



Rapport

Web Application Firewall (F5)

Réalisé par:

ALAOUI-KASMI Fatima-Ezzahra
NASSIRI Selma
PEZONGO Mickael

Encadré par:

Mr.YASSINE MALEH

PLAN :

I-Remerciement.

II -Présentation du Projet F5 :

- 1.La couche applicative
- 2.Les différentes menaces liées à la couche applicative.
- 3-Qu'est-ce qu'un WAF ?
- 4-La différence entre un WAF, un IPS et un NGFW
- 5-Le F5 :
 - 5-1-Les différents modules de F5
 - 5-2-Les fonctionnalités de F5.

III- PRESENTATION DU LAB F5 :

« REMERCIEMENT »

Nous tenons à remercier non seulement comme devoir mais par grand respect et gratitude profonde notre encadrant : **MR.Yassine Maleh** à qui nous adressons nos sentiments de reconnaissance et de respect pour nous avoir guidés dans l'élaboration de ce travail, sa contribution et sa réalisation avec la patience et le dynamisme qui le caractérisent, son soutien ainsi ses directives précieuses durant le déroulement du projet ainsi sa disponibilité.

Nous ne manquerions pas de remercier tous ceux qui ont contribué de loin ou de près à la réalisation de ce travail. Enfin nous espérons que notre travail a été à la hauteur de la confiance qui nous a été accordée.

Enfin on espère vraiment que notre travail a été à la hauteur de la confiance qui nous a été accordée.

1.La couche applicative :

La couche application est la 7e couche du modèle OSI. Le rôle de la couche applicative

Apparaît dans la prise en charge des applications destinées aux utilisateurs finaux. C'est la couche la plus proche de l'utilisateur.

Les protocoles les plus connus dans la couche applicative :

- FTP (File Transfer Protocol)
- HTTP (Hypertext Transfer Protocol)
- IMAP (Internet Message Access Protocol)
- TFTP (Trivial File Transfer Protocol)
- POP (Post Office Protocol)
- DNS (Domain Name System)

PAYSAGE DES MENACES

Quelles sont les menaces de sécurité avancée ?

1.Déni de Service Volumétrique :

- Difficiles à filtrer à hauts volumes.
- Empêche les utilisateurs légitimes d'accéder au site.

Attaques ciblant le calcul ou la consommation de ressources :

- Gonfle artificiellement la consommation des ressources SaaS.
- Requiert une bonne compréhension des éléments induisant de la latence ou une Défaillance dans l'application.

2.Malware à base de navigateur Web :

- N'existe qu'en dehors du périmètre.
- Délivre pléthore de programmes malicieux aux postes de travail des utilisateurs.

3.Spear Phishing :

- Cible des organisations spécifiques, à la recherche d'accès non autorisés à des données Confidentielles.
- Les auteurs recherchent le gain financier, le troc de secrets ou des informations militaires.

4.Advanced Persistent Threats (APT) :

- Cybercrime ciblé et furtif durant un temps prolongé
- Lent et silencieux afin d'éviter les mécanismes de détection

3-Qu'est-ce qu'un WAF ?

Comme c'est déjà expliqué la couche application est faible en termes de sécurité.

La majorité des attaques ciblent cette couche.

D'où la nécessité un firewall destiné a la couche applicative.

WAF : Un pare-feu applicatif Web (WAF) protège les applications Web contre diverses attaques en couche applicative comme les scripting (XSS), l'injection SQL, et l'empoisonnement par cookie, Entre autres. Les attaques affectant les applications sont la principale cause de failles.

Comment fonctionne le WAF ?

Le WAF analyse les requêtes HTTP et applique un ensemble de règles pour séparer les codes bénins des codes malveillants.

Les parties principales des conversations HTTP qu'un WAF analyse sont les requêtes GET et POST.

Les requêtes GET sont utilisées pour récupérer des données sur le serveur.

Les requêtes POST sont utilisées pour envoyer des données à un serveur afin de changer son état.

Un WAF peut adopter 2 approches différentes pour analyser et filtrer le contenu de ces requêtes http :

1. Liste blanche
2. Liste noire
3. Sécurité hybride

Quel que soit le modèle de sécurité utilisé par un WAF, il fonctionne toujours pour analyser les interactions HTTP et réduire / éliminer le trafic malveillant avant qu'il n'atteigne le serveur.

La différence entre un WAF, un IPS et un NGFW

Un IPS est un produit de sécurité à visée plus large. Il est généralement basé sur des signatures et des politiques, ce qui signifie qu'il peut vérifier les vulnérabilités connues et les vecteurs d'attaque en se basant sur une base de données établie de signatures et de politiques.

Un pare-feu applicatif Web (WAF) protège la couche application et est spécifiquement conçu pour analyser chaque requête HTTP/S au niveau de la couche application. Il est généralement conscient de l'utilisateur, de la session et de l'application, et connaît les applications Web impliquées et les services qu'elles offrent. De ce fait, on peut considérer un WAF comme un intermédiaire entre l'utilisateur et l'application elle-même.

Un pare-feu de nouvelle génération (NGFW) surveille le trafic sortant vers Internet — via les sites Web, les comptes de courrier électronique et le SaaS. En d'autres termes, il protège l'utilisateur (et non l'application Web). Un NGFW appliquera des politiques basées sur l'utilisateur et ajoutera un contexte aux politiques de sécurité en plus d'ajouter des fonctionnalités telles que le filtrage des URL.

Les différents modules de F5

On distingue 4 modules de F5 BIG-IP à savoir :

1. BIG-IP LTM pour le load balancing.
2. BIG-IP DNS Pour la gestion du DNS.
3. BIG-IP ASM pour le pare-feu d'application web.
4. BIG-IP APM pour la gestion des authentifications et autorisations pour les accès distants.

Les fonctionnalités de F5

Les différentes fonctionnalités de F5 sont :

1. Le load balancing qui est une technique utilisée pour répartir uniformément les charges de travail sur plusieurs serveurs ou autres ressources informatiques, afin d'optimiser le rendement, la fiabilité et la capacité du réseau.
2. Le firewall applicatif qui permet de faire un filtrage applicatif pour sécuriser les sites contre les attaques applicatives comme les injections SQL, le cross site Scripting et de nombreuses autres attaques répertoriées.
3. Le proxy qui joue le rôle d'intermédiaire en se plaçant entre deux hôtes pour faciliter ou surveiller leurs échanges de ces derniers.

