UNIVERSITE SIDI MOHAMED BEN ABDELLAH FACULTÉ DES SCIENCES ET TECHNIQUES FÈS DÉPARTEMENT D'INFORMATIQUE

PROJET DE FIN D'ETUDES

LICENCE SCIENCES ET TECHNIQUES
GÉNIE INFORMATIQUE

SOLUTION CIS BENCHMARK POUR UNE MEILLEURE SÉCURITÉ

LIEU DE STAGE : ORANGE MAROC

RÉALISER PAR : SOUFIANE ALAMI HASSANI

ENCADRÉ PAR :

MR. KHALID ZENKOUAR

DEVANT LE JURY COMPOSÉ DE :

Pr. F. Mrabti

Pr. A. Boushaba

Pr. K. Zenkouar

SOUTENU LE : 07/06/2017

ANNÉE UNIVERSITAIRE : 2016-2017

بسم الله الرحمان الرحيم

سبحانك لا علم لنا إلا
ما علمتنا إنك أنت
العليم الحكيم

صدق الله العظيم

Sommaire

Remerciements

C'est une tâche très agréable, mais bien délicate, de présenter mes remerciements à tous ceux qui m'ont aidé dans la réalisation de ce travail.

Qu'il me soit permis d'exprimer en premier lieu ma gratitude au Doyen de la Faculté des Sciences et Techniques de Fès : Professeur, IJJAALI Mustapha pour ses encouragements, l'apport considérable dont j'ai bénéficié et l'intérêt qu'il m'a toujours manifesté.

J'exprime ma haute considération et mes vifs remerciements à tous mes enseignants du Département des sciences de l'Informatique pour les enseignements qu'ils m'ont prodigués tout au long de mes années de formation dans la filière Sciences de l'informatique.

Tout particulièrement, je remercie Pr.Khalid Zenkouar , qui a dirigé mon travail tout au long de mon stage avec ses précieux conseils, ses recommandations et son riche savoir-faire.

Mes vives reconnaissances à Mon encadrant Professionnelle M. CHAN ALOUAT Mohamed qui a eu la gentillesse de m'accueillir dans son bureau, partager avec moi sa bonne humeur, ses connaissances, ses conseils et sa disponibilité durant l'encadrement.

Mon grand dévouement à M. ALAOUI Hafid qui m'a hébergé chez lui durant toute la période de stage pour son accueil chaleureux, sa sympathie et la confiance qu'il m'a accordée.

Ce travail a été réalisé au sein du Département de sécurité Informatique de Meditelecom Orange Maroc Casablanca, pendant une durée de deux mois. Je tiens donc à témoigner toute ma reconnaissance à tous le personnel administratif et technique de cet établissement pour l'assistance et l'aide qu'ils m'ont prodigué pour réaliser ce stage. De nombreuses personnes dont les noms ne sont pas cités m'ont aidé, encouragé, conseillé. J'espère pouvoir un jour leur témoigner ma reconnaissance.

Je tiens à exprimer mes affectueuses reconnaissances à mes parents particulièrement ma mère pour son aide, son soutien et ses encouragements, ma famille à qui j'ai beaucoup d'estime et de reconnaissance spécialement ma tante et mon oncle maternelle que j'aime beaucoup.

Enfin mes chers Professeurs pour avoir accepté de faire partie du Jury. J'exprime ma très haute considération, mon profond respect et mes vifs remerciements.

Introduction Générale

Aujourd'hui, la sécurité de l'information est très importante et critique pour toute organisation. Tout problème ou mauvaise configuration peu mener un pirate à obtenir vos données et les mettre à vendre sur le DarkNet prévenir et mieux de guérir, sécuriser le système d'information est devenue une tâche primordiale. En effet, certaines histoires d'intrusions sont bien connues, elles ont été relayées par les médias, et font aujourd'hui partie de la légende du piratage informatique, exemples des dernières attaques : base de données de la société LinkedIn, contenant 117millions de Combinaisons d'Identifiants et de Mots de passe, est à vendre à 2000 euros par des pirates. Yahoo contenant 500 millions de mot de passe est à vendre sur le Darknet et récemment la plus grande attaque de ransomware, Wannacry qui a affecté des millions de serveurs et qui a chiffré leurs données, demandant de l'argent pour décrypter leurs données.

Dans ce contexte et afin de se conformer aux dernières réglementations et des normes de sécurité ISO/CEI 27001 pour renforcer la sécurité de leur système information. La société ORANGE a opté pour une solution de corrélation de logs et d'audit des administrateurs et utilisateurs à haut privilèges.

L'objectif principale de ce stage consiste à mettre en place une solution CIS Benchmark pour mieux sécuriser les serveurs Linux (RedHat, AIX IBM) en créant des scripts bash qui font un audit et un correctif s'il trouve une vulnérabilité ou une faiblesse sur le système d'exploitation. Ensuite, après l'exécution de nos scripts Bash, il faut tester leur fiabilité en utilisant la plateforme Coralys, cette plateforme a pour finalité de scanner les vulnérabilités sur les serveurs.

Le présent rapport sera organisé comme suit : Le premier chapitre présente d'une manière générale le contexte de travail et les objectifs de mon projet de Stage. Dans un premier lieu je vais commencer par une présentation de la société ORANGE MAROC comme étant mon organisme d'accueil, ensuite une description générale à propos du projet et en dernier lieu la planification du projet. Le deuxième chapitre présente les différents system d'exploitation, outils et les plateformes utiliser pour scanner les vulnérabilités sur les serveurs test. Le troisième chapitre est divisé en trois parties. Premièrement, la réalisation d'un script Bash pour RedHat v.6 et v.7. Ensuite, la réalisation d'un script Bash pour la machine AIX IBM. Finalement un scan de vulnérabilités avec Coralys sera effectué pour tester la fiabilité des scripts réalisé.

Chapitre I: Contexte générale du projet

Ce chapitre présente d'une manière générale le contexte de travail et les objectifs de mon projet de Stage.

Dans un premier lieu je vais commencer par une présentation de la société ORANGE MAROC comme étant mon organisme d'accueil, ensuite une description générale à propos du projet et en dernier lieu la planification du projet.

I.1 Présentation de l'organisme d'accueil

a. À propos de Orange

Créée en 1999 suite à un partenariat entre des investisseurs marocains et les groupes Telefonica et Portugal Telecom qui en détenaient 32,18 % chacun, Orange opère sur lemarché marocain des télécommunications. Orange développe et commercialise ses produits etservices sous la marque Orange. Ses offres s'adressent aussi bien au marché des Particuliersqu'à celui des PME et des Grandes Entreprises.

En juillet 2005, la société a été adjudicataire d'une licence de téléphonie Fixe, luipermettant de devenir le second opérateur fixe après Maroc Telecom. Par ailleurs, en juillet 2006, une licence 3G lui a été attribuée pour l'établissement et l'exploitation de réseauxpublics de télécommunications au Maroc.

En septembre 2009, les deux Groupes Portugal Telecom et Telefonica, ont cédé leurparticipation dans le capital d'Orange (64%) au profit de la Caisse de Dépôt et de Gestion(CDG) et de FinanceCom, avec son partenaire RMA Watanya. Le montant de cettetransaction s'élève à EUR 800 millions.

En septembre 2010, le Groupe FRANCE TELECOM rachète 40% du capital d'ORANGE auprès des deux actionnaires marocains à parts égales.

L'actionnariat de Orange devint : 40% pour Orange (Groupe France Telecom), 30% pour laCaisse de dépôt et de gestion (CDG) et 30% pour Finance Com

Par ailleurs, Orange trouve également ses origines dans ses défis stratégiques, sesforts engagements ainsi que dans les multiples nobles rôles sociaux et culturels qu'elle joue ausein de l'environnement

géographique dans lequel elle opère (sponsor, éducation et actions de solidarité). Le tableau ci-dessous présente la fiche technique d'Orange.

Raison sociale	Medi Telecom SA
Forme juridique	Société anonyme
Création	1999
Activité	Opérateur de télécommunication
Produits	Produits et service de téléphonie fixe, mobile et Internet
Directeur général	YVES GAUTHIRE
Site corporatif	www.orange.ma

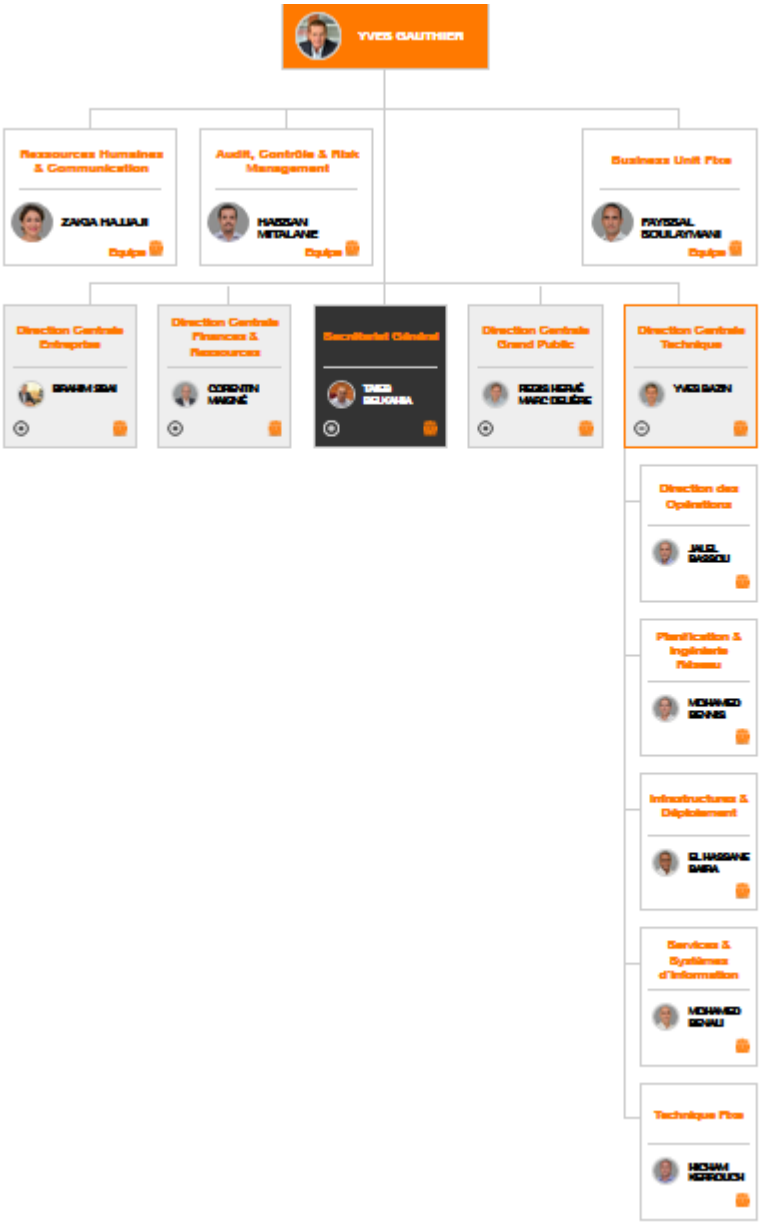
Tableau 1 : Fiche technique d'Orange

Les dates clés de l'évolution d'Orange sont :

- **1999 :** Création de Meditel permettant la démonopolisation du marché (licence 2G).
- **2005 :** Attribution de la licence fixe et la licence 3G
- **2009 :** Rachat de FinanceCom des actions de Telefonica et Portugal Télécom
- **2010 :** Cession par les Groupes CDG et FinanceCom de 40% du capital d'Orange au Groupe France Télécom
- **2011 :** Conclusion du partenariat avec le groupe France Telecom.
- **2013 :** Lancement du projet SRAN et avancement dans le projet SU (Service Universel).
- **2015 :** Préparation et début de la commercialisation du projet 4G
- **2016 :** Préparation et début de la commercialisation du projet IMS

b. Organigramme d'Orange

La figure ci-dessous montre l'organigramme d'Orange :



I.2 Présentation du projet :

Le projet consiste en l'étude des bonnes configurations system d'exploitation, des serveurs métiers moyennent une analyse de risques.

