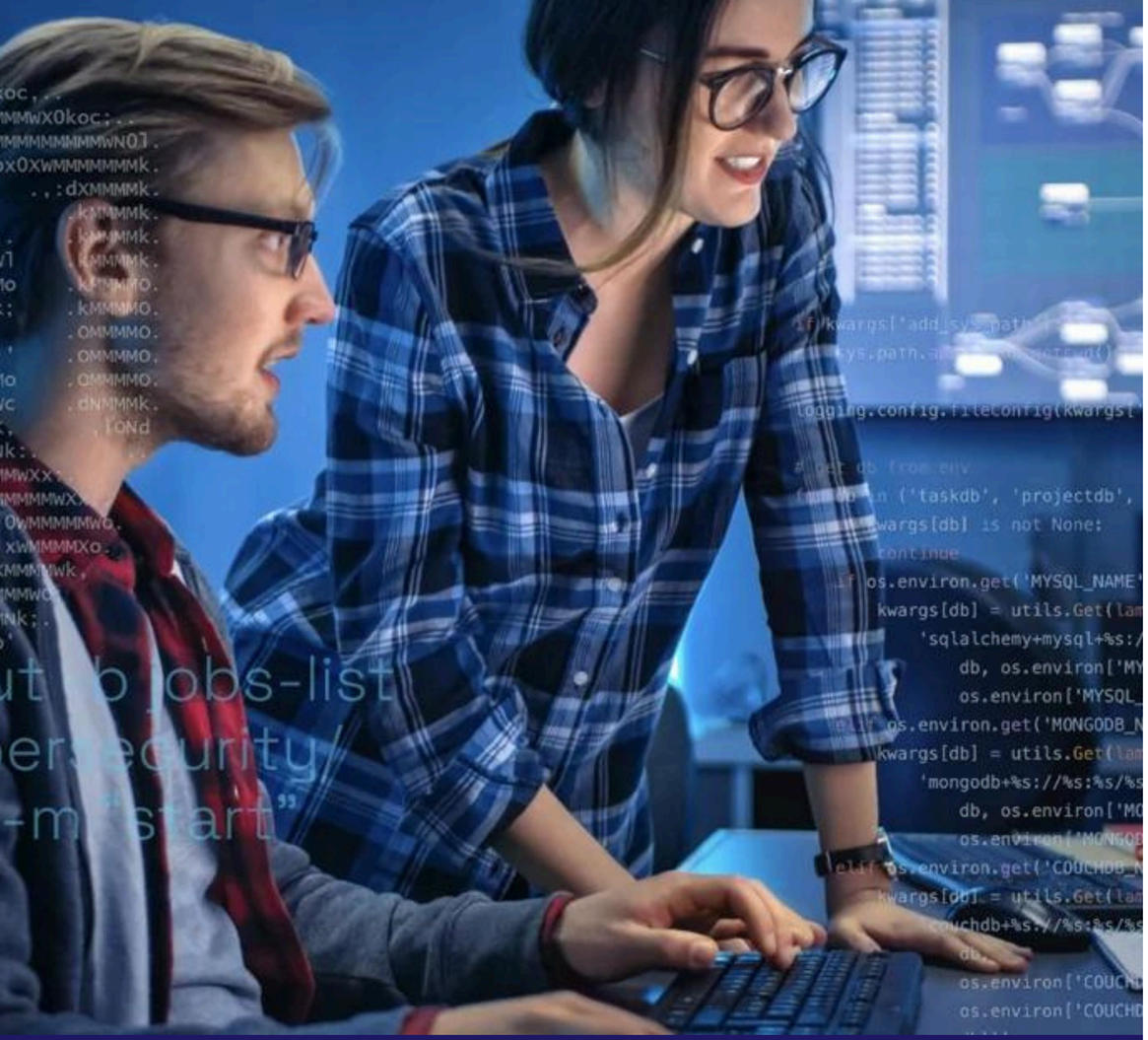
CYBERNETIC-SECURITY

SALON N° 4 DE CYBERSECURITÉ

CYBERNETIC-SECURITY



SALON DE CYBERSECURITY

Thème

Ethical Hacking : Techniques de Détection d'intrusion et Contre-Mesures

(Cybersécurité)

L'Équipe

DR PAPA MORY GYEUE
Expert en Cybersécurité
Spécialiste des Méthodes et Systèmes de Protection de l'Information
Enseignant chercheur

M. ERHAD FALEU
Ingénieur en Cybersécurité
Risk Manager

M. ISSIAGA KALTAMBA
Responsable SOC 1 et 2
ASTO (Analyste SI)
Consultant en Cybersécurité

Sommaire

OBJECTIF DU SALON

- INTRODUCTION À LA DÉTECTION D'INTRUSION
  - DÉFINITION
  - IMPORTANCE EN CYBERSÉCURITÉ
  - TYPES DE DÉTECTION
- PRINCIPES DE FONCTIONNEMENT DES SYSTÈMES DE DÉTECTION D'INTRUSION (IDS)
  - SURVEILLANCE EN TEMPS RÉEL
  - ANALYSE DES MODÈLES
  - RÉACTION AUX INTRUSIONS

