Glossaire – Concepts Clés de l'Attaque Responder (NTLM via HTTP)

NTLM (NT LAN Manager)

NTLM est un ancien protocole d'authentification de Microsoft utilisé pour vérifier l'identité d'un utilisateur sur un réseau Windows, sans transmettre son mot de passe en clair. Il repose sur un challenge/réponse cryptographique basé sur un hash du mot de passe.

Pourquoi c'est important :
NTLM est vulnérable à plusieurs attaques comme Pass-the-Hash, Relay Attack et la capture de hash, ce qui en fait une cible fréquente pour les outils comme Responder.

UNC (Universal Naming Convention)

UNC est une norme Windows utilisée pour accéder à des ressources réseau à distance, comme des dossiers ou imprimantes partagées. Elle suit le format \\NomMachine\Partage.

Exemple : \\192.168.1.100\documents

Pourquoi c'est important :
Un lien UNC malveillant peut déclencher une tentative d'authentification automatique NTLM vers l'IP de l'attaquant, permettant de capturer les identifiants de l'utilisateur.

Responder

Responder est un outil d'attaque en post-exploitation qui usurpe des services réseau comme LLMNR, NBNS, et WPAD pour capturer des identifiants (NTLM) envoyés par des machines Windows sur le réseau local.

Fonction principale :
Il intercepte les requêtes de résolution de nom de machine et répond avec sa propre IP pour piéger les postes clients et récupérer les hash NTLM.

Hash (Empreinte cryptographique)

Un hash est une empreinte numérique fixe générée à partir d'un mot de passe ou d'un autre contenu via un algorithme (comme MD4, SHA-1, etc.). Dans NTLM, le mot de passe de l'utilisateur est transformé en hash, qui est ensuite utilisé pour s'authentifier.

Pourquoi c'est important :
Même sans connaître le mot de passe original, un attaquant peut capturer le hash NTLM et tenter de le cracker (bruteforce, dictionnaire) ou de le relayer dans une autre session d'authentification.

LLMNR (Link-Local Multicast Name Resolution)

LLMNR est un protocole utilisé par Windows pour résoudre des noms d'hôtes en l'absence d'un DNS, en envoyant une requête sur le réseau local.

Problème :
Un attaquant peut répondre à ces requêtes, se faisant passer pour une autre machine et ainsi piéger l'utilisateur.

NBNS (NetBIOS Name Service)

NBNS est une ancienne méthode de résolution de noms sur les réseaux Windows, qui fonctionne comme LLMNR mais via le protocole NetBIOS.

Problème :
Tout comme LLMNR, NBNS peut être usurpé par un attaquant via des outils comme Responder, pour intercepter des connexions et capturer des identifiants.