HERRAMIENTAS DE EXPLOTACIÓN WINDOWS

Jordi Masó Pla

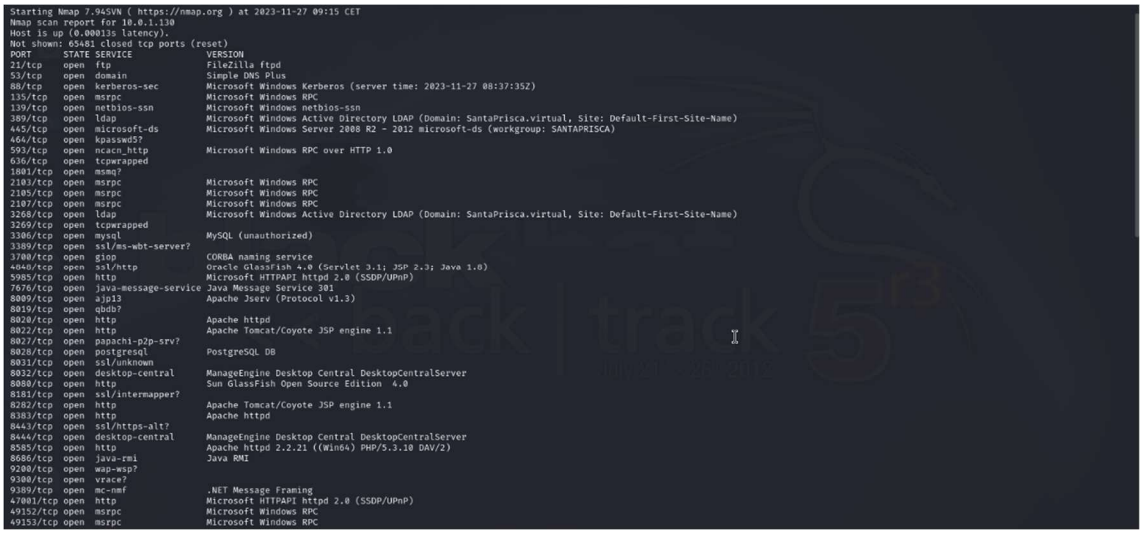
INDICE

1. DESCUBRIMIENTO

En este ejercicio realizaremos ataque manual a una máquina de laboratorio de Windows server 2012 R2. Con las técnicas manuales intentaremos conseguir las credenciales y acceso al sistema.

1.1 NMAP

Empezamos con la herramienta nmap para saber qué servicios están corriendo en esta máquina, realizamos un escaneo de los puertos tcp activos y encontramos una gran variedad de puertos abiertos tal como puerto 21 ftp, puerto 53 dns, puerto 88 Kerberos, puerto 135 nsrpc, puerto 389 ldap, puerto 445 smb, puerto 3306 MySQL, puerto 8020 Apache httpd, puerto 8585 WordPress.



El siguiente paso es realizar un escáner de los puertos udp por si hay algún servicio interesante corriendo, con en el puerto 161 snmp, que podemos obtener algo de información.

1.2. NMBLOOKUP, NSLOOKUP

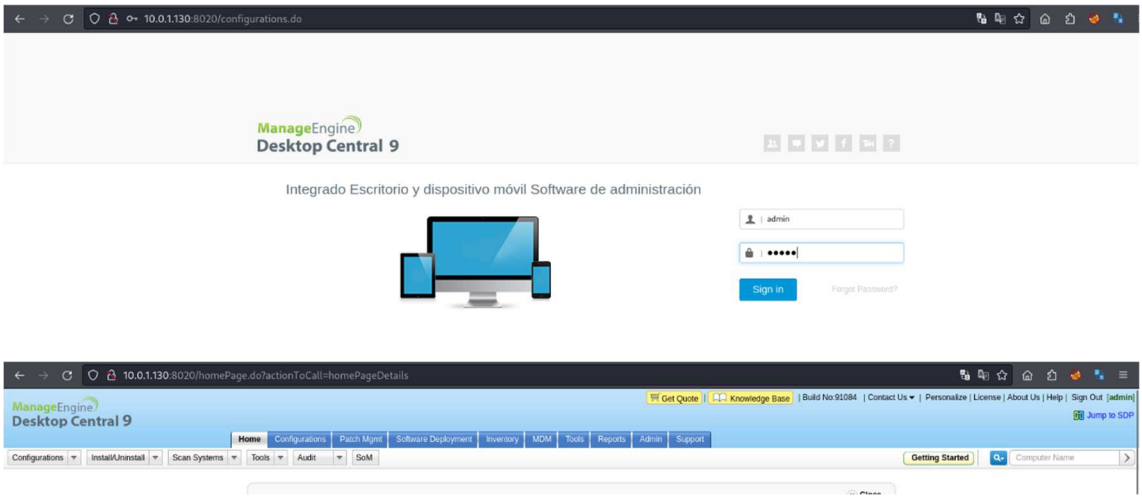
Con la herramienta nmblookup haciendo peticiones al puerto 53 del dns, podemos encontrar información del nombre de la maquina y su dominio, que en nuestro caso el nombre de la maquina es Enigma y el dominio es SANTAPRICA.VIRTUAL. Con el comando nslookup haciendo peticiones al mismo servicio nos dan el mismo resultado que nmblookup.