II. PRESENTATION DU LAB F5

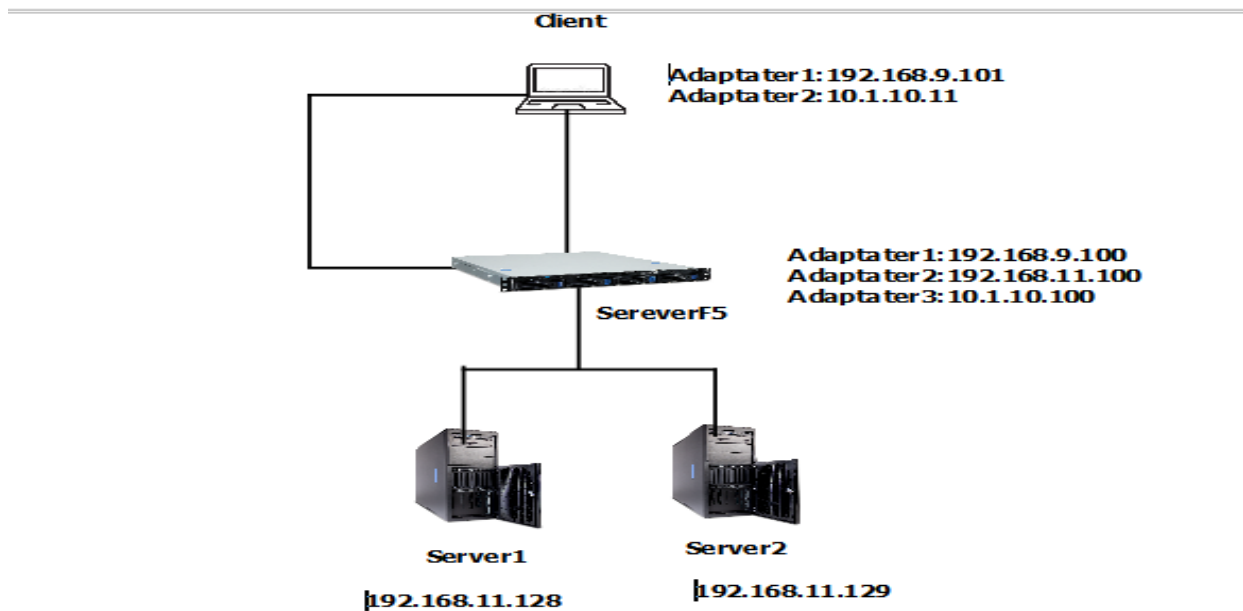
Notre LAB sera élaboré en plusieurs étapes qui suivent :

- ◆ Schéma du LAB
- ◆ Déploiement de F5 sur VMWARE station
- ◆ Récupération d'une licence F5
- ◆ Lancement et configuration de F5
- ◆ Node, Pool, Virtual Servers
- ◆ Sécurisation d'une Application Web avec F5

Sans plus tarder passons au vif du sujet.

1. Schéma du LAB

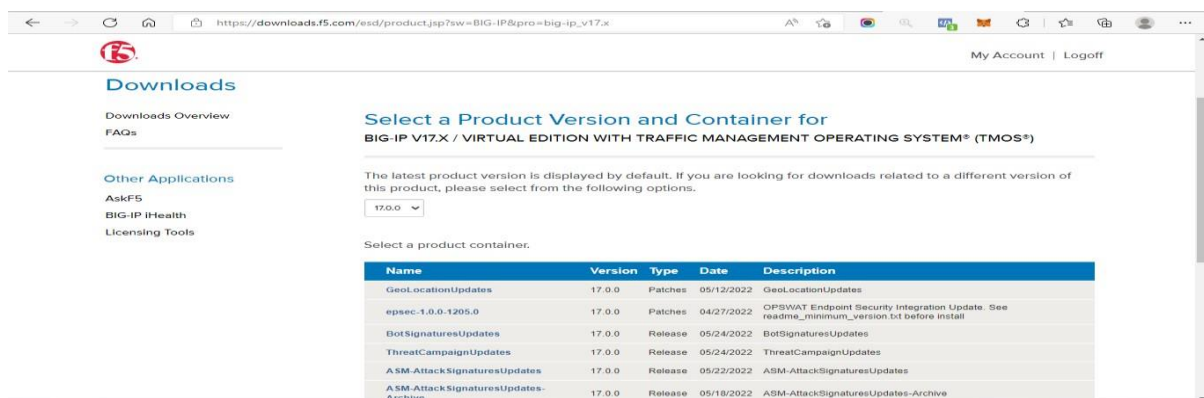
Notre LAB sera constitué de 4 machines dont 2 servers applicatifs, une machine cliente et la machine F5 comme le montre le schéma suivant :



2. Déploiement de F5 sur VMware Workstation

Pour installer F5, on doit d'abord se rendre sur la plateforme <https://downloads.f5.com>

Ensuite on s'enregistre puis on télécharge l'image ova de la machine F5 selon les versions souhaiter

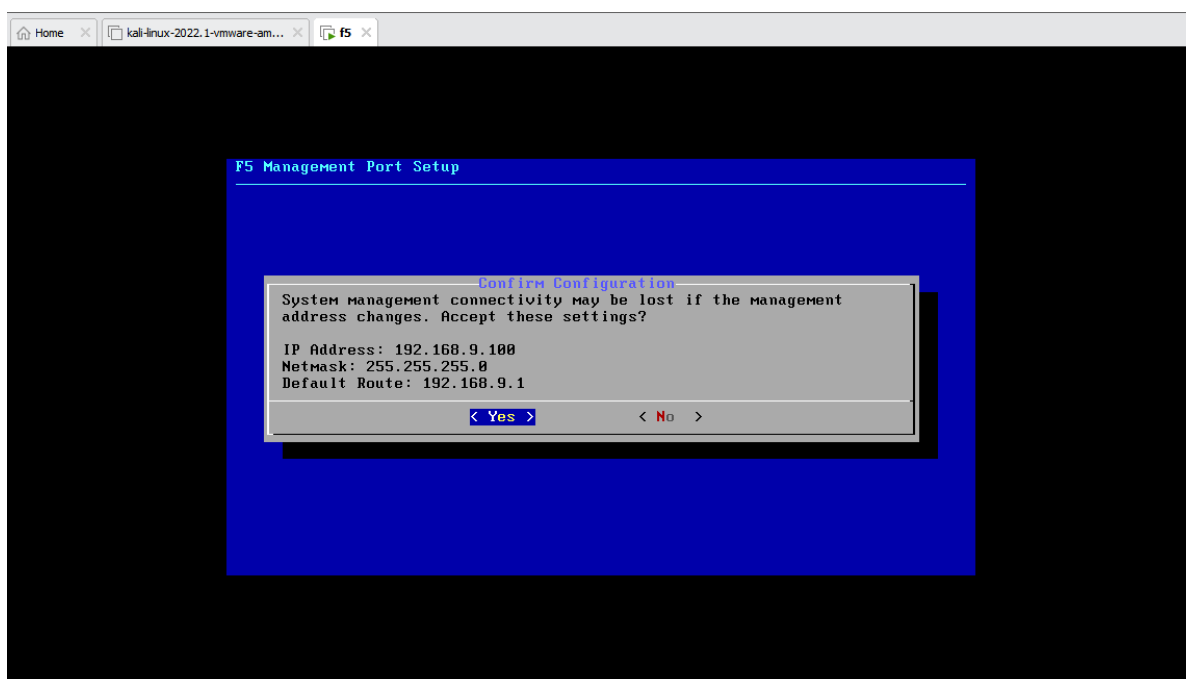


Ensuite on ouvre l'image téléchargée, puis on configure les 4 interfaces de F5 et on démarre la machine

