**Análisis Forense**

# Análisis forense en Linux Server - SSH

### 

### 

| ÍNDICE |
| --- |
| [**Análisis forense en Linux Server - SSH 1**](#_n6arwwmay01c)  [1. Contexto 2](#_hl79aikr2mgz)  [1.1.Objetivos 2](#_vxlmkytfe5xf)  [1.2 Ficheros 2](#_wrhbljp9e47w)  [1.3 Herramientas 2](#_wrhbljp9e47w)  [2. Práctica 3](#_s593ln4wjma3)  [Obtener la zona horaria en la que está corriendo el sistema. 3](#_kjeofx98hq18)  [¿Cuál es la instalación del SO? 3](#_u8j3vcd3akwu)  [Fecha 4](#_hb3tq43hsysd)  [Averiguar la dirección IP del equipo atacante. 4](#_py1g1928x3cp)  [Alternativas 4](#_o97a86bil0cv)  [Averiguar las credenciales con las que ha logrado entrar. 5](#_e8437nabha77)  [Obtener un listado de acciones realizadas por el atacante una vez comprometido nuestro servidor. 5](#_9ffpu6j4z6q7)  [Bibliografía 9](#_n8d2h5hidi9f) |
| Análisis forense en Linux Server - SSH |
| Contexto |
| Una máquina Ubuntu con un servidor SSH que ha sufrido un ataque tan sencillo como la fuerza bruta. |
| 1.1.Objetivos |
| 1. Obtener la zona horaria en la que está corriendo el sistema. 2. ¿Cuál es la instalación del SO? 3. Averiguar la dirección IP del equipo atacante. 4. Averiguar las credenciales con las que ha logrado entrar. 5. Obtener un listado de acciones realizadas por el atacante una vez comprometido nuestro servidor. |
| 1.2 Ficheros |
| 1. Imagen de disco   8d1f86b44c6b5c9655e2df5b31576b529a954f461b5800cad0a5430d7aec9f16 volcado\_metasploitable3\_2.img |
| 1.3 Herramientas |
| * ewf-tools (ewfverify, ewfmount) * The Sleuth Kit (mmls) |
| Práctica |
| Montaje previo |
|  |
| Cambio de directorio root |
|  |
| Obtener la zona horaria en la que está corriendo el sistema. |
| **cat /etc/localtime** |
|  |
| No especifica la zona horaria en **/etc/timezone**, solamente el |
|  |
| ¿Cuál es la instalación del SO? |
| **lsb\_release -a** |
|  |
| Ubuntu 14.04.6 LTS |
| Alternativa → **cat /etc/hosts/release** |
| Fecha |
| cd /; stat lost+found |
|  |
|  |
| Averiguar la dirección IP del equipo atacante. |
| **cat /var/log/auth.log | grep 'sshd'** |
|  |
|  |
| Ip → **10.0.16.5** |
| Alternativas |
| **last -i** |
| **lastlog** |
| Averiguar las credenciales con las que ha logrado entrar. |
| **cat /var/log/auth.log | grep “session opened”** |
|  |
| Usuario → vagrant |
| Password → |
|  |
| Exceptuando las dos últimas sesiones vagrant desde remoto estuvo ejecutando comandos con permisos de superusuario (sudo) y usando las sesiones de :   * chewbacca * Dirmngr * boba\_fett |
| Vagrant cerró la sesión a las 18:04:27, no ha habido más conexiones remotas |
| **cat var/log/auth.log | grep sshd** |
|  |
| Ventana de tiempo de la intrusión |
| **17.51.07 - 18:04:27** |
| Obtener un listado de acciones realizadas por el atacante una vez comprometido nuestro servidor. |
| Comandos que requieren permisos de superusuario ejecutados por vagrant durante la intrusión. |
| **cat /var/log/auth.log | grep sudo** |
|  |
| Comandos de vagrant sin timestamp |
|  |
|  |
|  |
| Remotamente el último comando del usuario fue poweroff, se puede hacer intersecciones en el anterior documento para contemplar la posible sesión. |
|  |
|  |
|  |

| Bibliografía |
| --- |
| <https://www.sqlitetutorial.net/sqlite-show-tables/> |
| <https://www.loc.gov/preservation/digital/formats/fdd/fdd000406.shtml> |
|  |