- TYPES DE SYSTÈMES DE DÉTECTION D'INTRUSION
  - BASÉS SUR LES SIGNATURES (IDS SIGNATURE-BASED)
  - BASÉS SUR LES ANOMALIES (IDS ANOMALY-BASED)

- SYSTÈMES DE DÉTECTION ET DE PRÉVENTION D'INTRUSION (IDS/IPS)
  - DIFFÉRENCE ENTRE IDS ET IPS
    - IDS : SYSTÈMES DE DÉTECTION D'INTRUSION.
    - IPS : SYSTÈMES DE PRÉVENTION D'INTRUSION QUI PRENNENT DES MESURES PROACTIVES.

- LES OUTILS NECESSAIRES

INTRODUCTION À LA DÉTECTION D'INTRUSION

Définition : L*a détection d'intrusion est le processus de surveillance des activités sur un système ou un réseau pour détecter des comportements anormaux ou suspects qui pourraient indiquer une tentative d'intrusion.*

Importance: *La détection d'intrusion est essentielle en cybersécurité car elle permet d'identifier rapidement les tentatives d'attaques avant qu'elles ne causent des dommages. Elle protège les données sensibles, assure la conformité aux réglementations, et réduit les risques internes et externes. En détectant et en répondant efficacement aux menaces, elle renforce la résilience des systèmes, préserve la continuité des activités, et maintient la confiance des clients et partenaires dans la sécurité des infrastructures IT.*

TYPES DE DÉTECTION

1. **DÉTECTION BASÉE SUR LES SIGNATURES**
2. **DÉTECTION BASÉE SUR LES ANOMALIES**
3. **DÉTECTION BASÉE SUR LES HEURISTIQUES**
4. **DÉTECTION BASÉE SUR L'ANALYSE COMPORTEMENTALE**
5. **DÉTECTION HYBRIDE**

PRINCIPES DE FONCTIONNEMENT DES SYSTÈMES DE DÉTECTION D'INTRUSION (IDS)

- **SURVEILLANCE EN TEMPS RÉEL** : COLLECTE DE DONNÉES SUR LES ÉVÉNEMENTS SYSTÈME ET RÉSEAU.
- **ANALYSE DES MODÈLES** : IDENTIFICATION DES COMPORTEMENTS ANORMAUX.
- **RÉACTION AUX INTRUSIONS** : ALERTER LES ADMINISTRATEURS OU BLOQUER LES ACTIONS MALVEILLANTES.

TYPES DE SYSTÈMES DE DÉTECTION D'INTRUSION

- Basés sur les Signatures (IDS signature-based) :
  - Fonctionnement : Identification des attaques en se basant sur des signatures connues.
  - Avantages et Inconvénients : Efficace pour les menaces connues, moins pour les nouvelles attaques.
- Basés sur les Anomalies (IDS anomaly-based) :
  - Fonctionnement : Détection des écarts par rapport au comportement normal.
  - Avantages et Inconvénients : Capable de détecter des menaces inconnues, mais sujet aux faux positifs.

SYSTÈMES DE DÉTECTION ET DE PRÉVENTION D'INTRUSION (IDS/IPS)

- Différence entre IDS et IPS :
  - IDS : Systèmes de Détection d'Intrusion.
  - IPS : Systèmes de Prévention d'Intrusion qui prennent des mesures proactives.

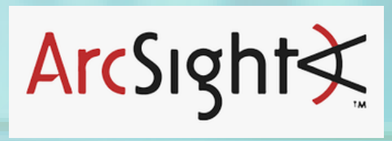
LES OUTILS NECESSAIRES

SYSTÈMES DE DÉTECTION D'INTRUSION (IDS)

OUTILS D'ANALYSE DE COMPORTEMENT

SYSTÈMES DE PRÉVENTION D'INTRUSION (IPS)

OUTILS DE GESTION ET DE CORRÉLATION DES JOURNAUX (SIEM)



OUTILS DE SURVEILLANCE ET D'ANALYSE RÉSEAU

MERCI

POUR VOTRE ATTENTION

PHASE PRATIQUE

WWW.CYBERNETIC-SECURITY.COM

Plus d'information

SITE WEB: CYBERNETIC-SECURITY.COM

EMAIL: INFO@CYBERNETIC-SECURITY.COM

TÉLÉPHONE:

+221 78 833 88 47

+221 78 896 49 96

+221 76 355 19 09

@CYBERNETIC-SECURITY

@CYBERNETIC-SECURITY

@CYBERNETIC-SECURITY