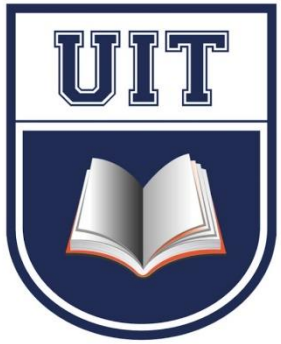


Cybersécurité

L3 RI

AUDIT DE LA SECURIT DES SI

Nizar Ben Neji
nizarbenneji@gmail.com

2020 / 2021

Audit de la Sécurité

Diverses étapes d'une mission d'audit

Etape 1

Préparation de l'audit

1 **Préparation de l'audit**

— Etude de l'existant
  - Métier
  - Acteurs
  - Clients et prestataires

— Collecte, lecture et révision des documents

— Identification du périmètre et des éléments à auditer
  - Processus
  - Zones
  - Systèmes et Applications

— Elaboration du planning de réalisation de la mission d'audit

— Rencontres et entretiens avec les responsables pour l'implication et la sensibilisation et la présentation du plan d'exécution de la mission

Etape 1

Préparation de l'audit

1 **Préparation de l'audit (Documentation)**

1. Organigramme de l'organisme avec le nom et la fonction des principaux responsables, ✓
2. Présentation des activités, des produits et des clients, ✗
3. Rapports des précédentes missions des audits internes ou externes,
4. Méthodologie d'appréciation des risques IT,
5. Rapport d'appréciation des risques IT,
6. Plan de continuité d'activité (PCA)/Plan de continuité informatique (PCI)

SYSTEME D'INFORMATION

7. Organigramme de la Direction des systèmes d'information ;
8. Note de désignation & Fiche de poste du Responsable de la Sécurité de l'information (RSSI) ;
9. Description et schéma de l'architecture fonctionnelle et applicative,
10. Description et schéma de l'architecture technique (système et réseau),
11. Liste des serveurs, progiciels, et équipements réseaux et sécurité (Switchs, Routeurs, Firewalls, IPS, IDS, etc.),

