Nmap buzut.fr

Généralités

Nmap doit être lancé en root
- O --> Détection de l'OS
- v --> verbose

Découverte des hôtes

-PB --> scan par défaut. Utilise à la fois les paquets ACK et ICMP
-sL --> liste les cibles (list scan)
-sP --> détermine si les hôtes sont en ligne (ping scan)
-PO --> tente le scan sans ping préalable
-PT --> ping TCP
-PU --> ping UDP
-PI --> ping ICMP
-Pn --> considère tous les hôtes comme en ligne

Techniques de scan

-sV --> test les ports ouvert pour déterminer le service en écoute
-sS --> Syn scan(génère un paquet syn, si le client répond par Syn-ACK, renvoi un RST)

Scans furtifs sF | sX | sN :

Plus difficilement détectable que le Syn scan, ces types de scan auront de moins bons résultats. Les ports fermés doivent répondrent RST alors que ceux ouverts ne doivent pas répondre.

-sF --> Fin scan (paquet avec le flag SYN - ne complète pas le handshake TCP)
-sX --> Xmas scan (combinaison flags FIN, URG et PUSH)
-sN --> Null scan (paquet sans aucun flag)

Leurres

-f --> Fragmente les paquets
-D --> obscurcis le scan avec des leurres – <decoy1 [,decoy2][,ME],...>
ex : nmap 192.168.0.* -D 192.168.9.23, 192.168.9.26, ME, 192.168.9.03
-S --> usurpe l'adresse source (à utiliser avec -e pour spécifier l'interface et -PN –
ex : sudo nmap 192.168.0.* -S 192.168.0.4 -e eth0 -PN