Conclusiones

En el principio de este informe se ha definido un objetivo a lograr y los capítulos anteriores son la prueba de que dicho objetivo se cumplió, al conocer algunos conceptos previos, establecer una metodología de análisis y aplicar lo anterior para llevar a cabo el diseño y desarrollo de los programas necesarios.

A pesar de satisfacer los alcances que en un principio fueron definidos para la "Herramienta TRUMAN ampliada", aún quedan funcionalidades por mejorar y agregar, códigos por optimizar y características que madurar. Es importante hacer énfasis en que las herramientas de seguridad informática, en general, tienen un tiempo de vida reducido que va de meses hasta algunos pocos años en los mejores casos, por lo tanto es vital mantenerlas al tanto de los últimos avances y tendencias.

Los resultados obtenidos son satisfactorios, ya que las pruebas realizadas con diversos tipos de malware proyectaron información que se esperaba se presentara en los análisis. La herramienta se desempeñó bien en todos sus procesos de ejecución; a excepción de algunos casos muy puntuales, donde el código malicioso en ejecución afectaba un punto en particular y provocaba un rompimiento en el flujo de la herramienta TRUMAN.

En relación a lo anterior se puede comentar la ocasión en que algunos códigos maliciosos provocaban un congelamiento de la terminal de comando, y en particular, una interrupción del programa que los ejecuta, lo cual no permitía que este programa siguiera su curso y se reiniciara el equipo cliente, por lo tanto permanecía como si se tratara de un ciclo infinito y debía ser reiniciado manualmente. Esto era un grave problema, porque ocurría con frecuencia. La solución fue agregar un proceso más en ejecución, de tal manera que las labores de ejecutar el programa malintencionado y llevar a cabo la cuenta regresiva para el reinicio del sistema fueran independientes.

Otro caso representativo es el de un software malicioso que particularmente afectaba ciertas interfaces gráficas. Este provocaba el mal comportamiento de una pequeña interfaz gráfica que utiliza el comando “shutdown”, el cual era usado para reiniciar el sistema cliente Microsoft Windows XP con la opción “-r”; y de igual forma no permitía que se siguiera el flujo del ciclo de análisis. La solución al problema fue posible mediante la herramienta WMIC de Microsoft Windows que puede reiniciar el sistema de manera transparente y sin interfaces gráficas.

También se realizaron cambios en el programa CGI de Perl que funciona como transmisor del archivo ejecutable malicioso. Los cambios fueron orientados a mantener el estado del proceso mediante la escritura de un archivo, el cual se utilizó como una bandera para causar el disparo de ciertas actividades. Esto se relaciona directamente con la función del script /etc/init.d/services.sh

Para proteger a la red adyacente de la infección por algún gusano de red que se ejecute, se establece un firewall que sólo permite la salida a Internet y en ningún momento permite conexiones hacia redes internas de carácter privadas con direcciones IP 192.168.0.0/16, 172.16.0.0/12 y 10.0.0.0/8.

Las problemáticas de los tres casos anteriores no se tenían contempladas en el plan inical del proyecto en el DSC/UNAM-CERT, surgieron en el desarrollo y en la etapa de pruebas del mismo. Evidentemente no eran parte primordial del objetivo resolverlas, sin embargo no atenderlas afectaba el propósito fundamental de la herramienta automatizada.

En el anexo 11 de este informe se expone un reporte significativo que la herramienta genera, en el cual se aprecia la información que se obtiene después del análisis de una muestra código malicioso particularmente activa.

Para finalizar, este proyecto es una opción libre y funcional para el análisis de códigos maliciosos orientado a investigadores, como ya se mencionó al principio. Es posible que requiera numerosos y significativos cambios en un corto plazo, no obstante puede ofrecer grandes ventajas sobre las demás herramientas de su tipo al ser liberado mediante este informe, de tal forma que cualquiera pueda usarlo y modificarlo. Su arquitectura es sencilla y se tiene la certeza de que se trata de un análisis cien por ciento realista. Además ha sido programado para trabajar de forma automatizada, es decir, sin necesidad de interacción humana durante el análisis de algún código malicioso.