HƯỚNG DẪN THIẾT LẬP CHÍNH SÁCH BẢO MẬT WEB SERVER TOMCAT 7

I. Nội dung hướng dẫn

- Hướng dẫn thiết lập an toàn cho Webserver Tomcat 7 nhằm đảm bảo 7 tiêu chuẩn ATTT bao gồm:

II. Chi tiết hướng dẫn

1. Cài đặt Web Server đảm bảo an toàn.

- Web Server phải được cài đặt trên hệ điều hành an toàn, đã được thiết lập cấu hình chính sách bảo mật: Tham chiếu mục 1 Tiêu chuẩn An toàn thông tin hệ điều hành.

- Phiên bản Web Server không mắc lỗ hổng bảo mật, được cập nhật tất cả bản vá security:

o Đối với các hệ thống cài mới: Sử dụng Tomcat phiên bản mới nhất (Tham khảo tại: http://tomcat.apache.org/). Tại thời điểm hiện tại, phiên bản tối thiểu được phép cài đặt là: 7.0.63 đối với Tomcat 7, 6.0.44 đối với Tomcat 6.

o Các hệ thống sử dụng Tomcat 5 phải nâng cấp lên Tomcat 6 hoặt Tomcat 7.

o Các Web Server Tomcat phải được cập nhật các bản vá security đã được Trung tâm An ninh mạng Viettel và Phòng Công nghệ thông tin Tập đoàn cảnh báo.

2. Gỡ/tắt bỏ các thành phần mặc định khi cài đặt Web Server

- Gỡ bỏ các thư mục/trang mặc định.

o Xóa file, thư mục tại đường dẫn CATALINA_HOME/webapps (ROOT, balancer, jsp-examples, servlet-examples, tomcat-docs, webdav, manager, docs, examples)

o Xóa file CATALINA_HOME/conf/Catalina/localhost/host-manager.xml và CATALINA_HOME/conf/Catalina/localhost/manager.xml.

- Tắt các Module/Extension không sử dụng

o Trên file server.xml tại đường dẫn CATALINA_HOME/conf/server.xml, tìm dòng <connector … protocol=”AJP/…”> và chuyển sang dạng ghi chú.

```
<!-- Define an AJP 1.3 Connector on port 8009 -->
<!-- <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" /> -->
```

o Restart lại Tomcat.

3. Thay đổi các thành phần mặc định.

- Thay đổi thông báo lỗi mặc định của Web Server.

o Tạo các error.html ở thư mục gốc của ứng dụng với nội dung phù hợp với từng ứng dụng.

o Mở file web.xml tại đường dẫn CATALINA_HOME/conf/web.xml, thay đổi thông báo lỗi với các mã lỗi 400, 401, 402, 403, 404, 500, 501, 502, 503, bằng cách thêm các nội dung sau vào trước thẻ đóng </web-app>

```
<error-page>
<error-code>400</error-code>
<location>/error.html</location>
</error-page>
<error-page>
<error-code>401</error-code>
<location>/error.html</location>
</error-page>
<error-page>
<error-code>402</error-code>
<location>/error.html</location>
</error-page>
<error-page>
<error-code>403</error-code>
<location>/error.html</location>
</error-page>
<error-page>
<error-code>404</error-code>
<location>/error.html</location>
</error-page>
<error-page>
<error-code>500</error-code>
<location>/error.html</location>
</error-page>
<error-page>
<error-code>501</error-code>
<location>/error.html</location>
```

```
</error-page>
<error-page>
<error-code>502</error-code>
<location>/error.html</location>
</error-page>
<error-page>
<error-code>403</error-code>
<location>/error.html</location>
</error-page>
```

- Restart lại Tomcat.

- Chỉ cho phép thực thi các phương thức GET, POST, HEAD.

- Mở file web.xml tại đường dẫn CATALINA_HOME/conf/web.xml thêm các dòng sau ở cuối file trước thẻ đóng </web-app>

```
<security-constraint>
<web-resource-collection>
<web-resource-name>restricted methods</web-resource-name>
<url-pattern>/*</url-pattern>
<http-method>PUT</http-method>
<http-method>DELETE</http-method>
<http-method>OPTIONS</http-method>
<http-method>TRACE</http-method>
</web-resource-collection>
<auth-constraint />
</security-constraint>
```

- Restart lại Tomcat.

4. Cấu hình giới hạn truy cập.

- Giới hạn địa chỉ IP truy cập vào trang, chức năng quản trị.

- Mở file server.xml tại đường dẫn CATALINA_HOME/conf/server.xml

- Chỉ cho phép truy cập cổng SHUTDOWN từ địa chỉ loopback : Thêm thuộc tính address="127.0.0.1" trong thông số về cổng SHUTDOWN.

```
<Server address="127.0.0.1" port="8005" shutdown="SHUTDOWN">
```

- Restart lại Tomcat.

- Không cho phép liệt kê file, thư mục.

