

CHAPITRE 4 :

LA SECURITE DANS L'OPENSTACK

4.1 Introduction :

Dans ce chapitre nous allons présenter une étude sur la sécurité dans l'OpenStack, et puis en a explique comment utilise les outils de l'analyse les vulnérabilités et les outils de l'attaque d'un Cloud.

4.2 Création d'un Groupe de sécurité:

Les questions de sécurité, au sein d'OpenStack sont de la responsabilité du projet de sécurité. Le projet de sécurité est un effort horizontal au sein d'OpenStack qui est composé de ce qui était auparavant appelé le Groupe de sécurité OpenStack. L'équipe de gestion des vulnérabilités est également une partie du projet de sécurité.

Pour créer et configurer un groupe de sécurité on suit les étapes suivantes :

- Cliquez sur l'onglet Accès et Sécurité et sélectionnez Groupes de sécurité, et puis cliquez sur le bouton Créer groupe de sécurité.

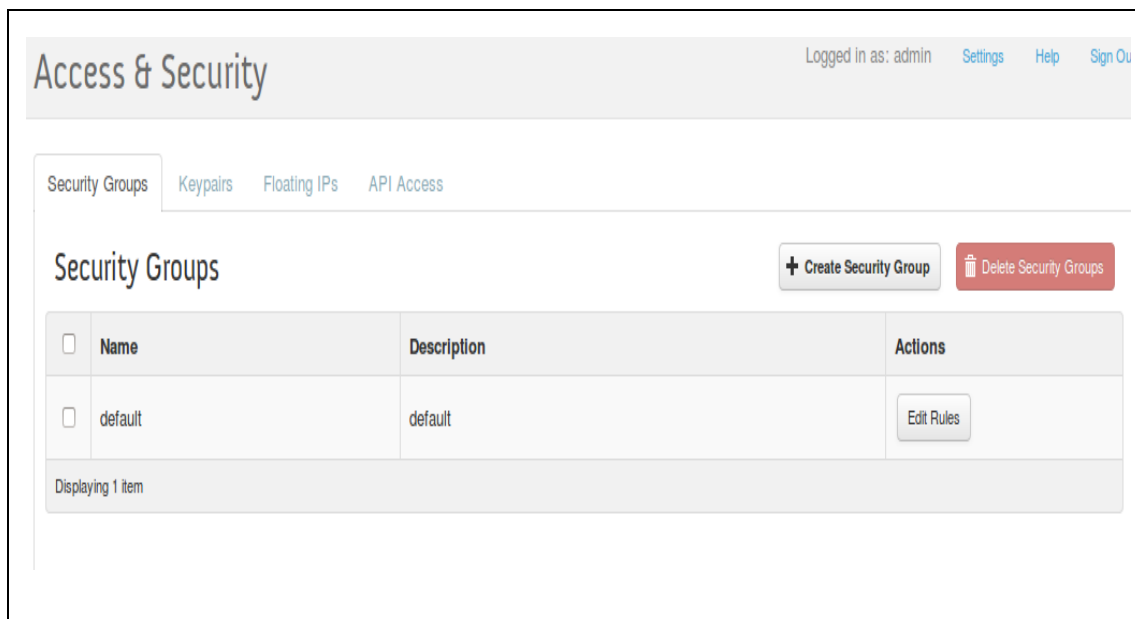


Figure 4.1: L'interface de la page Access & Security.

- Entrez le nom de votre nouveau groupe de sécurité et de la description, Cliquez sur le bouton Créer groupe de sécurité.

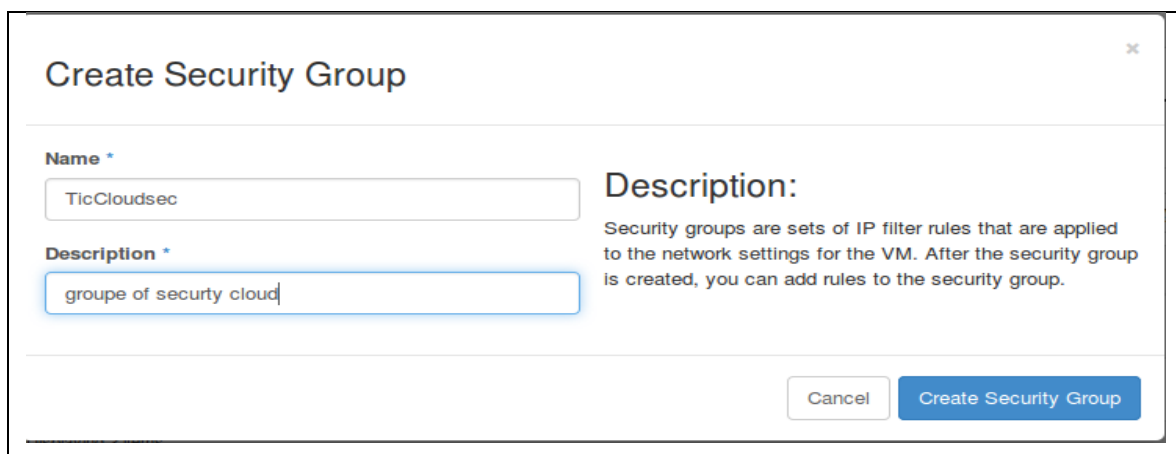


Figure 4.2: L'interface de la fenêtre Create Security Groupe.

- Après cela, nous pouvons voir le nouveau groupe de sécurité dans la liste des groupes.

