DNS SPOOF

Installer le paquet dsniff

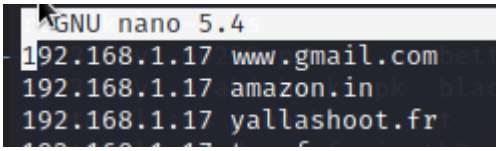
Ensuite lancer une attaque arp d'abord pour ce faire passer par le serveur DNS

Arpspoof <ipserveurDNS>

Une fois la table ARP infecter on passe au DNS

L'ip de mon kali est 192.168.1.17

Après créer un fichier hosts.txt ou il y'aura le mappage entre le FQDN et notre IP

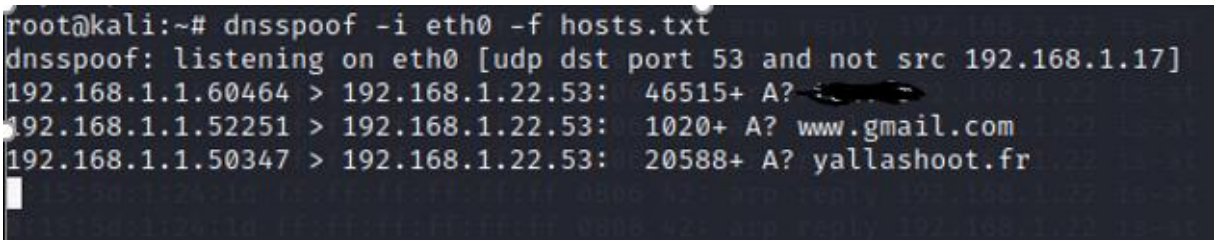


#Pour les sites en https il faut configurer son serveur web en https

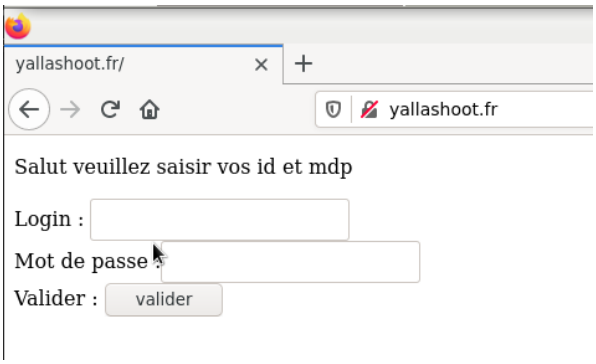
Ensuite lancer cette commande

Dnsspoof -i eth0 -f hosts.txt

Ensuite toute les trames vers le serveur DNS arriveront chez nous donc notre machine attaquante renverra des réponses DNS en ce faisant passer par le serveur DNS si j'essaye d'accéder sur le site toz.fr ou yallashoot il y'aura cela qui apparaitra dans le terminal d'abord



Je vais aller sur le site yallashoot.fr depuis une machine cliente



Voilà on voit bien que c'est rediriger vers le serveur web de la machine kali attaquante

Le Dns de pihole n'est pas vulnérable car il utilise le DNSSEC plusieurs fois j'ai essayer avec sa ne fonctionne pas