Le login et mot de passe par défaut sont : Login : root

Mot de passe : default

Après cela on tape la commande config puis on assigne une adresse IP de la première Interface à F5 qu'on va ensuite utiliser pour ouvrir l'interface web



3. Récupération d'une licence F5

Pour avoir une licence gratuite F5 on se rend sur free trials puis on demande sa licence et au bout de quelques minutes on doit recevoir la licence par mail valable 30 jours :

The screenshot shows a web browser window with the URL <https://downloads.f5.com/trial/>. The page has a dark blue header with the F5 logo and navigation links: Solutions, Products, Community, Partners, Education, About Us, and My Account | Logout. Below the header is a blue bar labeled "PRODUCTS". The main content area is divided into two columns. The left column, titled "Evaluation Information", contains four dropdown menus: "What is the purpose of this trial?" (Currently evaluating ADC/LB products), "What is your job function?" (Security architect/engineer), "Which trial would you like?" (BIG-IP VE and BIG-IQ), and "How many licenses would you like?" (3). Below these is a note: "A trial key for BIG-IQ and BIG-IQ DCD will be included in your request." and a captcha challenge: "Please enter only the 3 black text in the captcha below." with a "5xyc15" image and a "Reload Challenge" button. A text input field contains "5y1". The right column, titled "My Contact Information", shows the email "The registration key(s) will be emailed to: pezongomickael67@gmail.com" and a "Not you? Click here to logout." link. Below this is the contact information for Mickael Pezongo: Etudiant, USMS, Immeuble 44 firdaws, Khouribga, 25000, Morocco, 0696947675. At the bottom of the left column is a blue button labeled "Request license keys".

You're ready to start your free 30-day trial.

Thank you for requesting a trial. Below are the registration keys you'll need to get started. These keys expire 30 days from today if not activated.

BIG-IP Registration key(s):

OMLNS-JHZPG-XCRXB-EXXPR-DXDYVXO (BIG-IP VE Trial)

QBSYM-EIOLX-EMVGQ-SAWBF-VSJLDP (BIG-IP VE Trial)

RHVEF-DKKQJ-ESCOD-DMJJZ-KVGZDOH (BIG-IP VE Trial)

BIG-IQ Registration key(s):

LZXHD-AXSEPB-WOY-XAHXVTF-SMSDQVK (BIG-IQ Data Collection Device)

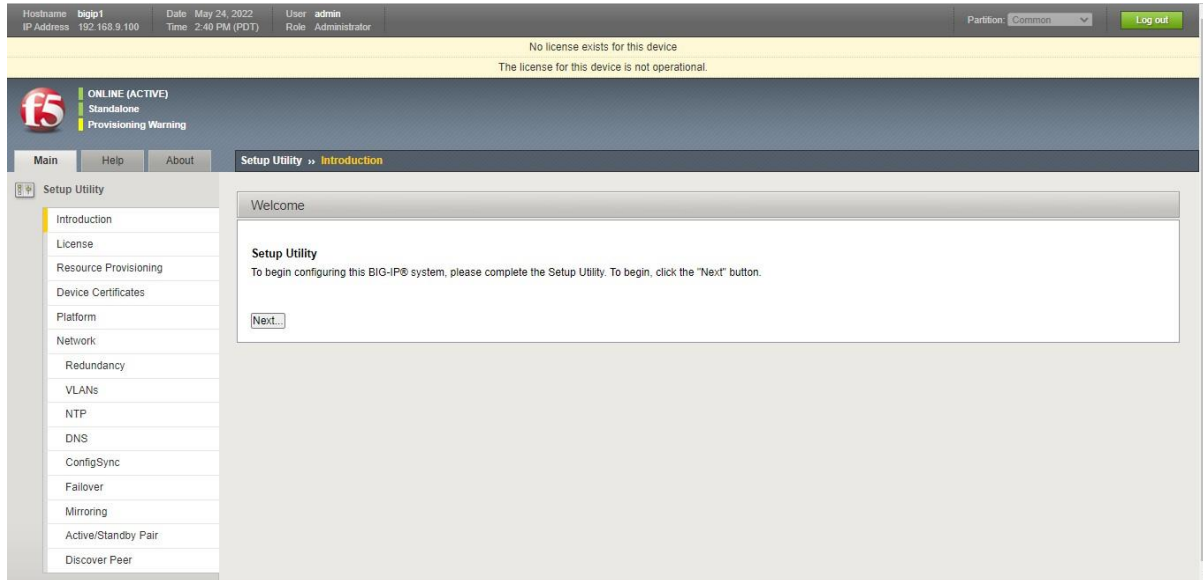
GOELS-OINQTA-RHJ-QQIZBJJ-XBBEYRJ (BIG-IQ Console Node)

Evaluation duration: 30 days

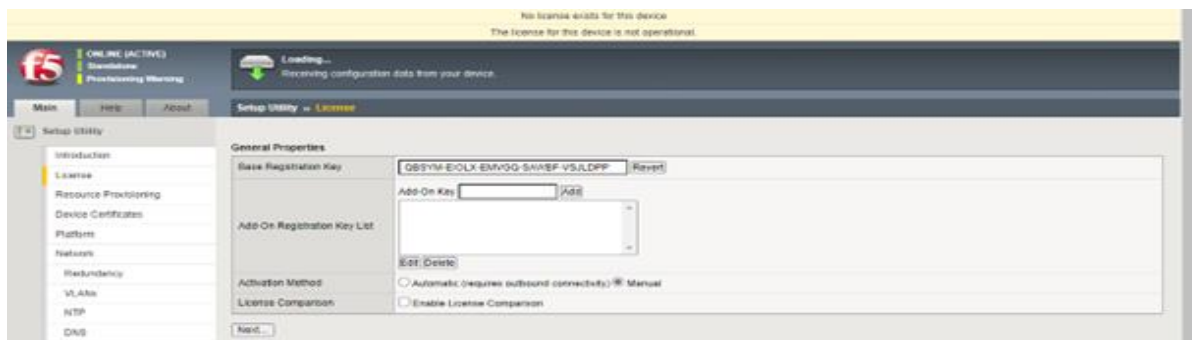
Contact: pezongomickael67@gmail.com

4.Lancement et configuration de F5

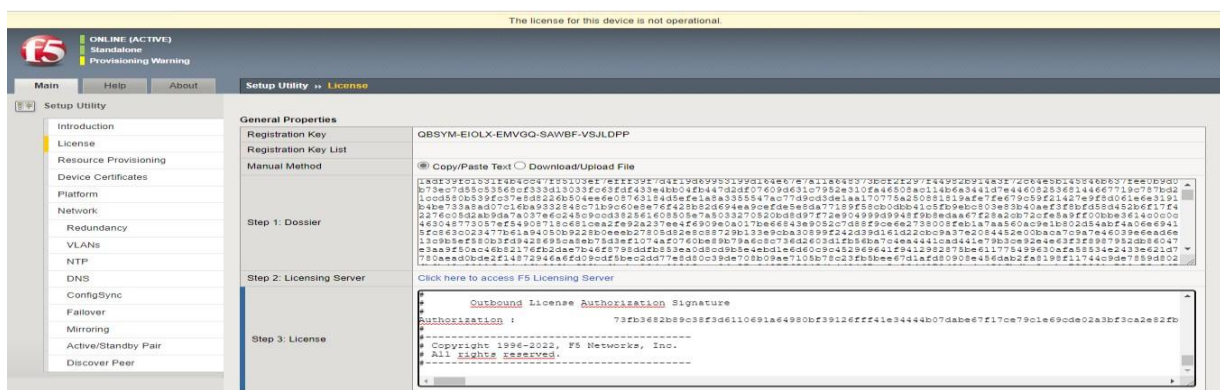
Après démarrage on se rend sur un navigateur web puis on tape l'adresse IP de la Machine F5 et on suit les étapes suivantes :