Suite à cette analyse nous avons constatés les risques suivants :

- Mauvaise config sur le system d'exploitation
- Services non utilisés
- Configuration par default
- Modification de la configuration lors de l'installation d'un programme

Mon travail consiste à trouver une solution efficace et permanente pour maintenir ce type de risque et éviter les exploits d'une manière à améliorer la sécurité pour ne pas être utiliser par de attaquants pour avoir un accès non autorisé.

I.3 Objectif du projet :

Les principaux objectifs à atteindre par le présent projet de fin d'études sont :

- mettre en place un system de benchmark de configuration capable de détecter les anomalies et les failles de sécurité system

- créer un programme automatique qui permet d'appliquer systématiquement les solutions recommander par le system Benchmark

- scanner les serveurs concerner par cette solution de Benchmark en utilisant Coralys et nmap. Cette solution permet de tester l'efficacité des modification apportées par le programme.

I.4 Contraintes du projet :

La réalisation de ce projet s'impose à des contraintes qui ne peuvent pas être négligée, ils se présentent comme suit :

- Des contraintes temporelles,

- Des contraintes au niveau de l'accès des serveurs de test, de privilège pour exécuter le programme et lancer un scan

I.5 Conduite du projet :

La conduite de projet, aussi appelée gestion de projet ou management de projet, est une démarche qui a pour but de structurer et assurer le bon déroulement d'un projet.

a. Organisation du projet

L'organisation du projet est résumée dans les tableaux suivants :

- ***Acteurs côté Orange :***

Acteur	Rôle
Mr. Mohamed Chan ALOUAT	Encadrant, au sein d'Orange Maroc

- ***Acteurs Côté stagiaire :***

Acteur	Rôle
Soufiane Alami Hassani	Étudiant Génie informatique.

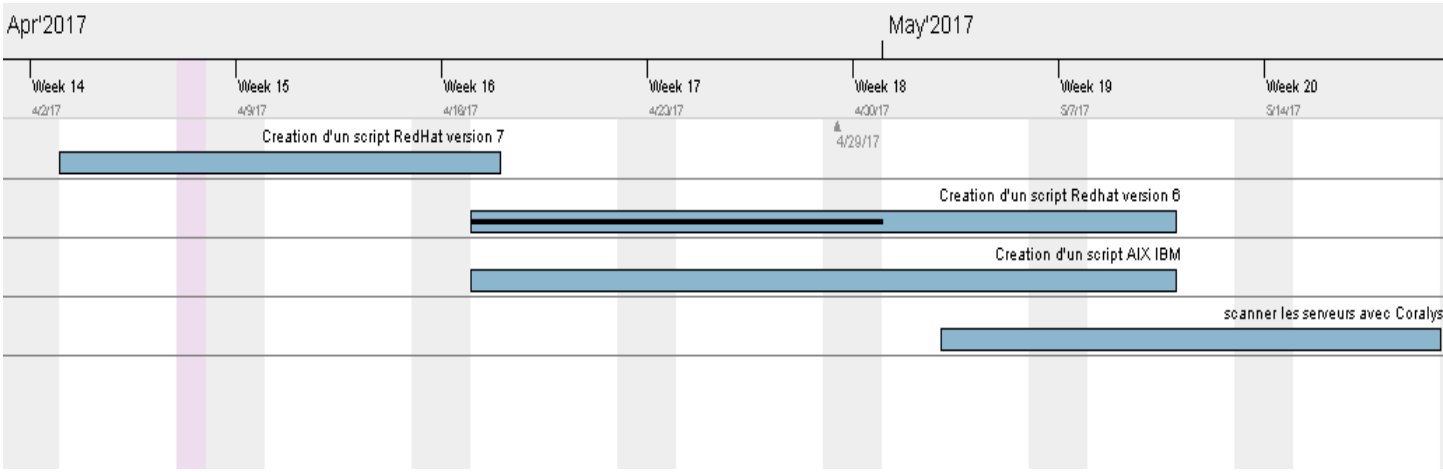
- ***Acteurs Côté FST :***

Acteur	Rôle
Mr. KHALID ZENKOUAR	Encadrant, au sein de la FST

b. Planification du projet :

La planification est une étape primordiale dans un projet. Elle présente une vision générale sur les étapes de développement, et les estimations concernant le délai du projet.

La figure suivante représente le planning final de ce projet de fin d'étude :



I.6 Conclusion :

Cette partie introductive a été consacrée essentiellement à la présentation de l'environnement dans lequel mon stage a été effectué. Elle a aussi mis l'accent sur la présentation du contexte de mon projet.

Chapitre II. Présentation des système d'exploitation et les outils utiliser

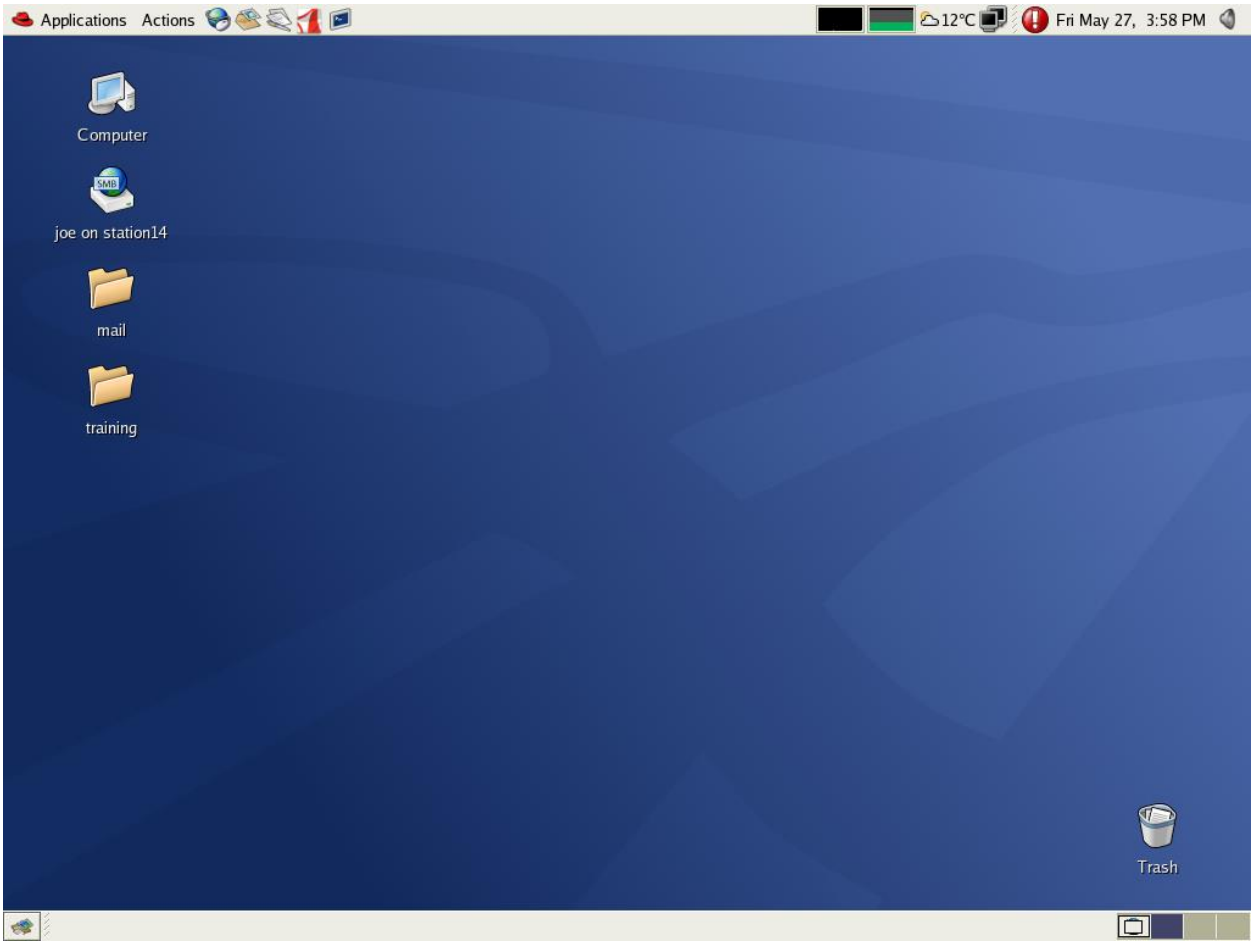
Ce chapitre présente les différents system d'exploitation, outils et les plateformes utiliser pour scanner les vulnérabilités sur les serveurs test.

II.1 RedHat :

Red Hat Linux (RHEL) est une distribution Linux développée par RedHat et ciblée sur le marché commercial. RedHat Enterprise Linux est publié dans les versions de serveur pour x86, x86-64, Itanium, PowerPC et IBM System z, et des versions de bureau. Tout le soutien et la formation officiels du RedHat, ainsi que le programme de certification RedHat, se concentrent sur la plate-forme RedHat Enterprise Linux. RedHat Enterprise Linux est souvent abrégé pour RHEL, bien qu'il ne s'agisse pas d'une désignation officielle.

La première version de RedHat Enterprise Linux portant le nom a été lancée sur le marché comme « RedHat Linux Advanced Server».

RedHat utilise des règles de marque strictes pour restreindre la redistribution gratuite de leurs versions officiellement supportées de RedHat Enterprise Linux, mais fournit toujours son code source. Les dérivés tiers peuvent être construits et redistribués en éliminant les composants non-libres, comme les marques commerciales de RedHat.



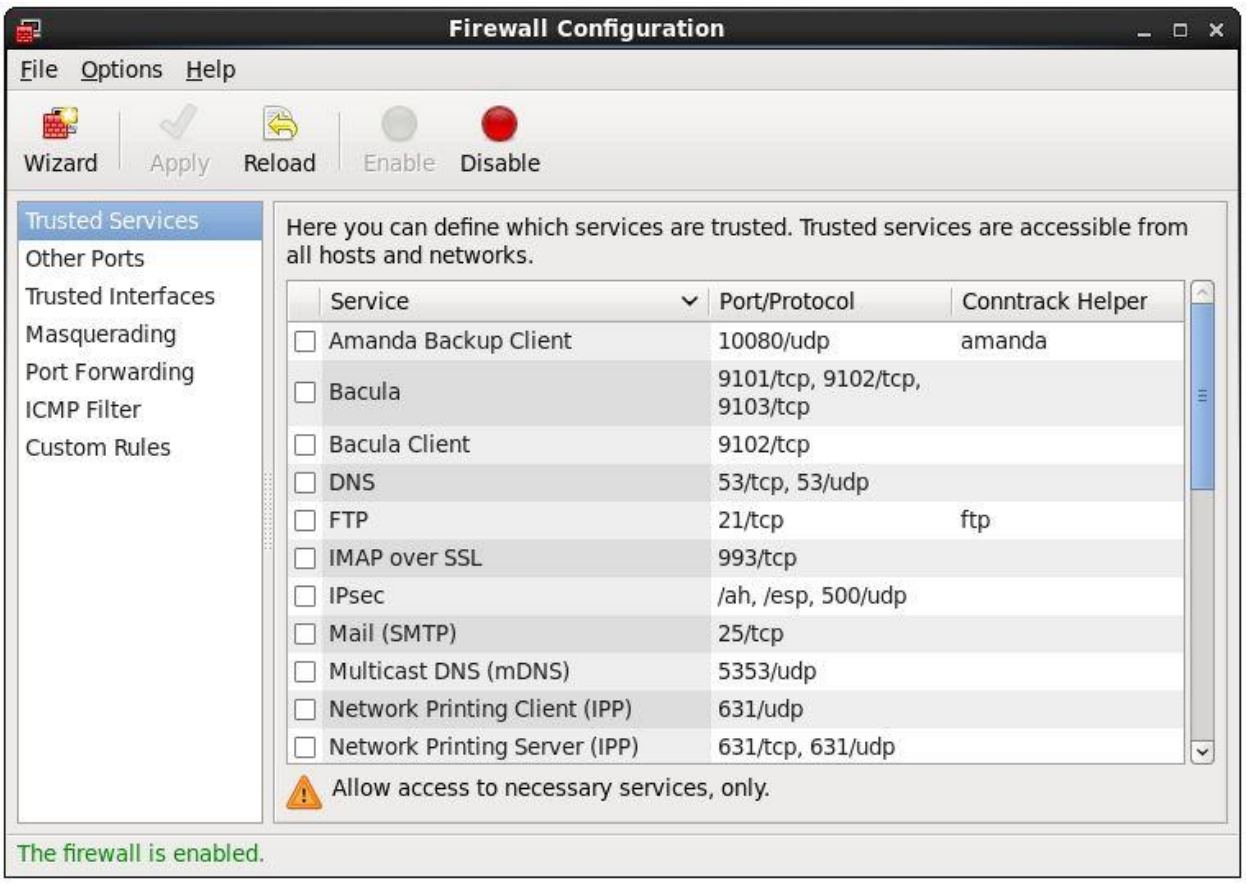
Redhat linux Desktop

L'image représente le bureau GNOME RedHat

Pourquoi RedHat ?