1.3 SNMP

Con el servicio snmp del puerto 161 que este operativo en este host y con el comando snmp-check nos muestra un resultado muy interesante como información del sistema operativo y los nombres de los usuarios de las cuentas de esta máquina.

2 ESPLOTACION DE LOS SERVICIOS

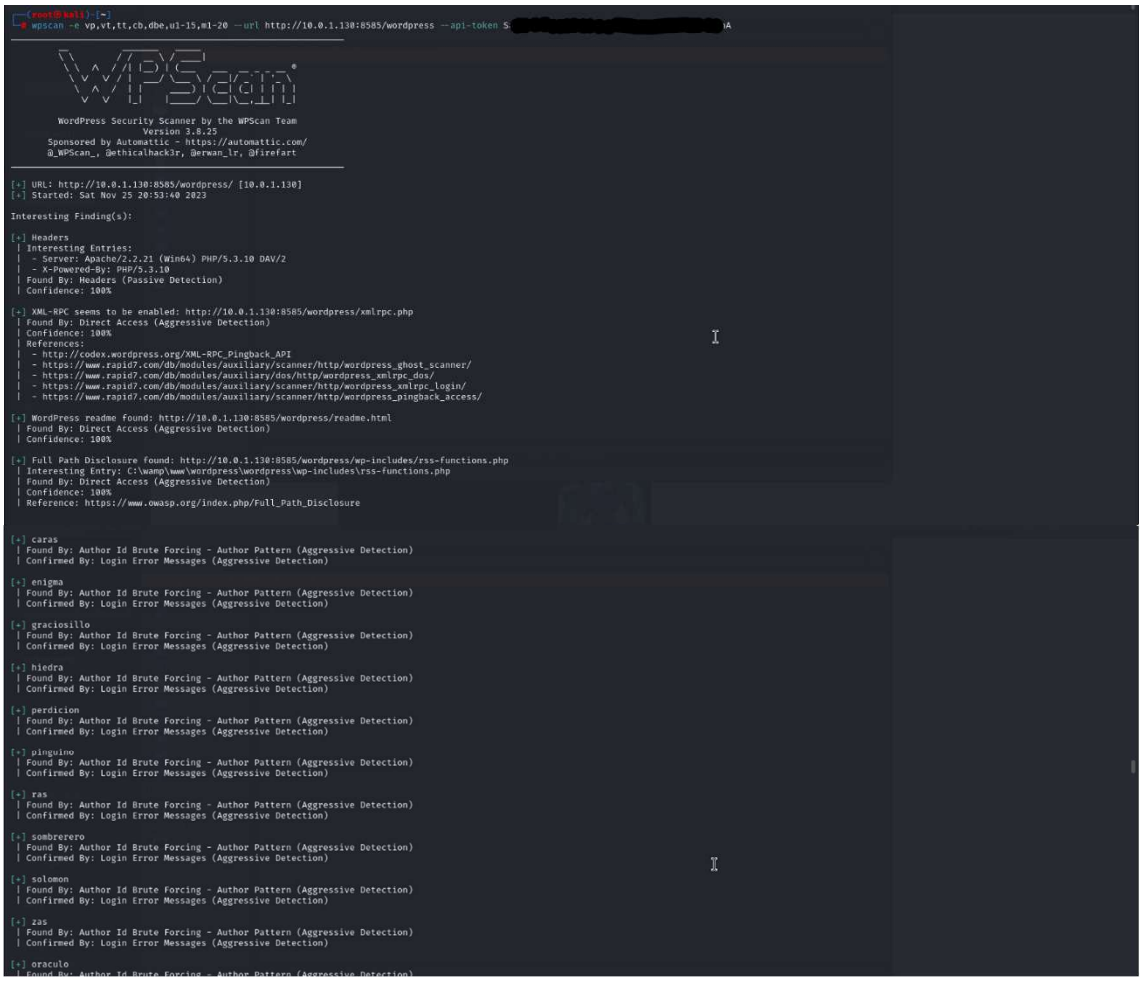
Desde el navegador y accediendo a la ip de nuestro objetivo con el puerto 8020, donde nos conectamos al ManageEngine Desktop y un login que con las credenciales “admi” password “admin” accedemos al servicio como administrador.