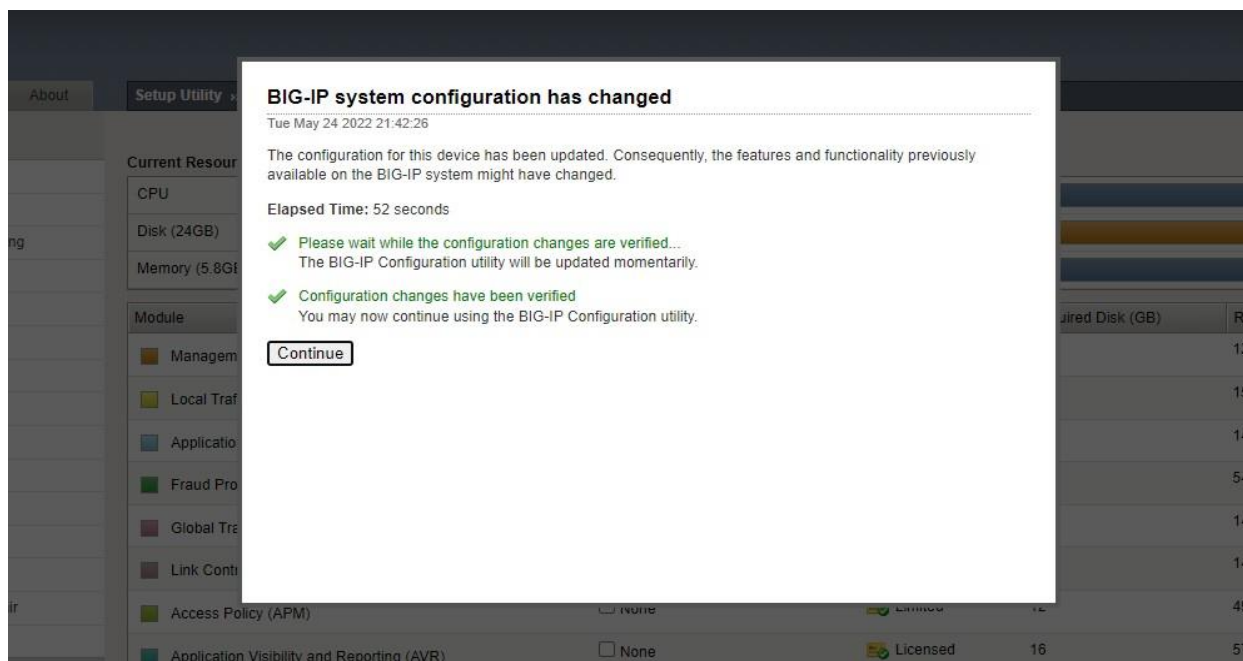
On clique sur Next :



On entre notre licence puis Next :



On copie le premier texte puis on clique sur le lien en bas et là on va coller le texte pour pouvoir récupérer le texte de step3 et après on clique sur Next

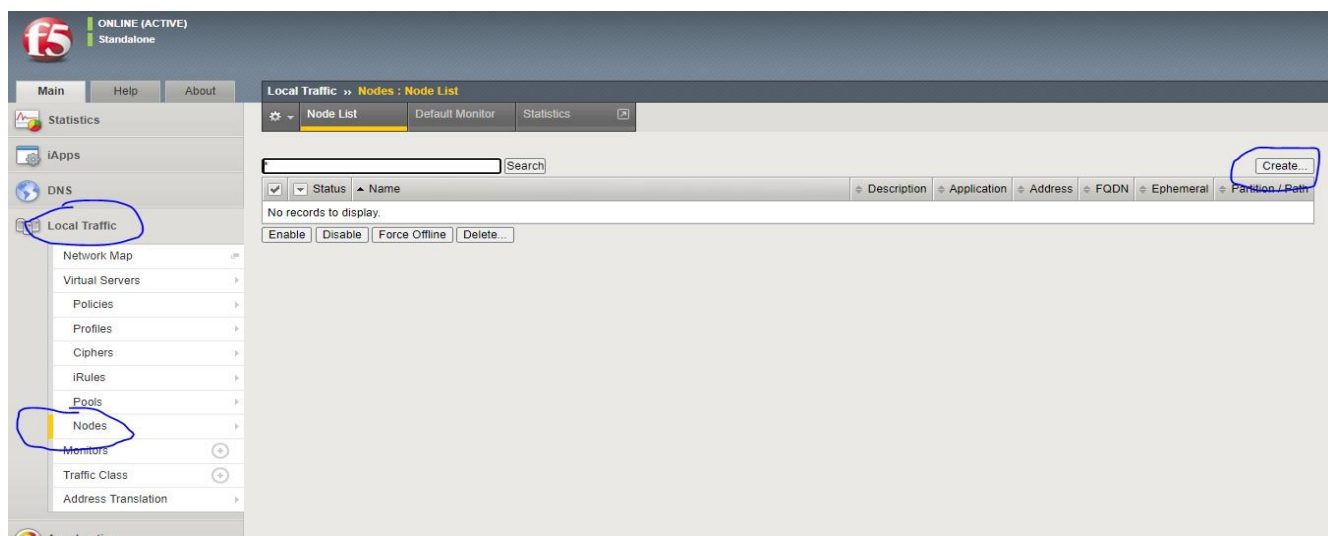


On clique sur continue et après cette notre licence est activé.

