



Institut Supérieur d'Informatique DAKAR

Département Réseaux et Systèmes

Classe : M1 SSIM

Module : Cryptologie

Prof : DR. KHALIFA

Rapport d'Analyse et de Surveillance Réseau
avec NTOPNG, Nessus



ntop



Réalisé par :

Khadim Rassoul THIAM

Khadim MBAYE

Mamadou DIENG

Année Académique 2024 - 2025

SOMMAIRE

Introduction

1. NTOPNG : Surveillance du Trafic Réseau

1.1 Présentation de NTOPNG

1.2 Installation et Configuration

1.3 Analyse du trafic réseau

1.4 Cas d'utilisation et exemples

2. Nessus : Analyse des Vulnérabilités

2.1 Présentation de Nessus

2.2 Installation et Configuration

2.3 Détection des vulnérabilités

2.4 Cas d'utilisation et exemples

Conclusion

Références

Introduction

La cybersécurité et la surveillance réseau sont des éléments essentiels pour garantir l'intégrité, la disponibilité et la confidentialité des systèmes d'information. Dans ce rapport, nous explorons l'utilisation de **NTOPNG** pour la surveillance du trafic réseau et **Nessus** pour l'analyse des vulnérabilités. Ces outils permettent d'améliorer la visibilité et la sécurité d'un réseau informatique en identifiant les menaces et en optimisant les performances.

1. NTOPNG : Surveillance du Trafic Réseau

1.1 Présentation de NTOPNG

NTOPNG (Next-Generation Network Traffic Monitoring) est un outil avancé de surveillance du trafic réseau. Il permet d'afficher en temps réel les flux réseau, d'identifier les utilisateurs et de détecter d'éventuelles anomalies. Ses principales fonctionnalités incluent :

- La visualisation du trafic en temps réel.
- L'analyse des protocoles et des connexions.
- L'intégration avec d'autres outils comme Elasticsearch.
- La détection de comportements suspects sur le réseau.

1.2 Installation et Configuration

1.2.1 Pré-requis système

- Un serveur sous Linux (Ubuntu/Debian/CentOS) ou Windows.
- Une carte réseau configurée en mode promiscuité pour capturer le trafic.
- Accès administrateur pour l'installation.