2.1 WPSCAN

En la fase de descubrimiento emos detectado un WordPress y con la herramienta wpscan vamos ha intentar explotar este servicio para conseguir una vulnerabilidad o credenciales validas para seguir utilizando en otros servicios del sistema.

Al lanzar los comandos de wpscan nos muestra al instante varias vulnerabilidades que se pueden exportar con Mestasploit Framework, y otras herramientas de automatización de explotación. En otro pate nos muestra los usuarios registrados en este host.

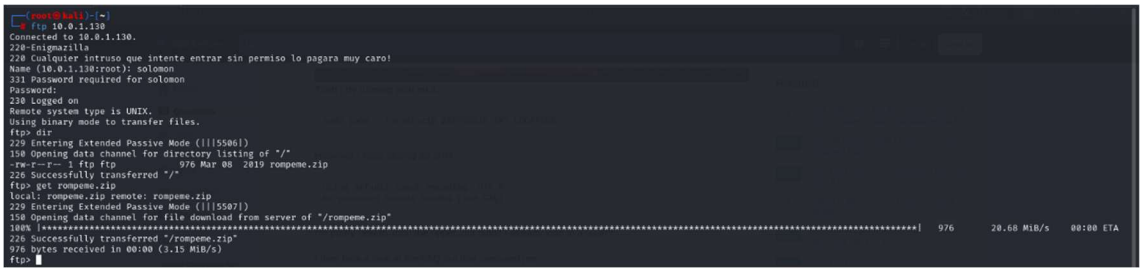


Al tener lo usuarios pasamos un ataque de diccionario para conseguir una credencial validad para poder explotar otros servicios. Con la herramienta wpscan y el servicio rpc realizamos el ataque de password con los usuarios encontrados y un diccionario pequeño de Metasploti.

El resultado del ataque de diccionario con los usuarios nos muestra un resultado de usuario Solomon password 12345678. Con estas credenciales podemos empezar a explotar otros servicios.

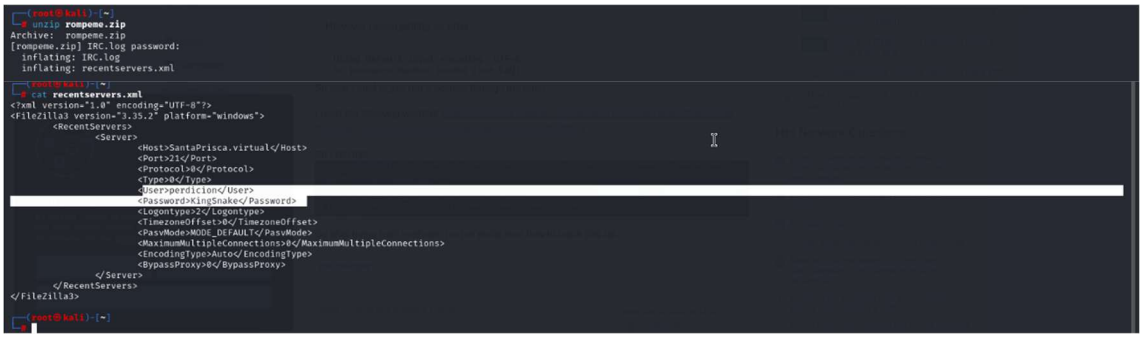
2.2 FTP

Con las credenciales obtenidas con wpscan las comprobamos con el servicio ftp. Las credenciales son válidas con el servicio, dentro de este usuario hay un fichero comprimido en zip llamado rómpeme.zip, que procedemos a descargarlo para comprobar la información que hay dentro.