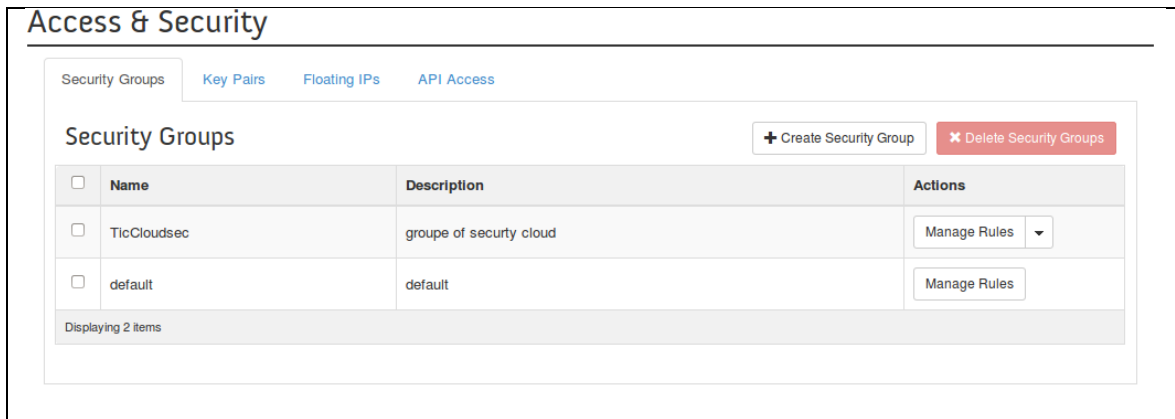


Figure 4.3: La liste des groupes de sécurité.

4.2.1. La rédaction des règles d'un groupe :

Appuyez sur le bouton Modifier les règles à côté du groupe de sécurité que vous souhaitez ajouter des règles / modifier. Nous allons utiliser le TicCloudsec Groupe de sécurité, d'abord ajouter une règle pour permettre les connexions SSH¹ entrantes sur le port 22.

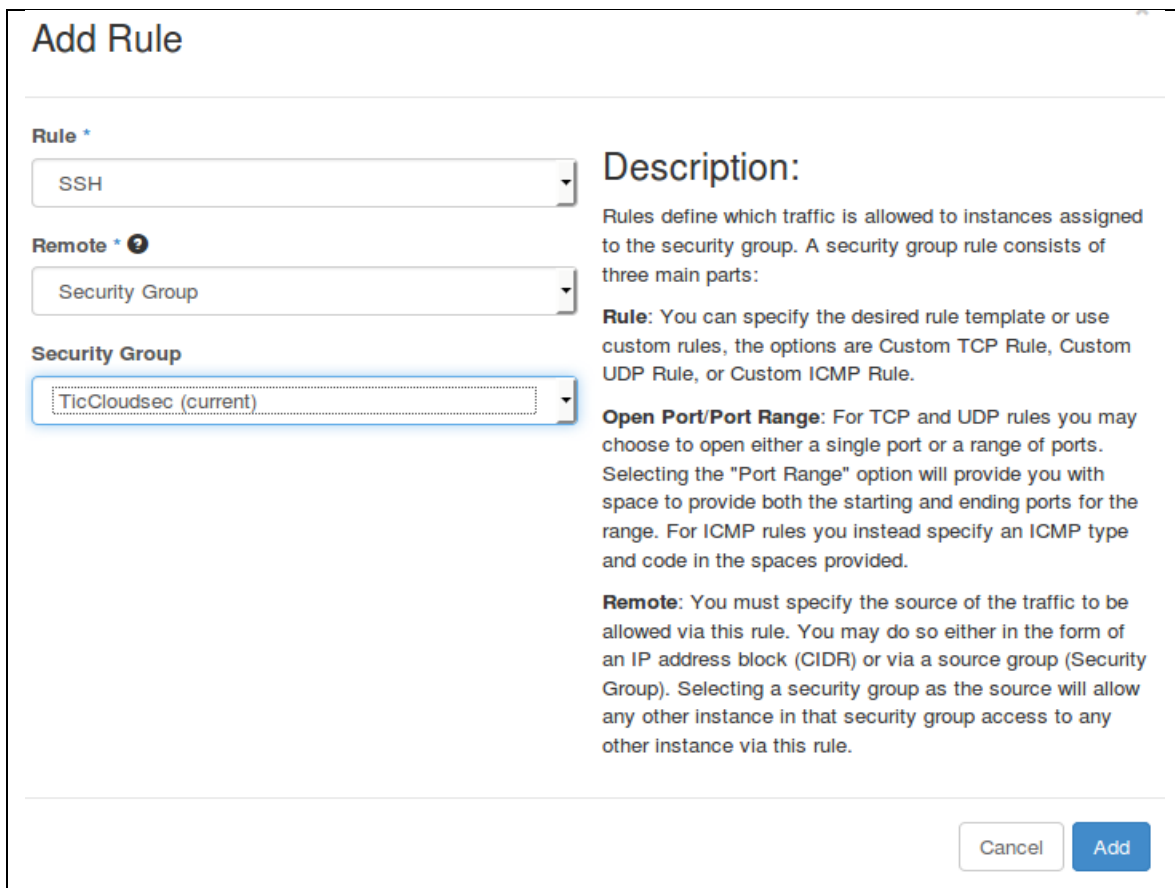


Figure 4.4: L'interface de la page pour ajouter des règles.

Maintenant, l'accès ssh est activé provenant de l'adresse IP spécifiée à toutes les machines virtuelles qui ont ce groupe de sécurité associé avec elles.

¹ **SSH** : Secure Shell un protocole de communication sécurisé.

La liste de tous les règles qui ajouter.

<input type="checkbox"/>	Direction	Ether Type	IP Protocol	Port Range	Remote	Actions
<input type="checkbox"/>	Ingress	-	ICMP	-1 (All ICMP)	TicCloudsec	Delete Rule
<input type="checkbox"/>	Ingress	-	TCP	1 - 65535	TicCloudsec	Delete Rule
<input type="checkbox"/>	Ingress	-	TCP	22 (SSH)	TicCloudsec	Delete Rule

Displaying 3 items

Figure 4.5: La liste des règles.

Ensuite, nous avons à générer une paire de clés qui seront utilisés pour authentifier les utilisateurs dans les machines virtuelles. Cliquez sur l'onglet "paires de clés" sur "l'accès et la sécurité" et cliquez sur "Créer une paire de clés".

Create Key Pair

Key Pair Name *

mykey

Description:

Key pairs are ssh credentials which are injected into images when they are launched. Creating a new key pair registers the public key and downloads the private key (a .pem file).

