**Hacking**

**ético**

# 

# 

[**1.Realizar un host discovery, para descubrir la IP de la máquina víctima. 3**](#_t5kklwfdq5yk)

[2. Sistema operativo y versión del Kernel de la máquina víctima. 3](#_gawwsim5035b)

[Os y kernel 5](#_e3px1fyip03h)

[Kernel 5](#_xjoc3rumrnk1)

[3. Enumera los puertos TCP abiertos máquina víctima. 6](#_99s00vapf58i)

[4. Versión y puerto de los siguientes servicios: FTP, SSH, MySQL, Distccd e IRC de la máquina víctima. 6](#_5e9jrfuxupt5)

[5. Guarda el resultado anterior en formato xml y muestra el contenido en formato html. 7](#_wbhsp0n21rk3)

[6. Comprueba el estado (abierto, cerrado o filtrado) de los puertos UDP de los servicios DNS y DCHP. 8](#_z0f72y6jffre)

[7. ¿Puedes conectarte al servicio FTP con el usuario anónimo? Muestra captura con el comando nmap donde se vea que se permite esta conexión anónima. Por cierto, ¿quién será user? 9](#_thk5hoppdtjb)

[8. Sí puedes, conéctate con el usuario anónimo al servicio FTP. 10](#_m280w8a18di)

[9. Descargarte una carta y el hash asociado a la misma para comprobar si ha sido modificada. 10](#_qgrvj94b9x6c)

[10. Si corriges las faltas de ortografía, comprueba si ahora es correcta. (No olvides recoger la bandera) 12](#_nkws6ylnad)

[11. Intenta iniciar sesión con las credenciales encontradas. 13](#_38vc5kqpqyp6)

[12. Con lo encontrado, usando en metasploit un módulo auxiliar que permite escanear ftp\_login por fuerza bruta. Y recuerda, ¿quién será “user”? 15](#_c5uwv9t82668)

[14. Buscar vulnerabilidad en el servicio IRC: CVE, exploit a utilizar. ¿has conseguido ser root? 15](#_yua72ua1z42v)

| 1.Realizar un host discovery, para descubrir la IP de la máquina víctima. |
| --- |
|  |
| Nmap -p- 10.0.2.1-254 -T5 -n -vv |
|  |
|  |
| 2. Sistema operativo y versión del Kernel de la máquina víctima. |
|  |
| Poca info de la ip 10.0.2.4, es mi máquina host.  Ip de máquina victima 10.0.2.15 |
|  |
| Servicios abiertos |
|  |
| Os y kernel |
|  |
|  |
| Kernel |
| 3. Enumera los puertos TCP abiertos máquina víctima. |
|  |
| 4. Versión y puerto de los siguientes servicios: FTP, SSH, MySQL, Distccd e IRC de la máquina víctima. |
|  |
|  |
|  |
|  |
|  |
|  |
| 5. Guarda el resultado anterior en formato xml y muestra el contenido en formato html. |
|  |
|  |
|  |
| 6. Comprueba el estado (abierto, cerrado o filtrado) de los puertos UDP de los servicios DNS y DCHP. |
| El servidor dns suele estar en el puerto 53, en nuestra máquina este puerto nos aparece como isc bind tras un escaneo de servicio, se confirma. |
|  |
|  |
|  |
| Servidor dns en 53 |
|  |
| Servidor dhcp en 111? |
| 7. ¿Puedes conectarte al servicio FTP con el usuario anónimo? Muestra captura con el comando nmap donde se vea que se permite esta conexión anónima. Por cierto, ¿quién será user? |
|  |
| 8. Si puedes, conéctate con el usuario anónimo al servicio FTP. |
|  |
| 9. Descargarte una carta y el hash asociado a la misma para comprobar si ha sido modificada. |
|  |
|  |
| 10. Si corriges las faltas de ortografía, comprueba si ahora es correcta. (No olvides recoger la bandera) |
| No está modificada |
| Al cambiar los caractéres no coinciden los hashes |
| 11. Intenta iniciar sesión con las credenciales encontradas. |
| .tips nos indica ir al servicio web |
| Código fuente |
|  |
| usuario → rincon  Clave → Rincon123 |
|  |
|  |
|  |
| 12. Con lo encontrado, usando en metasploit un módulo auxiliar que permite escanear ftp\_login por fuerza bruta. Y recuerda, ¿quién será “user”? |
| Misclaves.txt es un diccionario.  Usuario puede ser rincon. Ftp usa unix asi que un usuario al menos hay.  Acceso a ftp explicado anteriormente. |
| 14. Buscar vulnerabilidad en el servicio IRC: CVE, exploit a utilizar. ¿has conseguido ser root? |
|  |
|  |