1.2.2 Étapes d'installation sous Linux

1. Mettre à jour le système

```
sudo apt update && sudo apt upgrade -y
```

2. Installer NTOPNG et ses dépendances

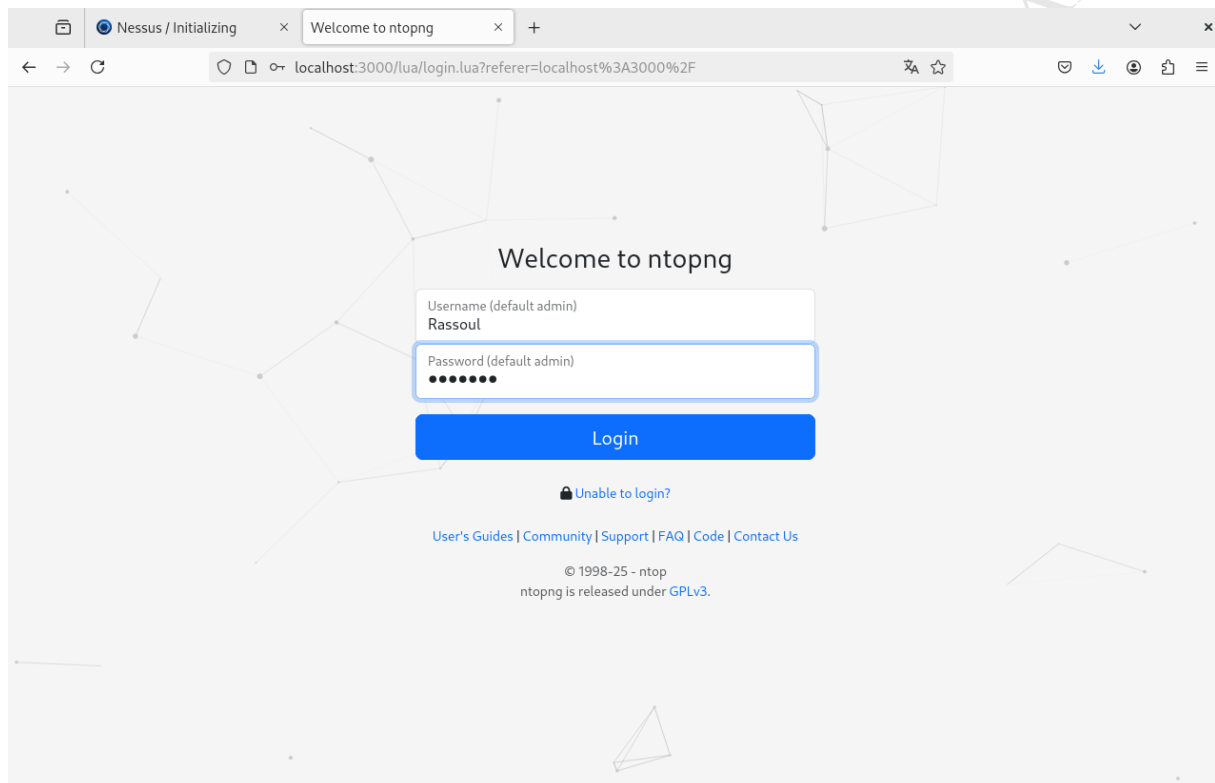
```
sudo apt install ntopng -y
```

3. Configurer NTOPNG en éditant le fichier /etc/ntopng/ntopng.conf

4. Démarrer le service

```
sudo systemctl start ntopng
```

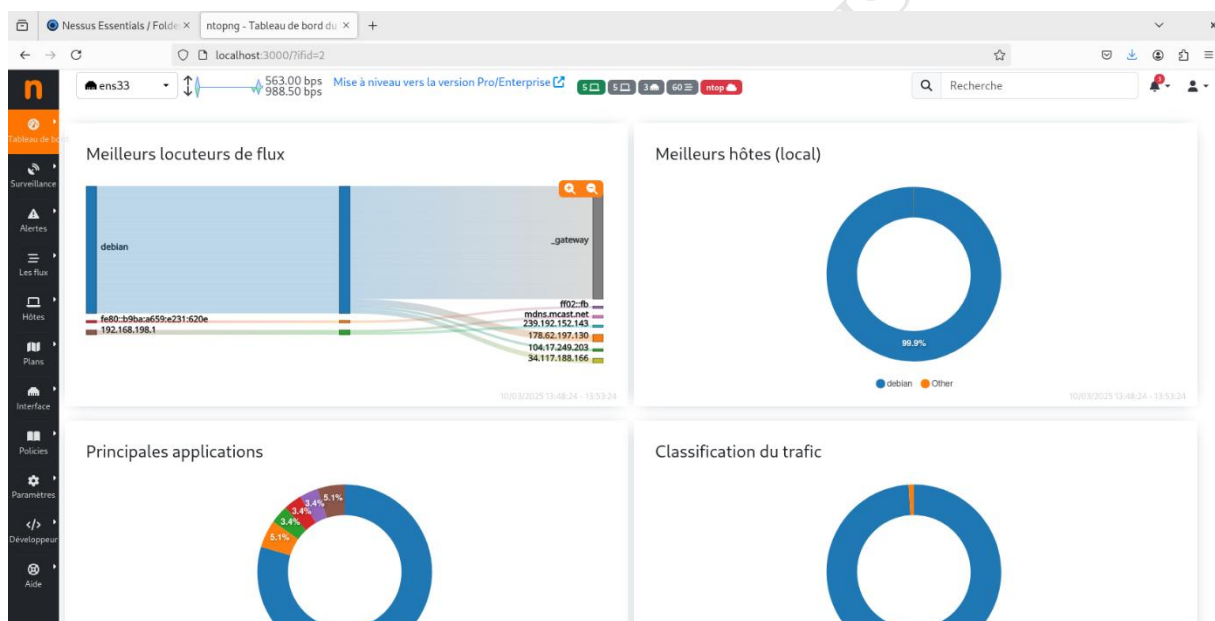
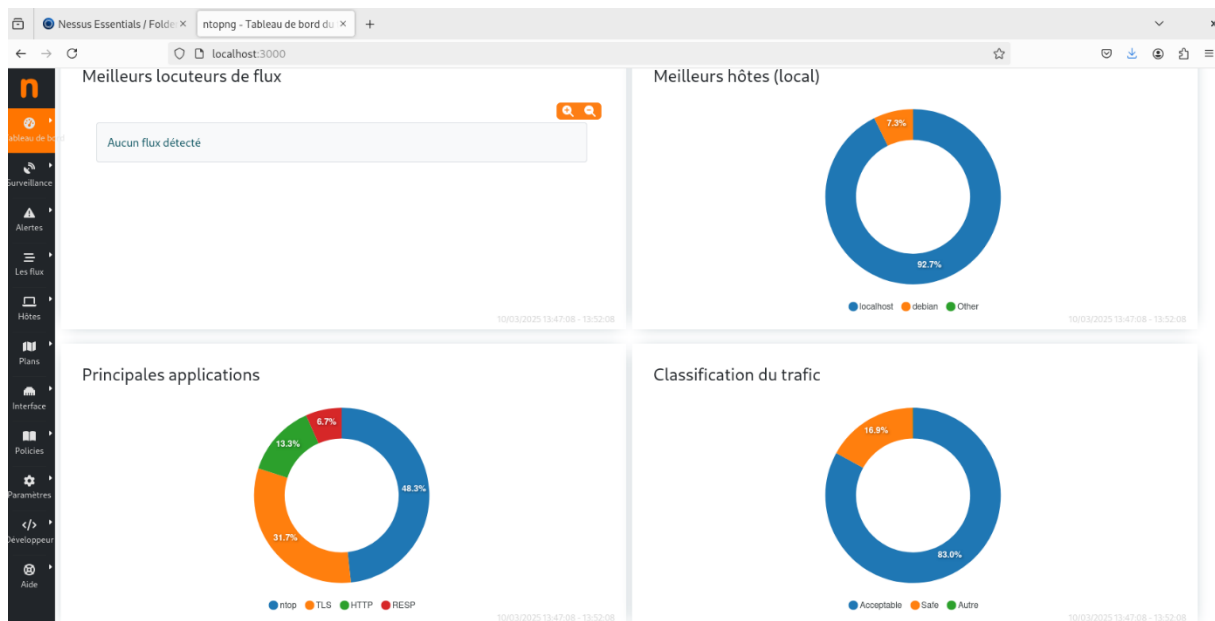
5. Accéder à l'interface web via `http://<IP_du_serveur>:3000`



