TALLER DE ENUMERACION

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.

A partir del scanning realizado anteriormente a nuestra maquina Windows 2000 ya tenemos una buena cantidad de información, para lo cual la siguiente fase es probar e investigar un poco más, haremos ENUMERACION o verificación de los servicios y puertos tratando de sacar info de ellos, esto es lo que conocemos con enumeración del objetivo. Para lo cual tendremos que manejar herramientas lo menos intrusivas posibles como tolos Shell de comandos y algunas no instalables o de versiones portables.

Uno de los aspectos importante ahora es determinar y probar que el dominio o la maquina esta activa y respondiendo no solo a nivel de TCP sino de todo el proceso de red a otras acciones de contacto con ella, y para esto NSLOOKUP nos puede ayudar bastante.

Con este comando conoceremos la resolución de nombres y la actividad del equipo en la red.

Nslookup 186.83.62.101 dando la ip del objetivo nos puede resolver el nombre del pc y luego lo verificaremos con una tool grafica o portable.

Una de las formas de acceso o de contacto para determinar si los puertos que trabajan bajo el protocolo SMB como son 139 y 445 están bajo posibilidad de penetración es hacer una SESION NULA, o sea aprovecharnos de una falencia como estas para lograr ingresar más adelante al objetivo con un usuario genérico y una contraseña nula, para esto lo haremos con los comandos NET USE del sistema operativo de manera nativa.

Net use \\186.83.62.101\IPC$ “”/U:”” de esta forma si el resultado no es error sino un contacto efectivo debemos ya saber que será este uno de los puntos de acceso posibles sin antes no verificar que por ahí existan posibles trampas para nosotros como un HONEYPOT que nos rastree o un IDS que nos deje en evidencia.

También es parte del trabajo de la enumeración si la sesión nula es activa determinar hasta donde podemos sacar información de los usuarios del sistema ya que por medio de ellos es que lograremos finalmente ingresar al sistema, no hay otra forma de dentro del sistema tener un control de la maquina objetivo mas adelante. Asi que lo haremos con la herramienta USERDUMP, de la siguiente manera.

Userdump \\186.83.62.101 (nombre de usuario)

Userdump \\186.83.62.101 administrator

O si tenemos posibles nombres ya verificados de otros usuarios probar con ellos también.

Normalmente el ID del usuario administrador o sus similares con privilegios es 500, acá están nuestros objetivos para lograr saber sus claves y permisos dentro del sistema.

Si logramos tener info del ID de los usuarios deberemos sacar ya la info del usuario como tal y para esto tenemos que manejar USERINFO.

Userinfo \\186.83.62.1 administrator

También este dato lo podemos averiguar con la tool DUMPSEC, seria instalarla y activar su scaneo.

Para ya dejar como ultima info por probar dentro de nuestro procedimiento esta determinar l info relevante del usuario o usuarios del sistema, lo podemos hacer con:

sid2user \\186.83.62.101 SID RID

Si es un dominio tambien conocer info de este con:

Net view /Dominio:nombre del dominio

Net view /ipobjetivo

Este procesos con todas las herramientas nos han dejado si hacemos el recuento varia info relevante que vamos a completar con la búsqueda de posibles vulnerabilidades sobre esta información del sistema, lo haremos de varias formas una que s la mas recomendada por mi para empezar es buscar en la web; www.milw0rm.com información sobre exploit o vulnerabilidades que podamos tener para usarlas, o en sesiones como metasploit para buscar herramientas que nos permitan usarlas en pro de determinar si hay acceso al objetivo.

SALUDOS…. BUEN FIN DE SEMANA