

Guarda

# Audit de sécurité

RSX 101

Dorian Tamburrini – Jérôme Boyer - Kacper Karcz  
5-20-2022

## Sommaire

Configuration en place .....	2
Equipements physiques utilisés dans l'infrastructure .....	2
Récapitulatif de toutes les machines présentes dans l'infrastructure .....	2
Configuration serveur web .....	2
Fonctionnalités mise en place sur les machines.....	3
Serveurs web : .....	3
Borne wifi.....	4
Routeur .....	4
Pare-feu / pfSense.....	4
Résultats OpenVAS & Nessus .....	5
OpenVAS.....	5
Nessus.....	5

## Configuration en place

### Equipements physiques utilisés dans l'infrastructure

- Linksys WRT54GL utilisé en tant qu'access point
- PC Portable n°1 utilisé en tant que pare-feu pfSense
- PC Portable n°2 utilisé afin d'héberger le routeur, ainsi que les machines virtuelles

### Récapitulatif de toutes les machines présentes dans l'infrastructure

- Borne wifi
- Machine pare-feu / pfSense dédiée
- Routeur Kali permettant de connecter les machines virtuelles au pare-feu
- Deux serveurs Web tournants avec une redondance Heartbeat
- Un serveur Active Directory
- Poste client Windows

### Configuration serveur web

- OS utilisé : Kali
- Logiciel HTTP : Apache HTTP Server
- Langage site : PHP
- Système de gestion BDD SQL : PostgreSQL

## Fonctionnalités mise en place sur les machines

### Serveurs web :

#### Au niveau du site web :

- Code non visible via l'inspecteur
- Informations serveur caché au niveau de l'inspecteur
- Index désactivé
- Liens symboliques désactivés
- Ignore les requêtes http
- Ecoute seulement les requêtes HTTPS sur le port 443
- Certification TLS 1.3 et clés à 4096 bits
- Première authentification avec httpasswd
- Seconde authentification au niveau PHP
- Base de données Postresql avec mot de passe crypté
- Limitation du trafic sur le site réduit à 1 mo/s pour tous les utilisateurs
- Curl bloqué par l'authentification httpasswd

#### Au niveau des machines :

- Libapache2-mod-security2 actif (firewall contre les attaques en brute force)
- Libapache2-mod-evasive actif (détection et protection contre les DDOS et les attaques HTTP brute)
- TRACE HTTP Request désactivé
- Port SSH changé
- Suppression des logiciels utilisant des protocoles non sécurisés (FTP, telnet, rlogin/rsh...)
- Mise en place d'une politique de mots de passe à 32 caractères

#### Pare-feu des machines :

- Règles IPTABLES à jour bloquant toutes les requêtes extérieur en dehors du port HTTPS pour le site, port SSH ouvert seulement aux machines aptes
- PSAD (Port Scan Attack Detector) mis en place, bloque les IP des machines qui scannent un nombre anormal de ports sur les machines web par le biais de règles IPTABLES.

#### Redondance :

- Mise en place de Heartbeat, passage de l'IP virtuel du site sur la machine secondaire quand la première n'est plus détectée

#### Sauvegarde :

- Sauvegarde de la base de données SQL via les outils PostgreSQL sur les deux machines
- Réalisation de la sauvegarde toutes les 6 heures à l'aide de Cron sur les deux machines
- Envoi sécurisé via Rsync de la base de données sur l'autre machine

### Borne wifi

- Séparation des employés et des invités via la création de 2 réseaux wifi
- Masquage du SSID du réseau dédié pour les employés
- Blocage de l'accès à la page status sans l'insertion des identifiants
- Mise en place d'un relais DHCP