1.3 Analyse du trafic réseau

NTOPNG permet :

- **La surveillance en temps réel** des connexions actives.
- **L'identification des flux réseau** pour comprendre quels appareils consomment le plus de bande passante.
- **La détection des anomalies** en repérant des pics de trafic inhabituels ou des connexions suspectes.



1.4 Cas d'utilisation et exemples

- **Optimisation du réseau** : identifier les applications gourmandes en bande passante.
- **Détection des menaces** : repérer un comportement anormal indiquant une attaque DDoS ou une exfiltration de données.
- **Audit des connexions** : suivre les accès des utilisateurs aux ressources critiques.

ens33 179.10 bps / 270.30 bps Mise à niveau vers la version Pro/Enterprise

Flux en direct | Analyse

Hôte	Protocole	Application	Statut	QoS	État du flux TCP	DSCP	Type de trafic	Pools d'hôtes	Réseaux	Actions	Vu pour la dernière...	Durée	Protocole	Score	Flux	Thpt réel	Nombre total d'o...	Info
	TCP:TLS.ntop		PPP								00:09	02:07	TCP:TLS.ntop		debian	784.97 bps ↑	6.38 KB	shop.ntop.org
	TCP:TLS		PPP								00:03	02:03	TCP:TLS		debian	1.29 Kbps ↑	5.69 KB	unpkg.com
	TCP:TLS.Mozilla		PPP								00:39	02:37	TCP:TLS.Mozilla		debian	783.82 bps ↓	3.69 KB	contile.services.mozilla.com
	TCP:HTTP.OCSP		PPP								00:11	02:06	TCP:HTTP.OCSP	10	debian	575.88 bps ↑	3.13 KB	POST D'ACCORD r10.o.lencr...
	TCP:HTTP.OCSP		PPP								00:11	02:06	TCP:HTTP.OCSP	10	debian	575.88 bps ↑	3.13 KB	POST D'ACCORD r10.o.lencr...
	UDP:MDNS		PPP								00:03	00:04	UDP:MDNS		itachisn	1.74 Kbps ↑	1.24 KB	_dosvc_tcp.local Périodique
	UDP:MDNS		PPP								00:03	00:04	UDP:MDNS		ItachiSN	1.63 Kbps ↑	1.12 KB	_dosvc_tcp.local
	UDP:SSDP		PPP								00:12	00:12	UDP:SSDP		ItachiSN		334.00 B	239.255.255.250
	UDP:DNS		PPP								00:03	00:03	UDP:DNS		debian		278.00 B	unpkg.com Périodique
	UDP:DNS		PPP								00:04	00:04	UDP:DNS		debian		278.00 B	unpkg.com Périodique

