

Exploitation

Ecoute du trafic sur un réseau local

Attaque de type « Man In The Middle »

- Prérequis
 - Corrompre le cache ARP d'une ou plusieurs machines
 - Activer le « forwarding » :
 - Linux : `%echo 1 > /proc/sys/net/ipv4/ip_forward`
 - Windows :
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters, clé « IPEnableRouter », valeur = 1

Exploitation

Ecoute du trafic sur un réseau local

Attaque par ARP Poisoning : MITM

IP A / MAC A parle avec IP Routeur / MAC Routeur

Cache ARP
IP Routeur / MAC Routeur



Host A

Cache ARP
IP A / MAC A



Routeur

Switch ou répartiteur



Pirate