Etape 1

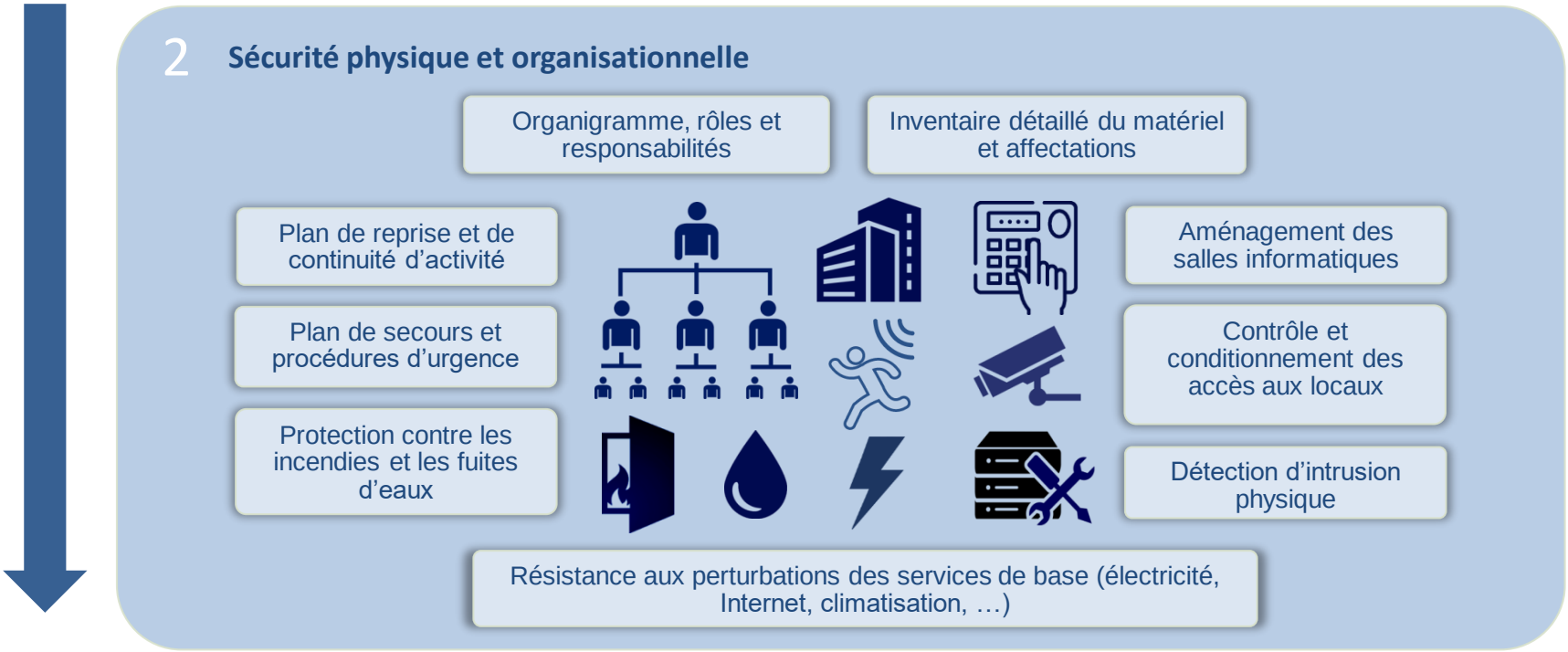
Préparation de l'audit

1 **Préparation de l'audit (Documentation)**

12. Manuels et Procédures d'exploitation informatique,
13. Procédures de contrôle des accès logiques et physiques,
14. Profils d'accès au système d'information,
15. Liste des prestataires de services informatiques avec les contrats des prestations,
16. Politique actuelle de sécurité informatique (Procédures, Chartes, règles, guides et manuels existants),
17. Planning des projets impactant le système d'information,