Showing page 1 of 4: total 40 rows

ntopng Community v.6.3.250310 (Debian GNU/Linux 12 (bookworm)) | © 1998-24 - ntop | 13:55:20 +0000 UTC | Uptime: 20:51

localhost:3000/ua/hosts_stats.lua?version=&network=&traffic_type=&mode=&pool=

Hôtes | Actif

Acti...	Adresse IP	Nom	Les flux	Alertes	Score	CVE	Vu depuis	Répartition du trafic	Débit	Nombre total d'octets
	34.117.188.166		1				03:15	Envoyé Reçu		8.62 KB
	41.208.140.8	r10.o.lencr.org	2		10		02:44	Envoyé Reçu		6.25 KB
	104.17.249.203		1				02:41	Envoyé Reçu		6.16 KB
	178.62.197.130		1				05:48	Envoyé Reçu		22.54 KB
	192.168.198.1	ItachiSN	2				20:50	Envoyé Reçu		17.07 KB
	192.168.198.2	_gateway	41		15		21:21	Envoyé Reçu	2.50 Kbps ↑	245.87 KB
	192.168.198.133	debian	46		50		21:21	Reçu	3.15 Kbps ↑	673.39 MB
	224.0.0.251	mdns.mcast.net	1				20:50	Reçu		14.13 KB
	239.192.152.143		1				17:29	Reçu		644.00 B
	239.255.255.250		1				00:50	Reçu		334.00 B

Showing page 1 of 2: total 12 rows

ntopng Community v.6.3.250310 (Debian GNU/Linux 12 (bookworm)) | © 1998-24 - ntop | 13:55:49 +0000 UTC | Uptime: 21:20

2. Nessus : Analyse des Vulnérabilités

2.1 Présentation de Nessus

Nessus est un scanner de vulnérabilités utilisé pour identifier les failles de sécurité sur un réseau ou un système. Il est développé par **Tenable** et est largement adopté dans l'industrie de la cybersécurité.

2.2 Installation et Configuration

2.2.1 Pré-requis système

- Un système sous Linux ou Windows.
- Un accès administrateur pour l'installation.
- Une connexion Internet pour les mises à jour de la base de vulnérabilités.