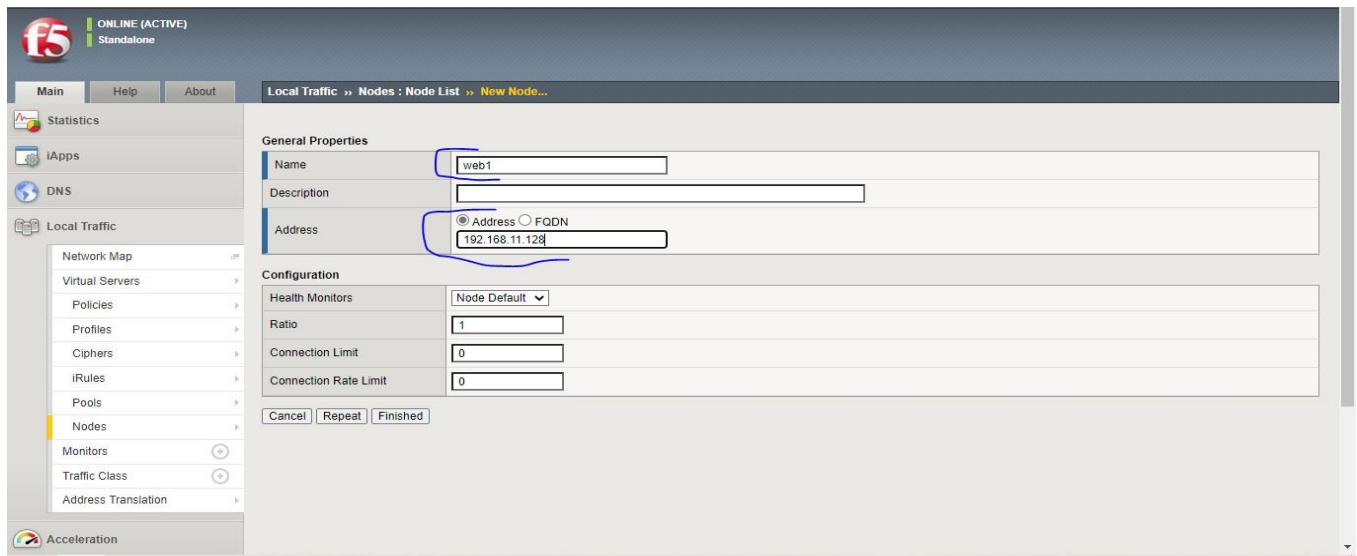
4. Nodes, Pool, Virtual Servers

a. Nodes

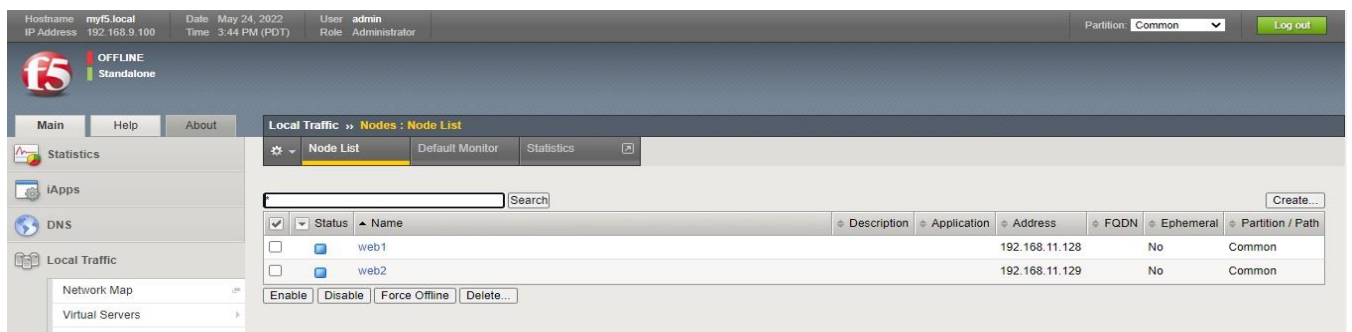
Les nodes sont des adresse IP de nos différentes machines qu'on associe à F5. Pour créer un nodes on se rend sur local traffic puis dans nodes et on clique sur create



Puis on entre le nom et l'adresse IP de la machine



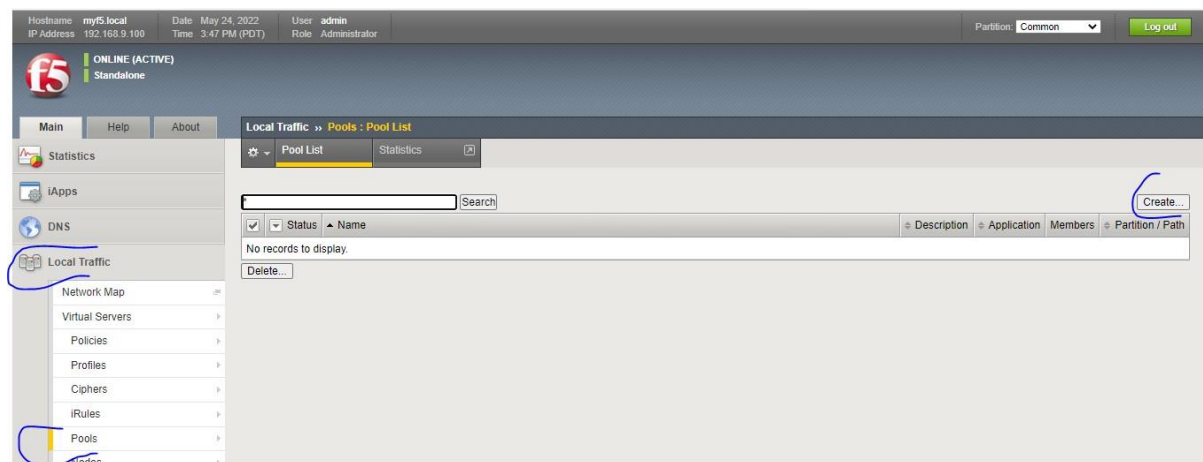
Après dans nodes list on retrouve toutes les machines qu'on a créé



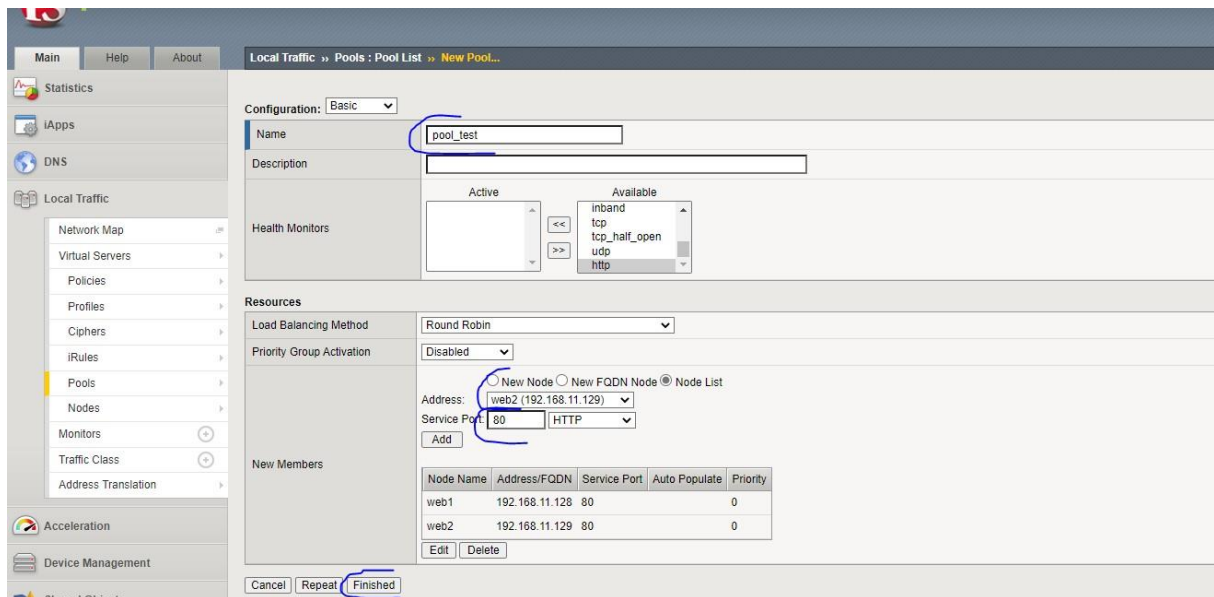
B-Pool :

Les pools dont de adresses IP associées a des protocoles comme le protocoles http ou https.