Protect and use the key as you would any normal ssh private key.

Cancel Create Key Pair

Figure 4.6: L'interface de création le paire de clés.

Téléchargez et enregistrez le fichier de clé. Il sera utilisé pour se connecter à des machines virtuelles à partir de l'extérieur.

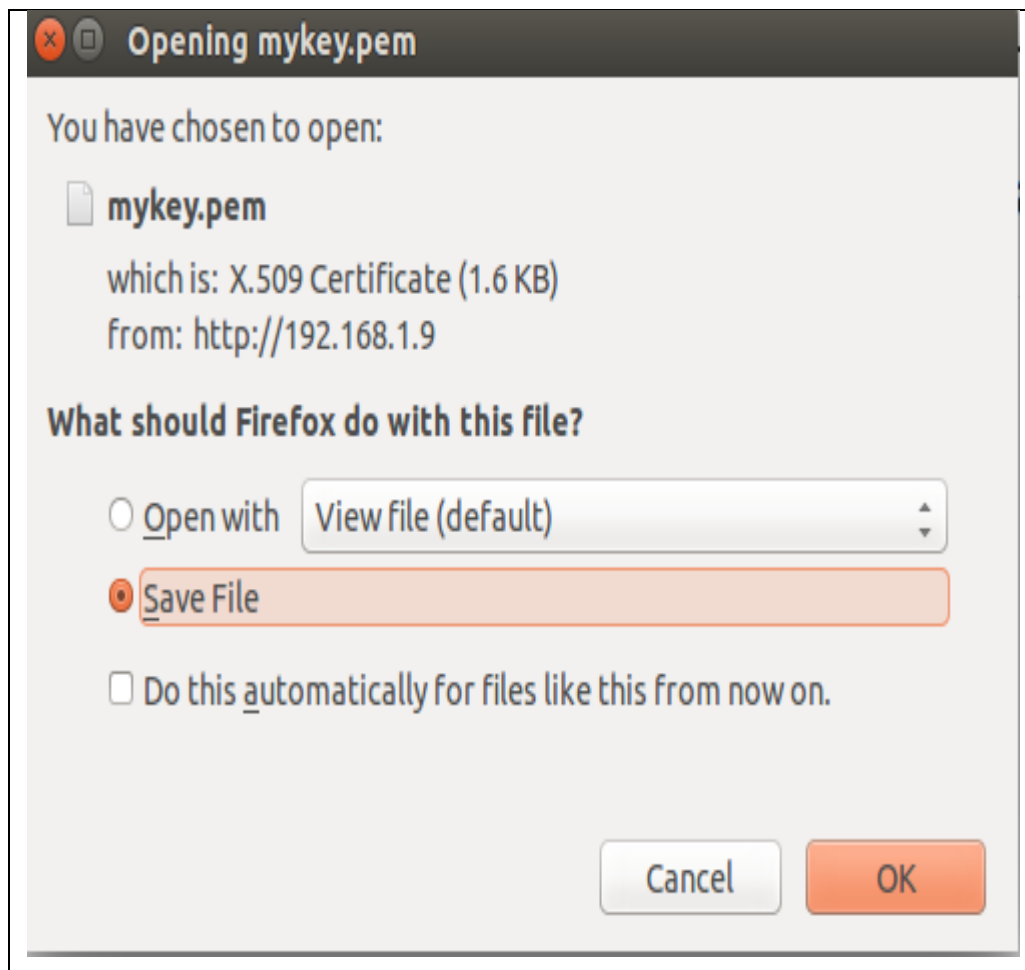


Figure 4.7: La fenêtre de téléchargement le fichier de clé.

4.2.2. La création des instances :

Une instance est une machine virtuelle que OpenStack dispose sur un nœud de calcul.

Maintenant, nous pouvons créer une instance en utilisant le groupe de sécurité et la paire de clés que nous avons créés. Cliquez sur le lien "Instances" sous l'onglet "Project" et cliquez sur "Lancer instance".

Launch Instance

Details * Access & Security * Post-Creation Advanced Options

Availability Zone

nova

Instance Name *

moussa

Flavor * ?

m1.nano

Instance Count * ?

1

Instance Boot Source * ?

Select source

Specify the details for launching an instance.
The chart below shows the resources used by this project in relation to the project's quotas.

Flavor Details

Name	m1.nano
VCPUs	1
Root Disk	0 GB
Ephemeral Disk	0 GB
Total Disk	0 GB
RAM	64 MB

Project Limits

Number of Instances 0 of 10 Used

Figure 4.8: L'interface de création des instances.

Dans l'interface utilisateur, vous pouvez configurer l'exemple en fournissant un nom, taille, etc.... sous l'onglet "Détails".

Sous l'onglet "Accès et Sécurité" nous pouvons choisir la paire de clés et le groupe de sécurité que nous créons ci-dessus.

Keypair

mykey

Admin Pass

Confirm Admin Pass

Security Groups

☒ default

Control access to your instance via keypairs, security groups, and other mechanisms.

Cancel Launch

Figure 4.9: L'interface de l'ajout de la clé et du groupe.

Après avoir configuré l'instance, cliquez sur "Lancer". Puis attendre l'instance entre un état "Running".

