ON
DELETE NO ACTION ON UPDATE NO ACTION,
  ADD CONSTRAINT `fk_HOST_SERVICE_has_VULN_VULN1` FOREIGN KEY (`VULN_id`)
REFERENCES `VULN` (`VULN_id`) ON DELETE NO ACTION ON UPDATE NO ACTION;

--
-- Contraintes pour la table `HOST_USER_PASSWORD`
--
ALTER TABLE `HOST_USER_PASSWORD`
  ADD CONSTRAINT `fk_HOST_USER_PASSWORD_HOST1` FOREIGN KEY (`HOST_id`)
REFERENCES `HOST` (`HOST_id`) ON DELETE NO ACTION ON UPDATE NO ACTION,
  ADD CONSTRAINT `fk_HOST_USER_PASSWORD_PASSWORD1` FOREIGN KEY
(`PASSWORD`) REFERENCES `PASSWORD` (`PASSWORD`) ON DELETE NO ACTION ON
UPDATE NO ACTION,
  ADD CONSTRAINT `fk_HOST_USER_PASSWORD_USER1` FOREIGN KEY (`USERNAME`)
REFERENCES `USER` (`USERNAME`) ON DELETE NO ACTION ON UPDATE NO ACTION;

--
```

```
-- Contraintes pour la table `RPI_SCAN`
--
ALTER TABLE `RPI_SCAN`
  ADD CONSTRAINT `fk_RPI_has_SCAN_RPI1` FOREIGN KEY (`RPI_id`) REFERENCES
`RPI` (`RPI_id`) ON DELETE NO ACTION ON UPDATE NO ACTION,
  ADD CONSTRAINT `fk_RPI_has_SCAN_SCAN2` FOREIGN KEY (`SCAN_id`)
REFERENCES `SCAN` (`SCAN_id`) ON DELETE NO ACTION ON UPDATE NO ACTION;

--
-- Contraintes pour la table `TOOL`
--
ALTER TABLE `TOOL`
  ADD CONSTRAINT `fk_TOOL_HOST1` FOREIGN KEY (`HOST_id`) REFERENCES `HOST`
(`HOST_id`) ON DELETE NO ACTION ON UPDATE NO ACTION;
COMMIT;

/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;
/*!40101 SET CHARACTER_SET_RESULTS=@OLD_CHARACTER_SET_RESULTS */;
/*!40101 SET COLLATION_CONNECTION=@OLD_COLLATION_CONNECTION */;
```