Computação Forense – Exercícios – Lista 09

Questões

1. Análise do servidor:
   a) Instale um sistema GNU/Linux em uma máquina virtual ou em um computador que você tenha acesso pela rede. Esse sistema será nosso servidor.
      Obs.: Se for em uma máquina virtual, coloque a placa de rede em modo Bridge.
   b) Configure o IP do seu servidor para que você tenha acesso de outra máquina.
   c) Em seu servidor, instale o Apache2:
      ```
      sudo apt-get install apache2 libapache2-mod-php7.0
      ```
   d) Apague o conteúdo da pasta /var/www/html.
   e) Crie uma página chamada *index.php*, com o seguinte conteúdo:
      ```
      <?
      date_default_timezone_set('America/Sao_Paulo');
      $msg = "(".date("d/m/Y H:i")."): ".$_SERVER['REMOTE_ADDR']."\n";
      $fp = fopen('ips.txt', 'a');
      fwrite($fp, $msg);
      fclose($fp);
      echo $_SERVER['REMOTE_ADDR'];
      ?>
      ```
   f) Crie um arquivo chamado *.htaccess*, com o seguinte conteúdo:
      ```
      <Files "ips.txt">
      Order Allow,Deny
      Deny from all
      </Files>
      ```
   g) De outro computador, utilize o navegador para acessar seu servidor criado.
   h) Tente acessar o arquivo *ips.txt* pelo navegador. Ex.: http://IP_DO_SERVIDOR/ips.txt
   i) Quais informações puderam ser obtidas pelo *index.php*?
   j) Agora, dê o seguinte comando no servidor:
      ```
      sudo tail -f /var/log/apache2/{error,access}.log
      ```
      Acesse novamente seu servidor e também tente acessar páginas inexistentes.
      I. Quais são as informações que você obtém dos logs?
      II. Quais poderiam ser utilizadas em uma perícia forense?
      III. Utilizando informações desse logs, como obter:
         i. De que local do mundo que sua página foi acessada?
         ii. Em que momento que foi acessada?
         iii. Quais foram as tentativas de ataque (acesso inapropriado).
   k) Baixe o log de meu servidor (jeiks.net), dia 09/12, em:
      <http://jeiks.net/wp-content/uploads/2017/12/access_jeiks_net.zip>
      Responda:
      I. Sabendo que a hora do servidor é configurada em PST, quais foram os horários dos acessos ao site?
      II. Sobre os IPs que mais acessaram o site:
         i. Quais os foram?
         ii. De onde eles são (local do mundo)?
         iii. Qual cliente que foi utilizado?

   l) Ainda no seu servidor, responda sobre os arquivos da pasta */var/log :*
      I. Quais informações que cada um deles provê?
      II. Utilizando o *auth.log*, quais foram os logins mal sucedidos em seu servidor?
      III. Utilizando o *dpkg.log*, qual foi a ordem de instalação de pacotes em seu servidor?
      IV. Como ler as informações do *wtmp*?
   m) No seu servidor, dê o comando:

sudo netstat -antp

E responda:

I. Quais são as portas desnecessárias que estão abertas?
II. Quais são os processos que estão fornecendo essas portas?
(Dica: sudo fuser -v PORTA/PROTOCOLO. Exemplo: sudo fuser -v 4381/tcp)
III. Como essas informações podem ser utilizadas na perícia?

2. Analisando o acesso feito pelo cliente:
   a) O que são arquivos sqlite?
   b) Como identificá-los no computador? (Dica: comandos *find* + *file*)
   c) Obtenha as pastas locais de seus navegadores de Internet e salve em um local para perícia.
   No Windows, baixe e utilize os seguintes aplicativos:
   <http://jeiks.net/wp-content/uploads/2017/12/Forense_Navegadores.zip>
   No linux, instale o *sqlitebrowser*
      I. Quais são as informações que puderam ser recuperadas?
      II. Como essas informações podem ser utilizadas na perícia?