AYI NEDJIMI Consultants

Responder : Guide Complet pour le Pe

20 April 2026 • Mis à jour le 20 April 2026 • 48 min de lecture

Guide expert Responder : LLMNR/NBT-NS poisoning, WPAD exploitation, c
opératoire complet pentest AD.

Avertissement légal : Les techniques présentées dans cet article sont destinées e
offensive dans un cadre légal : tests d'intrusion mandatés, compétitions CTF, envi
contre des systèmes sans autorisation explicite est illégale et punissable par la loi
décline toute responsabilité en cas d'usage malveillant.

Lors d'un test d'intrusion interne pour un groupe industriel du CAC40, j'ai démarré
— un simple câble Ethernet, aucun identifiant, aucune connaissance préalable de
avait capturé 23 hashes NTLMv2, dont celui d'un compte de service avec des priv
Directory était compromis avant la pause café. Ce scénario, loin d'être exceptionn
outils les plus redoutés — et les plus efficaces — de l'arsenal offensif pour le pent
(SpiderLabs), cet outil Python exploite les failles fondamentales des protocoles de
WPAD. Ce guide exhaustif vous emmène des fondamentaux protocolaires jusqu'a
par les combinaisons avec Impacket et les stratégies de détection. Que vous soye

sécurité cherchant à durcir votre AD, cette ressource couvre l'intégralité du spectr
permettre de maîtriser pleinement le **responder pentest** dans un environnement A

Qu'est-ce que Responder ?

Responder est un outil open source de poisoning et de capture d'identifiants résea
pseudonyme lgandx. Publié initialement sur GitHub en 2012, il a révolutionné les te
de faiblesses protocolaires que Microsoft maintient pour des raisons de rétrocomp
facto dans les engagements red team et les certifications offensives (OSCP, CRTP

Le principe fondamental de Responder repose sur un constat simple : lorsqu'un po
d'hôte via DNS, il se rabat sur des protocoles de résolution broadcast ou multicast
et **mDNS** (port UDP 5353). Ces protocoles, par conception, font confiance à n'imp
Responder se positionne comme un serveur rogue qui répond à toutes ces requêt
services factices.

Concrètement, Responder embarque un ensemble complet de serveurs factices :

- **Serveur SMB** — capture les authentifications NTLM lors de tentatives de conne
- **Serveur HTTP/HTTPS** — intercepte les requêtes web et force l'authentification
- **Serveur WPAD** — distribue un fichier PAC malveillant pour rediriger le trafic pro
- **Serveur LDAP** — capture les identifiants lors de requêtes d'annuaire
- **Serveur FTP** — intercepte les connexions FTP en clair
- **Serveur SQL** — capture les authentifications Microsoft SQL Server
- **Serveur DNS** — répond sélectivement aux requêtes DNS
- **Serveurs IMAP/POP3/SMTP** — capture les identifiants de messagerie