

Identification des services en écoute

- Services en écoute caractéristiques des machines Windows
 - Portmapper MS-RPC - 135/TCP
 - Service Location : Service permettant la réalisation des appels de procédures distantes
 - Service de noms NETBIOS – 137/UDP
 - NetBios Name Service : Utilisé pour enregistrer les noms NetBios dans la base Wins.
 - Service de transport NETBIOS sur UDP - 138/UDP
 - NetBios Datagram Service : Utilisé par le service explorateur réseau (SMB browser service)
 - Service de transport NETBIOS sur TCP - 139/TCP
 - NetBios Session Service : Utilisé pour accéder aux ressources réseaux (partages de fichiers et d'imprimantes)
 - Service SMB/CIFS – 445/TCP
 - Microsoft DS : Protocole SMB (Server Message Block) est utilisé entre autres pour le partage de fichiers dans Windows. Détaché de NetBios depuis Windows 2K/XP.
 - Service Terminal Server – 3389/TCP

Identification des services en écoute

- Services classiques hébergés par des serveurs Windows
 - Serveur WINS – 42/TCP
 - Serveur DNS – 53/UDP
 - Serveur HTTP – 80/TCP et/ou 81/TCP
 - Serveur HTTPS – 443/TCP
 - Mandataire HTTP – 8080/TCP
 - KDC Kerberos – 88/UDP
 - Serveur LDAP – 389/TCP (et LDAPSSL – 636/TCP)
 - Serveur RDP – 3389/TCP
 - Serveur VNC – 5900/TCP
- 88/UDP et 389/TCP == AD DS (contrôleur de domaine)