La sécurité a toujours été une considération importante lors de la sélection d'un système d'exploitation serveur, RedHat offre une solution sécuriser pour les entreprises comme Orange, implémentation d'un Pare-feu pour filtrer le trafic entrant, IPS Basé sur la signature des attaques des virus pour se protéger des virus attaque.

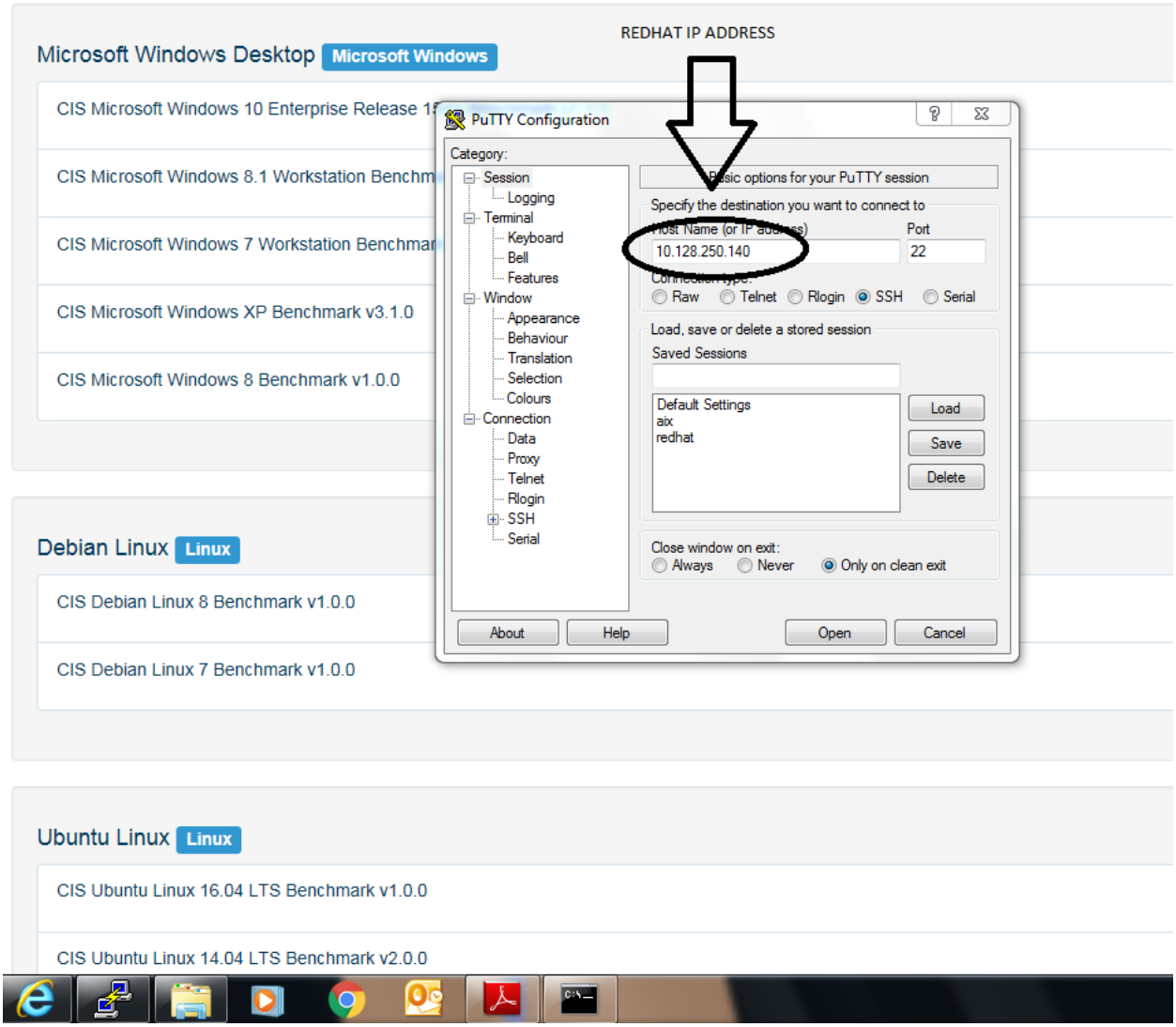
Orange utilise RedHat pour la majorité de ses serveurs pour des services Web(http://www.orange.ma/), SMTP(service mail),SMNP(service de management), Storage, Backup, authentification des utilisateurs et gestion des bases de données.



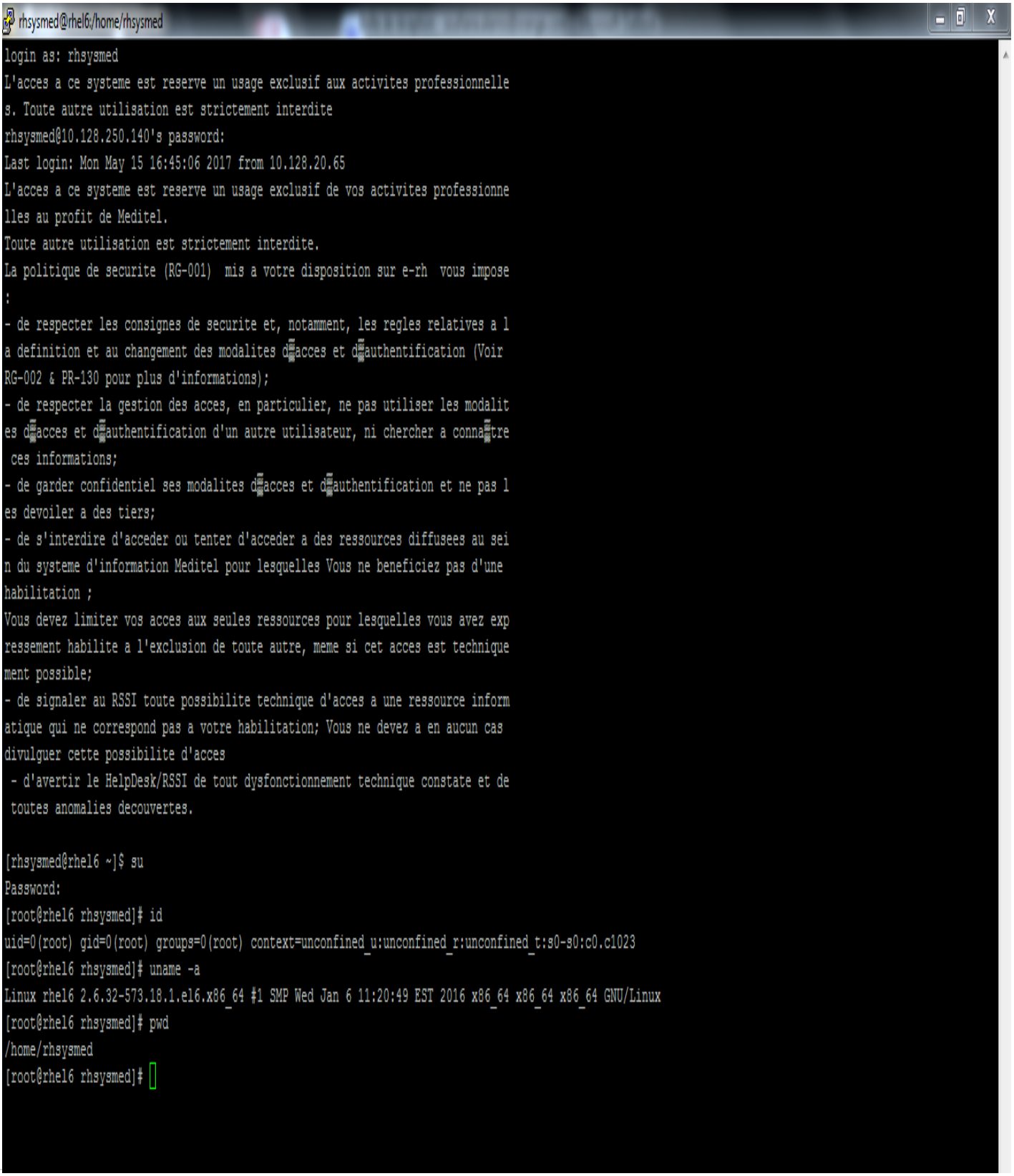
(utilisation d'un Firewall ou Pare-feu sur RedHat)

Connexion à la machine RedHat ?

Pour se connecter à la machine RedHat avec une adresse IPv4 il faut utiliser Putty dans une machine windows qui ouvre un tunnel SSH du client au serveur

