AYI NEDJIMI Consultants

Bettercap & Ettercap : Guide MITM

20 April 2026 • Mis à jour le 20 April 2026 • 49 min de lecture

Guide complet Bettercap et Ettercap : techniques MITM (ARP/DNS spoofin exploitation AD. Comparatif et défenses.

L'interception de trafic réseau constitue l'un des vecteurs d'attaque les plus redou Depuis les premières démonstrations d'ARP spoofing dans les années 2000 avec Bettercap en 2026, les outils de Man-in-the-Middle (MITM) ont connu une évolutio avec une architecture monolithique, vers Bettercap, développé en Go avec une ap de la discipline du pentest réseau. Cette transition n'est pas simplement technique manière dont les professionnels de la sécurité offensive abordent l'interception, l'a Que vous meniez un audit réseau, un test d'intrusion Active Directory, ou une éval MITM attack tools reste incontournable pour tout consultant en cybersécurité offe profondeur Ettercap et Bettercap, leurs techniques d'attaque, leurs modes opérato scénarios d'exploitation Active Directory complets.

Points clés de cet article

- Comprendre l'évolution d'Ettercap vers Bettercap et les raisons techniques de
- Maîtriser les techniques d'ARP spoofing pentest, DNS spoofing, DHCP spoofing
- Déployer Bettercap pour le pentest Active Directory : LLMNR poisoning, NTLM
- Automatiser les attaques avec les caplets Bettercap et la REST API
- Mettre en place les défenses adaptées : DAI, DHCP snooping, 802.1X, détection

Ettercap : l'outil historique du Man-in-the-Middle

Origines et philosophie

Ettercap est né en 2001, développé par Alberto Ornaghi (ALoR) et Marco Valleri (N concept même de test d'intrusion réseau en était à ses balbutiements, Ettercap a suite complète d'attaques Man-in-the-Middle. Son nom, contraction de « Ethernet capturer et manipuler le trafic transitant sur un segment Ethernet local. Écrit intégr Linux avec une attention particulière portée à la performance brute et à l'accès ba révolutionnaire pour l'époque, a permis à des générations de pentesters d'appren projet est hébergé sur GitHub Ettercap et continue de recevoir des mises à jour co considérablement ralenti depuis 2020.

Architecture technique d'Ettercap

L'architecture d'Ettercap repose sur un noyau central qui gère les interfaces résea paquets, et un système de plugins extensible. Le noyau intercepte les paquets via travers une chaîne de dissecteurs protocolaires qui extraient les informations pert IMAP, etc.), et les transmettent aux modules d'attaque actifs. Les principaux comp