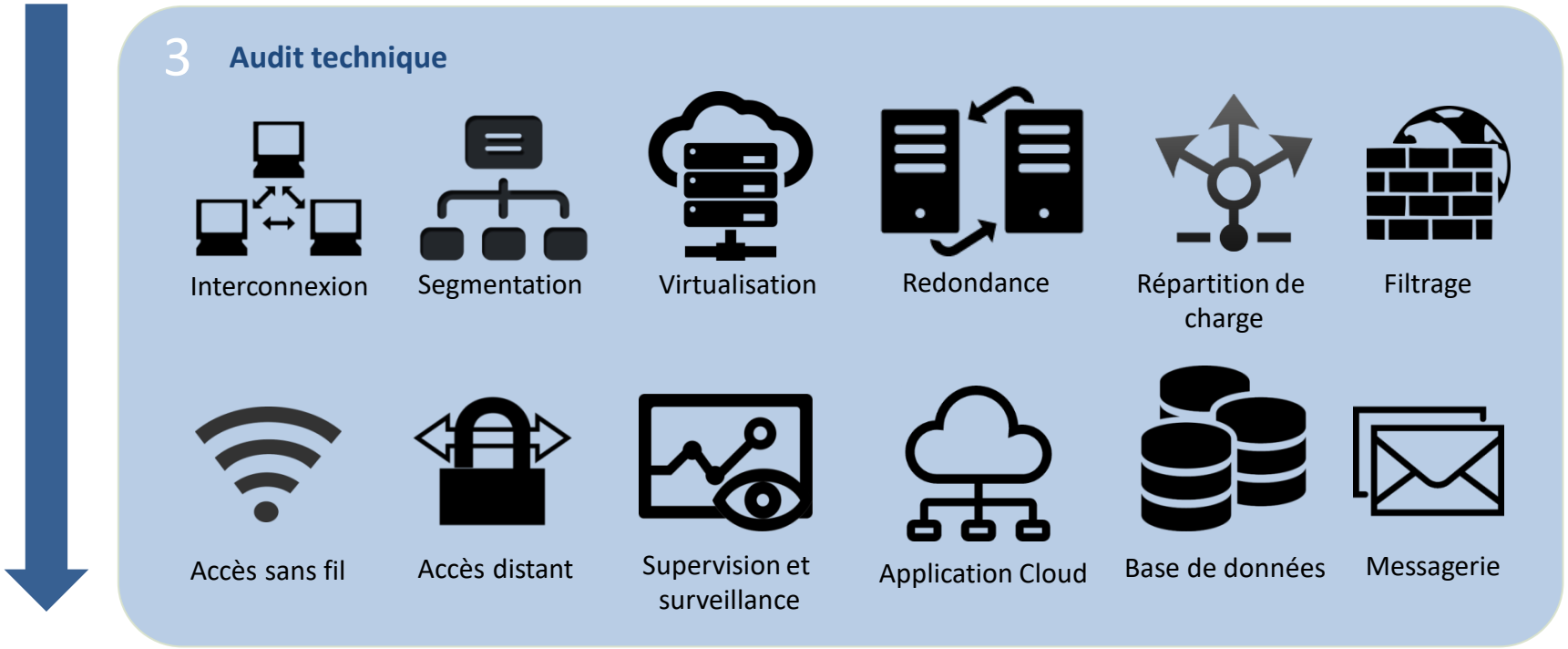
Etape 2

Sécurité physique et organisationnelle



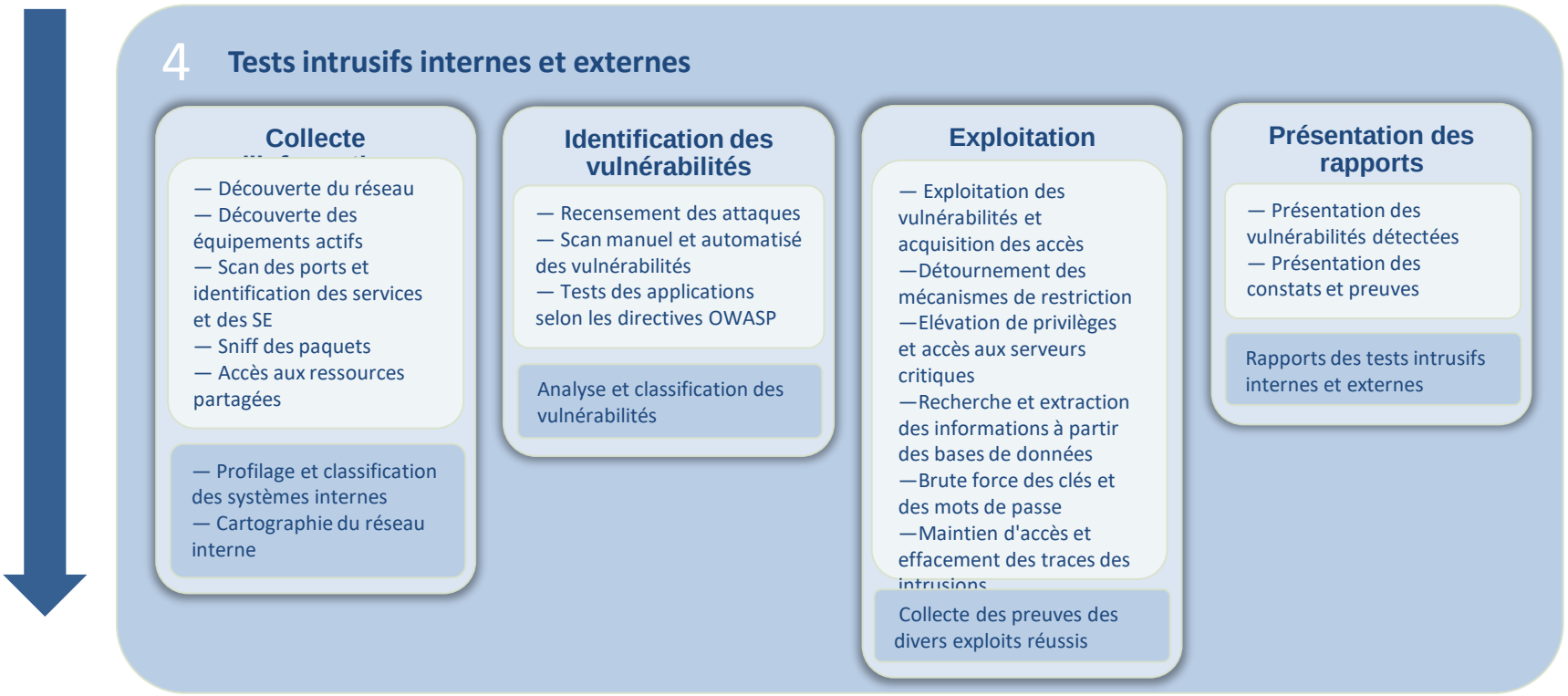
Etape 3

Audit technique



Etape 4

Tests intrusifs

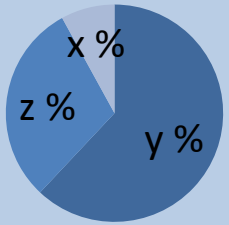


Etape 5

Synthèse et élaboration des livrables

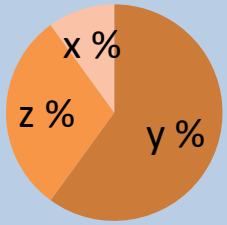
5 **Rapports d'audit:**

a. Rapport d'audit organisationnel et d'analyse des risques
b. Rapport d'audit technique et des tests intrusifs
c. Plan de traitement des risques et plan d'actions correctives et préventives des vulnérabilités et des non-conformités
d. Rapport de synthèse pour la direction générale



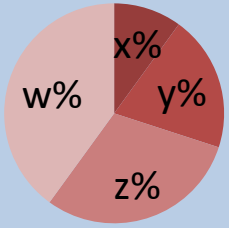
Haut
Important
Modéré

Niveau d'impact



Complexe
Moyenne
Simple

Complexité du traitement



Immédiat
Court terme
Moyen terme
Long terme

Urgence du traitement

Etape 5

Synthèse et élaboration des livrables

Table des matières

Rapport d'audit technique

Audit technique et tests intrusifs

- L'audit technique du système d'information vise à évaluer le niveau de sécurité du réseau, des systèmes et des diverses applications utilisées: interconnexion, segmentation, redondance, répartition de charge, virtualisation, filtrage, accès aux réseaux (Wifi, accès distant, …), supervision et surveillance, entrepôts de données, sauvegardes, services et applications (métier, messagerie, …).
- Les scénarios envisagés pour les tests intrusifs :
  - **Scénario 1**: l'auditeur simule le comportement d'un pirate informatique connecté du réseau interne comme étant invité sans qu'il n'est de droits ou d'habilitations
  - **Scénario 2**: l'auditeur simule le comportement d'un utilisateur légitime malveillant ayant les privilèges typiquement accordés à un utilisateur de l'entreprise et connecté du réseau interne.

