IDS: ClamAV [Signature-based]

Oleh:

Idris Winarno

Outline

- Apache2 + PHP + ClamAV
- Proftpd + ClamAV

Tentang ClamAV (1)

- Merupakan anti virus open source untuk mendeteksi trojan, virus, malware dan serangan-serangan lain.
- Merupakan standard open source untuk mail gateway scanning software.
- Meliputi multi-thread scanner daemon dan juga perintah-perintah command line untuk melakukan scanning dan juga melakukan update secara otomatis.
- Mendukung banyak format dari file dan juga berbagai macam file kompresi.
- Dapat dijalankan pada Linux, Windows, maupun Mac.

** https://www.proweb.co.id/articles/email/clamav.html*

Tentang ClamAV (2)

- Database virus yang ditangani ini diupdate setiap 5 jam sekali.
- ClamAV ini merupakan standar antivirus yang digunakan dalam cPanel.
- ClamAv juga dapat mendeteksi email phishing, suatu email yang memancing kita melakukan aksi tertentu yang berpotensi merugikan kita.
- Proses yang disediakan ClamAv adalah
  - ClamAV library
  - clamscan
  - Freshclam Program freshclam ini akan mengupdate database virus. Program freshclam ini akan mendownload main.cvd, daily.cvd dan bytecode.cvd .
  - clamd
  - clamdscan
  - clamconf
  - script untuk start clamd dan freshclam dalam mode daemon.

** https://www.proweb.co.id/articles/email/clamav.html*

Tentang ClamAV (3)

- Untuk pengguna Windows, ada program Antivirus yang menggunakan ClamAv yaitu Immunet. Fitur dari Immunet antara lain:
  - **Real-time Detection**
  - Scann yang bisa dijadwal
  - Scan yang cerdas secara cermat dan dapat dikonfigurasi
  - Custom Detection
  - Quarantine
- ClamAv juga digunakan pihak ketiga yang bisa kita lihat pada halaman https://www.clamav.net/downloads .
- ClamAV ini digunakan pihak ketiga antara lain dalam:
  - MTA (Mail Transfer Agents)
  - POP3 (Post Office Protocol)
  - **Web dan FTP**
  - Filesys MUA

** https://www.proweb.co.id/articles/email/clamav.html*

Apache2 + PHP + ClamAV

- Installasi apache2, PHP, dan ClamAV
  - # apt-get install apache2 php clamav clamav-daemon

- Persiapkan folder penampung untuk file hasil upload
  - # mkdir /var/www/html/files
  - # chown www-data:www-data /var/www/html/files

Konfigurasi Freshclam dan Clamav-daemon

- # vim /etc/clamav/freshclam.conf

  HTTPProxyServer proxy3.eepis-its.edu

  HTTPProxyPort 3128

- # /etc/init.d/clamav-freshclam stop
- # freshclam
- # vim /etc/clamav/clamd.conf

  TCPSocket 3310

  TCPAddr 127.0.0.1

  LocalSocket /var/run/clamav/clamd.sock

Disable PHP Engine

- Non-aktifkan engine PHP pada folder penampung file hasil upload
  - # vim /etc/apache2/apache.conf
  - Ubah →

```
#<Directory />
#   AllowOverride None
#   Require all denied
#</Directory>
```

→ AllowOverride None
AllowOverride All

  - # /etc/init.d/apache2 restart
  - # vim /var/www/html/files/.htaccess

    php_flag engine off

Download library clamav untuk PHP

- # apt-get install git
- # cd /var/www/html
- # export https_proxy=http://proxy3.pens.ac.id:3128
- # git clone https://github.com/kissit/php-clamav-scan.git

Script untuk upload

vim /var/www/html/index.php

```
<html>
<head>
<title>..:: Upload File ::..</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
</head>

<body>
<?php
        require "php-clamav-scan/Clamav.php";
        $clamav = new Clamav();
        if(isset($_POST['upload'])){
                $fileName = $_FILES['userfile']['name'];
                $tmpName  = $_FILES['userfile']['tmp_name'];
                $fileSize = $_FILES['userfile']['size'];
                $fileType = $_FILES['userfile']['type'];

                $filePath = "/var/www/html/files/";
                $result    = move_uploaded_file($tmpName, $filePath.$fileName);
                if (!$result)
                        die("Error uploading file $tmpName to $fileName");

                if(!get_magic_quotes_gpc()){
                        $fileName  = addslashes($fileName);
                        $filePath  = addslashes($filePath);
                }

                if(!$clamav->scan($filePath.$fileName)){
                        unlink($filePath.$fileName);
                        die("File bervirus");
                }
                echo "<br>File $fileName uploaded<br>";
        }
?>
<form action="" method="post" enctype="multipart/form-data" name="uploadform">
  <table width="350" border="0" cellpadding="1" cellspacing="1" class="box">
    <tr>
      <td width="246">
        <input type="hidden" name="MAX_FILE_SIZE" value="2000000">
        <input name="userfile" type="file" class="box" id="userfile">
         </td>
      <td width="80"><input name="upload" type="submit" class="box" id="upload" value="  Upload  "></td>
    </tr>
  </table>
</form>
</body>
</html>
```

Ujicoba

- Download salah satu script (malware) di:
  - http://www.r57c99.com/
  - https://r57.gen.tr/

- Upload file malware!

Tugas

- Integrasikan ClamAV dengan layanan proftpd
- Konfigurasi ClamAV untuk realtime detection
  - Hint: FANOTIFY