iGNITE Technologies

CREDENTIAL DUMPING

INTERNAL MONOLOGUE

WWW.HACKINGARTICLES.IN

Contenido

Introducción

Mientras se realizan operaciones del Equipo Rojo, es posible encontrarse con un escenario en el que el atacante no puede utilizar Mimikatz. Esto podría deberse a que casi todos los programas antivirus o de malware detectarán la presencia de Mimikatz tan pronto como llegue a la máquina de destino. Este es el escenario en el que un atacante puede realizar un ataque de monólogo interno. Para realizar este ataque, se requirió una herramienta desarrollada por Elad Shamir de Missing Link Security.

Al estar en contacto con el Mecanismo de seguridad de Windows, estará familiarizado con NetNTLM. Es un protocolo basado en respuesta a desafíos que se utiliza donde Windows no puede aplicar la autenticación basada en Kerberos. En este método, el servidor envía un desafío de 8 bytes con el hash NTLM como clave al usuario. El hash es un hash MD4 de la contraseña del usuario. Hay dos versiones de NetNTLM. Ambos son vulnerables. La versión 1 de NetNTLM se introdujo hace bastante tiempo y actualmente está deshabilitada de forma predeterminada.

En un sentido general, el ataque de degradación se realizó contra el propio Mimikatz. Después de la explotación de la máquina objetivo, el atacante, ya sea usando Mimikatz o manualmente, puede editar claves de registro como LMCompatibilityLevel con valores como 0,1,2 que pueden hacer que el dispositivo comprometido use la versión anterior o degradada de NTLM para interactuar. con otros servidores SMB y puede llevar a cambiar a otros usuarios y servidores.

Sin embargo, en este ataque que se describe en la demostración, no se utiliza Mimikatz y, en cambio, el atacante invoca una llamada a un procedimiento local desde una aplicación en modo de usuario al paquete de autenticación NTLM a través del SSPI. Esto calcula la respuesta NetNTLM que analizamos anteriormente en el contexto del usuario que inició sesión. El ataque inhabilita inherentemente los controles preventivos NetNTLMv1, luego extrae todos los tokens de inicio de sesión que no son de red de los procesos actualmente en ejecución y se hace pasar por los usuarios asociados. Para cada usuario suplantado, NTLM SSP invoca localmente una respuesta NTLMv1 al desafío elegido y luego restaura los valores originales de las claves de registro analizadas anteriormente. Ahora el hash capturado se puede descifrar con la herramienta de tu preferencia, como John the Ripper o Hash Cat.

GitHub: monólogo interno

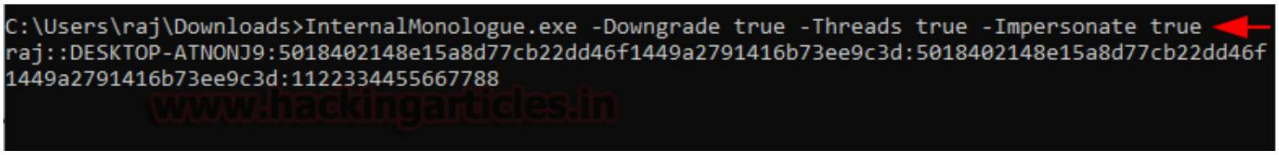
Explotación

Tiene la opción de compilar el ejecutable usted mismo obteniendo los binarios de GitHub. Sin embargo, para esta demostración, descargaremos el ejecutable.

Descargar InternalMonologue.exe

Después de descargar el ejecutable, supongamos que el atacante tiene el punto de apoyo inicial en la máquina objetivo.
Es necesario transferir el ejecutable a la máquina de destino y ejecutarlo con ciertos parámetros. El parámetro Degradar debe tener el valor "verdadero" para degradar la versión. Luego, el parámetro Threads también debe contener el valor verdadero y, finalmente, para realizar la suplantación, el valor del parámetro Impersonate también debe ser verdadero. Al ejecutar con éxito el ejecutable, el atacante puede extraer con éxito el hash v1 degradado del usuario objetivo, como se demostró.