Rapport d'audit technique

Outillage de l'audit

Etape	Outils
Recueil d'information	Nmap Netdiscover …
Identification des vulnérabilités	Nessus Sn1per Rapid7 Nexpose Acunetix Vega scanssl/sslyze …
Tests de pénétration	Metasploit …

Rapport d'audit technique

Types des vulnérabilités

Organisation	Vulnérabilité liée l'organisation du système audité ou sa documentation absente ou non appliquée
Conception	Vulnérabilité liée à la structure, la conception et les diverses fonctionnalités offertes par un système
Configuration	Vulnérabilité liée à une configuration inadaptée du système ou correctif non appliqué
Implémentation	Vulnérabilité liée au code source, au choix technique ou choix d'une version d'un logiciel ou d'un matériel
Gestion	Vulnérabilité liée à la gestion et à l'exploitation du système

Rapport d'audit technique

Niveau d'impact

H	Haut	Une vulnérabilité ayant un impact haut lorsque son exploitation aurait un effet défavorable très critique sur l'activité métier de la société et une incidence significative sur les clients et les partenaires **et/ou** l'actif en question est très attractif pour les attaquants **et/ou** l'exploitation de la vulnérabilité est très simple en termes de compétences techniques et de ressources matérielles et financières.
I	Important	Une vulnérabilité est jugée importante lorsque son exploitation aurait un effet défavorable considérable sur l'activité métier de la société **et/ou** l'actif en question est moyennement attractif **et/ou** l'exploitation de la vulnérabilité est moyennement complexe.
M	Modéré	Une vulnérabilité est jugée modérée lorsque son exploitation aurait un effet défavorable mineur sur l'activité métier de la société **et/ou** l'actif en question est peu attractif **et/ou** l'exploitation de la vulnérabilité est très complexe.

Rapport d'audit technique

Complexité de mise en oeuvre

C	Complexe	Mise en œuvre de la recommandation est difficile **et/ou** les actions à entreprendre sont compliquées, impliquant plusieurs entités et touchant plusieurs systèmes **et/ou** la correction nécessite un budget et doit être formalisée sous forme de projet à part.
M	Moyenne	Mise en œuvre de la recommandation est moyennement difficile impliquant au moins deux entités et peut être menée à bien sans charge significative.
S	Simple	Mise en œuvre de la recommandation est simple à réaliser par une seule personne sans impact majeur sur son calendrier.

Rapport d'audit technique

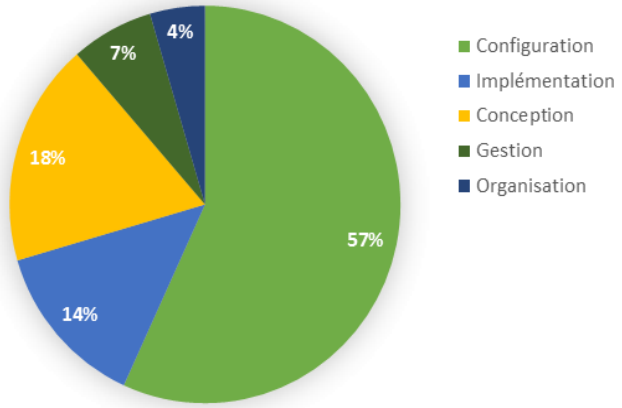
Urgence de traitement

- **Immédiat** : la correction de la vulnérabilité doit être réalisée dans un délai **inférieur à 1 mois**.
- **Court terme**: la correction de la vulnérabilité doit être réalisée dans un délai de **1 à 3 mois**.
- **Moyen terme**: la correction de la vulnérabilité doit être réalisée dans un délai de **3 à 6 mois**.
- **Long terme**: la correction de la vulnérabilité doit être réalisée dans un délai **supérieur à 6 mois**.

