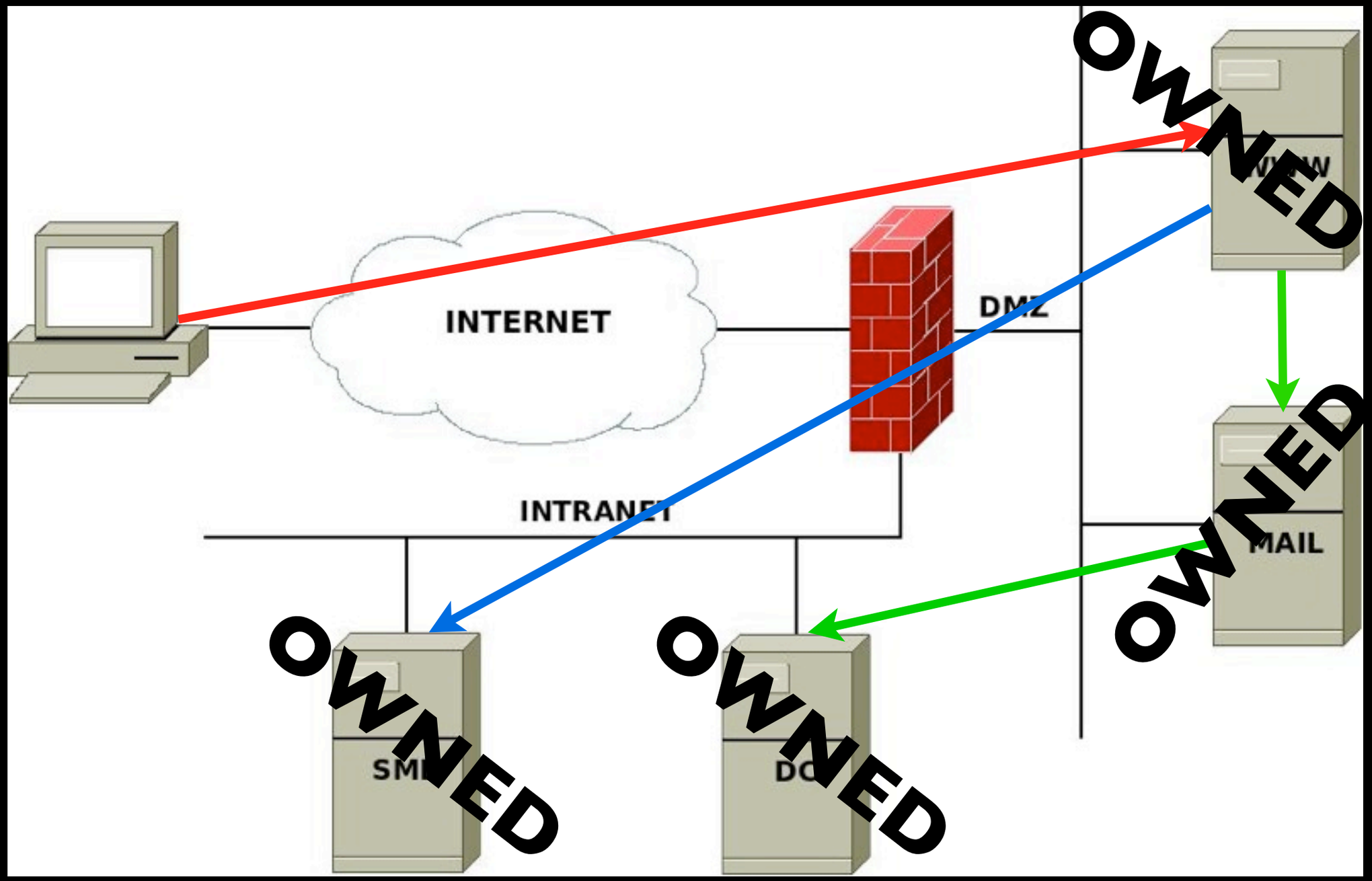
Windows Post-Explotation

How to using a Hash

¿Quién soy?