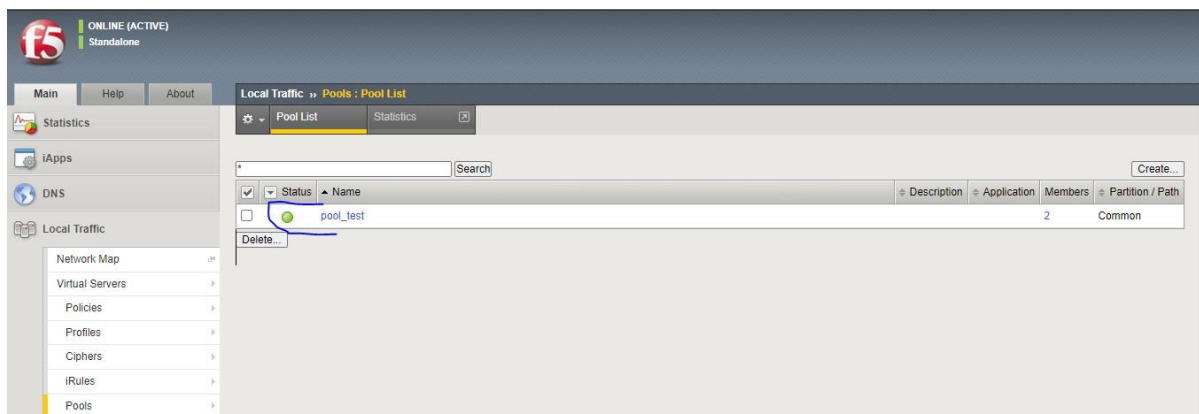
Pour créer un pool, on se rend sur local traffic ensuite sur pools puis sur create



Là on entre le nom du pool puis les machines associées a ce pool et le protocole a utiliser après cela on clique sur finished



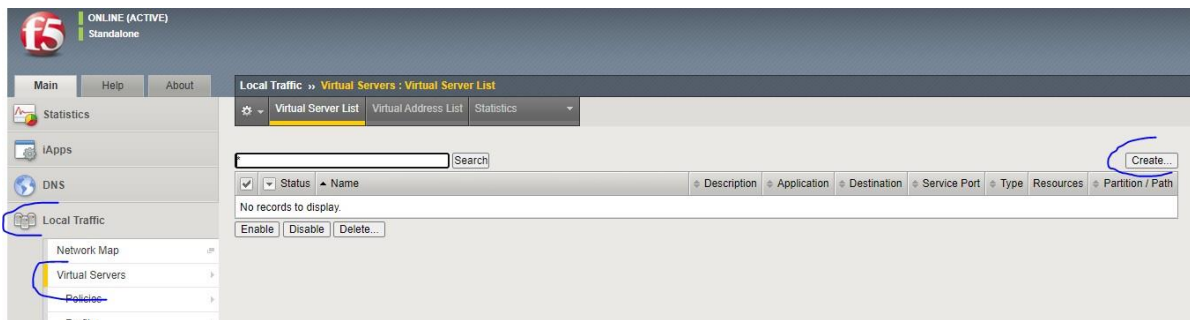
Si tous fonction bien nous devrions voir notre pool en vert comme le montre l'image Suivante :



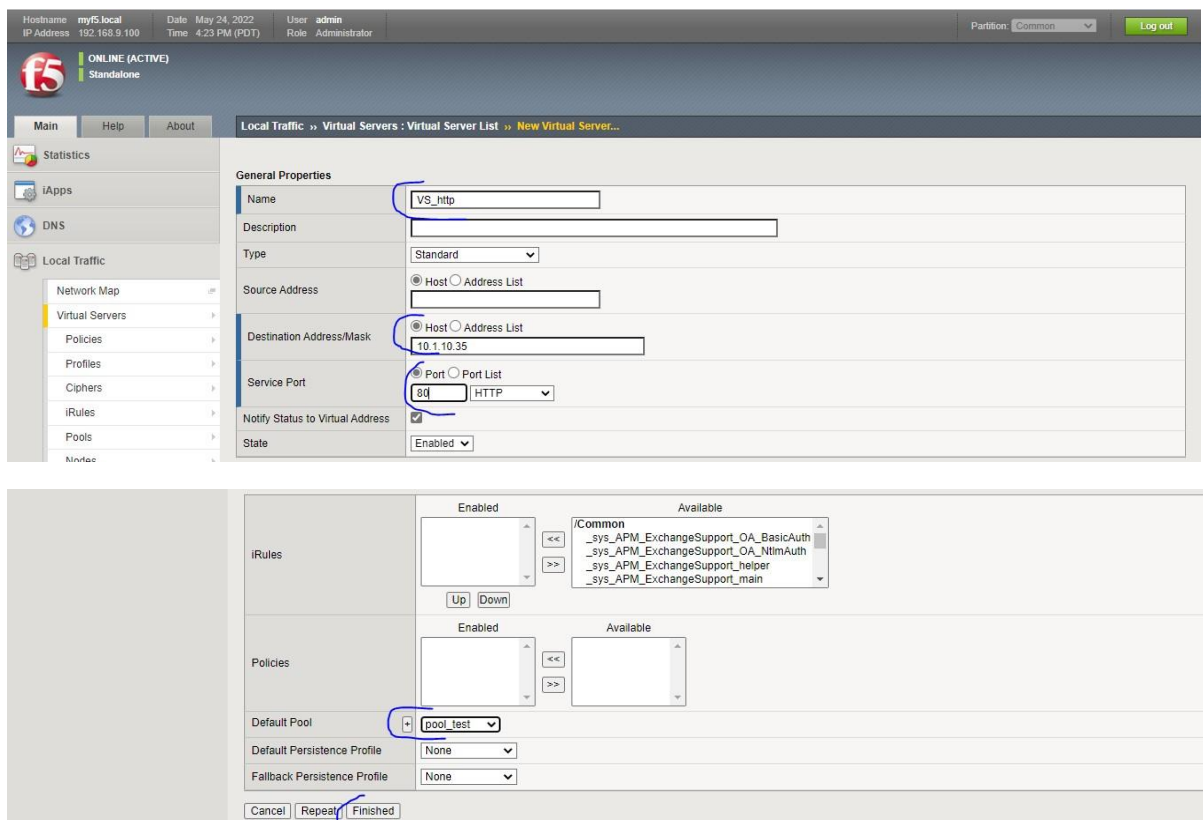
Si le voyant s'allume en rouge donc il y a un dysfonctionnement et il faut corriger cela