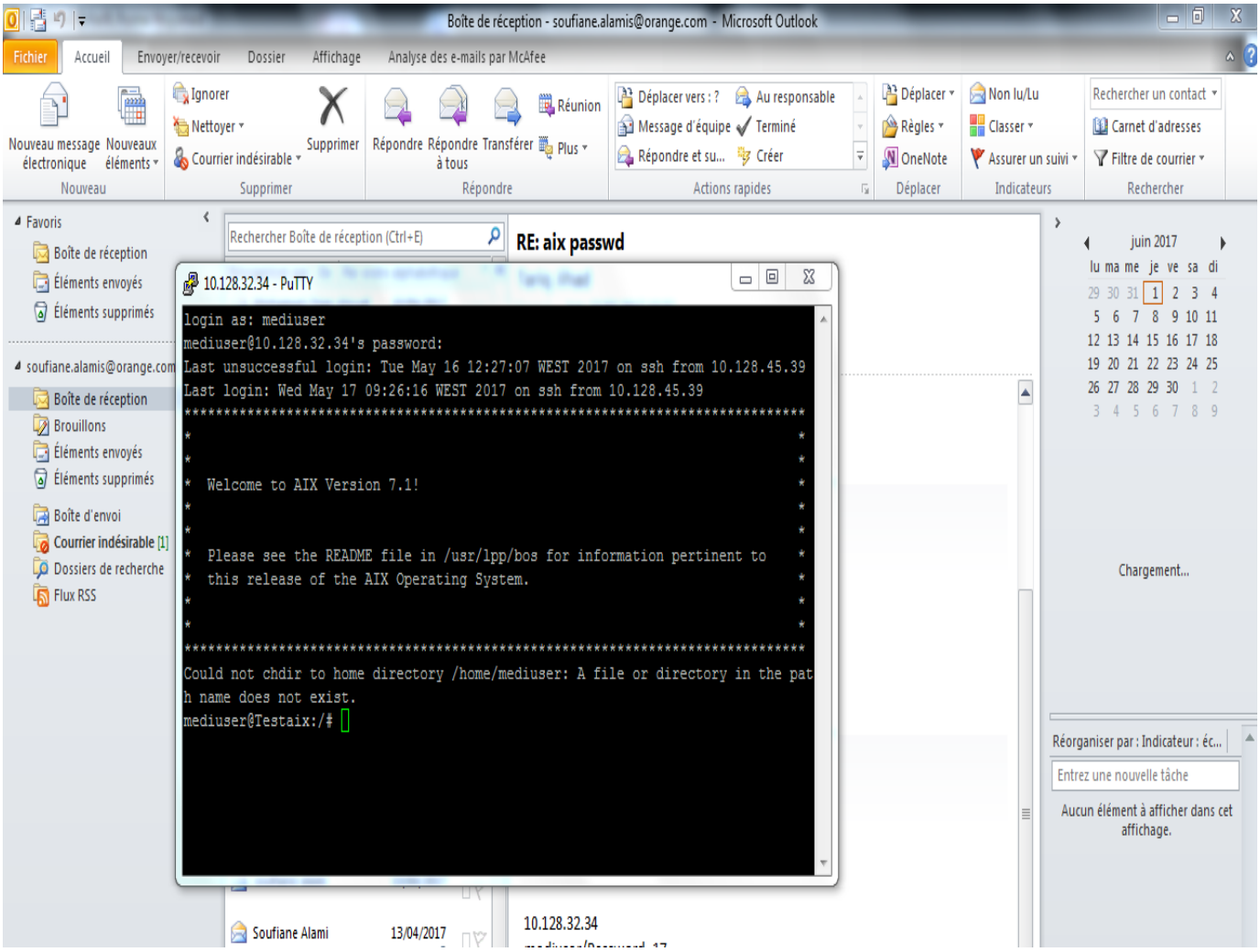


Après l'authentification sur la machine un terminal se lance en utilisant les commandes linux en peu manipuler la machine


rhsysmed@rhel6:/home/rhsysmed
login as: rhsysmed
L'acces a ce systeme est reserve un usage exclusif aux activites professionnelle
s. Toute autre utilisation est strictement interdite
rhsysmed@10.128.250.140's password:
Last login: Mon May 15 16:45:06 2017 from 10.128.20.65
L'acces a ce systeme est reserve un usage exclusif de vos activites professionne
lles au profit de Meditel.
Toute autre utilisation est strictement interdite.
La politique de securite (RG-001) mis a votre disposition sur e-rh vous impose
:
- de respecter les consignes de securite et, notamment, les regles relatives a l
a definition et au changement des modalites d'acces et d'authentification (Voir
RG-002 & PR-130 pour plus d'informations);
- de respecter la gestion des acces, en particulier, ne pas utiliser les modalit
es d'acces et d'authentification d'un autre utilisateur, ni chercher a connaitre
ces informations;
- de garder confidentiel ses modalites d'acces et d'authentification et ne pas l
es devoiler a des tiers;
- de s'interdire d'acceder ou tenter d'acceder a des ressources diffusees au sei
n du systeme d'information Meditel pour lesquelles Vous ne beneficiez pas d'une
habilitation ;
Vous devez limiter vos acces aux seules ressources pour lesquelles vous avez exp
ressement habilite a l'exclusion de toute autre, meme si cet acces est technique
ment possible;
- de signaler au RSSI toute possibilite technique d'acces a une ressource inform
atique qui ne correspond pas a votre habilitation; Vous ne devez a en aucun cas
divulguer cette possibilite d'acces
- d'avertir le HelpDesk/RSSI de tout dysfonctionnement technique constate et de
toutes anomalies decouvertes.
[rhsysmed@rhel6 ~]$ su
Password:
[root@rhel6 rhsysmed]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@rhel6 rhsysmed]# uname -a
Linux rhel6 2.6.32-573.18.1.el6.x86_64 #1 SMP Wed Jan 6 11:20:49 EST 2016 x86_64 x86_64 x86_64 GNU/Linux
[root@rhel6 rhsysmed]# pwd
/home/rhsysmed
[root@rhel6 rhsysmed]#

II.2 AIX IBM :

AIX est un système d'exploitation UNIX (OS) de classe entreprise pour l'architecture du processeur POWER qui se trouve dans IBM Power Systems. L'entreprise mondiale d'aujourd'hui doit compter sur une infrastructure sécurisée, hautement disponible et capable de s'adapter rapidement aux besoins changeants de l'entreprise. AIX offre ces fonctionnalités et plus, avec la performance, la fiabilité et la sécurité des données.



Pourquoi AIX ?

AIX maintient une attention et une réputation de sécurité solides et durables. Les fonctionnalités de sécurité comprennent Trusted AIX pour durcir facilement les paramètres de sécurité du système et Trusted Execution pour contrôler l'intégrité du système.

AIX bénéficie de la meilleure fiabilité de sa classe et est bien reconnu comme ayant le plus faible délai d'attente non planifié année après année. Les serveurs IBM sont constamment considérés comme les plus fiables par les analystes de l'industrie. Ce puissant système d'exploitation UNIX continue de fournir Fonctionnalités de changement de jeu telles que AIX Live Update qui vous permettent d'appliquer de nouveaux niveaux d'OS sans redémarrer le système.

II.3 NMAP :

Network Mapped (Nmap) est un outil de détection de réseau et de détection d'hôte qui est très utile pendant plusieurs étapes de test de pénétration. Nmap ne se limite pas à la simple collecte d'informations et d'énumérations, mais c'est aussi une utilité puissante qui peut être utilisée comme détecteur de vulnérabilité ou par un scanner de sécurité. Ainsi, Nmap est un outil polyvalent, et il peut être exécuté sur de nombreux systèmes d'exploitation différents, y compris Windows, Linux, BSD et Mac. Nmap est un utilitaire très puissant qui peut être utilisé pour :

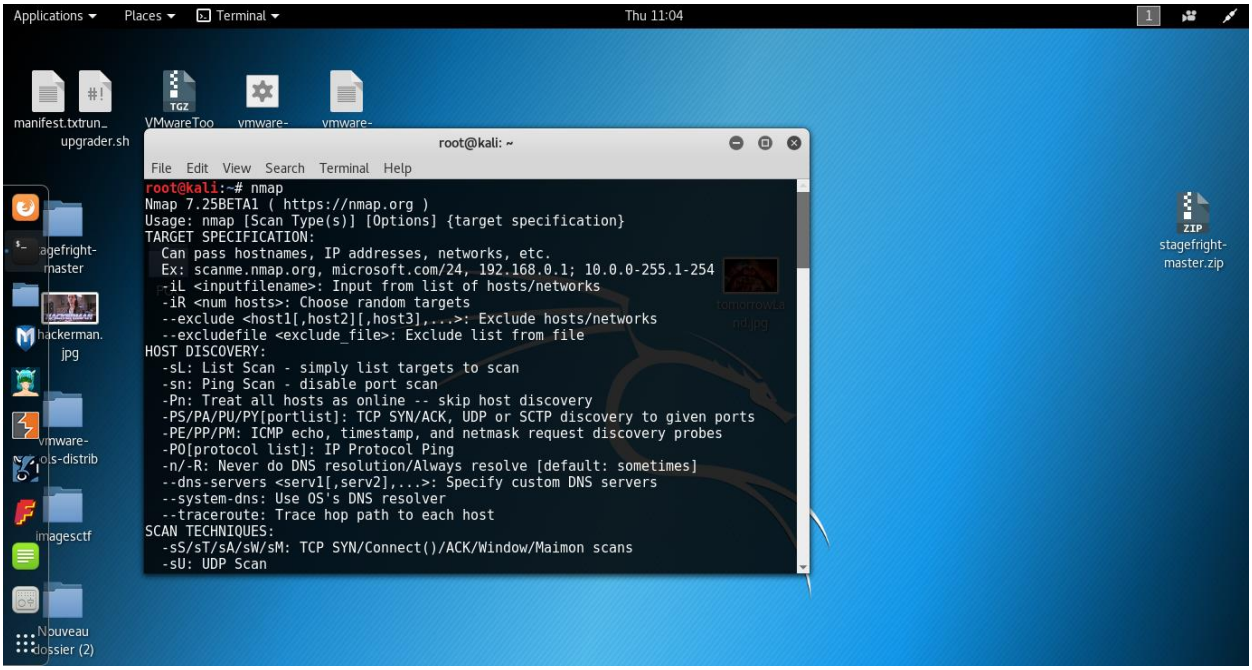
Détecter l'hôte en direct sur le réseau (découverte de l'hôte)

Détecter les ports ouverts sur l'hôte (découverte ou énumération du port)

Détectez le logiciel et la version sur le port respectif (découverte du service)

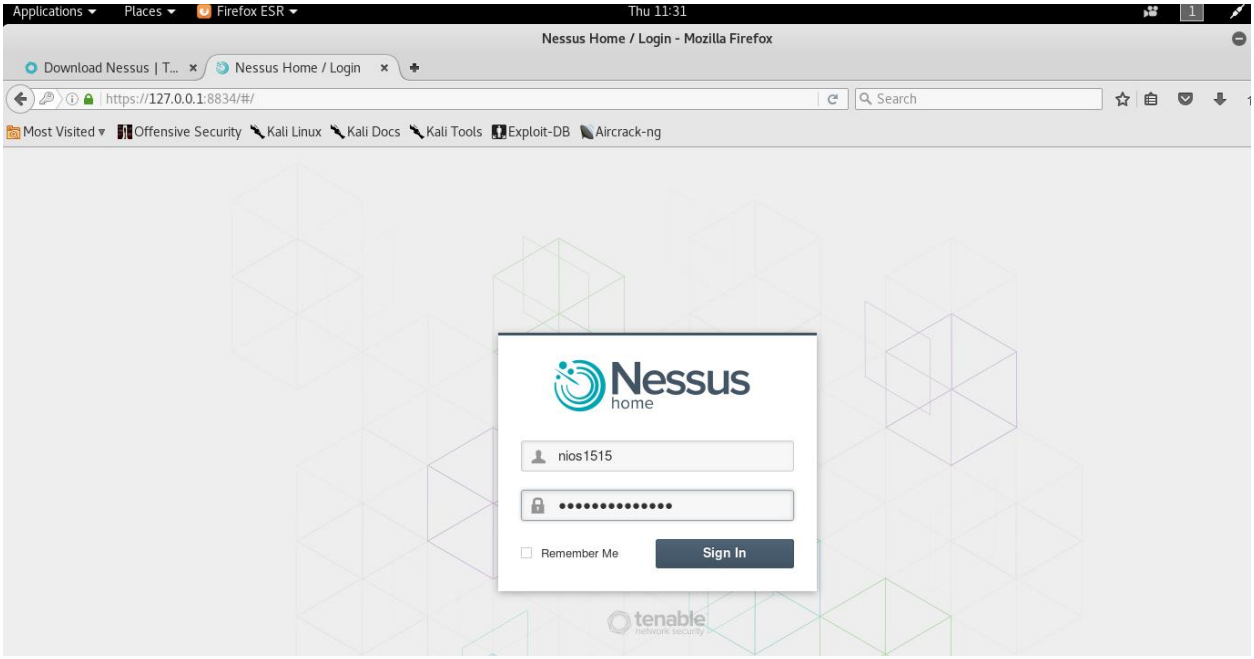
Détecter le système d'exploitation, l'adresse matérielle et la version du logiciel

