

# USCB12 - Hacking réseau

## Présentation

### Prérequis

RSX101, RSX112

## Objectifs pédagogiques

### Description :

Nous montrons ici comment un attaquant peut détourner les mécanismes réseaux à des fins d'exploitation offensive. Les points abordés ont pour objectif de comprendre les mécanismes mis en œuvre pour obtenir des effets comme la découverte de la topologie d'un réseau, le détournement de trafic, l'entrave réseau, etc.

*Remarque : Afin que ce cours ne soit pas détourné à des fins malveillantes, l'ensemble des techniques présentées font partie des techniques de bases, largement documentées et facilement détectables voire inopérantes sur les systèmes actuels.*

### Objectifs pédagogiques :

Obtenir une compréhension fine des mécanismes réseaux et comprendre comment ils peuvent être détournés. Chaque technique étudiée s'accompagne d'un point sur les contre-mesures à mettre en place. L'ensemble des TP seront réalisés à partir de réseaux virtuels.

## Compétences

### Compétences acquises :

- Comprendre les mécanismes intimes du réseau
- Comprendre les mécanismes de détournements à des fins malveillantes
- Analyse des échanges réseaux
- Forger des paquets réseaux
- Savoir mettre en place des contre-mesures

### Savoirs :

- Utiliser scapy, outils de scan, ARP, DNS, TCP, UDP

## Programme

### Contenu

- Introduction
  - Rappels sur les protocoles réseaux
  - Analyse et compréhension des échanges réseaux à partir de captures pcap
  - Forger des paquets avec scapy
- Observation du réseau, découverte de sa topologie et propriétés
  - Recherche de machines
  - Identification de firewall
  - Recherche de bannière (déterminer le système d'exploitation distant)
  - Recherche de ports ouverts (ICMP Scanning, TCP Half Open, TCP Connect, UDP, Balayage furtif, etc.)
  - Contre-mesure
- Détournement, Injection du trafic
  - Man-in-the-Middle
  - ARP Poisonning
  - DNS Poisonning
  - Prédiction des numéros de séquence TCP.
  - Vol de session TCP : Hijacking (Hunt, Juggernaut).
  - Contre-mesure

Mis à jour le 22-04-2022



**Code : USCB12**

Unité spécifique de type mixte

3 crédits

**Responsabilité nationale :**

EPN05 - Informatique / 1

**Contact national :**

Cnam Centre Régional de Bretagne

Zoopôle Les Croix  
2 rue Camille Guérin  
22440 Ploufragan

0 972 311 312

Isabelle Guée

[bzh\\_master\\_cybersecurite@lecnam](mailto:bzh_master_cybersecurite@lecnam)

- Chaînage de proxy
- Evasion aux IDS et aux pare-feu
  - Fragmentation de paquets
  - Routage par la source
  - Adresse IP de leurre
  - IP Address Spoofing
  - Attaque d'insertion

## Modalités de validation

- Examen final

## Description des modalités de validation

Examen de 2 heures