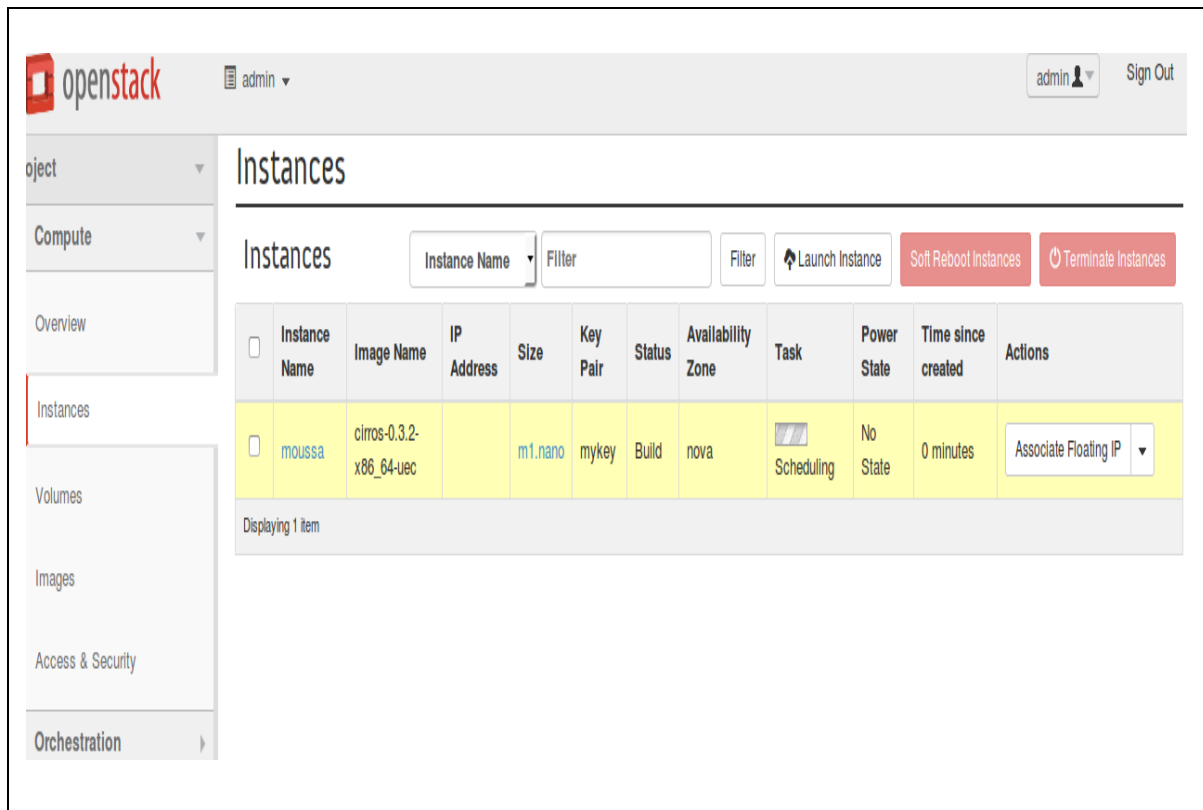


Figure 4.10: La liste des instances.

4.2.3. Une vue d'ensemble sur le système :

Dans la figure 4.11 une vue d'ensemble "overview" sur les ressources utilisées dans ce système.

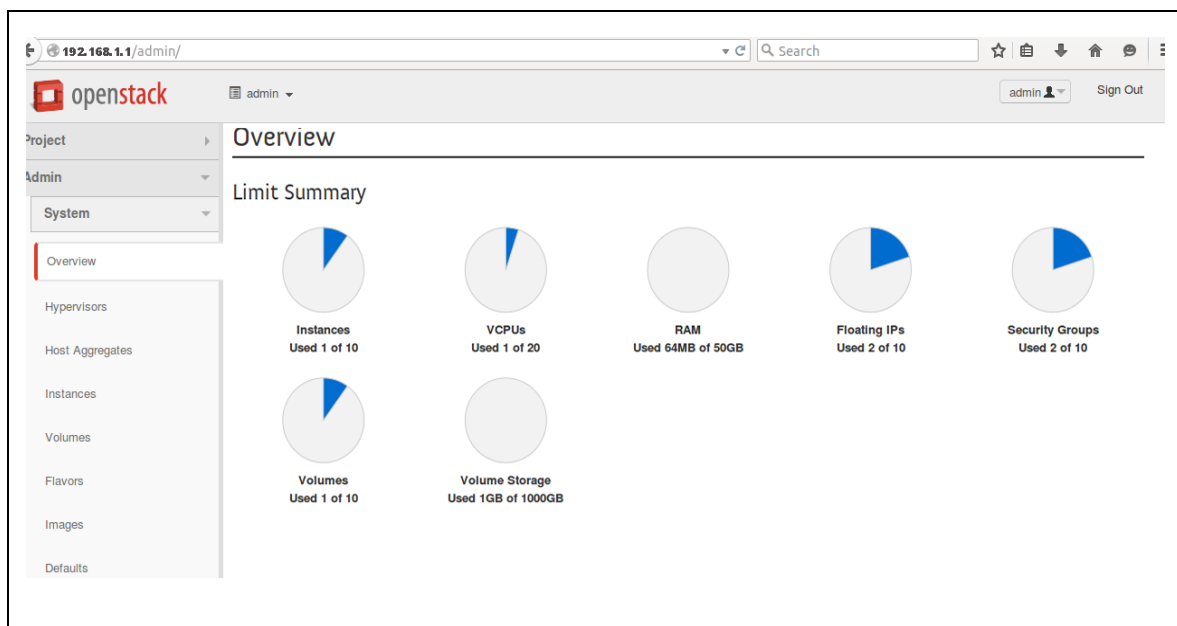


Figure 4.11: Une vue d'ensemble sur le système.

4.3 Les scanners des vulnérabilités:

Un scanner de vulnérabilité est un programme conçu pour identifier des vulnérabilités dans une application, un système d'exploitation, ou un réseau,cloud.

Les scanners de vulnérabilité peuvent être utilisés dans des objectifs licites ou illicites :

- objectifs licites : les experts en sécurité informatique des entreprises utilisent les scanners de vulnérabilité pour trouver les failles de sécurité des systèmes informatiques et des systèmes de communications de leurs entreprises dans le but de les corriger avant que les pirates informatiques ne les exploitent ;
- objectifs illicites : les pirates informatiques utilisent les mêmes équipements pour trouver les failles dans les systèmes des entreprises pour les exploiter à leur avantage.

Il existe plusieurs programmes :

- Nexpose, un scanner de vulnérabilité de Rapid7 (propriétaire de Metasploit).
- Nessus.
- OpenVAS, un scanner de vulnérabilité libre.
- Snort, un système de détection d'intrusion.
- Nmap, un scanner de ports.