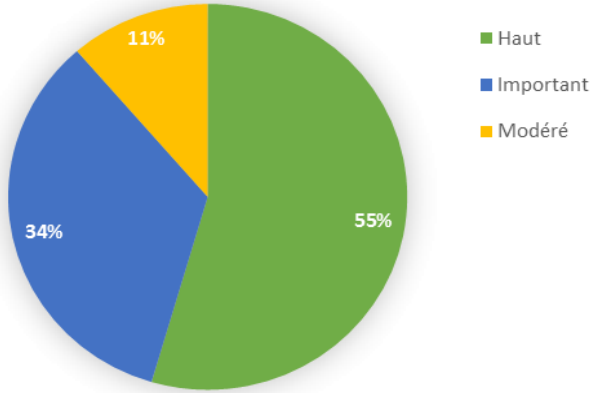
	Niveau d'impact			
Complexité de mise œuvre	Valeur	Modéré	Important	Haut
	Simple	Court terme (C)	Immédiat (I)	Immédiat(I)
	Moyenne	Moyen terme (M)	Court terme (C)	Immédiat(I)
	Complexe	Long terme (L)	Moyen terme (M)	Court terme (C)

Rapport d'audit technique

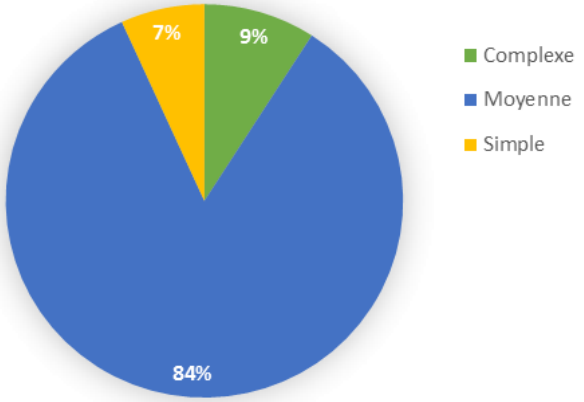
Synthèse des vulnérabilités



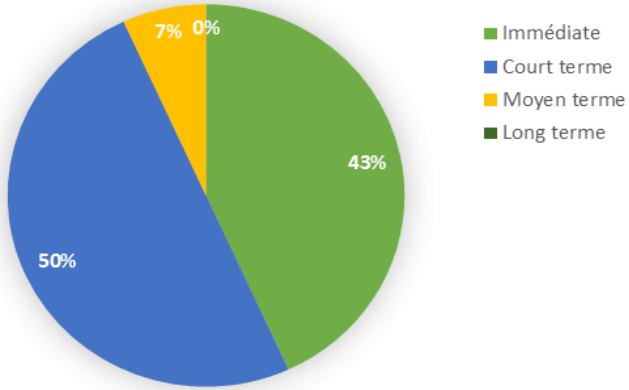
Répartition des vulnérabilités par type



Répartition des vulnérabilités par niveau d'impact



Répartition des vulnérabilités selon la complexité du traitement



Répartition des vulnérabilités selon l'urgence du traitement

Rapport d'audit technique

Liste détaillée des vulnérabilités

ID	Elément impacté	Type	Description	Impact	Recommandation	Complexité du traitement	Urgence du traitement
V_01.	Infrastructure réseau et sécurité	Configuration	Insuffisance détectée au niveau du filtrage réseau. Bien que les LANs des utilisateurs soient définis, le filtrage mis en place n'est pas suffisant pour contrôler et gérer les communications entre les diverses zones du réseau. Cette vulnérabilité peut engendrer une propagation rapide de malware au niveau de tout le réseau et il peut également y avoir des attaques par rebond à partir d'Internet ou du réseau interne.	H	Réviser et renforcer les mécanismes de filtrage pour tous les trafics circulants entre les différentes zones du réseau.	M	C
V_02.	Infrastructure réseau et sécurité	Conception	Absence d'un site de backup distant vu que le Datacenter de Nfidha héberge uniquement les serveurs de production.	H	Nécessite d'un site de backup distant afin de garantir la pérennité des données et la continuité d'activité en cas d'incident	C	C
V_03.	Infrastructure réseau et sécurité	Conception	Absence d'un réseau dédié pour le management des équipements réseau et des équipements de sécurité. Le réseau de management doit être complétement isolé du réseau de production et d'Internet. Par exemple, l'accès aux interfaces d'administration des diverses solutions réseau, sécurité et virtualisation était possible à partir du réseau Wifi comme montre la Figure 1 en Annexe.	H	Concevoir et mettre en place un réseau d'administration dédié. Mettre à jour la configuration de tous les équipements réseaux et sécurité de manière à ce qu'ils ne peuvent être administrés qu'à partir des machines d'administration explicitement spécifiées et appartenant au réseau d'administration dédié. Le réseau d'administration doit être isolé	M	C