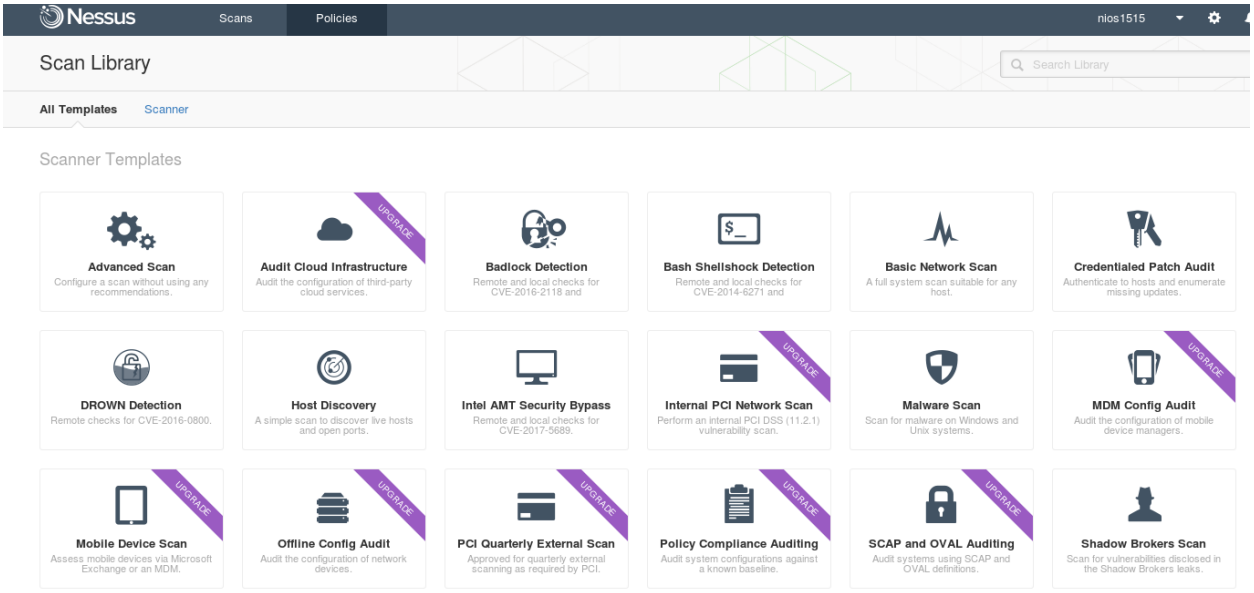
Détecter les trous de vulnérabilité et de sécurité (scripts Nmap)



II.4 Nessus :

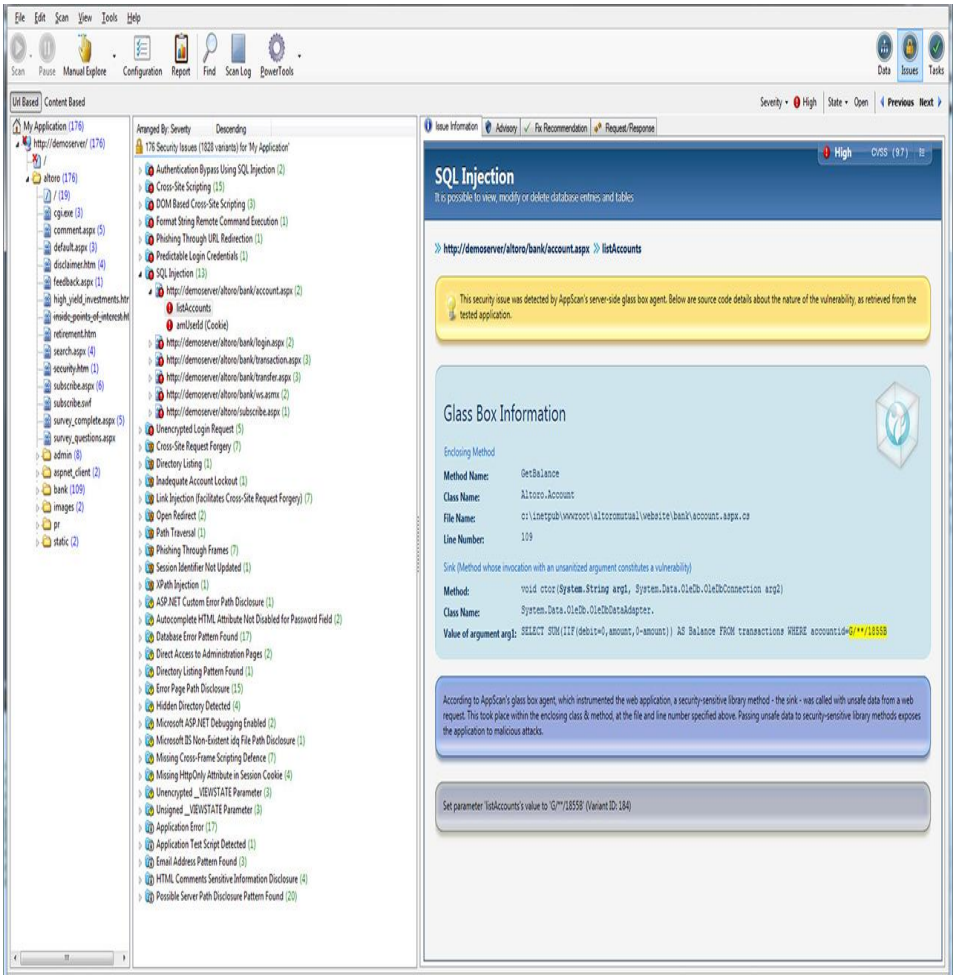
Nessus est une plate-forme de vulnérabilité pour les auditeurs et les analystes de sécurité. Les utilisateurs peuvent planifier des analyses sur plusieurs scanners, utiliser des assistants pour créer rapidement et rapidement des stratégies, planifier des analyses et envoyer des résultats par courrier électronique. Nessus prend en charge plus de technologies que tout autre fournisseur, y compris les systèmes d'exploitation, les périphériques réseau, les hyperviseurs, les bases de données, les tablettes / téléphones, les serveurs Web et les infrastructures critiques.


Applications
Places
Firefox ESR
Thu 11:31
Nessus Home / Login - Mozilla Firefox
Download Nessus | T...
Nessus Home / Login
https://127.0.0.1:8834/#/
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Nessus
home
nios1515
Remember Me
Sign In
tenable


Nessus
Scans
Policies
nios1515
Scan Library
Search Library
All Templates
Scanner
Scanner Templates
Advanced Scan
Configure a scan without using any recommendations.
Audit Cloud Infrastructure
Audit the configuration of third-party cloud services.
Badlock Detection
Remote and local checks for CVE-2016-2118 and
Bash Shellshock Detection
Remote and local checks for CVE-2014-6271 and
Basic Network Scan
A full system scan suitable for any host.
Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.
DROWN Detection
Remote checks for CVE-2016-0800.
Host Discovery
A simple scan to discover live hosts and open ports.
Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.
Internal PCI Network Scan
Perform an internal PCI DSS (11.2.1) vulnerability scan.
Malware Scan
Scan for malware on Windows and Unix systems.
MDM Config Audit
Audit the configuration of mobile device managers.
Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.
Offline Config Audit
Audit the configuration of network devices.
PCI Quarterly External Scan
Approved for quarterly external scanning as required by PCI.
Policy Compliance Auditing
Audit system configurations against a known baseline.
SCAP and OVAL Auditing
Audit systems using SCAP and OVAL definitions.
Shadow Brokers Scan
Scan for vulnerabilities disclosed in the Shadow Brokers leaks.
UPGRADE

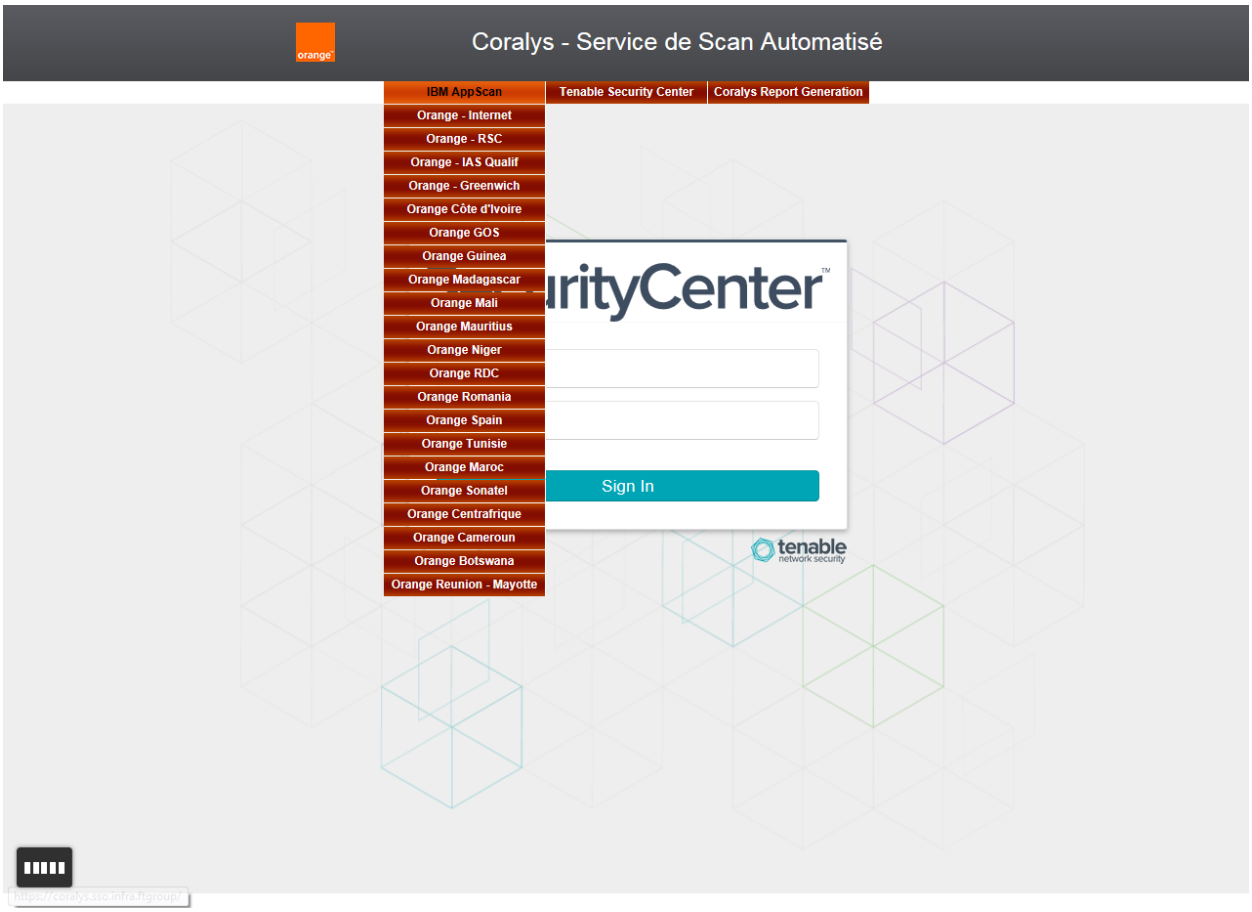
II.5 appscan :

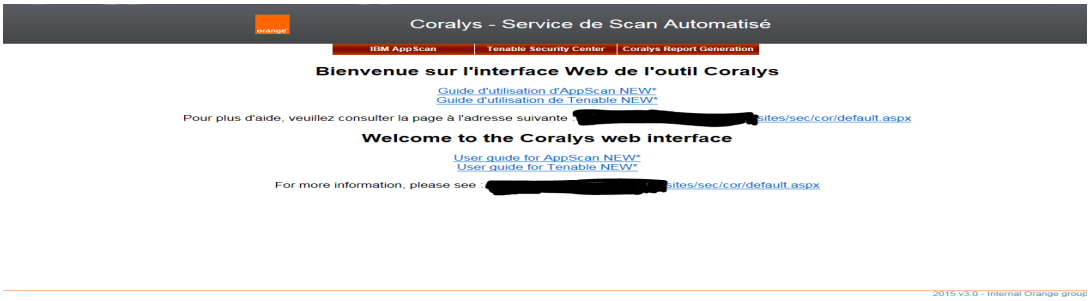
IBM Security AppScan améliore la sécurité des applications Web et la sécurité des applications mobiles, améliore la gestion des programmes de sécurité des applications et renforce la conformité réglementaire. En analysant les applications Web et mobiles avant le déploiement, AppScan permet d'identifier les vulnérabilités de sécurité et de générer des rapports et de corriger les recommandations.