Nous allons présenter une petite explication sur le meilleur scanner dans ce chapitre (Nessus, Nmap).

4.3.1. Nessus :

Nessus est un outil de sécurité informatique. Il signale les faiblesses potentielles ou avérées sur les machines testées. Ceci inclut, entre autres :

- Les services vulnérables à des attaques permettant la prise de contrôle de la machine, l'accès à des informations sensibles (lecture de fichiers confidentiels par exemple), des dénis de service.
- Les fautes de configuration (relais de messagerie ouvert par exemple)
- Les patchs de sécurité non appliqués, que les failles corrigées soient exploitables ou non dans la configuration testée.
- Les mots de passe par défaut, quelques mots de passe communs, et l'absence de mots de passe sur certains comptes systèmes. Nessus peut aussi appeler le programme externe Hydra pour attaquer les mots de passe à l'aide d'un dictionnaire.
- Les services jugés faibles (on suggère par exemple de remplacer Telnet par SSH).
- Les dénis de service contre la pile TCP/IP .
- Scan les vulnérables des Cloud Computing.[12]

Pour utiliser Nessus suivre les étapes suivantes :

Une fois Nessus installé et tous les plugins installés, lancez cette commande via le terminal :

/etc/init.d/nessusd start

Nessus est maintenant lancé. Rendez vous à l'adresse <http://127.0.0.1:8834> ou <http://votremachine:8834> pour vous connecter à Nessus. Laissez-le s'initialiser, puis vous serez redirigés vers la page de login où vous devrez vous identifier.

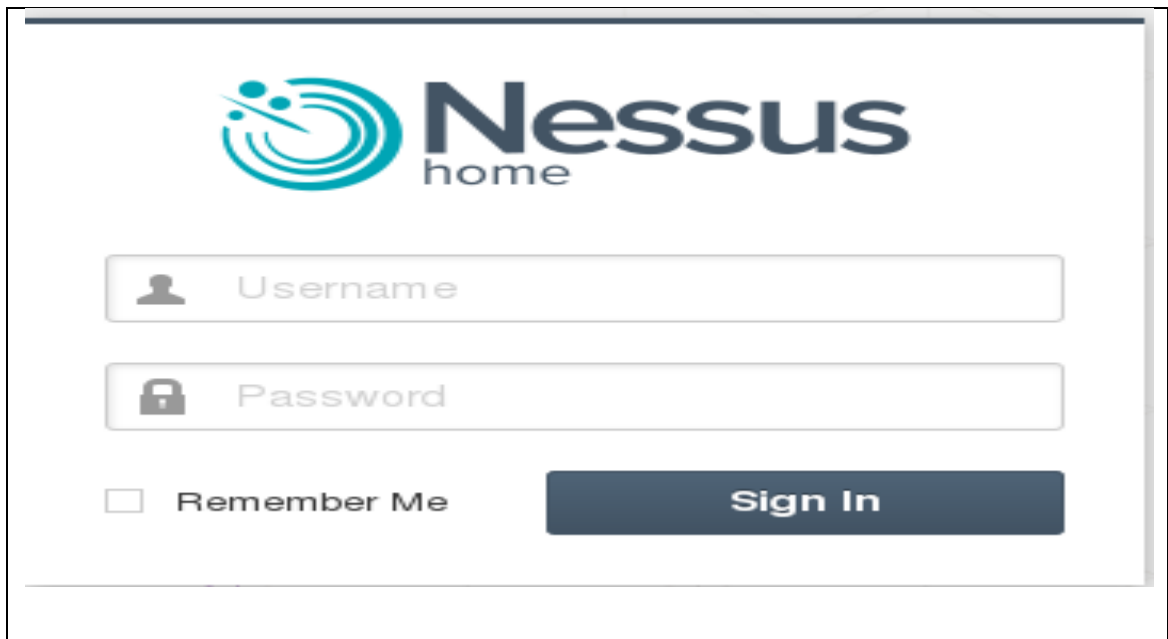


Figure 4.12: La page login sur Nessus.

Une fois identifié, vous serez amenés sur la page d'accueil, où il faudra en premier temps créer une nouvelle Policy. Cliquez sur le bouton en haut à gauche et cliquez sur Policy. et puis choisir le type de scan puis créez en une nouvelle avec les paramètres par défauts.