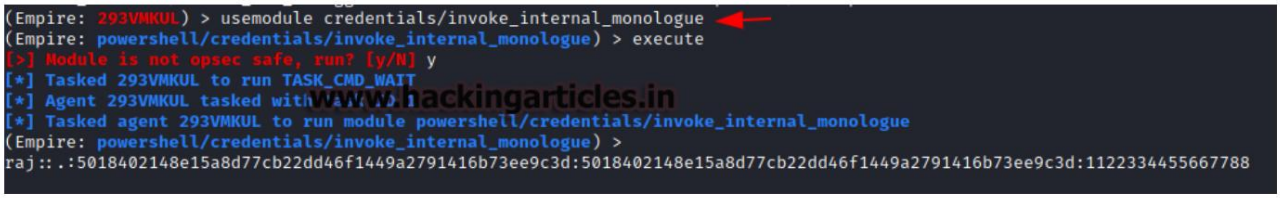
```
InternalMonologue.exe -Degradar verdadero -Subprocesos verdadero -Suplantar verdadero
```



Explotación del imperio PowerShell

Si el atacante decide comprometer la máquina objetivo a través de PowerShell Empire y tiene un agente activo, entonces puede realizar un ataque de degradación directamente desde PowerShell Empire. Dentro de las credenciales, PowerShell Empire tiene un módulo llamado invoke_internal_monologue que esencialmente realiza el mismo ataque que el ejecutable discutido anteriormente. Este método no implica transferir un ejecutable y ejecutarlo en la máquina de destino, lo que lo hace mucho más sigiloso.

usar credenciales del módulo/invoke_internal_monologue
ejecutar



Descifrado de hash

En ambas variantes de ataques que se realizaron anteriormente, se descubrió que el hash para el usuario raj era el mismo y ahora hay dos formas en las que se puede usar este hash. En primer lugar, el atacante puede utilizar directamente el hash para iniciar sesión realizando un Pass the Hash. Pero si el atacante quiere, puede descifrar el hash utilizando a John el Destripador. Almacene el hash extraído del usuario raj en un archivo en el escritorio de nuestro Kali Linux y asígnele un nombre hash.
Luego, utilizando John the Ripper para describir el formato como NetNTLM como se muestra a continuación, se puede observar que el hash se puede descifrar. Se descubrió que el hash era la contraseña "123".

john --format=netntlm hash --show

Conclusión

A veces, ideas tan simples como degradar la versión del mecanismo de autenticación pueden resultar peligrosas. Como este ataque no requiere ninguna herramienta que esté dirigida a varios mecanismos defensivos, puede pasar desapercibido y obtener esas credenciales. Esto es una prueba de que la seguridad está en constante evolución y que la única forma de adelantarse a un atacante es pensar como tal.

iGNITE Technologies

ÚNETE A NUESTRO PROGRAMAS DE ENTRENAMIENTO

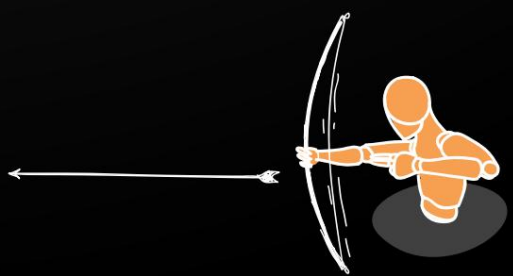
PRINCIPIANTE

- Hackeo ético
- Pentest de red
- Recompensa de errores
- Pentest inalámbrico
- Seguridad de la red Esenciales

AVANZADO

- Eructar Suite Pro
- Web Servicios-API
- Pro VAPT de infraestructura
- Computadora forense
- Pentest de Android
- Avanzado metasploit
- CTF

EXPERTO



- Operación del equipo rojo
  - APT's - Tácticas de ataque MITRE
  - Ataque de directorio activo
  - Evaluación de seguridad de MSSQL
- Escalada de privilegios
  - ventanas
  - linux

www.ignitetechnologies.in