2.2.2 Étapes d'installation sous Linux

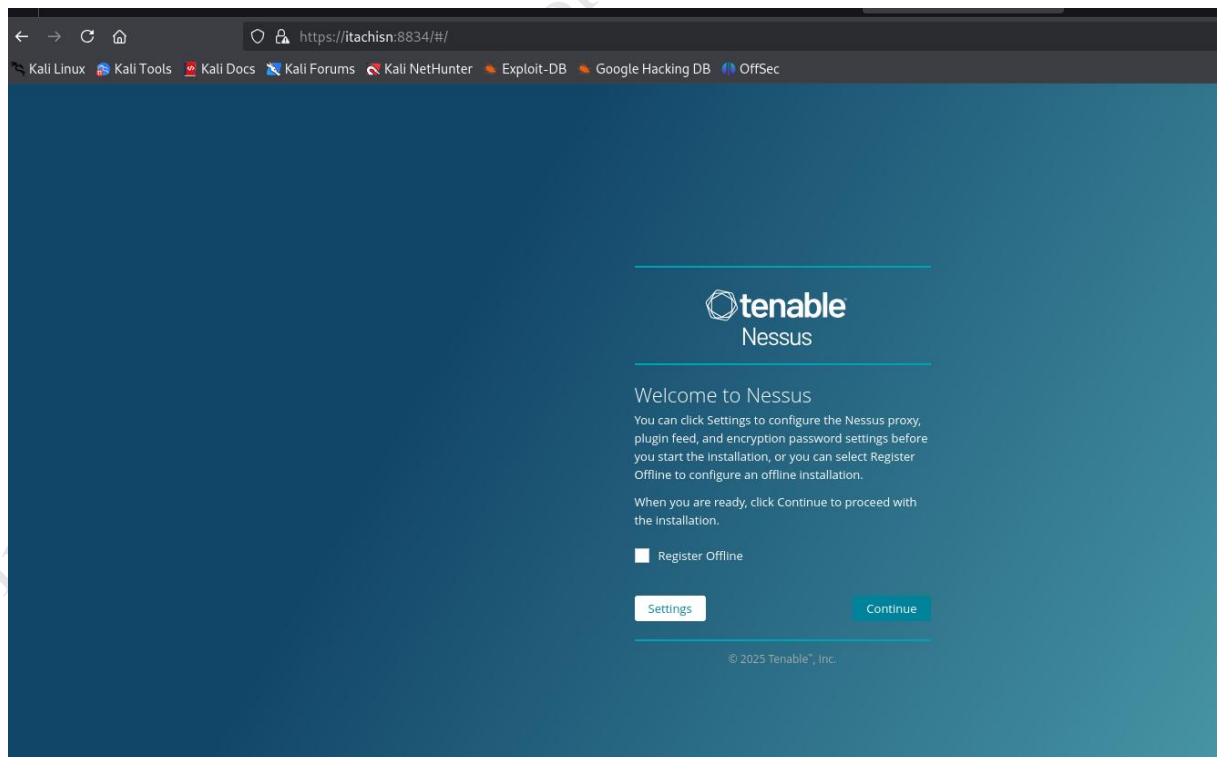
1. **Télécharger Nessus depuis le site officiel de Tenable.**
2. **Installer le package**

```
sudo dpkg -i Nessus-<version>.deb # Debian/Ubuntu
sudo rpm -ivh Nessus-<version>.rpm # CentOS/RHEL
```