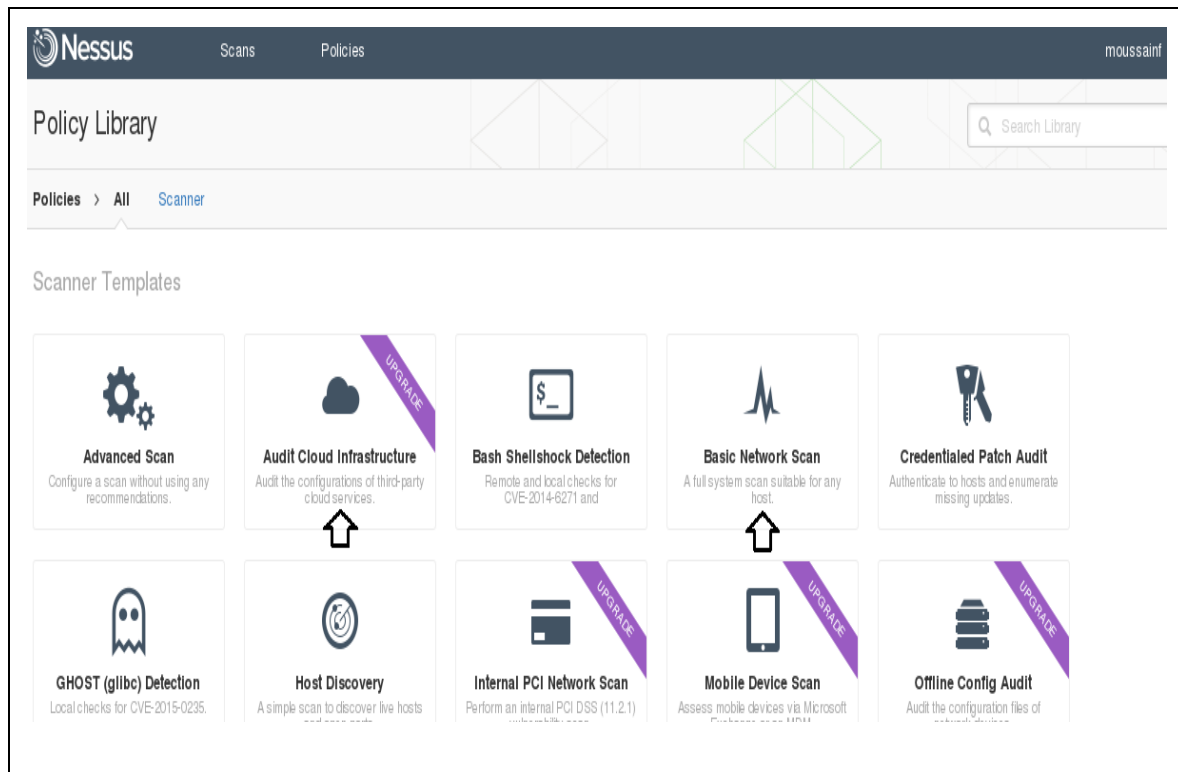


Figure 4.13: La page de la nouvelle Policy.

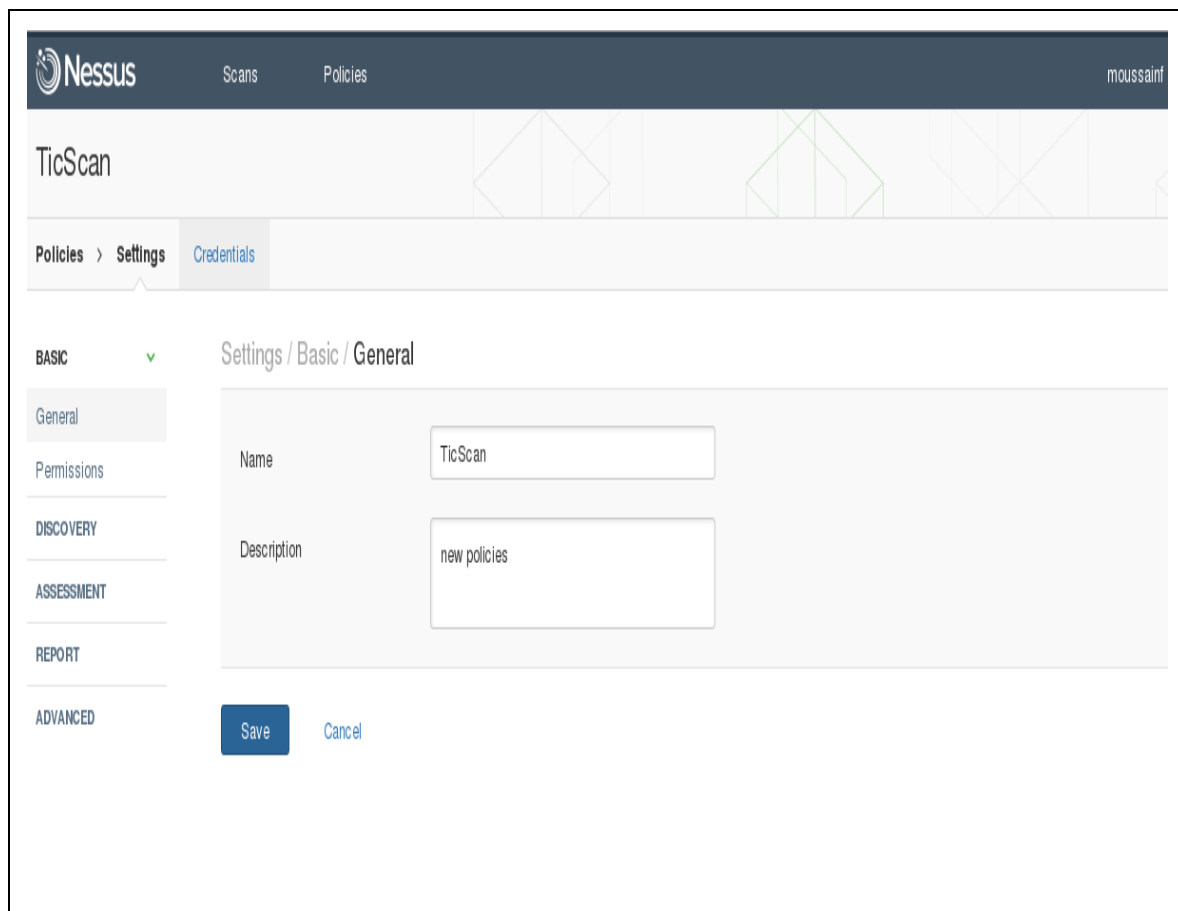


Figure 4.14: La configuration de Policy.

Pour effectuer un scan, cliquez sur New Scan et indiquez le nom du scan, la description, la police (celle que nous avons créé tout à l'heure) et la liste des hôtes à scanner.

Ici, mettez l'adresse IPv4 de la Target, pour nous ce sera 192.168.1.1 Le scan devrait se lancer. Attendez un moment, le temps que Nessus scan la machine(Cloud), puis une fois que Nessus vous indiquera que le scan est terminé, cliquez sur le scan pour afficher le résultat du scan.

The screenshot shows the 'New Scan / Basic Network Scan' configuration page in Nessus. The breadcrumb trail is 'Scan Library > Settings > Credentials'. The left sidebar has a 'BASIC' section with a green checkmark, containing 'General' (selected), 'Schedule', and 'Email Notifications'. Below this are 'DISCOVERY', 'ASSESSMENT', 'REPORT', and 'ADVANCED'. The main content area is titled 'Settings / Basic / General' and contains the following fields:

- Name:** TicScan
- Description:** scan vulnerability of cloud computing TicCloud
- Folder:** My Scans (dropdown menu)
- Scanner:** Local Scanner (dropdown menu)
- Targets:** 192.168.1.1

Figure 4.15: La configuration de scan.