II.6 Coralys :

Coralys est une plateforme développée par Orange dans le but de sécuriser ses serveurs et services (WEB, SMTP…), la plateforme est basée sur nmap, Nessus et appscan IBM elle est héberger sur un serveur interne accessible via un navigateur web après l'authentification il faut avoir des privilèges pour scanner les serveurs

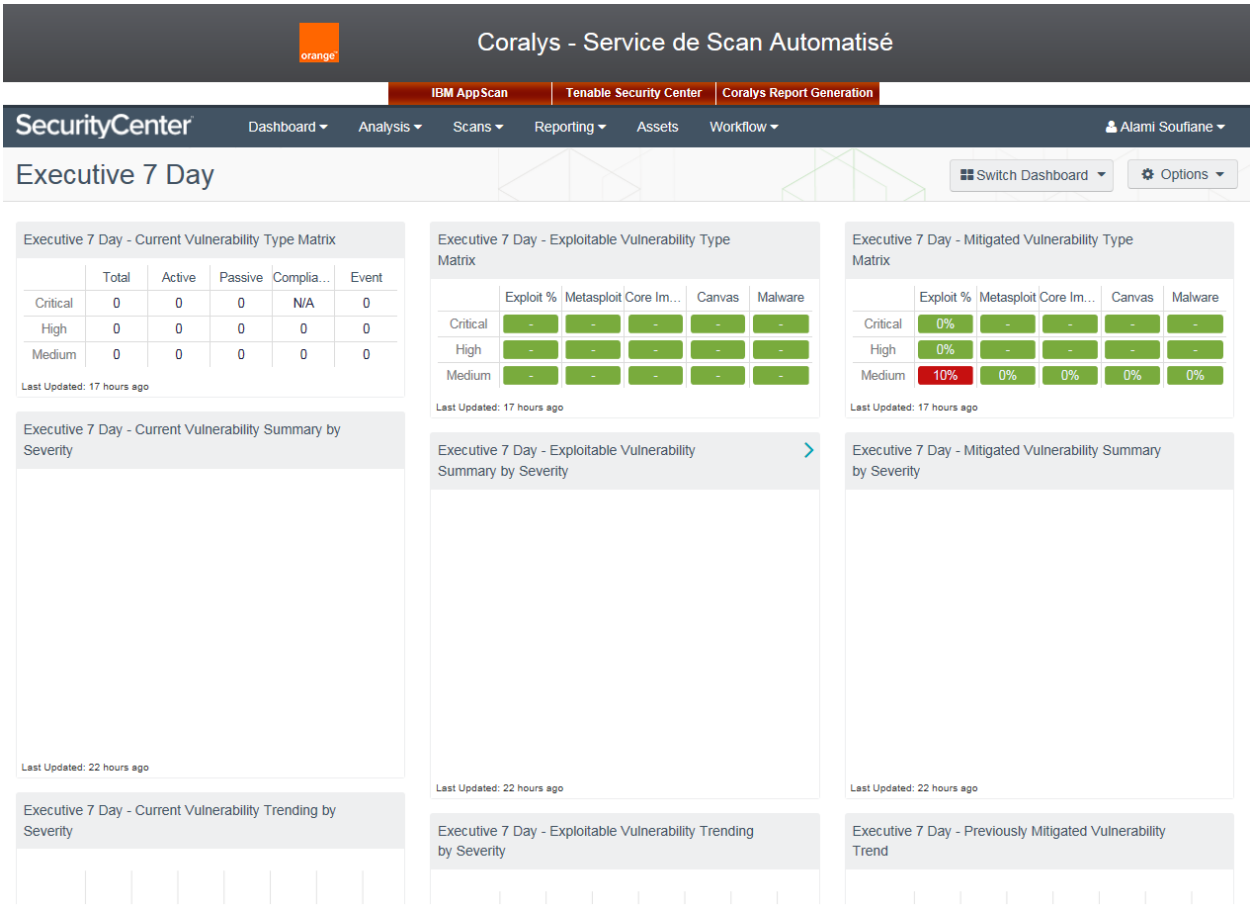




Coralys permet de :

- Scanner les vulnérabilités sur les serveurs et les matériels juste en lui donnant L'IP du serveur

- génération d'un rapport après le scan des vulnérabilités trouves



II.7 VI/VIM:

Vim est un éditeur de texte hautement configurable conçu pour créer et modifier tout type de texte très efficace. Il est inclus comme "vi" avec la plupart des systèmes UNIX et avec Apple OS X.

Vim est stable à la pierre et est en constante évolution pour devenir encore mieux. Parmi ses caractéristiques sont:

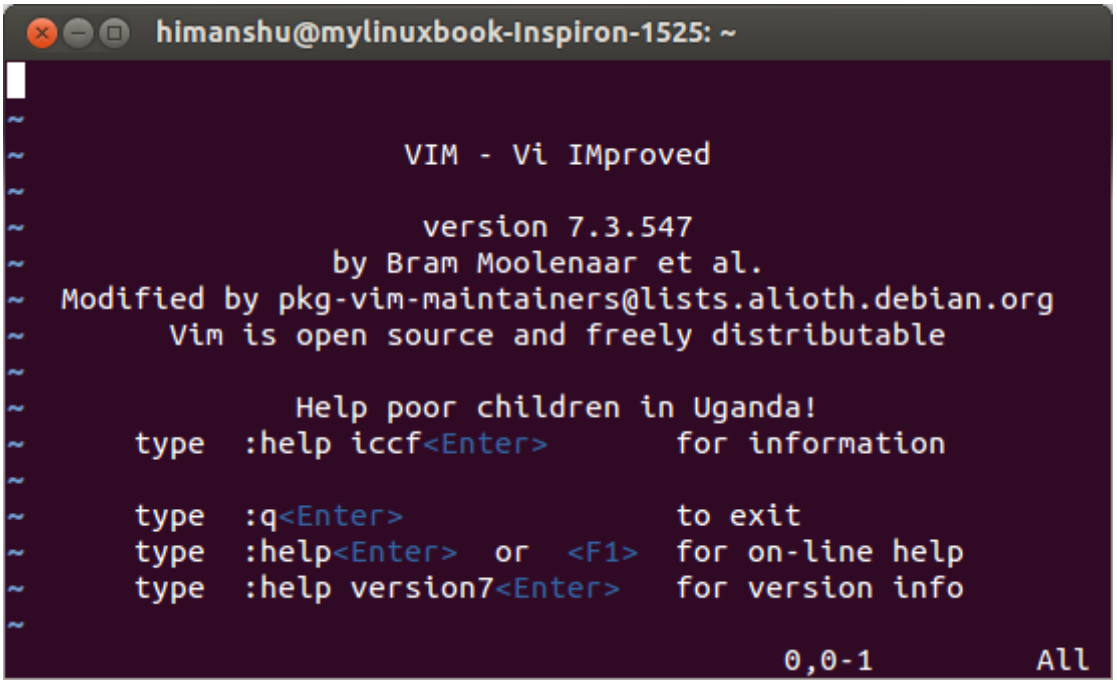
- Arbre défectueux persistant et multi-niveaux

- Système complet de plugins

- Prise en charge de centaines de langages de programmation et de formats de fichiers

- Recherche et remplacement puissants

- S'intègre avec de nombreux outils



II.8 CIS Benchmark :

Les repères CIS aide à protéger les systèmes, les logiciels et les réseaux contre les menaces cybernétiques évolutives actuelles. Développé par une communauté internationale d'experts de la cyber sécurité, les benchmarks CIS sont des lignes directrices de configuration pour plus de 100 technologies et plates-formes.

Plateformes :

Distribution Independent Linux

Microsoft Windows Desktop

Debian Linux

Ubuntu Linux

Microsoft IIS

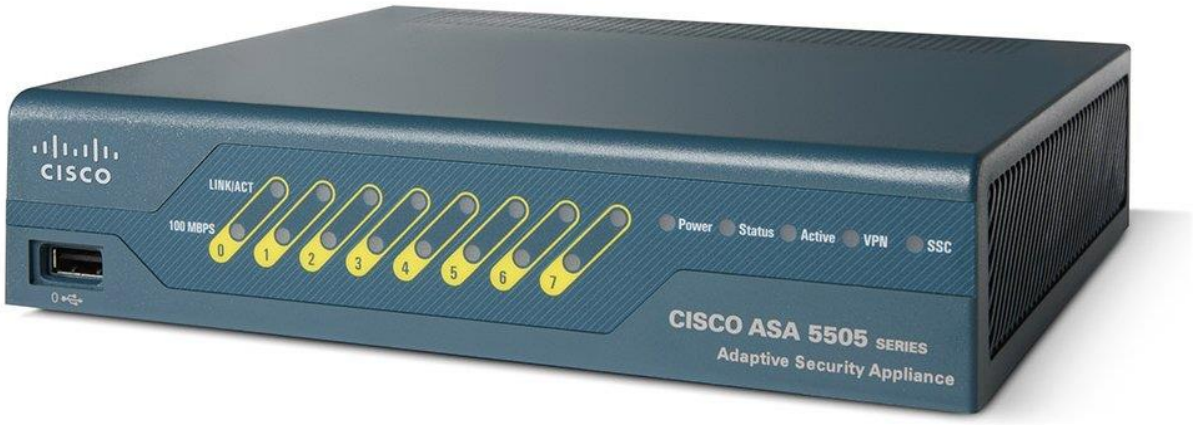
VMware

MongoDB

IBM DB2

Et tant d'autres.

II.9 cisco ASA 5505:



Est un pare-feu cisco de sécurité réseau qui surveille le trafic entrant et sortant du réseau et décide d'autoriser ou de bloquer un trafic spécifique en fonction d'un ensemble défini de règles de sécurité.

Les firewalls ont été une première ligne de défense en sécurité réseau depuis plus de 25 ans. Ils établissent une barrière entre les réseaux internes sécurisés et contrôlés qui peuvent être fiables et non fiables en dehors des réseaux, comme Internet.

Un pare-feu peut être un matériel, un logiciel ou les deux.

II.10 cisco ISE:

Cisco Identity Services Engine (ISE) est un produit d'administration réseau qui permet la création et l'application de politiques de sécurité et d'accès pour les périphériques de point de connexion connectés aux routeurs et aux commutateurs de l'entreprise. L'objectif est de simplifier la gestion des identités à travers divers appareils et applications.

Chapitre III: Travaille Technique

Ce chapitre est divisé en trois partie. Premièrement, la réalisation d'un script Bash pour RedHat v.6 et v.7. Ensuite, la réalisation d'un script Bash pour la machine AIX IBM. Finalement un scan de vulnérabilités avec Coralys sera effectué pour tester la fiabilité des scripts réaliser.