3. **Démarrer le service**

```
sudo systemctl start nessusd
```

4. **Accéder à l'interface web** via `https://<IP_du_serveur>:8834`



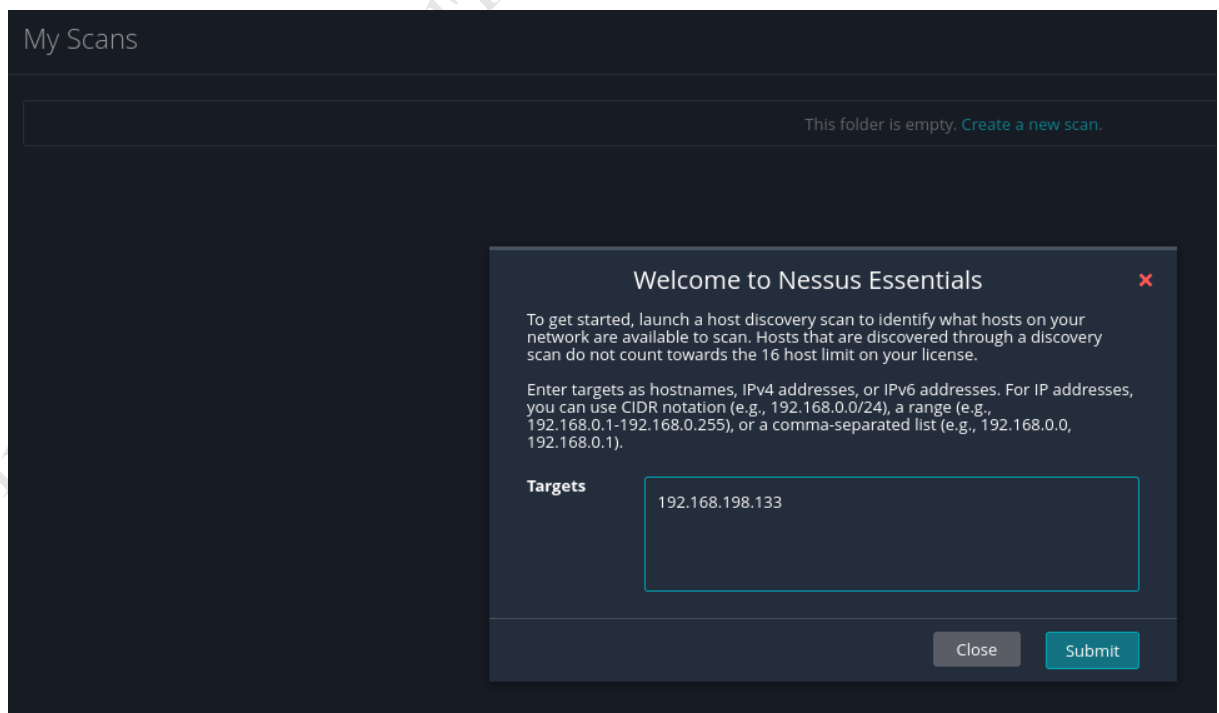
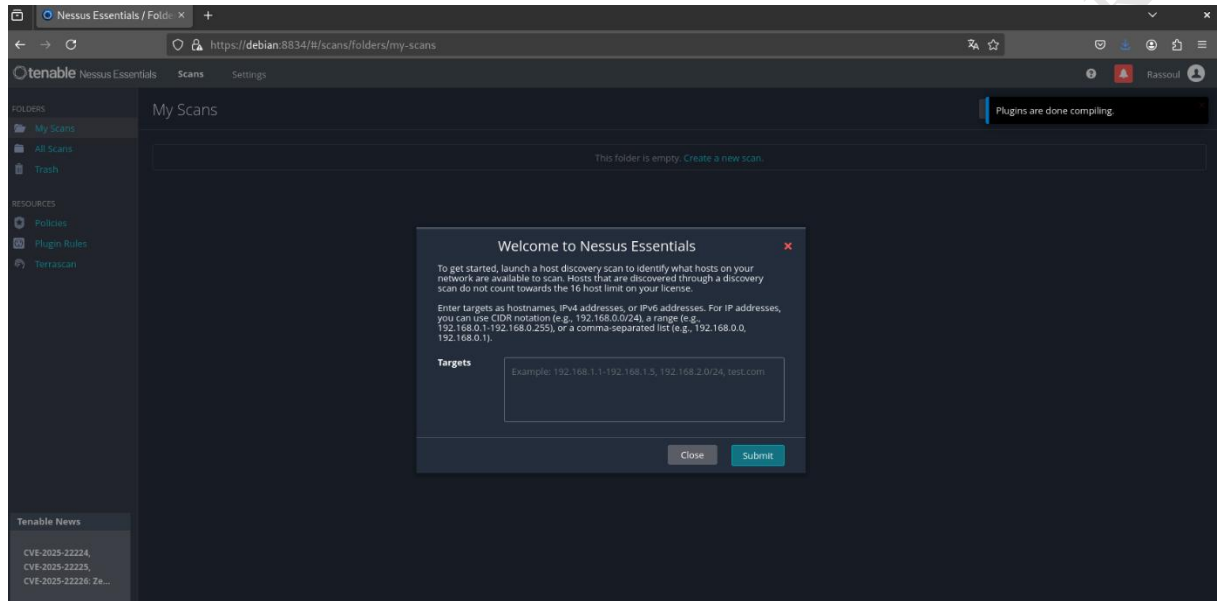
5. **Créer un compte et enregistrer Nessus avec une licence.**

