TALLER DE SCANNING

CURSO FASES DE UN ATAQUE.

NIVEL BASICO

Partiendo de que estamos ya con la poca o mucha información de nuestro objetivo realizaremos los procesos de scaneo y de enumeración para lograr obtener la mayor cantidad de datos efectivos del objetivo y así después llegar a realizar el acceso y seguir adelante con las fases finales logrando lo pensado.

ESCANEO BASICO

Haremos un scaneo TCP tipos conect() que es un básico no muy discreto ya que se logra con este una conexión efectiva con el objetivo, lo realizaremos para determinar los puertos abiertos del objetivo y los servicios que corren en este:

1. Nmap -sT 186.83.62.101 (Esta es la ip de nuestro Windows server 2003 en el taller)
2. Luego haremos un barrido en la red para conocer que otras máquinas tenemos al alcance, también con nmap nuestra tool del momento.

   Nmap –sP 186.83.62.0/25 Teniendo en cuenta que la red es de tipo B tomaremos un bit más de la máscara para ver que maquinas tenemos en la red activas y en escucha con sus puertos.

3. Ahora que hemos determinado nuestro objetivo necesitamos conocer que sistema operativo tiene para poder llegar al servidor y no de pronto a un cliente por que el objetivo es la información del sistema central. Nmap nos continua ayudando en este trabajo así:

   Nmap –O 186.83.62.101 este sería otro sacn a nivel de tcp.

4. Además de conocer a nivel de TCP que puertos están en escucha, recordemos que también podremos realizar ataque de tipo DoS sobre la capa de transporte en el protocolo UDP, para esto debemos conocer que puertos están a la escucha en el objetivo, así:

   Nmap –sU 186.83.62.101

5. Si ya contamos con los puertos, las direcciones MAC, los servicios, el sistema operativo que funciona y sus datos, otro aspecto importante es las versiones de los servicios, con estas podremos determinar más adelante que posibles exploit o tolos tendremos que usar y que tipo de técnica de penetración usar para lograr al momento del acceso estar dentro de la maquina objetivo. Seguimos usando nmap para nuestras tareas.

Nmap –sV 186.83.62.101 aca nos permitirá verificar servicios y sus versiones. Con base en esta info las vulnerabilidades del objetivo saltan a la vista.

SALUDOS…. BUEN FIN DE SEMANA