b. Virtual Servers

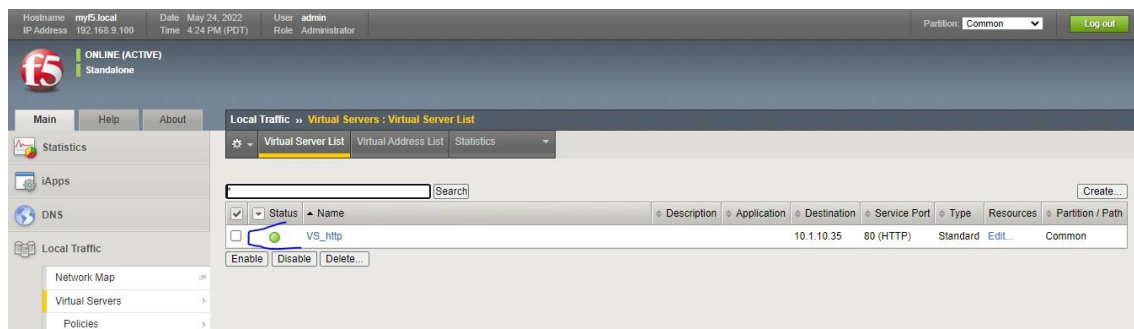
Les Virtual servers sont des serveurs virtuels qui nous permettrons de faire le load balancing sur nos différentes machines qui lui sont associées. Pour créer un VS on se rend sur local traffic puis sur virtuals servers et on clique sur create



Maintenant on lui donne un nom, puis l'adresse IP de destination qui correspond à Notre external network, le protocole puis les pools associés et on clique sur finished

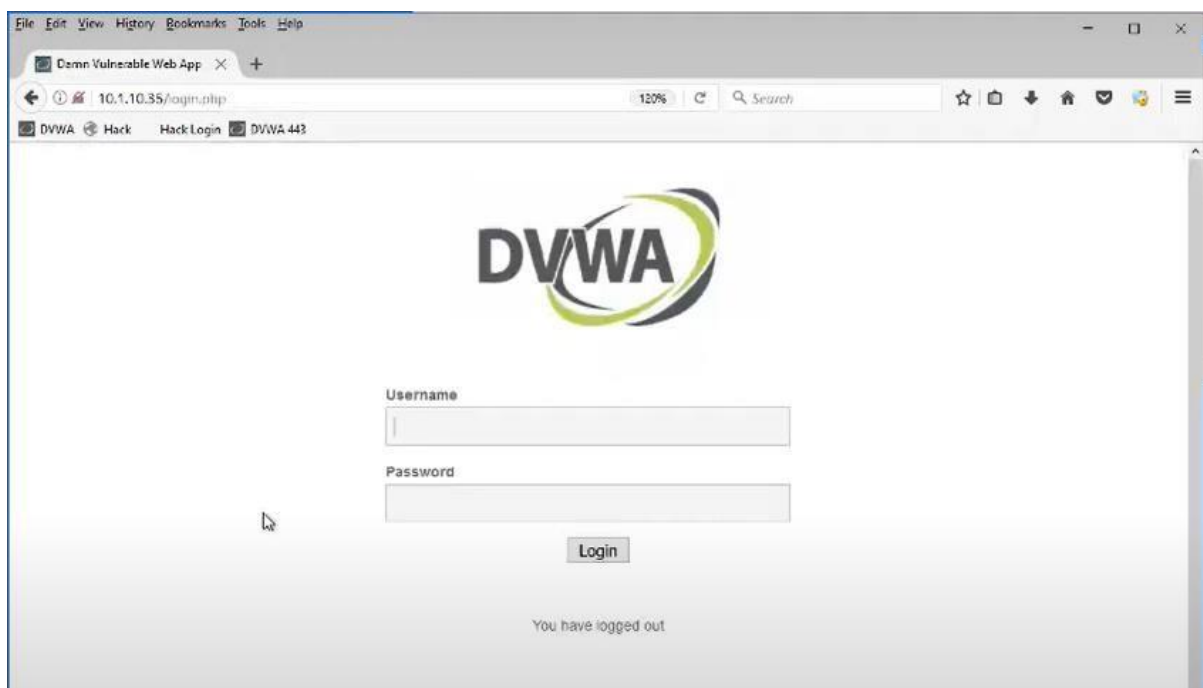


Si tout à fonctionner on doit voir le voyant s'allumer en vert



Si le voyant s'allume en rouge donc il ya un disfonctionnement et il faut corriger cela Puis en tapant l'adresse ip du virtual server, on doit accéder directement à nos

Machines en interne. C'est en fait le mode load balancing de F5 qui permet cela. Dans notre cas c'est la machine DVWA nommé web1 qu'on a utilisé en interne pour pouvoir tester également les vulnérabilités.



5. Sécurisation d'une Application Web avec F5

a. Test de vulnérabilités sur la machine DVWA

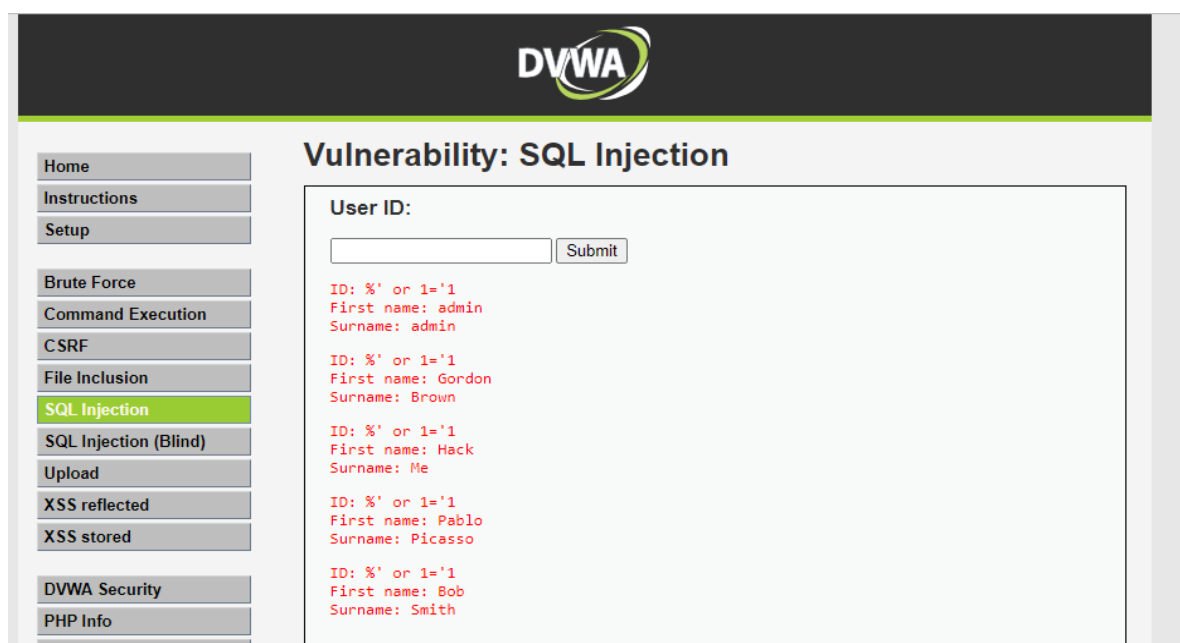
Maintenant nous allons dans un premier temps tester la vulnérabilité de la machine en effectuant des commandes d'intrusions :

Commande execution



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The left sidebar contains a menu with options: Home, Instructions, Setup, Brute Force, Command Execution (highlighted), CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area is titled "Vulnerability: Command Execution". It features a "Ping for FREE" section with a text input field containing "1 | cat /etc/passwd" and a "submit" button. Below the input field, a list of system users and their home directories is displayed in red text, including root, daemon, bin, sys, sync, games, man, lp, mail, news, uucp, proxy, www-data, backup, list, irc, gnats, nobody, libuuid, syslog, dvwa, sshd, messagebus, and usbmux.