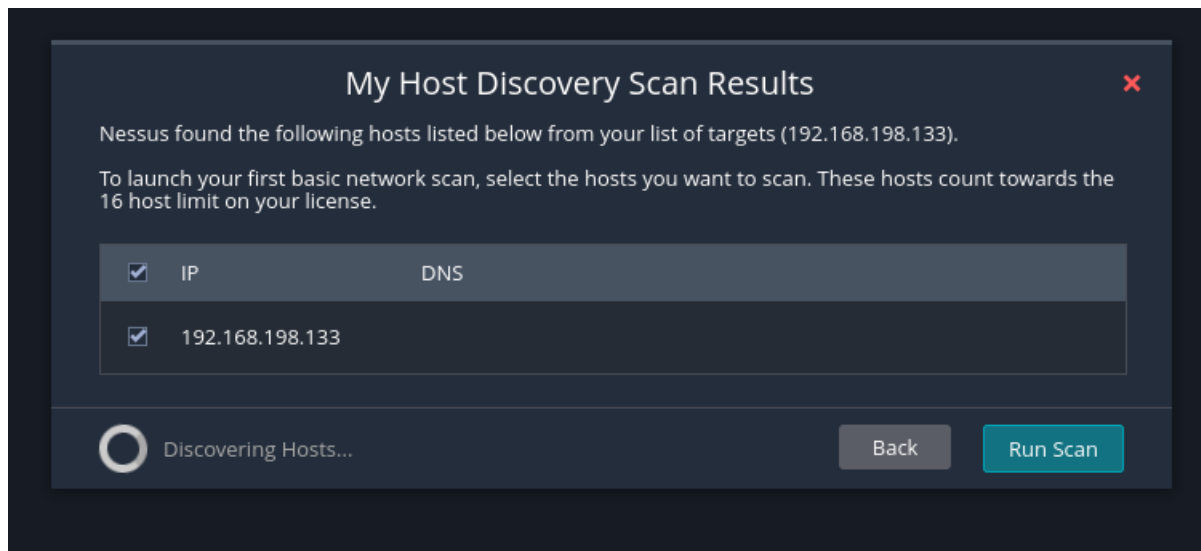
2.3 Détection des vulnérabilités

Nessus propose plusieurs types de scans :

- **Scan de vulnérabilités générales** : recherche des failles courantes.

On renseigne l'hôte à scanner

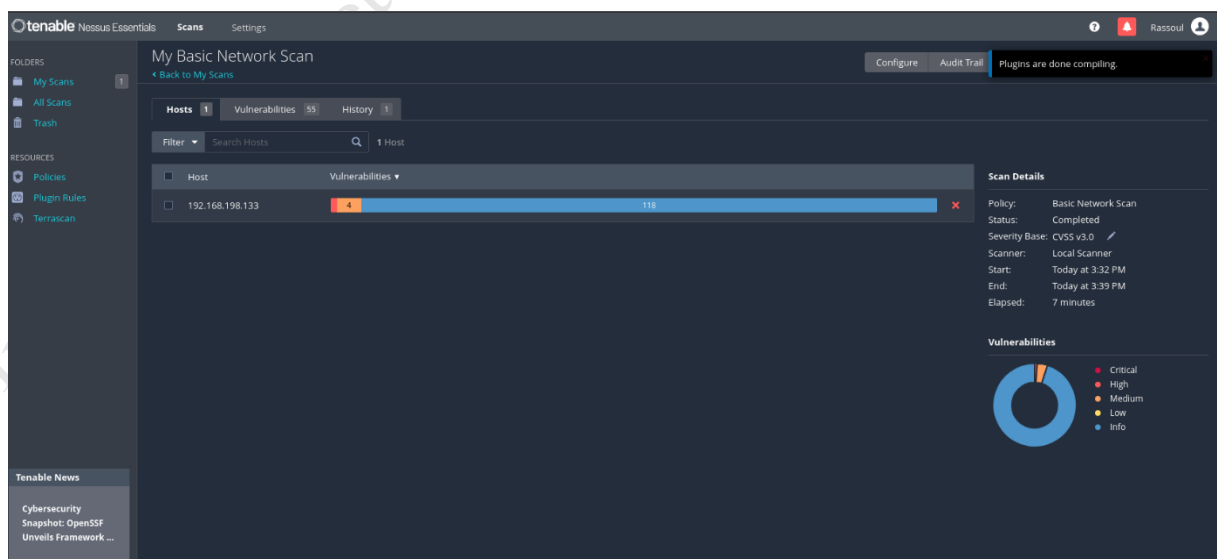




- **Scan des ports ouverts** : identification des services accessibles depuis l'extérieur.
- **Scan de configuration** : vérification des paramètres système pour détecter des mauvaises configurations.
- **Scan des correctifs manquants** : analyse des mises à jour de sécurité non appliquées.

