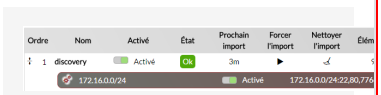
Découverte réseau

Shinken Enterprise vous permet de détecter automatiquement des équipements réseau et des serveurs physiques dans votre infrastructure pour faciliter et accélérer leur import dans la configuration.

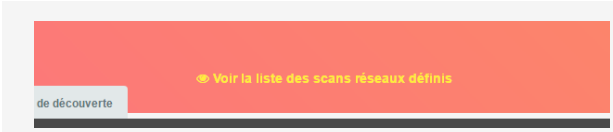
Editer et ajouter une liste de scan réseau

Le scan réseau peut être défini dans le Menu de la configuration.

Commencez par cliquer sur la source "discovery" dans la page principale .

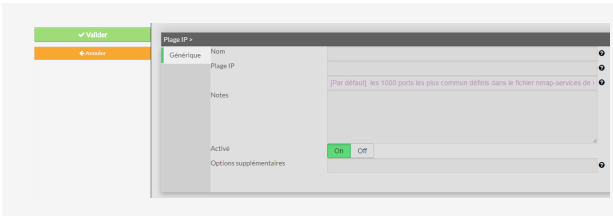


Puis cliquez sur "voir la liste des scan réseau"



Vous pouvez activer un nouveau scan avec le bouton "Ajouter un nouveau scan".

Puis vous verrez la page de configuration d'un nouveau scan.



Vous devez définir les paramètres suivants:

- Nom
- IP range: doit correspondre à la définition de la commande nmap

Par exemple: 172.16.1.1-254

- intervalle de scan en minutes
- Vous pouvez également ajouter des notes au sujet de ce scan

Ajouter un nouveau scan va le rendre automatiquement actif et vous verrez très rapidement apparaître de nouveaux éléments.

Ajouter un nouveau port dans une règle

Sans règles, les données générées par la découverte sont sans intérêt. Les règles sont définies dans le fichier the /etc/shinken/discovery_rules.cfg
Voici un exemple de comment définir le modèle d'hôte "ftp" pour tout ce qui est détecté par nmap avec le port TCP/21 ouvert:
Il y a 3 parties principales dans la règle:

- **discoveryrule_name**: doit être unique
- **creation_type**: doit être un hôte
- **openports**: regexp au sujet du port qui correspondra .Le ^ et $ est pour la regexp, Donc 21 et seulement 21 correspondre, et pas 210 par exemple.
- **+use**: qu'utilisera l'objet. Vous pouvez ajouter autant de propriétés que souhaité.

```
define discoveryrule {
discoveryrule_name
FtpRule
creation_type host
openports ^21$
+use ftp
}
```

Liste des ports par défaut pour les règles de modèles d'hôtes

Selon les ports ouverts détectés suites aux différents scans, des modèles d'hôtes seront ajoutés automatiquement aux machines détectées.

Les ports par defaut ainsi que leur modèles associés sont les suivants:

Port	Modèle d'hôte appliqué
27017	*mongodb*
53	*dns*
25	*smtp*
465	*smtps*
3306	*mysql*
22	ssh
110	pop3
995	pop3s
9100	printer-hp
1521	oracle
80	http
443	https
1433	mssql
2301	hp-asm
143	imap
993	imaps
389	ldap
636	ldaps

Sécurité: paramètres de la commande nmap

La commande nmap lancée par la source discovery utilise les paramètres suivants:

- **-PE** : Ping Scan (Echo Request)
- **-sU** : Scan UDP
- **-sT** : Scan TCP
- **--min-rate 1000** : Envoie un minimum de 1000 paquets par secondes

- **--max-retries 3** : Effectue au maximum 3 retransmissions en cas d'erreur sur les scan de ports
- **-T4** : Optimisation de performances
- **-O** : Detection des systèmes d'exploitation
- **-oX** : Export XML (utilisé pour l'interprétation de données par Shinken)