4.3.2. Nmap :

Nmap est un scanner de ports libre créé par Fyodor et distribué par Insecure.org. Il est conçu pour détecter les ports ouverts, identifier les services hébergés et obtenir des informations sur le système d'exploitation d'une machine distante,

Ce logiciel est devenu une référence pour les administrateurs réseaux car l'audit des résultats de Nmap fournit des indications sur la sécurité d'un réseau. Il est disponible sous Windows, Mac OS X, Linux, BSD et Solaris. [12]

On utilise le Nmap parce que le OpenStack est installé sur une machine Virtual, donc La figure 4.15 montré le scan de Nmap :

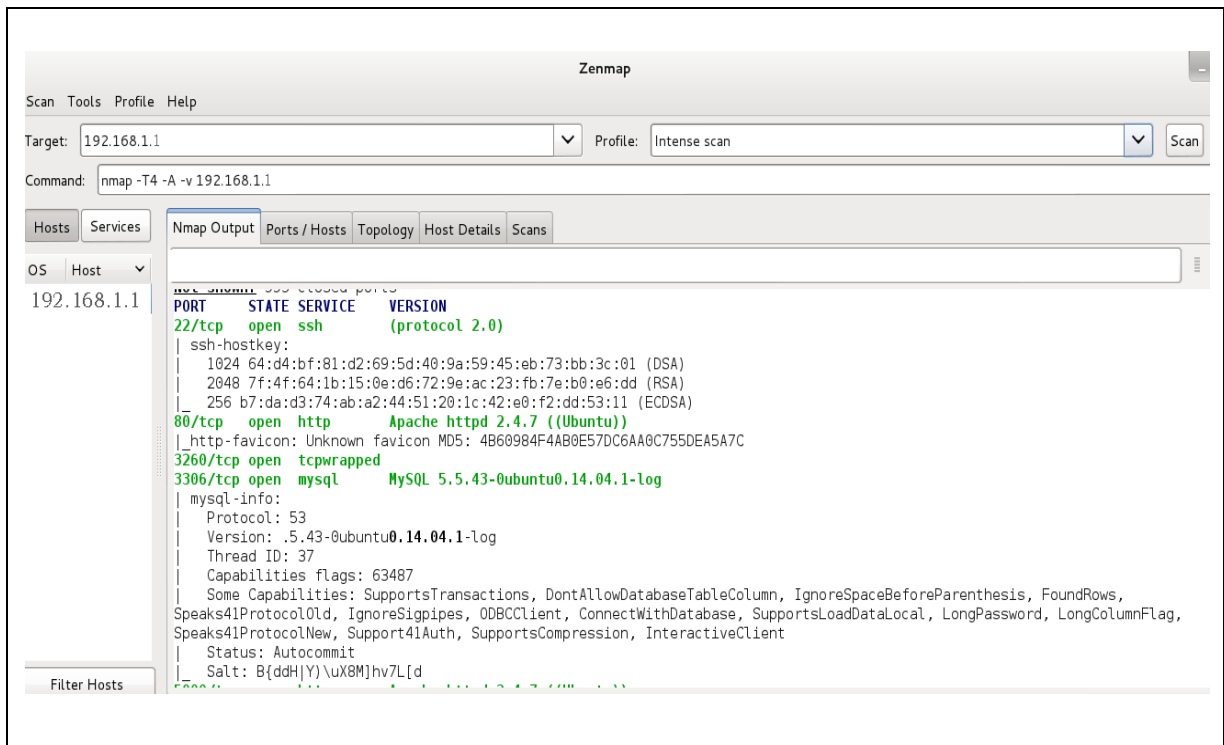


Figure 4.16: Nmap.

4.4 Les techniques d'attaque :

Il existe deux types d'attaques :

- **Attaques passives** : elles ne modifient pas le comportement du système, et peuvent ainsi passer inaperçues.
- **Attaques actives** : elles modifient le contenu des informations du système ou le comportement du système. Elles sont en général plus critiques que les passives.

4.4.1. Footprinting :

Le Footprinting est la technique consistant à récolter des informations sur des systèmes informatiques et toutes les entités auxquelles ils sont rattachés. Cela est effectué par le biais de plusieurs techniques, Dans le jargon de la sécurité informatique, le Footprinting se réfère généralement aux étapes précédant une attaque. Pour faire du Footprinting, nous allons utiliser :

- **Maltego** : est une application de l'intelligence de la source et la criminalistique ouverte. Il vous offrira une manière facile de la collecte des informations ainsi que la représentation de ces informations dans un format facile à comprendre. [14] Exemple qui nous présente sur le cloud **dropbox.com**, dans la figure 4.16.