El fichero está cifrado con contraseña, pero con la herramienta zip2john podemos extraer el hash, con este hash utilizamos John the Ripper con un diccionario para romper el hash del fichero. Una vez pasado John con el diccionario vemos que a obtenido la contraseña del fichero para poder extraer el contenido del, la contraseña es “simpleplan”.

Procedemos a extraer el contenido del fichero y dentro hay dos ficheros mas uno es IRC.log y el otros recentservers.xml. al abrir el fichero recentservers.xml dentro hay un usuario y una contraseña nueva, usuario “perdicion” password “KingSnake”.



2.3 SMB

Comprobamos si las credenciales obtenidas hasta ahora son validas en el servicio smb, con las credenciales de solomon podemos acceder a toda la unidad del sistema operativo poniendo en grabes problemas el sistema operativo y su información.

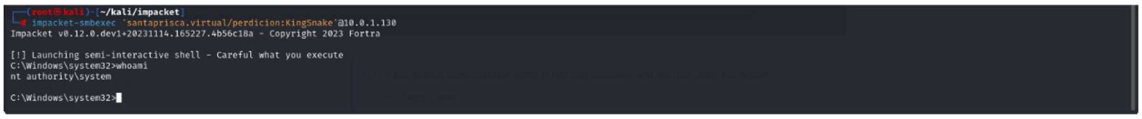
2.4 ENUM4LINUX

Probamos la herramienta enum4linux con el usuario perdicion y el password KingSnake, y el resultado que nos muestra es principalmente el mismo que ja teníamos, con otras herramientas, pero hay una parte que muestra las políticas de las contraseñas. Las características principales son: no tienen mínimo de caracteres, no caducan, no tienen complejidad y no hace falta cambiarlas con el paso del tiempo.

También muestra los usuarios registrados en esta máquina como anteriormente emo vistos.

2.5 IMPACKET

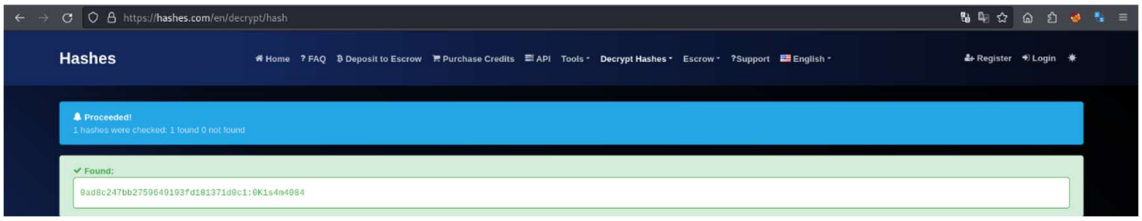
La herramienta impacket y el módulo smbexec y las credenciales de perdicion observamos que podemos acceder al sistema con unos privilegios muy altos de “authority\system”, con estos privilegios podemos navegar por todo el sistema operativo.



2.6 CRACKMAPEXEC

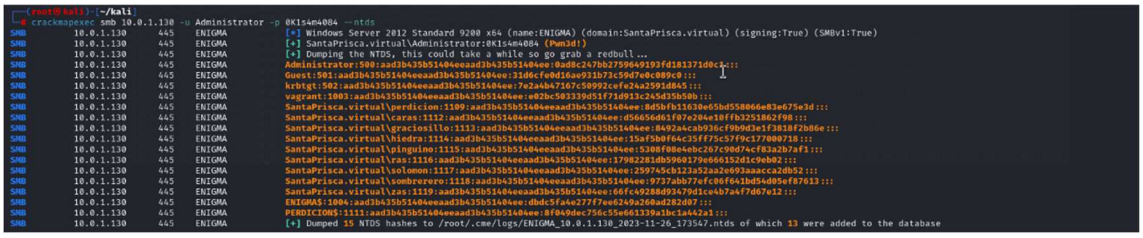
Crackmapexec es una herramienta multifuncional donde podemos explorar multitud de vectores de ataque a una máquina, en este caso utilizaremos el protocolo smb y las credenciales del usuario perdicion. Unas de las primeras intervenciones es intentar que nos muestre el fichero SAM del host para conseguir todas las credenciales posibles. En este primer intento nos muestra dos credenciales el de “Administrator” y una cuenta de “Guest”.