- Jose Selvi (jselvi@pentester.es)
- Hacking Ético & Pentesting
- Telefónica Ingeniería de Seguridad
- Pentester.es

Post-Explotation



Post-Explotation

- Usar la información obtenida y visibilidad
- Típico:
  - **Obtención de Hashes/ Contraseñas**
  - Pivoting de conexiones
- Generalmente muy poca protección

Windows Hashes

- Dos tipos: **LM** (LanMan) y NTLM
- LM muy antiguo (y debil...)
- Compatibilidad: LM persiste hasta Vista/ 2008

Administrador:
500:**7022b6466c68884f6905068007dd26fd**:
33fdfd9ebdfc4049b014d9ed957992c2:::

LANMAN Hash

Algoritmo:

1) Obtenemos la contraseña
2) Convertimos todos los caracteres a mayusculas
3) Completamos con espacios hasta llegar a 14 caracteres
4) Separamos en 2 partes de 7 caracteres
5) Le añadimos un byte de paridad para tener 2 partes de 8 bytes
6) Usamos cada una de las partes como clave de cifrado DES de un texto fijo (siempre idéntico)
7) Obtenemos 8 bytes de CipherText
8) Juntamos ambas partes para formar el Hash LANMAN (16 bytes)

LANMAN Hash

HiPoPoTaMo

↓

HIPOPOTAMO

↓

H	I	P	O	P	O	T	A	M	O	_	_	_	_

H	I	P	O	P	O	T	

↓

70	22	B6	46	6C	68	88	4F

A	M	O	_	_	_	_	

↓

69	05	06	80	07	DD	26	FD

↓

70	22	B6	46	6C	68	88	4F	69	05	06	80	07	DD	26	FD

Debilidades LM

- No existen minúsculas
  - Con mayusculas y números tenemos casi todas las contraseñas
    - Permutando Mays/Mins obtenemos la contraseña real
- Máximo 7 caracteres
  - Podemos crackear cada parte por separado
- El hash de 7 espacios es conocido
  - Podemos saber cuándo la contraseña es de menos de 7 caracteres


DEMO
Post-Explotation Crackeando Hashes

Windows Auth

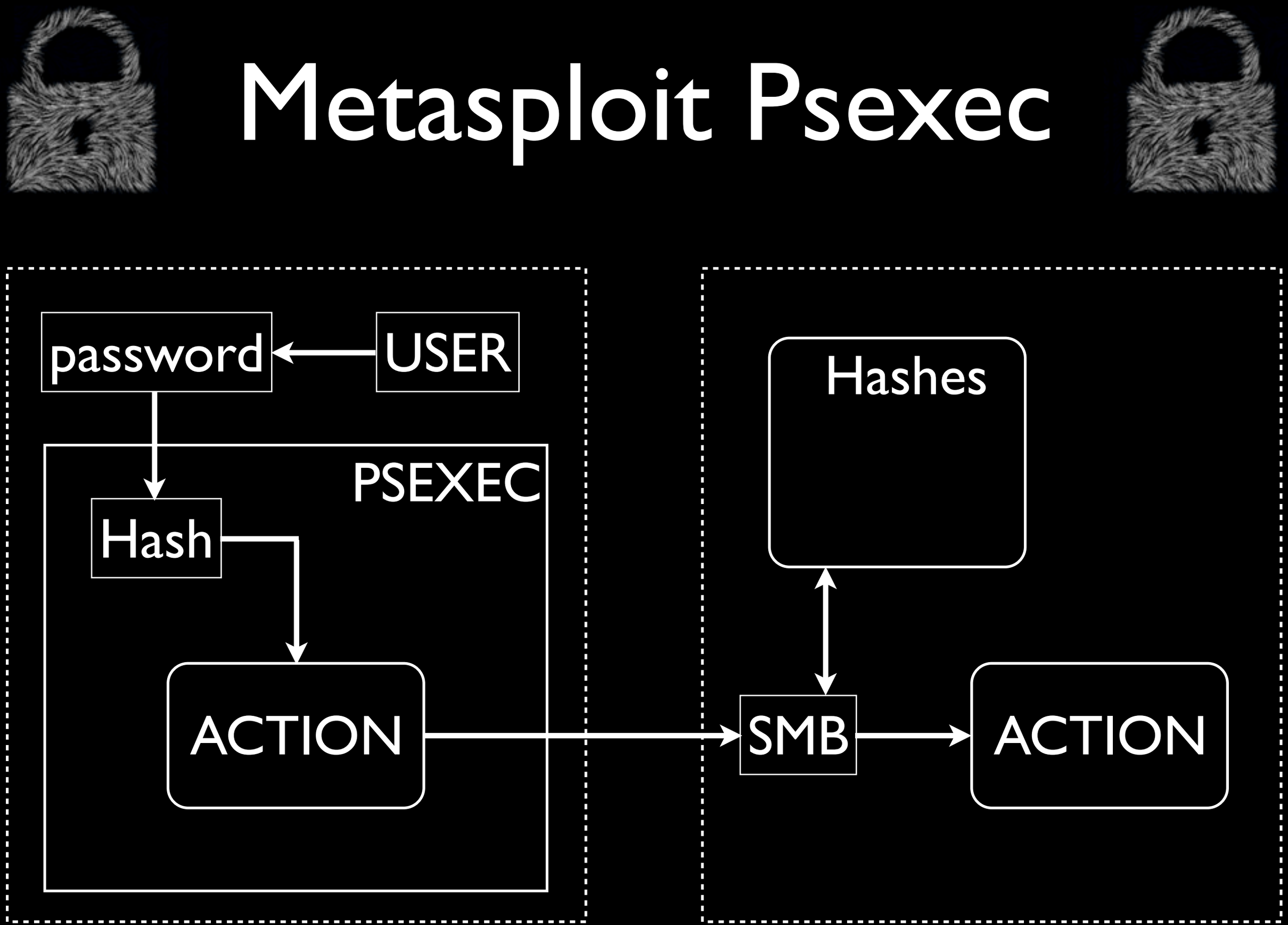
- “Single Sign-On” en Software Microsoft
- Login guarda en memoria los hashes
- Usa luego en Hash para autenticar