### Routeur

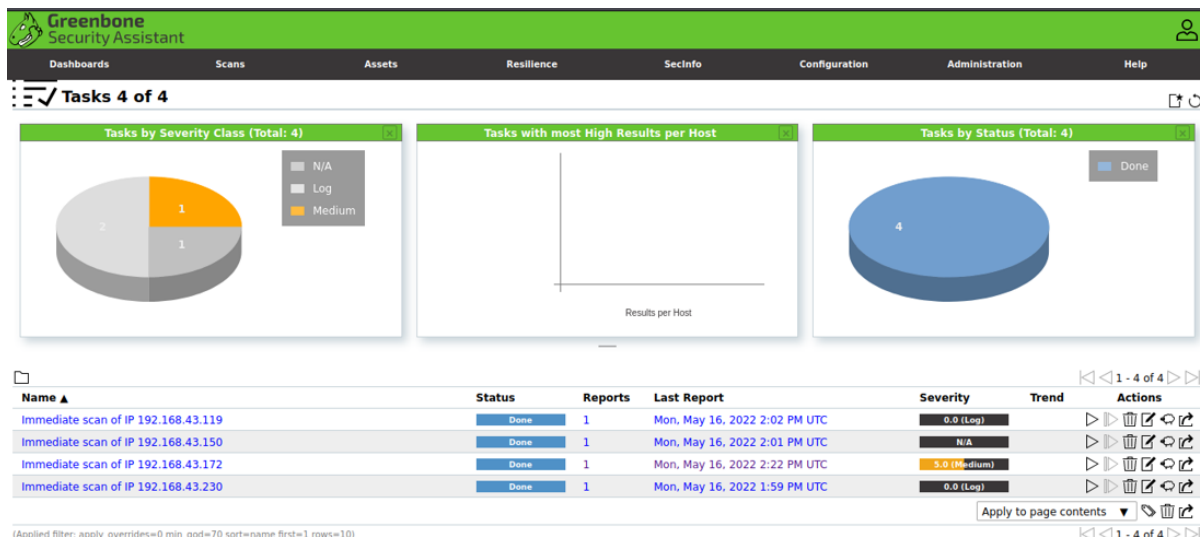
- Application de règles de pare-feu
- Port forwarding et NAT en place

### Pare-feu / pfSense

- Mise en place d'un serveur DHCP distribuant les IP dans le réseau Wifi
- Application de règles de pare-feu bloquant les requêtes anormales
- Port forwarding jusqu'au serveur web

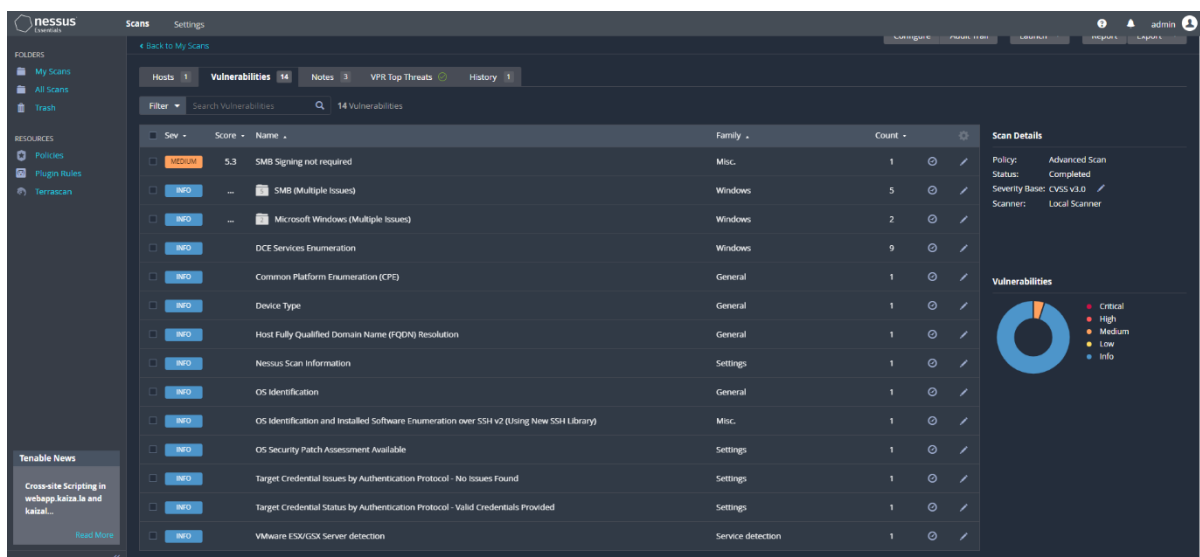
## Résultats OpenVAS & Nessus

### OpenVAS



Dans l'ordre, serveur web 1, serveur web placé sur l'IP virtuelle de Heartbeat, le PC physique de Kacper équipé de Windows 10, serveur web 2.

### Nessus



Liste des vulnérabilités recensées après un scan Nessus sur la machine AD. Il n'y a rien d'alarmant à part une vulnérabilité sur SAMBA.

Détail de la vulnérabilité en question :

nessus windows / Plugin #57608

Configure
Audit Trail
Launch
Report
Export

[Back to Vulnerabilities](#)

Hosts 1
Vulnerabilities 14
Notes 3
VPR Top Threats
History 1

MEDIUM
SMB Signing not required

**Description**

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

**Solution**

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

>
Plugin Details

Severity:
Medium

ID:
57608

Version:
1.19

Type:
remote

Family:
Misc.