Con hash del administrator lo pasamos por la web hashes.com para ver si lo puede romper y obtener unas credenciales en texto plano, el resultado ha sido afirmativo y las credenciales son “0K1s4m4084” esta el password del usuario Administator.



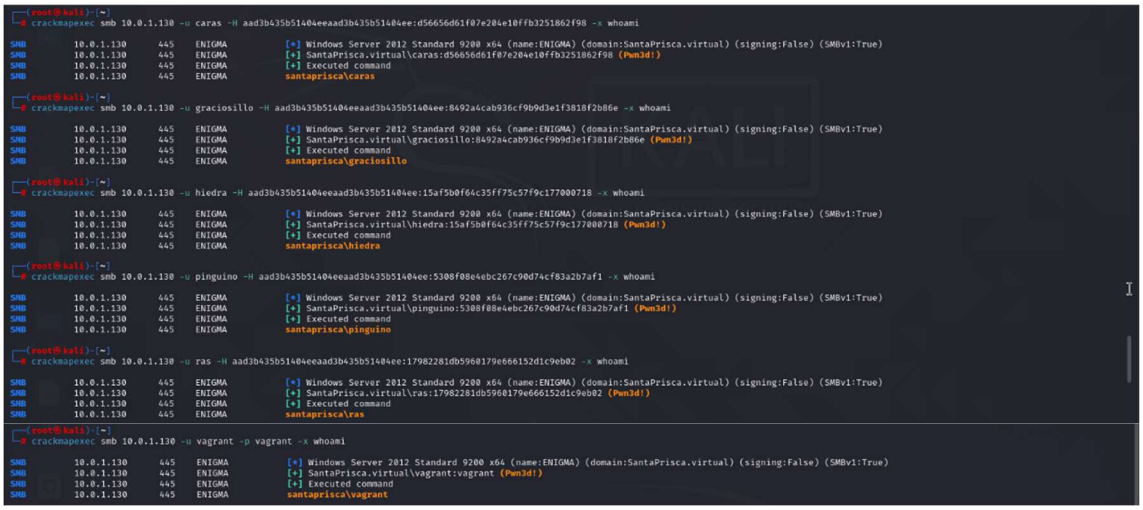
Con las credenciales del Administator vamos a comprobar las demás credenciales de los usuarios registrados en este host. Las primeras credenciales que nos muestra son la ya mencionada anteriormente de Administrator, Solomon y una nueva que es usuario “vagrant” password “vagrant”.

Con otro comando de crackmapexec del módulo de smb y las credenciales del Aministrator y su password con el argumento --ntds. Con ese comando nos devuelve los nombres de usuario y sus hashes respectivos.



2.6.1 VERIFICACION DE LOS USUARIOS

Procedemos a verificar los usuarios encontrados con sus hashes con la propia herramienta crackmapexec. Todos los usuarios y los hashes son válidos para acceder al host.



2.7 REVERSE SHELL CON METERPRETER

En esta ocasión realizaremos un Shell reverse con meterpreter y crackmapexec, la Shell se realizará con exploit de Metasploit Framework y la introduciremos a la maquina victima con crackmapexec. Abrimos Metasploit Framework buscamos el exploit multi/script/web_delivery, que es el que utilizaremos para crear la sesión de meterpreter seleccionamos el Payload Windows/x64/meterpreter/reverse_tcp y la opción de target seleccionamos Regsvr32, completamos los campos necesarios de la parte del exploit como del payload.

Lanzamos el exploit una vez todo configurado y nos aparecerá un comando para poder ejecutar en consola. Este comando lo utilizamos con la herramienta crackmapexec para cargar este exploit.

Al lanzar el comando con crackmapexec se nos abres el interprete de meterpreter como authority\system, con privilegios muy elevados, con meterpreter también podemos acceder a las cuentas de usuarios y sus hashes con el comando hashdump.