- Hashes locales en SAM
- Hashes de dominio se cachean

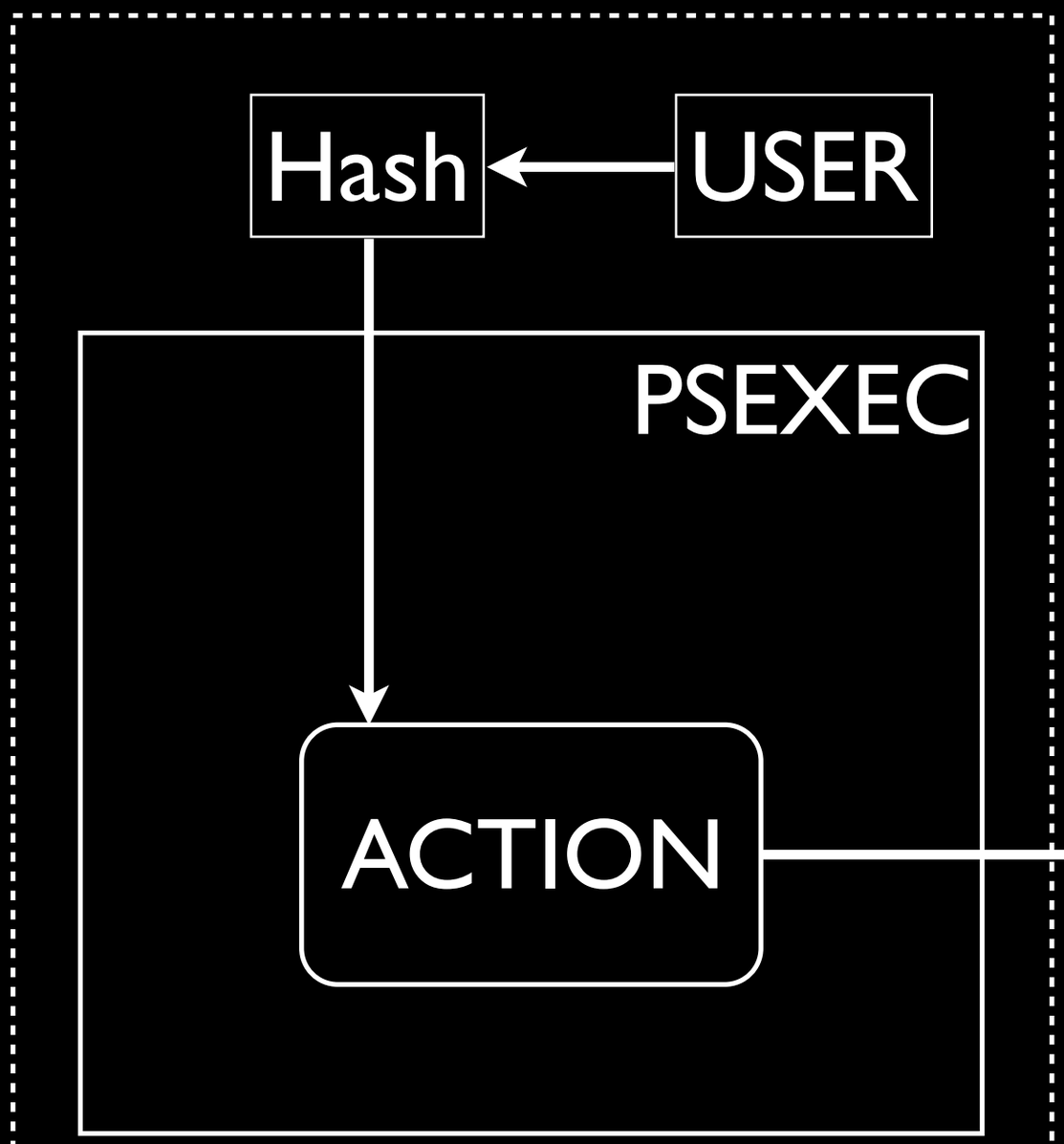
Pass-the-Hash

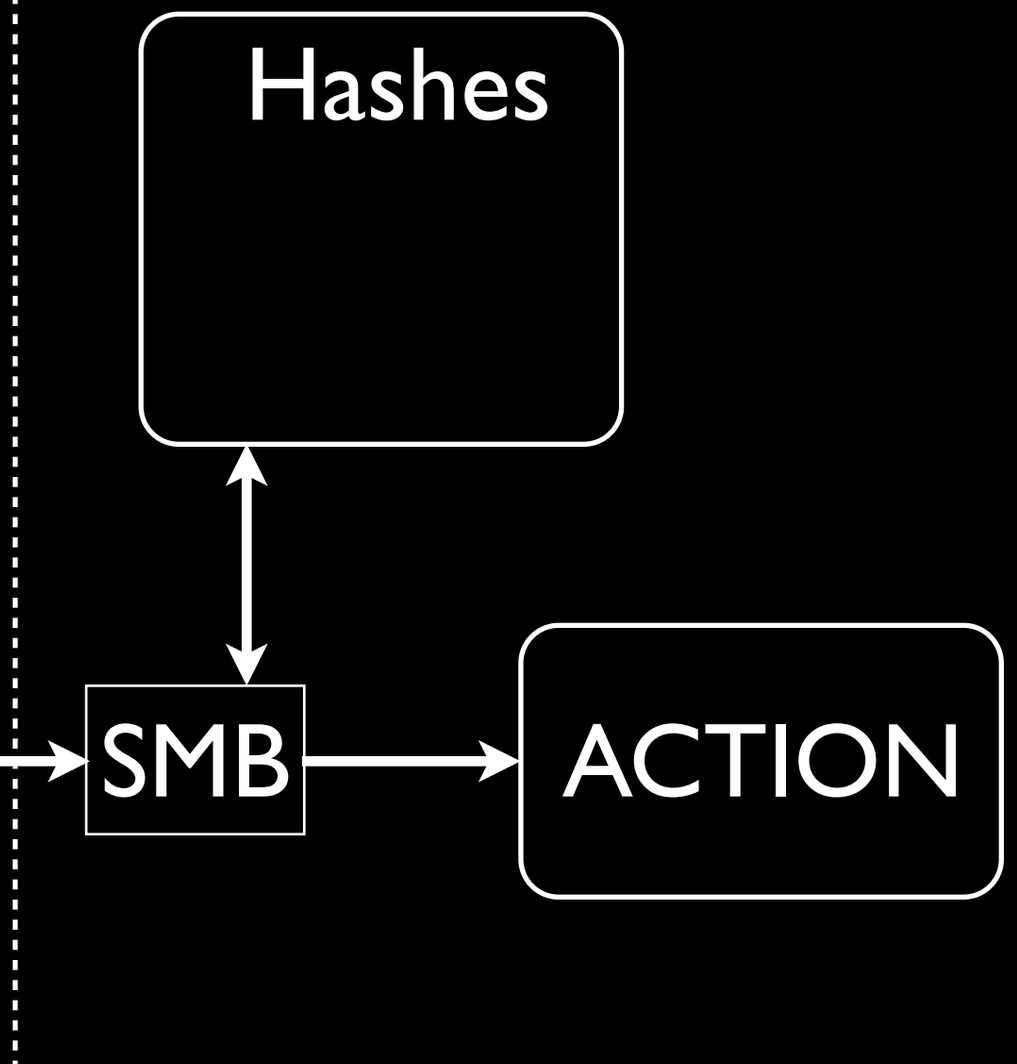
- Nos saltamos el paso de calcular el Hash
- Software:
  - Parches Samba
  - **Metasploit Framework Psexec**
  - **Pass-the-Hash Toolkit** (Hernán Ochoa)
- No importa la fortaleza de la contraseña