Une fois un scan terminé, Nessus fournit un rapport détaillant :

- **Les vulnérabilités critiques** avec des scores de sévérité.



My Basic Network Scan

Configure Audit Trail Plugins are done compiling.

Hosts 1 Vulnerabilities 55 History 1

Filter Search Vulnerabilities 55 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count		
MIXED				Nodejs Node.js (Multiple Issues)	Misc.	2		
MIXED				SSL (Multiple Issues)	General	11		
MIXED				Apache HTTP Server (Multiple Issues)	Web Servers	4		
INFO				SSH (Multiple Issues)	General	9		
INFO				HTTP (Multiple Issues)	Web Servers	7		
INFO				TLS (Multiple Issues)	Service detection	4		
INFO				TLS (Multiple Issues)	General	3		
INFO				DMI (Multiple Issues)	General	3		
INFO				SSH (Multiple Issues)	Misc.	3		
INFO				SSH (Multiple Issues)	Service detection	2		
INFO				SSH (Multiple Issues)	Service detection	2		
INFO				Netstat Portscanner (SSH)	Port scanners	13		
INFO				Remote listeners enumeration (Nessus)	Service detection	13		

Scan Details

Policy: Basic Network Scan
 Status: Completed
 Severity Base: CVSS v3.0
 Scanner: Local Scanner
 Start: Today at 3:32 PM
 End: Today at 3:39 PM
 Elapsed: 7 minutes

Vulnerabilities

My Basic Network Scan / SSL (Multiple Issues)

Configure Audit Trail Plugins are done compiling.

Hosts 1 Vulnerabilities 55 History 1

Search Vulnerabilities 7 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count		
MEDIUM	6.5			SSL Certificate Cannot Be Trusted	General	2		
MEDIUM	6.5			SSL Self-Signed Certificate	General	1		
INFO				SSL Certificate Information	General	2		
INFO				SSL Cipher Suites Supported	General	2		
INFO				SSL Perfect Forward Secrecy Cipher Suites Supported	General	2		
INFO				SSL Certificate with no Common Name	General	1		
INFO				SSL Cipher Block Chaining Cipher Suites Supported	General	1		

Scan Details

Policy: Basic Network Scan
 Status: Completed
 Severity Base: CVSS v3.0
 Scanner: Local Scanner
 Start: Today at 3:32 PM
 End: Today at 3:39 PM
 Elapsed: 7 minutes

Vulnerabilities

- Des recommandations pour corriger les failles identifiées.

My Basic Network Scan / Plugin #51192

Configure Audit Trail Plugins are done compiling.

Hosts 1 Vulnerabilities 55 History 1

MEDIUM SSL Certificate Cannot Be Trusted

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below:

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Solution

Purchase or generate a proper SSL certificate for this service.

See Also

<https://www.itu.int/rec/T-REC-X.509/en>
<https://en.wikipedia.org/wiki/X.509>

Output

Plugin Details

Severity: Medium
 ID: 51192
 Version: 1.19
 Type: remote
 Family: General
 Published: December 15, 2010
 Modified: April 27, 2020

Risk Information

Risk Factor: Medium
 CVSS v3.0 Base Score: 6.5
 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C/L/I:A/N
 CVSS v2.0 Base Score: 6.4
 CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N

2.4 Cas d'utilisation et exemples

- **Audit de la sécurité d'un serveur** pour vérifier la présence de failles connues.
 - **Test de conformité** pour s'assurer qu'un système respecte les bonnes pratiques de sécurité.
 - **Simulation d'attaques** en identifiant les vecteurs d'exploitation possibles.
-

Conclusion

L'utilisation conjointe de **NTOPNG** et **Nessus** permet d'assurer une meilleure surveillance et sécurité du réseau. NTOPNG offre une visibilité en temps réel sur les activités réseau, tandis que Nessus identifie les vulnérabilités critiques nécessitant une remédiation. Ensemble, ces outils constituent une solution efficace pour protéger une infrastructure contre les menaces et optimiser ses performances.

Références

- Documentation officielle de NTOPNG : <https://www.ntop.org/>
- Documentation officielle de Nessus : <https://www.tenable.com/products/nessus>