Utilisation de la distribution Kali dans le cadre du bloc 3 sur la cybersécurité

Description du thème

Propriétés	Description
Intitulé long	Utilisation de la distribution Kali dans le cadre du bloc 3 sur la cybersécurité.
Formation concernée	BTS Services Informatiques aux Organisations SLAM et SISR
Matière	Bloc 3 SLAM et SISR – Cybersécurité des services informatiques
Présentation	Activités en laboratoire permettant d'exploiter la distribution Kali Linux dans le cadre du bloc 3 sur la cybersécurité. Deux laboratoires composés de conteneurs sur Docker sont fournis. Des activités utilisant ces laboratoires sont proposées. D'autres activités ont vocation à être ajoutées.
Compétences	Protéger les données à caractère personnel. Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques. Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service. Assurer la cybersécurité d'une solution applicative.
Savoirs	Typologie des risques et leurs impacts. Principe de la sécurité : disponibilité, intégrité et confidentialité. Chiffrement, authentification et preuve : principes et techniques. Sécurité des applications Web : risques, menaces et protocoles. Cybersécurité : bonnes pratiques, normes et standards. Sécurité du développement d'application. Vulnérabilités et contre-mesures sur les problèmes courants de développement.
Transversalité	Bloc 1 et 2 du BTS SIO.
Prérequis	Connaissances de base concernant l'administration d'un système GNU/Linux, fondamentaux en matière de cryptographie, de certificat, fondamentaux réseaux (Ethernet, IP, TCP).
Outils	Kali avec le framework metasploit, serveur, client et routeur sous Debian 13, serveur metasploitable (v2). Conteneurs docker (laboratoires 1 et 2 mis à disposition). https://forge.apps.education.fr/reseau-certa/bts-sio/labos-kali-docker/lab1/ https://forge.apps.education.fr/reseau-certa/bts-sio/labos-kali-docker/lab2/
Mots-clés	Kali, cryptographie, chiffrement, certificat, analyse trames, empoisonnement arp, scanner de vulnérabilités, exploitation de vulnérabilités, exploit, metasploit, payloads, hameçonnage, typosquattage, typosquating, défiguration, ingénierie sociale, dns spoofing, remédiations, hygiène numérique, respect des bonnes pratiques.
Durée	De 1 à 4 heures par fiche.
Auteur.e(s)	Quentin Demoulières, Patrice Dignan, Apollonie Raffalli, Patrizio Valente, Cécile Nivaggioni avec la relecture de Valérie Martinez. Laboratoire sur Docker : Apollonie Raffalli avec les tests de Christelle Thiry pour la version 3.0.
Version	v 3.1
Date de publication	Juillet 2026

Ce support comporte des travaux pratiques permettant d'exploiter la distribution Kali Linux dans le cadre du bloc 3 sur la cybersécurité, plutôt en deuxième année (même s'il est possible d'envisager d'en étudier certaines en première année).

Les activités peuvent se traiter de manière indépendante. La progression proposée peut donc être modifiée et adaptée en fonction des outils disponibles et des spécificités de chaque établissement.
Les professeurs peuvent reprendre en l'état ces activités ou les modifier pour les intégrer dans leurs travaux en laboratoire.
Ce support a vocation à être enrichi avec de nouvelles activités.

Activités proposées

Activité 1 : attaque MITM d'un service SSH et mise en place de contre-mesures
Activité 2 : attaque MITM d'un service HTTP et mise en place de contre-mesures
Activité 3 : attaque de type injection SQL et mise en place de contre-mesures
Activité 4 : attaque par ingénierie sociale (hameçonnage associé à du typosquattage)
Activité 5 : exploitation d'une faille applicative du service FTP via l'outil « Metasploit »
Activité 6 : analyse et exploitation des failles de sécurité avec Nessus
Activité 7 : attaque de type DNS SPOOFING et propositions de contre-mesures

Les laboratoires sont fournis. À la première utilisation, la création des conteneurs peut prendre du temps (entre 10 mn et 30 mn selon les caractéristiques de la machine et le débit Internet) car les images doivent être téléchargées.