SQL injection

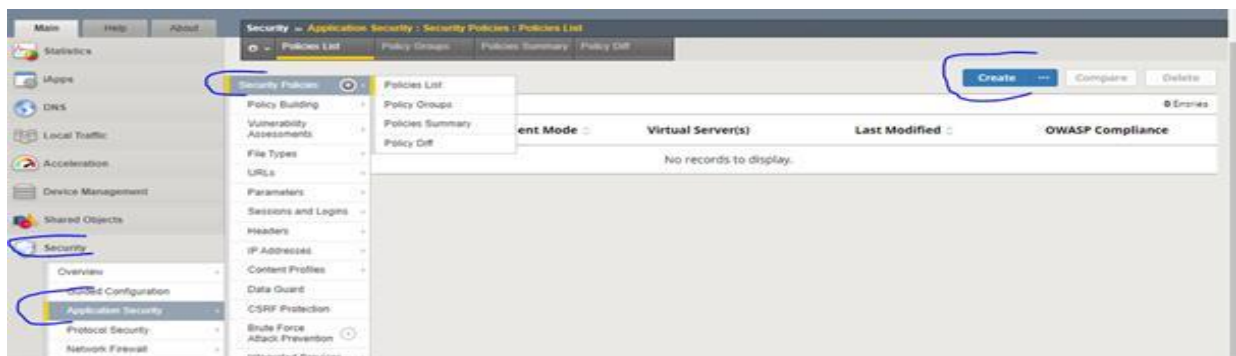


The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The left sidebar contains a menu with options: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (highlighted), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area is titled "Vulnerability: SQL Injection". It features a "User ID:" section with a text input field and a "Submit" button. Below the input field, a list of user details is displayed in red text, including ID, First name, and Surname for various users like admin, Gordon Brown, Hack Me, Pablo Picasso, and Bob Smith.



b. Protection avec F5

Pour protéger une application web avec F5, on doit d'abord s'assurer que la machine de l'application est associée à un virtual server. Maintenant on doit créer une politique de sécurité en nous rendant sur security>application security>security policies puis on clique sur create :



Ensuite on met le nom de la politique, on choisit le policy template (ici on choisit rapid deployment policy), on choisit le virtual server à appliquer puis tout en bas on choisit le mode bloquant pour bloquer les attaques entrantes et pour finir on clique sur save pour sauvegarder notre politique.

Security Policy Configuration

General Settings

Microservices

Attack Signatures

Threat Campaigns

Response and Blocking Pages

Policy Name *

Description

Policy Type ☒ Security ☐ Parent ?

Policy Template Learn more

Virtual Server ?

Application Language ?

Save **Cancel**

Security » Application Security : Security Policies : Policies List » Create New Policy...

Save **Cancel**

Security Policy Configuration

General Settings

Microservices

Attack Signatures

Threat Campaigns

Response and Blocking Pages

Application Language ?

Learning and Blocking

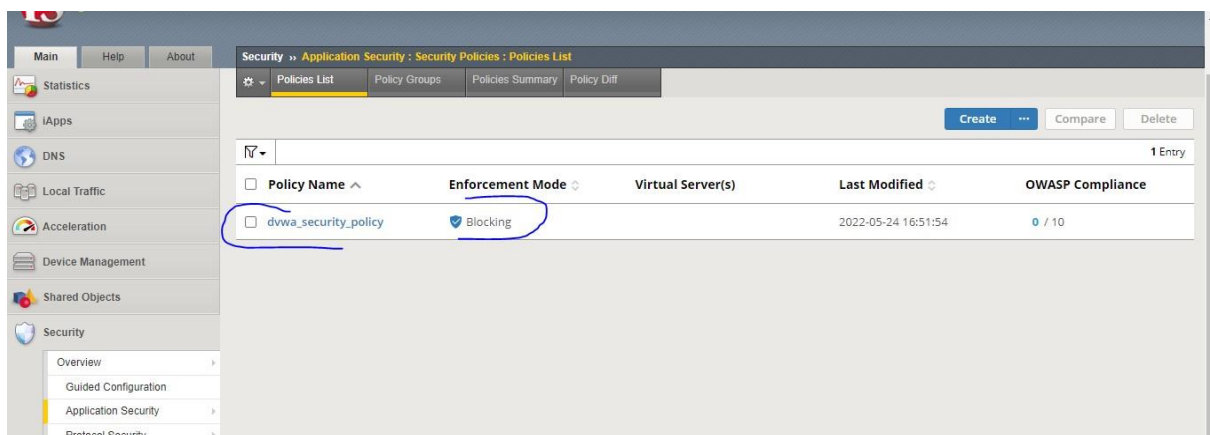
Enforcement Mode ☐ Transparent ☒ Blocking

Policy Building Learning Mode ☐ Automatic ☒ Manual ☐ Disabled ?

Auto-Added Signature Accuracy

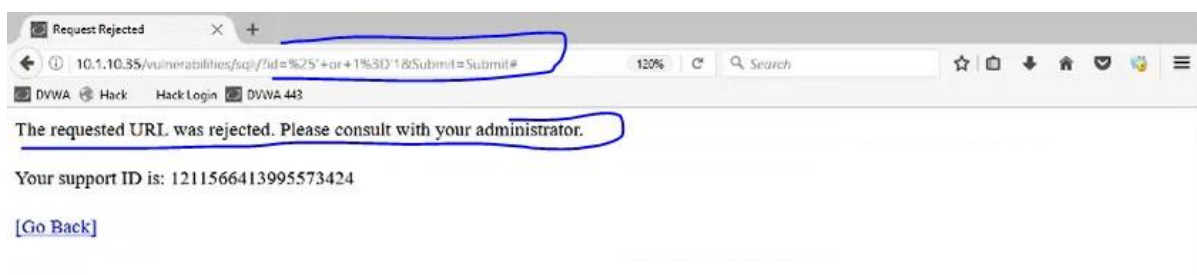
Signature Staging ☐ Enabled ☒ Disabled

Enforcement Readiness Period days



c. Re test des attaques sur la machine

Après la création de la politique de sécurité on va retester les attaques précédemment effectuées et là on peut remarquer que les attaques sont bloquées par F5.



Ainsi on peut voir que F5 BIG-IP permet de bloquer les attaques liées aux applications web notamment les injection SQL, les attaques XSS, les injections de commandes et plus encore.

A la fin de ce LAB nous pouvons attester que F5 BIG-IP est un excellent outil de sécurité notamment la sécurité des applications en empêchant les différentes attaques dont peuvent être victimes ces derniers.