NMAP **Park33r**

ESCANEO SOLO IP

comando	descripcion del analisis
-sn	hacer ping

ESCANEO DE PUERTOS

-sS ----------	TCP SYN (sigiloso)
-sT ----------	TCP Conect
-sY ----------	SCTP INIT
-sZ ----------	COOKIE ECHO de SCTP
-sW ----------	VENTANA TCP
-sF o -sX ----------	NULL,FIN,XMAS
-sA ----------	TCP ACX
-sU ----------	DUPD
-sO ----------	PROTOCOLO IP

*** Las opciones mas usadas comunmente son -sT -sS**

ESPECIFICAR PUERTOS Y OBJETIVOS

-p ----------	Agregamos los puertos 22,33 o 22-50000 (rango)
-p- ----------	Todos los puertos
-F ----------	Escaneo rapido de los 100 mas comunes

DESCUBRIMIENTO DE SISTEMAS

-Pn ----------	no hacer PING
-n ----------	no hacer resoluciones DNS
-sV ----------	Version de los sistemas
-O ----------	version sistema operativo

SCRIPTS LUA

Podemos ver los script en

-sC ----------	usar una serie de script ya cargados por defecto

--script <nombre script>

algunos script necesitaran que le pasemos argumentos

SALIDA

-oG <nombre>----------	formato grepeable
-oN <nombre>----------	formato nmap
-oX <nombre>----------	formato xml
-oA <nombre>----------	todos los formatos