III.1 réalisation d'un programme, script Bash pour RedHat :

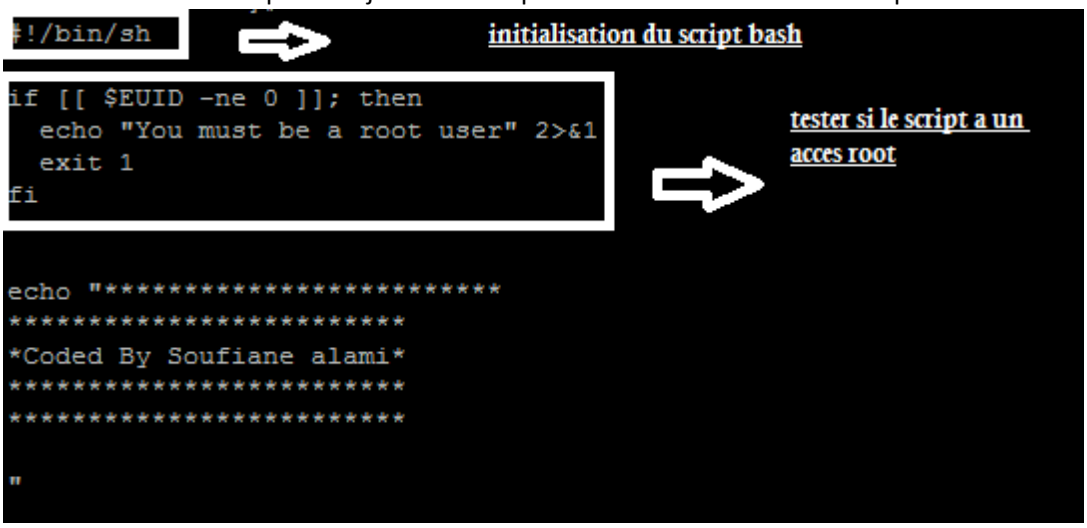
-Pour la réalisation du script CIS on a utilisé le langage de Scripting Bash pour linux qui est bien sur un langage puissant pour les machine linux and Unix qui va aider à exécuter les commandes linux avec des boucles et conditions

```
if [[ -e config.txt ]] ; then
else
fi
echo *.txt
cat input.txt >> output.txt 2>&1
```

Ce programme a pour but d'appliquer la sécurité recommandée depuis le document PDF benchmark CIS création d'un programme qui vérifie la configuration automatiquement du serveur et qui change la config si le serveur n'est pas correctement configuré

J'ai utilisé l'éditeur de texte VIM pour créer se script directement avec le protocole SSH, j'avais besoin d'un accès root car le script a besoin d'un au config system dans le dossier /etc pour tester si le script

était exécuté en tant que root j'ai écrit une petite condition en haut du script avant l'exécution



Après avoir tester le script ne doit pas avoir des problèmes de privilèges.

Pour commencer le travail il faut suivre le document Benchmark CIS de Redhat version 7 il y a une partie d'audit dans le document pour tester le system s'il est vulnérable ou non

Description:

The `cramfs` filesystem type is a compressed read-only Linux filesystem embedded in small footprint systems. A `cramfs` image can be used without having to first decompress the image.

Rationale:

Removing support for unneeded filesystem types reduces the local attack surface of the server. If this filesystem type is not needed, disable it.

Audit:

Run the following commands and verify the output is as indicated:

```
# modprobe -n -v cramfs
install /bin/true
```

Exemple sur le document PDF si la commande 'modprobe -n -v cramfs' donne une sortie différente c'est que la configuration system n'est pas là même que la configuration recommander

L'exemple dans le script bash

```
if ! [[ $(modprobe -n -v cramfs| grep 'install /bin/true') ]]; then
if ! [[ $(lsmod | grep cramfs) ]]; then
  echo "install cramfs /bin/true" >> /etc/modprobe.d/CIS.conf
 else
      echo "[+] cramfs checked" >> /var/log/cis.log &>/var/log/cis.log

 fi
 else
      echo "[+] cramfs checked">> /var/log/cis.log &>/var/log/cis.log
fi
```

Le script teste la condition de la commande si la commande donne un résultat positif il doit générer un fichier log dans le chemin suivant '/var/log/cis.log'

Si le résultat est négatif le script change la configuration system avec génération d'un log dans le même chemin dans cet exemple il modifie le fichier config CIS.conf dans le répertoire /etc/modprobe.d

Comme la recommandation du document

```
# lsmod | grep cramfs
<No output>
```

Remediation:

Edit or create the file `/etc/modprobe.d/CIS.conf` and add the following line:

```
install cramfs /bin/true
```

Critical Controls:

13 Data Protection
Data Protection

Ça montre que cette vulnérabilité est critique pour la protection des données et montre une partie pour la remédiation comme dans le script.

Le document CIS Benchmark a 347 pages et plusieurs conditions à mettre en place

1. Filesystem configuration
2. Configuration des mises a jours logiciels
3. Intégrité des fichiers system
4. Démarrage sécuriser
5. Process hardening
6. Mandatory access control
7. Services
8. Network configuration
9. IPv6
10. Firewall configuration
11. Configure logging

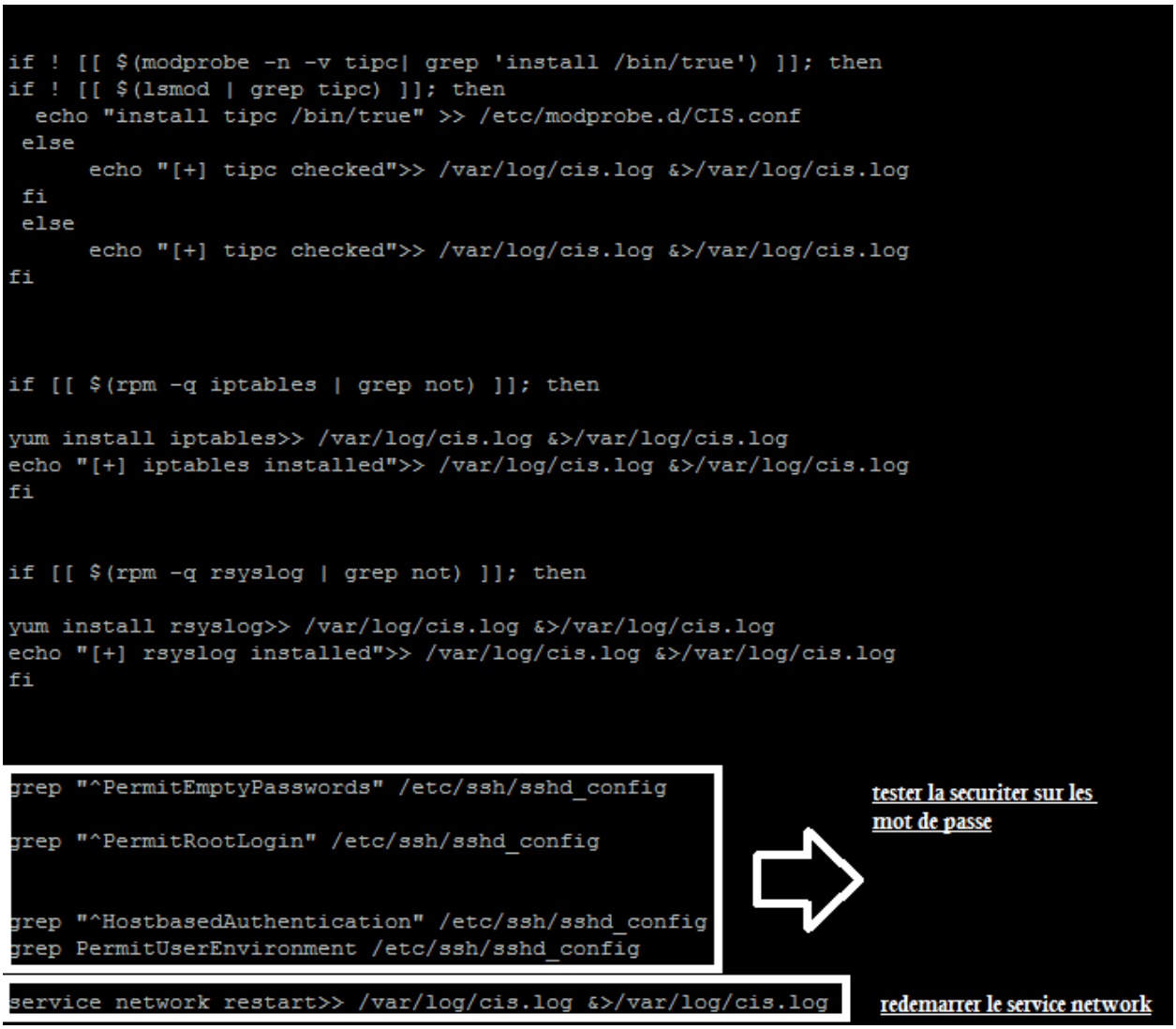
Le script pour RedHat version 7 contient plusieurs comme suivant :

```
[root@rhel6 CIS]# cat cis.sh
#!/bin/sh

if [[ $EUID -ne 0 ]]; then
  echo "You must be a root user" 2>&1
  exit 1
fi


echo "*************************
************************
*Coded By Soufiane alami*
************************
************************

"


if ! [[ $(modprobe -n -v cramfs| grep 'install /bin/true') ]]; then
if ! [[ $(lsmod | grep cramfs) ]]; then
  echo "install cramfs /bin/true" >> /etc/modprobe.d/CIS.conf
 else
      echo "[+] cramfs checked" >> /var/log/cis.log &>/var/log/cis.log

 fi
 else
      echo "[+] cramfs checked">> /var/log/cis.log &>/var/log/cis.log
fi


if ! [[ $(modprobe -n -v freevxfs| grep 'install /bin/true') ]]; then
if ! [[ $(lsmod | grep freevxfs) ]]; then
  echo "install freevxfs /bin/true" >> /etc/modprobe.d/CIS.conf

 else
      echo "[+] freevxfs checked">> /var/log/cis.log &>/var/log/cis.log
 fi
 else
    echo "[+] freevxfs checked">> /var/log/cis.log &>/var/log/cis.log
fi

if ! [[ $(modprobe -n -v jffs2| grep 'install /bin/true') ]]; then
if ! [[ $(lsmod | grep jffs2) ]]; then
  echo "install jffs2 /bin/true" >> /etc/modprobe.d/CIS.conf

 else
      echo "[+] jffs2 checked">> /var/log/cis.log &>/var/log/cis.log
 fi
 else
```

Après avoir tester tous les services et les configurations recommander par le document CIS Benchmark :

- La sécurité des services
- La sécurité des mots de passes
- La sécurité de la configuration

Il faut redémarrer les services avec génération d'un fichier log comme par : le service networking, le service apache2 web service s'il est utiliser