Rapport d'audit technique

Liste détaillée des vulnérabilités

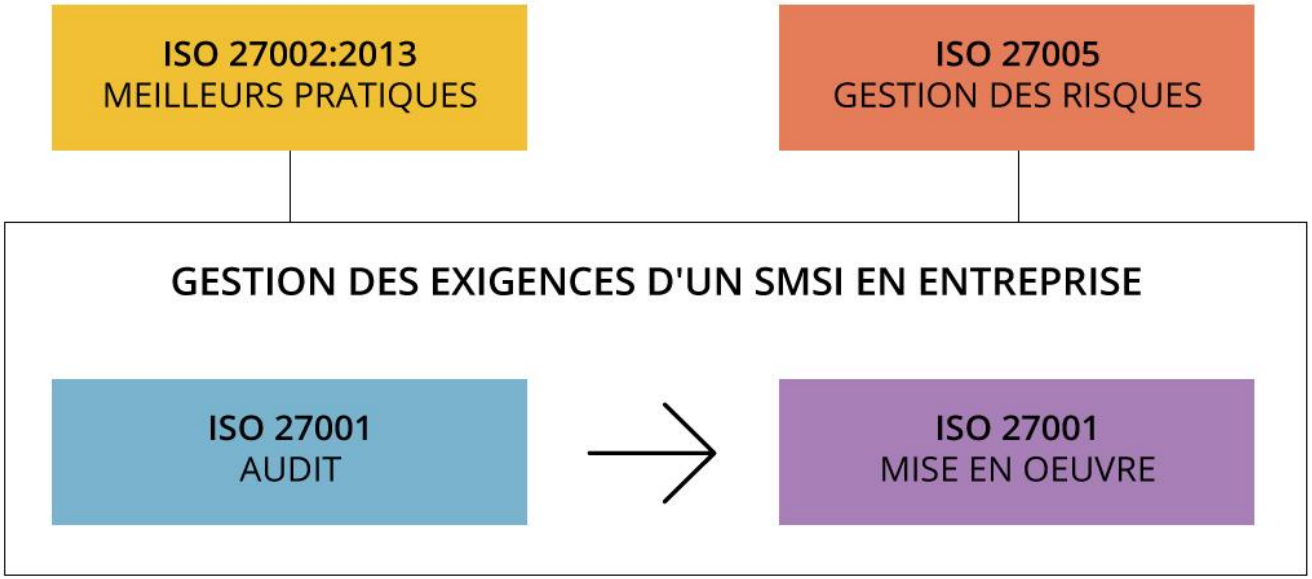
<table>
<tr>
<td>V_026</td>
<td>Serveurs et Machines des utilisateurs et des administrateurs</td>
<td>Configuration</td>
<td>Mise à jour de sécurité MS17-010 de Microsoft n'est pas appliquée au niveau des serveurs des serveurs suivants :
<table>
<tr><th>LAN</th><th>Hôte Vulnérable</th><th>Nom (.site.com.tn)</th></tr>
<tr><td>Site 1</td><td>10.216.1.83</td><td>file2</td></tr>
<tr><td></td><td>10.216.1.114</td><td>tunmail</td></tr>
<tr><td>Site 2</td><td>10.216.50.45</td><td>ptu-1g5q44j</td></tr>
<tr><td></td><td>10.216.50.122</td><td>-</td></tr>
<tr><td></td><td>10.216.50.127</td><td>deskop-vgal1lk.</td></tr>
<tr><td></td><td>10.216.50.141</td><td>-</td></tr>
<tr><td>Site 3</td><td>10.216.32.16</td><td>-</td></tr>
<tr><td>Site 1</td><td>10.216.16.164</td><td>-</td></tr>
<tr><td></td><td>10.216.29.220</td><td>-</td></tr>
</table>
Ce problème est présent sur les systèmes Windows dotés de versions obsolètes du service de partage de fichiers et d'imprimantes de Windows (SMB) rendant ainsi ces machines vulnérables à plusieurs types d'attaques :
– WannaCry
– Petya
– EternalBlue
– EternalChampion
– EternalRomance
– EternalSynergy
– uncredentialed check</td>
<td>H</td>
<td>Appliquer la mise à jour de sécurité MS17-010 au niveau de tous les serveurs vulnérables.</td>
<td>M</td>
<td>I</td>
</tr>
</table>