Metasploit Psexec

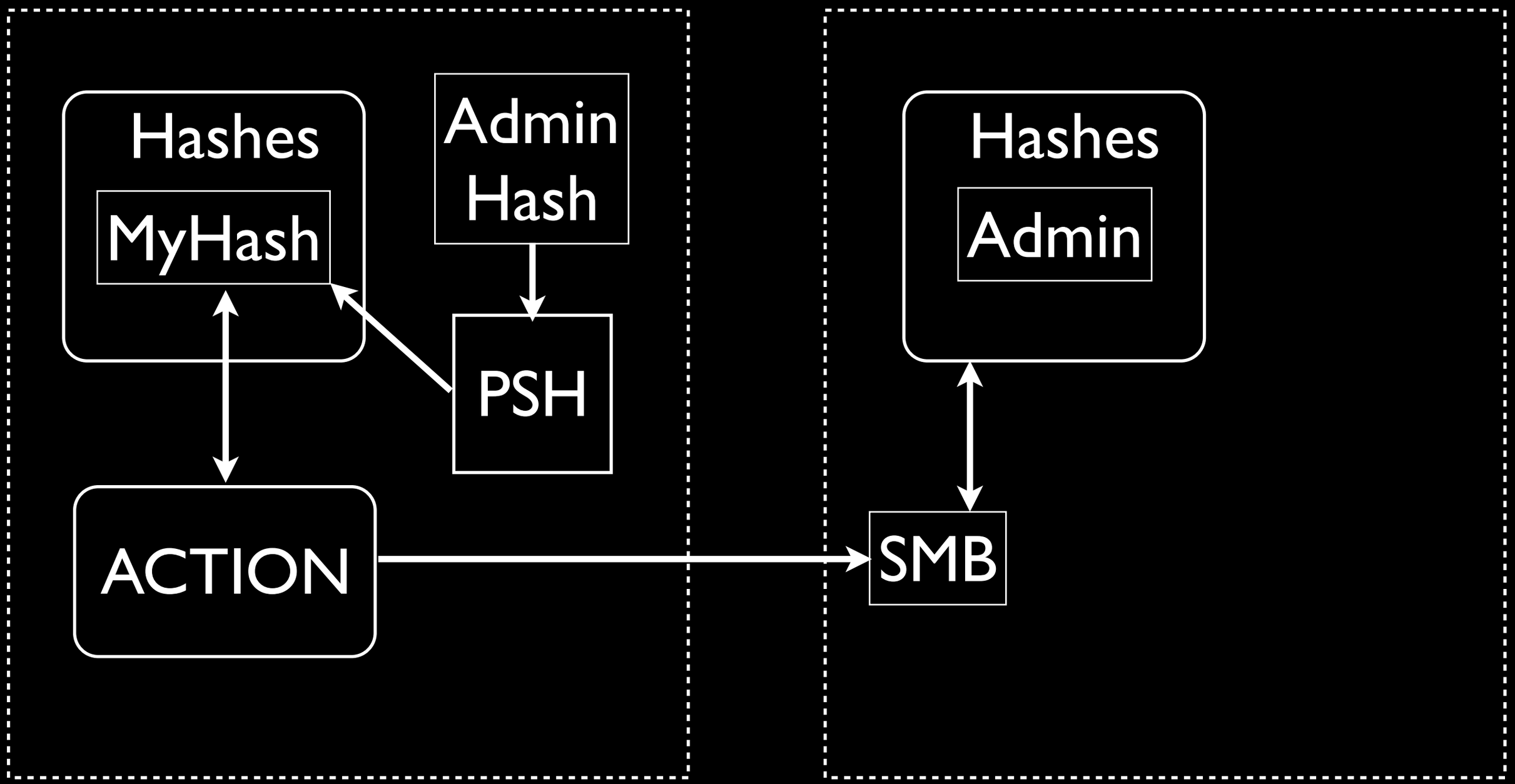


Metasploit Psexec





PSH Toolkit



PSH Toolkit

Hashes

Admin

ACTION

Hashes

Admin

SMB

ACTION

DEMO

Post-Explotation con Pass-The-Hash

Contramedidas

- Usar contraseñas de más de 14 caracteres
- No usar palabras diccionario

- Desactivar cachés de dominio en servidores
- HKLM\Software\Microsoft\WindowsNT \Current Version\Winlogon \CachedLogonsCount
- No usar mismas contraseñas

¡GRACIAS!
¿PREGUNTAS?

Jose Selvi
Pentester.es
http://www.pentester.es
jselvi@pentester.es