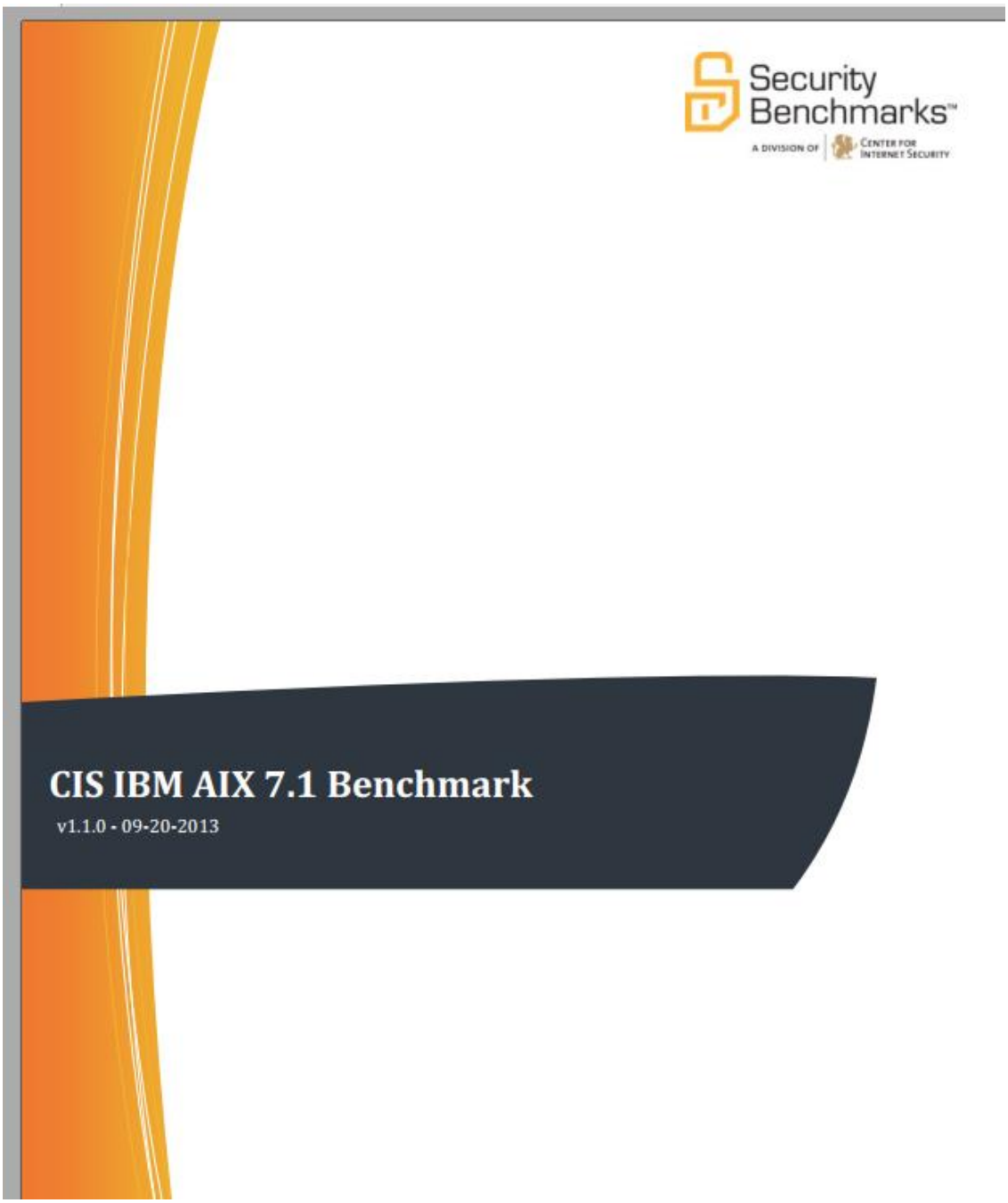


Le script teste plusieurs configurations et services :

- L'installation du Firewall iptables
- Redirection réseau
- Exige un mot passe pour l'authentification
- Installation des dépôt 'programme nécessaire '

III.2 réalisation d'un programme, script Bash pour IBM AIX :

Pour la réalisation du script j'ai suivi la même démarche que pour RedHat, avec le langage Bash



Le document a 221 pages avec audit et remédiation même chose que RedHat

1. Filesystem configuration
2. Configuration des mises a jours logiciels
3. Intégrité des fichiers system
4. Démarrage sécuriser
5. Process hardening
6. Mandatory access control
7. Services
8. Network configuration
9. IPv6
10. Firewall configuration
11. Configure logging

3.1.2 /etc/security/user - minage (Scored)

Profile Applicability:

- Level 1

Description:

Defines the minimum number of weeks before a password can be changed.

Rationale:

In setting the `minage` attribute, it prohibits users changing their password until a set number of weeks have passed.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a minage
```

The above command should yield the following output:

```
default minage=1
```

Remediation:

In `/etc/security/user`, set the default user stanza `minage` attribute to `1`:

```
chsec -f /etc/security/user -s default -a minage=1
```

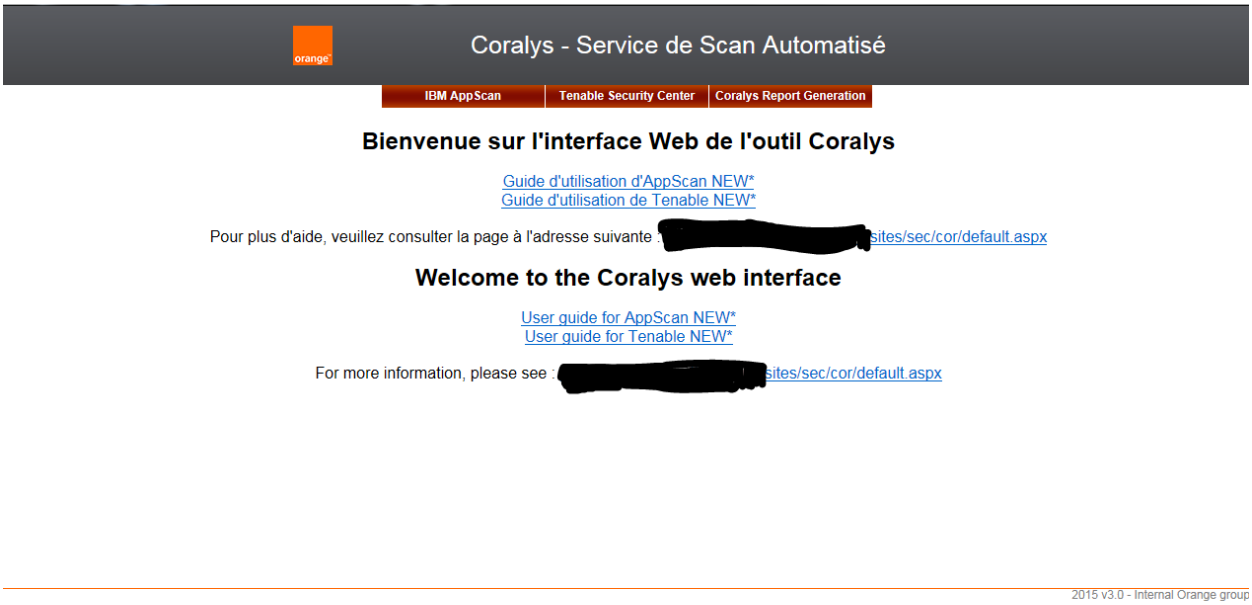

Le document contient une petite description, Audit et une remédiation

```
if ! [[ $(grep ^gpgcheck /etc/yum.conf | grep 'gpgcheck=1') ]]; then

echo 'please edit /etc/yum.conf and set gpgcheck=1'
echo "Edit any failing files in /etc/yum.repos.d/* and set all instances of gpgcheck to ' 1 '."
fi


if [[ $(rpm -q aide | grep not) ]]; then


yum install aide
aide --init
mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz

fi
```

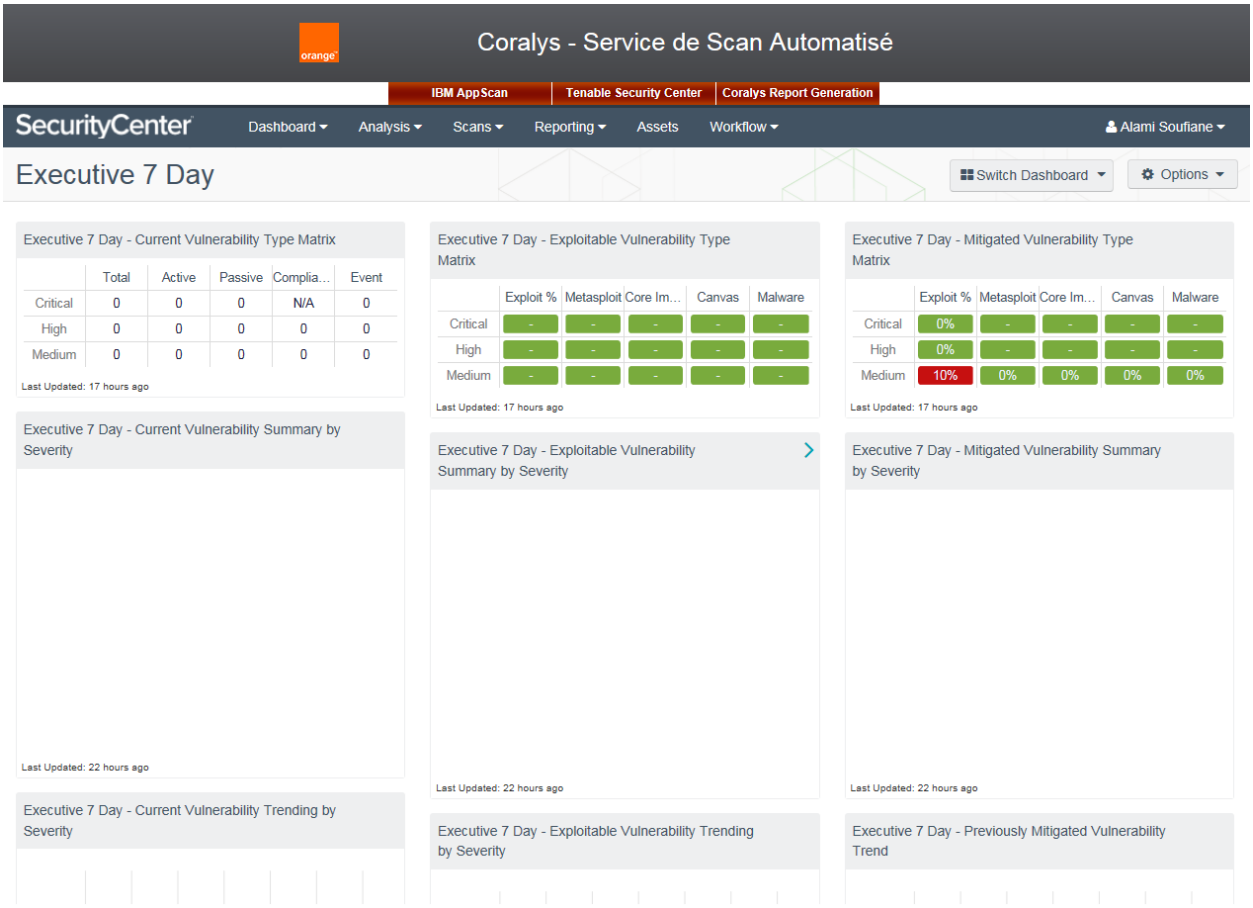
```
if ! [[ $(grep SELINUX=enforcing /etc/selinux/config | grep enforcing) ]]; then

echo "SELINUX=enforcing" >> /etc/selinux/config


fi
```

III.3 Scan des vulnérabilités avec Coralys :

Coralys est un scanneur de vulnérabilité puissant basé sur appscan et nmap permet de scanner les serveurs.



Après l'exécution du programme sur la machine Test RedHat et AIX j'ai pu scanner les serveurs avec leur IP adresse après 30 min le rapport générer contient juste des informations sur le system il n'y a pas de vulnérabilités critiques existent sur le serveur.



On peut conclure que le script à aider à sécuriser le system d'exploitation

Conclusion

Actuellement, nous assistons à un développement fulgurant des attaques menées sur les systèmes d'informations des grandes sociétés. Ainsi, face à cette perpétuelle menace, chaque opérateur est amené à bien sécurisé ces données. Dans ce travail, nous avons mis en place une solution CIS Benchmark pour mieux sécuriser les serveurs Linux (RedHat, AIX IBM) de la société Orange. Premièrement, nous avons créer deux scripts bash qui font un audit et un correctif s'il trouve une vulnérabilité ou une faiblesse sur le système d'exploitation serveur. Puis, nous avons testé leurs fiabilités en utilisant la plateforme Coralys.

Le long de l'élaboration de ce travail, on a rencontré pas mal des difficultés résidant essentiellement dans la phase de recherche et de documentation, surtout que le domaine de la sécurité informatique est très vaste. A cet égard, j'ai eu l'occasion de travailler avec de nouveaux systèmes d'exploitation serveur à savoir : RedHat, AIX IBM. Aussi, j'ai maitrisé la plateforme de vulnérabilité Coralys qui est basée sur AppScan et Nessus.

Finalement, ce stage de fin d'étude m'a permis d'avoir une expérience dans une entreprise multinationale comme ORANGE. Il m'a été bénéfique et avantageux, dans la mesure où il m'a permis de confronter le monde du travail de plus près et de m'engager dans un milieu professionnel pratique.

Reference

https://www-03.ibm.com/systems/power/software/aix/

https://access.redhat.com/articles/3078

https://www.cisecurity.org/cis-benchmarks/

http://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html

http://www.cisco.com/c/en/us/products/security/asa-firepower-services/index.html