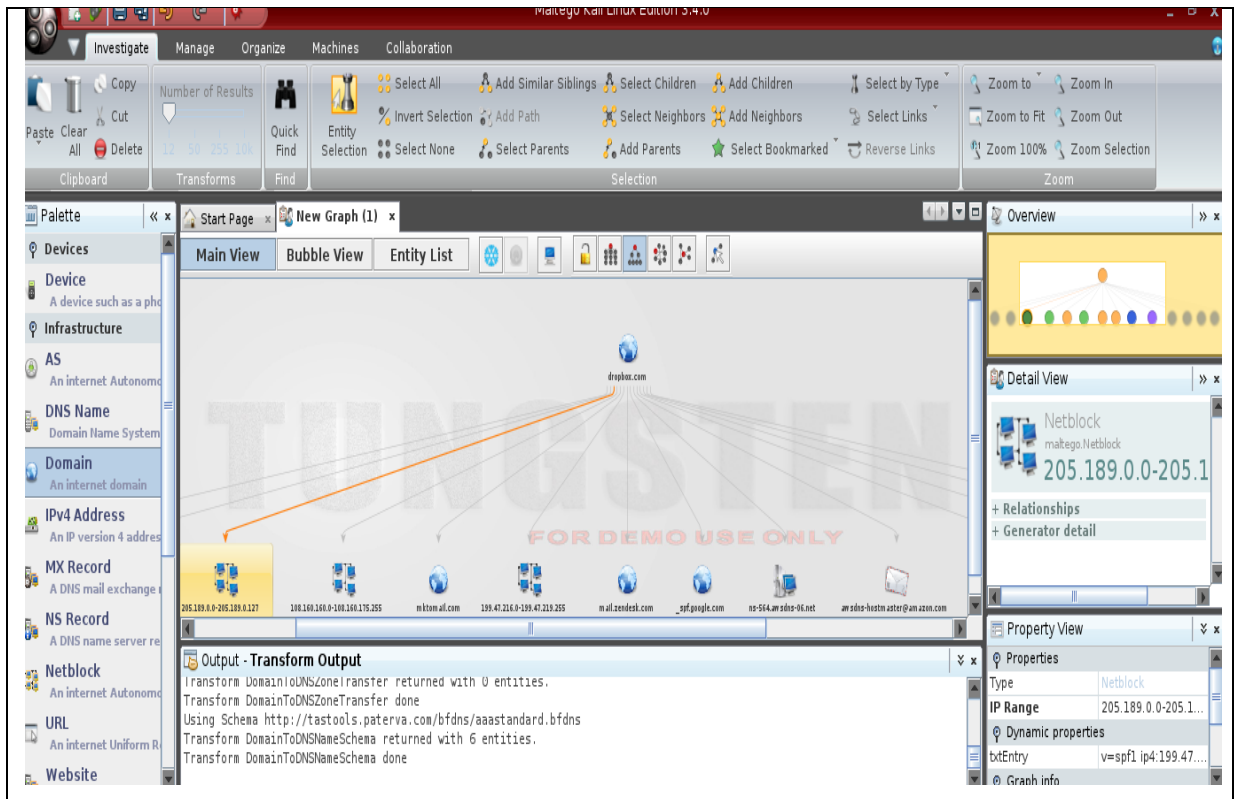


Figure 4.16 : Maltego Footprinting.

4.4.2. DOS Le déni de service:

Les attaques par déni de service ont pour seul but d'empêcher le bon fonctionnement d'un cloud et non de récupérer des informations.

Exemple : Slowloris est un script écrit en Perl utilise une attaque de type DoS (attaque par déni de service), il affecte en particulier les serveurs Apache 1.x et 2.x qui représentent 67% des serveurs sur le net.

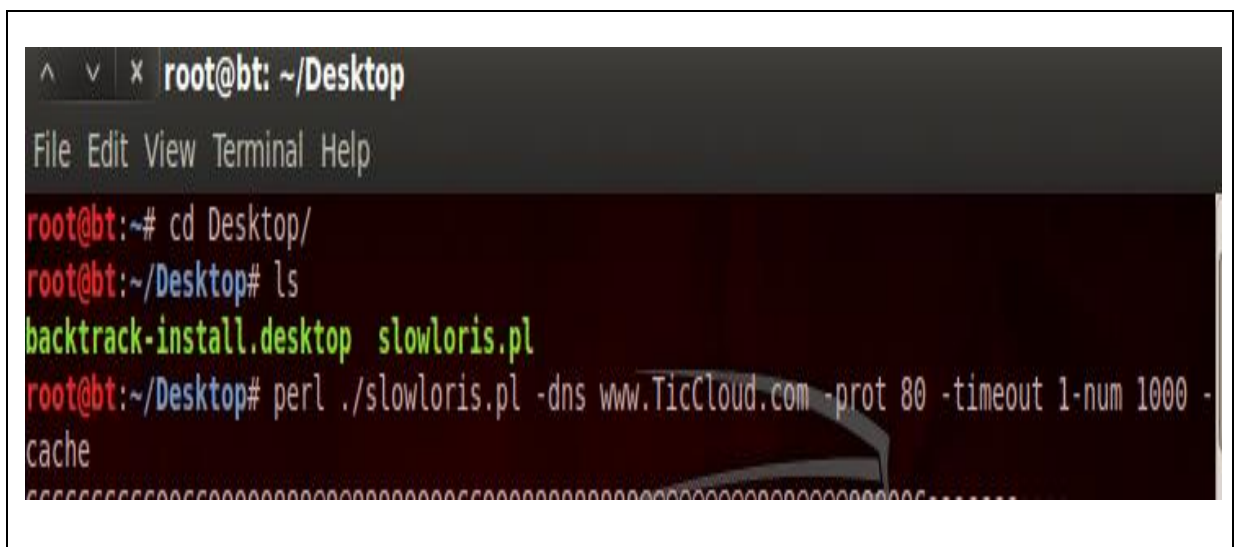


Figure 4.17 : Utilisation de Slowloris.

- La protection contre les attaques par déni de service :

La Protection contre ces attaques est d'organiser les communications des paquets et de mettre des règles strictes pour réglementer les télécommunications et les applications de réception et de traitement, et reste l'expérience de l'attaquant de se débarrasser de ces règles et, éventuellement, ainsi que d'étudier le mur et peut-être trouver que vous oubliez la nature des colis, qui fait prendre des mesures d'attaque par déni des services .

Les outils les plus importants pour aider à protéger contre des attaques par déni de service :

1. **CSF firewall (ConfigServer Services) :** Des systèmes les plus puissants, les pare-feux orientés vers des serveurs Linux, ce firewall des chiffres les tables IP pour les systèmes Linux exécutant et les rend très faciles.
2. **service Cloudflare :** Est un service qui permet de fournir une bonne protection pour Cloud Computing de la plupart des attaques, notamment les inondations, car il aide les visiteurs à naviguer sur le site avec toute la légèreté et la pièce en réduisant le nombre de demandes adressées, Ceci est grâce à son réseau mondial de l'intelligente distribuée dans le monde entier. [15]

4.5 Conclusion :

Dans cette dernière partie de notre projet, nous avons présentés la sécurité dans l'OpenStack, et les scanners des vulnérabilités utilisées actuellement dans Cloud Computing.