Apuntes de Sistemas Distribuidos, análisis de una botnet

Juan Carlos Miranda[1]

http://otroblogdetecnologias.blogspot.com/,
https://github.com/freelanceparaguay/,
juancarlosmiranda81@gmail.com

1 Pautas del trabajo

- Fecha de entrega: 10/04/2017.
- Horario de entrega: a las 17:20 horas.
- Forma de entrega: los ejercicios que involucren programación en un lenguaje serán evaluados en clase.
- Total de puntos: **5 puntos**. Configuración LAMP/WAMP 2p), explicación de servidor de control 1p), explicación del cliente Java y resultados 2p),

2 Objetivos

Que el alumno pueda comprender en forma básica el funcionamiento de agentes conectados bajo el concepto de sistemas distribuidos.

Que el alumno haga uso de técnicas de programación que involucren hilos de ejecución, sockets, protocolos de red.

Que el alumno implemente una solución tecnológica basada en lenguajes Java y PHP.

3 Pautas de presentación

1. El código deberá contener comentarios explicativos y presentar los resultados solicitados.
2. El autor del código deberá explicar el funcionamiento del mismo.
3. El trabajo es individual y su presentación también. Durante el desarrollo del mismo, los alumnos podrán discutir los enfoques de solución en grupo, pero la presentación del trabajo será individual.
4. **Las variables deberán contener nombres que expliquen su función. Ejemplos de variables de una sola letra es una mala práctica.**
5. Se espera que el software presentado cumpla con la funcionalidad para la cual fue creado, **por eso el autor del trabajo deberá poder demostrar que funciona correctamente su código con resultados**.
6. El plagio **será motivo de anulación del trabajo**.

4 Ejercicios de programación

Los conceptos de sistemas distribuidos pueden verse aplicados también en el ámbito del malware, específicamente en las botnets. Para los investigadores del área de seguridad de la información es importante conocer como funcionan los códigos maliciosos a fin de desarrollar técnicas defensivas contra los mismos. A la vez, varios malwares presentan técnicas innovadoras, las cuales pueden ser aplicadas a otro tipo de sistemas.

Para el efecto, se realizará una lectura guiada del artículo [1] enfatizando en los siguientes puntos:

- Arquitecturas distribuidas.
- Mecanismos de comunicación.
- Código fuente presentado.

Se solicita al alumno, que replique el código del cliente en lenguaje Java y que solucione posibles inconvenientes que limiten el funcionamiento básico del mismo. Se busca que se repliquen en el agente las siguientes funciones:

- Inicializar el agente.
- Conectar a un centro de control.
- Esperar órdenes de un centro de control en un ciclo infinito
- Recibir mensajes, interpretarlos y hacer algo.

En cuanto a la recepción de mensajes, el agente deberá ser capaz de recibir una orden desde el centro de control y mostrar un mensaje en pantalla simulando la ejecución de dicha orden.

5 Instalación y configuración del centro de control (C&C)

Se ofrece un código de servidor de control (C&C)implementado en lenguaje PHP y basado en [1] con algunas adaptaciones. Se puede descargarlo desde [3].

El C&C recibe y procesa en forma básica parámetros de entrada con solicitudes vía protocolo HTTP del tipo GET y POST.

Al ser un servidor de control educativo, ciertos detalles se han dejado de lado para posteriores implementaciones. No se contemplan los siguientes puntos:

- Protección contra SQL injection.
- Interfaces amigables de administración.

5.1 Materiales y herramientas

Se requiere tener instaladas las siguientes herramientas:

- Servidor LAMP o WAMP (Apache web server, Mysql o MariaDB, PHP)
- MySQL Workbench para diseño de tablas en caso de que se necesite.
- phpMyAdmin para administrar la base de datos, aunque las tareas pueden ser realizadas desde consola también.

5.2 Configuración de la base de datos

Para configurar la base de datos en un entorno Linux se pueden seguir los pasos a continuación.

```
mysql -u root -p
SET PASSWORD=PASSWORD('miclavesupersecreta');
mysql -u root -pmiclavesupersecreta
Maria DB []>GRANT ALL ON basedatosbot.* to apache@localhost IDENTIFIED BY 'miclavesupersec
mysql -u apache -pmiclavesupersecreta --database  basedatosbot
SET PASSWORD=PASSWORD('miclavesupersecreta');
```

Se sugiere las lecturas: Lesson: All About Sockets [4], Cap. 4 Interprocess Communication [8], Cap. 4, 4.3.1 Message- Oriented Transient Communication, [9].

En lo que se refiere al lenguaje PHP se puede utilizar como referencia [6] y [7].

5.3 Pruebas de funcionamiento del C& C

Para las pruebas del C&C, tanto GET o POST puede hacerse uso de la herramienta curl [2], también es posible utilizar un navegador web para el caso de parámetros del tipo GET.

Como aclaración, teniendo en cuenta que el artículo original lleva su tiempo, se adaptaron las instrucciones de conexión a la base de datos. **Actualmente en la comunidad de PHP se soportan dos métodos: mysqli y PDO_MySql, mayor información en** [5].

Como ejemplos, se adjuntan cadenas de prueba enviadas con la herramienta curl.

```
curl -d "botpwd=hola\&status=init" http:\/\/localhost\/api\/connect.php

curl -d "botpwd=hola\&status=start\&botid=0bebb85d4787ac4dd78a51488ed59ce1\&hostname=locall
```

5.4 Recomendaciones generales

Se recomienda realizar pruebas de funciones y métodos por separado. Siempre, conviene realizar una verificación general del código antes de la ejecución. En caso de problemas aislar las funciones, si es necesario, separarlas y probarlas por separado.

References

1. Byob: Build your own botnet. https://www.sans.org/reading-room/whitepapers/threats/byob-build-botnet-33729. [Web; accedido el 03/04/2017].
2. Curl, command line tool and library. https://curl.haxx.se/. [Web; accedido el 03/04/2017].
3. Ejemplo php c&c. https://github.com/freelanceparaguay/SistemasDistribuidos/tree/master/bot/api. [Web; accedido el 03/04/2017].
4. Java tutorial, lesson: All about sockets. http://docs.oracle.com/javase/tutorial/networking/sockets/index.html. [Web; accedido el 20/03/2017].
5. Overview of the mysql php drivers. http://php.net/manual/en/mysql.php. [Web; accedido el 03/04/2017].
6. Php net. https://www.php.net. [Web; accedido el 03/04/2017].
7. Referencias sobre php y html. https://www.w3schools.com. [Web; accedido el 03/04/2017].
8. G. Coulouris, J. Dollimore, T. Kindberg, and G. Blair. *Distributed Systems: Concepts and Design*. Addison-Wesley Publishing Company, USA, 5th edition, 2011.
9. A. S. Tanenbaum and M. v. Steen. *Distributed Systems: Principles and Paradigms (2Nd Edition)*. Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 2006.