Gestion des réseaux et sécurité opérationnelle

Domaine Ingénierie et Architecture
Filière Informatique et systèmes de communication
Orientation Réseaux et systèmes (ISCR)
Mode de formation Plein temps

Informations générales

Nom : Gestion des réseaux et sécurité opérationnelle
Identifiant : GRS
Années académiques : 2021-2022, 2022-2023
Responsable : Alain Bron
Charge de travail : 90 heures d'études
Périodes encadrées : 48 (= 36 heures)

Semestre	E1	S1	S2	E2	S3	S4	E3	S5	S6
Cours						24			
Laboratoire						24			

Connaissances préalables recommandées

L'étudiant-e doit connaître et savoir utiliser les notions suivantes :

- réseaux informatiques
- introduction à la sécurité de l'information

Les unités d'enseignement RXI et ISI permettent d'acquérir ces connaissances.

Objectifs

A l'issue de cette unité d'enseignement, l'étudiant-e sera capable de :

- expliquer les différents niveaux de gestion (Node, Network, Service & Business Management)
- présenter la méthodologie de modélisation d'un réseau informatique
- connaître le fonctionnement du protocole SNMP et les aspects sécuritaires
- connaître les différentes méthodes de monitoring des réseaux informatiques
- connaître les méthodes de "log management"
- connaître des solutions du marché (open source et commerciales)
- être capable de développer une règle de détection en partant d'une technique d'attaque
- être capable d'appliquer quelques méthodologies de dépannage d'un réseau

Contenu et formes d'enseignement

Répartition des périodes indiquée à titre informatif.

Cours: 24 périodes

- Introduction à la gestion des réseaux informatiques	1
- Introduction à l'approche des "Objets gérés". Protocole SNMP. Notion de MIB, SMIS, Syslog, SNMP	4
- Network programming, management and monitoring. Structure des données (JSON, YAML, XML, YANG), Ansible, RESTCONF, NETCONF	4
- Ségrégation de réseau (opérationnel vs. monitoring)	2
- Supervision d'infrastructure : concepts, architecture et technologies	2
- Gestion opérationnelle des correctifs de sécurité (méthodologie, suivi, détection avec Nessus/OpenVAS/Clair)	2
- Log management : principe, historique, architecture, methodologie, technologies (collecte/centralisation, processing, SIEM, alerting, ...). Environnements Windows WEF/EventID...	2
- Présentation de la suite ELK (ElasticSearch, Logstash, Kibana/Security). Analyse des logs (corrélations, analyses statistiques, machine learning)	1
- Présentation de la solution Splunk. Analyse des logs	1
- Présentation de la solution Azure Sentinel	1
- NSM : Network Security Monitoring : IDS, IPS, DPI avec Suricata, concepts, utilisation et limites	2
- Detection engineering : comment partir d'une attaque et implémenter une détection (MITRE ATT&CK)	2

Laboratoire: 24 périodes

- Syslog	4
- SNMP	4
- Déploiement monitoring infrastructure (Cacti, Nagios, Grafana...)	4
- Configuration et tests avec Nessus/OpenVAS/Clair/...	2
- Mise en place de la solution ELK pour une collecte dans un environnement Windows (Sysmon, Winlogbeat, Logstash, ElasticSearch et Kibana)	2
- Utilisation de la solution Splunk	2
- Utilisation de la solution Azure Sentinel	2
- Analyse de techniques (ex : persistance autorun ou service, ou infection de poste, en utilisant les tactiques et techniques du groupe APT29) et écriture de règles de détection dans un SIEM	4

Bibliographie

- Designing and building Security Operation Center, Nathans, Syngress.
- Logging and Logs Management, Chuvakin, Syngress.
- Network Security through Data Analysis, Collins, O'reilly.
- Crafting the infosec playbook, Bollinger, Enright, Valites, O'reilly.
- Network Management Fundamentals, Alexander Clemm, Cisco Press.
- Network Administrators Survival Guide, Anand Deveriya, Cisco Press.
- Essential SNMP, Douglas Mauro, Kevin Schmidt, O'Reilly.
- Network Analysis, Architecture, and Design, J. McCabe, Morgan Kaufmann.

Contrôle de connaissances

Cours : l'acquisition des matières de cet enseignement sera contrôlée au fur et à mesure par des tests et des travaux personnels tout au long de son déroulement. Il y aura au moins 2 tests d'une durée totale d'au moins 1.5 période.

Laboratoire : ils seront évalués sur la base des rapports de manipulation, à 3 reprises au minimum.

Examen : L'atteinte de l'ensemble des objectifs de formation sera vérifiée lors d'un contrôle final commun écrit d'une durée de 60 minutes.

Matériel autorisé :

- Information communiquée directement par l'enseignant.

Calcul de la note finale

Note finale = moyenne cours x 0.3 + moyenne laboratoire x 0.2 + moyenne examen x 0.5