- Mở file web.xml tại đường dẫn CATALINA_HOME/conf/web.xml tìm section <init-param> trong section <servlet> với ” <servlet-name>default</servlet-name>” thay đổi thuộc tính listings là false

```
<init-param>
<param-name>listings</param-name>
<param-value>false</param-value>
</init-param>
```

- Restart lại Tomcat.

5. Cấu hình phân quyền ứng dụng Web Server.

- Chạy tiến trình Web Server với tài khoản user được giới hạn quyền (không phải tài khoản quản trị, hoặc có quyền tương đương với tài khoản quản trị).
  - Tạo user riêng không thuộc nhóm tài khoản quản trị (root).
  - Đăng nhập và khởi chạy ứng dụng sử dụng tài khoản vừa tạo.
- Không cho phép thực thi các câu lệnh CGI, SSI: Mặc định Tomcat đã tắt CGI.

6. Sử dụng cơ chế mã hóa an toàn.

- Sử dụng thư viện mã hóa an toàn.
  - Đối với các hệ thống cài mới: Sử dụng phiên bản thư viện OpenSSL mới nhất. Tại thời điểm hiện tại, phiên bản tối thiểu là OpenSSL version 1.0.2d và 1.0.1p (release ngày 09/07/2015).
  - Các hệ thống sử dụng bộ thư viện OpenSSL phải được nâng cấp, cập nhật các bản vá security đã được Trung tâm An ninh mạng Viettel và Phòng Công nghệ thông tin Tập đoàn cảnh báo.
- Không sử dụng SSL version 2.0, SSL version 3.0.
  - Mở file server.xml tại đường dẫn CATALINA_HOME/conf/server.xml, tìm và gỡ bỏ nội dung: sslProtocols=”TLS” .
  - Thêm nội dung:

```
sslEnabledProtocols=”TLSv1, TLSv1.1, TLSv1.2”
```

  - Restart lại Tomcat.
- Thiết lập SSLCipherSuite an toàn cho webserver.
  - Mở file server.xml tại đường dẫn CATALINA_HOME/conf/server.xml. Tìm đến phần cấu hình SSL.
  - Cấu hình trường ciphers chỉ sử dụng các cipher an toàn:

```
ciphers="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_RC4_128_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA,SSL_RSA_WITH_RC4_128_SHA"
```

```
<Connector port="8443" protocol="org.apache.coyote.http11.Http11Protocol"
           maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
           clientAuth="false"
           sslEnabledProtocols="TLSv1, TLSv1.1, TLSv1.2"
           keystoreFile="/home/test/test.jks"
           keystoreType="JKS"
           keystorePass="123456"
           keyPass="123456"
           ciphers="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_RC4_128_SHA, TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA, SSL_RSA_WITH_RC4_128_SHA"
           />
```

- Restart lại Tomcat.

7. Cấu hình ghi log WebServer an toàn

- Đồng bộ thời gian cho máy chủ web với máy chủ thời gian, đảm bảo thời gian ghi trong log file là chính xác và đồng nhất.
- Web Server cần được thiết lập bật chế độ ghi log, ghi luân phiên/xoay vòng log file theo ngày
  - Mở file server.xml tại đường dẫn CATALINA_HOME/conf/server.xml.
  - Bổ sung thêm đoạn cấu hình sau vào server.xml nếu chưa có:

```
<Valve className="org.apache.catalina.valves.AccessLogValve"
directory="logs"
prefix="<TEN APP>_"
suffix=".log"
pattern="%h %{X-Forwarded-For}i %l %u %t &quot;%r&quot; %s %b &quot;%{Referer}i&quot; &quot;%{User-Agent}i&quot;"
resolveHosts="false"
fileDateFormat="yyyy-MM-dd"
rotatable="true" />
```

  - Trong đó:
    - directory: Thư mục đặt file log.
    - prefix: Tiền tố tên file.
    - suffix: Phần tên đuôi file.
    - pattern: Định nghĩa các trường ghi trong access log
    - resolveHosts: Có phân giải IP thành tên miền hay không? (true, false)
    - fileDateFormat: Là định dạng in ngày tháng, mặc định nếu không đặt thì mặc định sẽ là "yyyy-MM-dd"
    - rotatable: là biến cho phép rotate log hàng ngày, mặc định là true, tuy nhiên nếu là failse thì biến fileDateFormat sẽ không có tác dụng.
  - Restart lại Tomcat.
- Định dạng dữ liệu log phải có đủ thông tin phục vụ cho việc điều tra, truy vết vi phạm ATTT: Thực hiện trong bước trên.

- Log cần được lưu trữ tối thiểu 03 tháng trên máy chủ.
- Dựa vào dung lượng log trung bình 01 ngày, cần chuẩn bị dung lượng ổ cứng để lưu được log tối thiểu 90 ngày.
- Đặt lịch xóa file log lâu hơn 90 ngày nếu cần thiết để tránh đầy ổ cứng.
- Các đơn vị chủ động đẩy log định kỳ hàng ngày lên file server chung, đảm bảo lưu trữ 03 tháng, nén định dạng zip.