

# *Université Américaine de Kinshasa*

## FACULTE D'INFORMATIQUE



### Séminaire d'Audit et Sécurité Informatique

Sujet :

---

*Par*

...

Etudiants en L3 informatique

Encadreur:

C.T TSHIMANGA MUTOMBO Tshims

ANNEE UNIVERSITAIRE: 2024-2025

## « Parlez sur les sujets » :

Bien sûr, voici une liste de sujets que vous pourriez envisager de défendre dans le cadre d'un cours d'audit et de sécurité informatique :

1. L'importance de la conformité réglementaire en matière de sécurité informatique.
2. Les meilleures pratiques pour la gestion des identités et des accès.
3. L'impact de la cybersécurité sur la continuité des activités.
4. Les défis et les opportunités de la gestion des vulnérabilités.
5. L'analyse des risques en matière de sécurité informatique et les méthodologies associées.
6. L'évaluation de la sécurité des réseaux sans fil.
7. Les tendances émergentes en matière de cybermenaces et les stratégies de défense correspondantes.
8. L'importance de la sensibilisation à la sécurité informatique pour les employés.
9. L'évaluation de la sécurité des applications web.
10. Les implications de la sécurité des données dans le cloud computing.
11. L'importance de la gouvernance de la sécurité informatique dans les organisations.
12. L'évaluation de la conformité aux normes de sécurité telles que ISO 27001 ou NIST SP 800-53.
13. L'évolution des technologies de cryptographie et leur rôle dans la sécurité informatique.
14. Les défis de la sécurité des objets connectés (IoT) et les solutions possibles.
15. L'impact des attaques par ransomware et les stratégies de récupération des données.

## LES SUJETS A DEFENDRE DE TRANSMISSION DES DONNEES ET SECURITE INFORMATIQUE 2016-2017

Sujet 1	Sujet2	Sujet3
Adware	Filtrage des URL	Chiffrement
Application potentiellement indésirable (PUA) Attaque de force brute	Gestion unifiée des menaces (UTM)	DMZ
Botnet	IPS	IDS
Canular	IPsec	VPN
Centre de commande et de contrôle	Pare-feu	SSH
Chaîne de lettres	Pare-feu pour les applications (WAF)	SSL
Cheval de Troie	Reverse Proxy	IPSEC
Cheval de Troie de porte dérobée	Sécurité des appareils mobile s	Le service de sécurité de confidentialité

Cookie	Sécurité des systèmes d'extrémité	Le service de sécurité d'authentification
Malware de document	Sécurité sans fil	Le service de sécurité d'intégrité
Malware de messagerie	VPN/SSL VPN	Le service de sécurité de non-répudiation
Malware de secteur de démarrage	Contrôle HTTPS	Déchiffrement
Malware mobile	Contrôle d'accès réseau (NAC)	Intrusion
Menace avancée persistante («advanced persistent threat» ou APT)	Vol de données	Camouflage
Rootkit	Fuite de données	L'algorithme d'AES
Spam	Perte de données	L'algorithme DES
Spyware (ou logiciel espion)	Usurpation	L'algorithme RC4

Virus	Téléchargement passif	L'algorithme RC5
Virus parasite	Détection dans le cloud	L'algorithme RSA
Vulnérabilité	Pirateur de navigateurs	L'algorithme EL GAMAI
Attaque par déni de service	Dépassement de la mémoire tampon	L'algorithme ECC
Ransomware	Protection runtime	Audits de vulnérabilité
Correctifs	Les réseaux sans fils et les problèmes de sécurité	La gestion de la sécurité
Pot de miel (Honeypot)	Services d'authentification et annuaire	Faille dans SSL/TLS

Spearphishing		La protection des données de l'utilisateur
---------------	--	--

N.B :

- Le travail est individuel;
- Le travail est à défendre ;
- le travail comprend plus moins 15 pages
- le travail doit être relié ;
- Le 31 Mars 2024 dépôt physique de travail à 12h00' auprès du CP ;
- Le 31 Mars 2024 envoi du travail par la voie électronique en format PDF ou Word à l'adresse suivante : [tshims.tshimanga@unikin.ac.cd](mailto:tshims.tshimanga@unikin.ac.cd)
- Programme de défense :
  - vendredi le 04 Avril de 08H à 12H de 13H à 15H
  - Préparer 15 slides (diapos) pour la projection devant les amis.
  - Le 11 Avril interrogation générale.
  - Le 17 Avril examen d'audit et sécurité.