Rapport d'audit technique

Liste détaillée des vulnérabilités

<table>
<tr>
<td>V_034</td>
<td>Serveurs</td>
<td>Implémentation</td>
<td>Plusieurs problèmes relatifs à SSL/TLS ont été identifiés au niveau des serveurs et des divers équipements réseau et de sécurité de type:
<table>
<tr><th>Problème</th><th>Type</th></tr>
<tr><td>Weak Key Exchange (< 128 bits)</td><td>Configuration</td></tr>
<tr><td>Use of the insecure cipher algorithm RC4</td><td>Configuration</td></tr>
<tr><td>Use of SSL Weak and Medium Cipher Suites</td><td>Configuration</td></tr>
<tr><td>Use of SSLv3 which is obsolete and unsecure</td><td>Configuration</td></tr>
<tr><td>Use of SSLv2 which is obsolete and unsecure</td><td>Configuration</td></tr>
<tr><td>TLS/SSL Server is enabling the POODLE attack</td><td>Configuration</td></tr>
<tr><td>Not supporting the best protocol TLS v1.2 (newest)</td><td>Configuration</td></tr>
<tr><td>Few number of Authorized Cipher Suites</td><td>Configuration</td></tr>
<tr><td>HTTPS not forced</td><td>Configuration</td></tr>
<tr><td>Self-signed certificate</td><td>Certificate</td></tr>
<tr><td>Not trusted Server's Certificate</td><td>Certificate</td></tr>
<tr><td>SHA 1 Certificate (Server or CA)</td><td>Certificate</td></tr>
<tr><td>Not Valid Certificate (Self-signed, Expired, Revoked, ...)</td><td>Certificate</td></tr>
<tr><td>SSL Certificate with wrong Hostname</td><td>Certificate</td></tr>
</table>
</td>
<td>I</td>
<td>Pour corriger les problèmes relatifs à SSL/TLS :
– Il faut mettre en place une PKI d'entreprise (par exemple Microsoft CA) qui va émettre les certificats électroniques nécessaires pour sécuriser toutes les applications internes.
– Il faut inclure le certificat des autorités au niveau des magasins des autorités de confiance des logiciels utilisés (Systèmes d'exploitation, Navigateurs et autres).
– Il faut utiliser des certificats SSL valides (non expirés)
– Il faut utiliser des certificats SSL avec des noms de domaines corrects.
– Il ne faut pas utiliser des algorithmes de hachage obsolètes comme SHA1 pour la création des certificats électroniques.
– Il faut autoriser uniquement les protocoles de chiffrement forts comme TLS 1.0, TLS 1.1 et TLS 1.2 et désactiver le support des protocoles obsolètes comme SSLv2 et SSLv3.
– Il faut désactiver au niveau de la configuration du SSL/TLS l'usage les</td>
<td>C</td>
<td>M</td>
</tr>
</table>

Référentiels de sécurité



OWASP
Open Web Application
Security Project