Capítulo 5
Conclusiones y trabajo a futuro

"Despúes de escalar una montaña muy alta, descubrimos que hay muchas otras montañas por escalar"

Nelson Mandela.

En este Capítulo se presentan las conclusiones de este trabajo y se proponen ideas como posibles trabajos futuros.

Capítulo 5. Conclusiones y trabajo a futuro.

Al concluir este trabajo se corrobora la necesidad de incluir un área dedicada exclusivamente al monitoreo y control de la seguridad informática en cualquier red de cómputo. Existen muchas herramientas comerciales y gratuitas que pueden permitir establecer un esquema integral de seguridad después de un análisis sobre las necesidades y posibilidades reales. Lamentablemente la mayoría de las personas que toman las decisiones administrativas no están dispuestos a invertir grandes cantidades de dinero para estos rubros y los desarrollos se ven limitados a utilizar tecnología que paises de primer mundo tienen perfectamente controlada. Cuando las herramientas gratuidas llegan a México, ya son obsoletas en otros paises.

La implantación de este esquema de seguridad satisface la infraestructura de la red UDLA. Sin embargo, el modelo planteado podría satisfacer cualquier tipo de arquitectura de cómputo.

Las políticas y los procedimientos establecidos en este trabajo no se presentan en este documento por ser de caracter confidencial.

Como trabajo a futuro se sugiere iniciar proyectos de investigación que desarrollen las tecnologías de seguridad que se usan dentro de la UDLA. El contar con sistemas propietarios (sugerencia: telnet_udla, ftp_udla, web_udla) con métodos de encriptamiento (por ejemplo curvas elípticas) permitiría no tener ningua dependencia hacia la tecnología de segunda mano.

La seguridad física es otro aspecto que puede complementar este trabajo. El uso combinado de las bitácoras que registran el momento en que un posible intruso está delante de una computadora y la evidencia fílmica (por ejemplo) del rostro de la persona en una sala.

Para una aplicación a la medida de la UDLA de la herramienta Crack (Capítulo 3.3.1) se sugiere partir la tabla de passwords y procesarlas en varios CPS.

Es un hecho que aunque a los sistemas operativos y aplicaciones de una red se le apliquen los más recientes parches de seguridad éstos siguen expuestos al ataque de hackers avanzados, ya que al momento en que un parche es recién liberado es porque se

tenían ya semanas de que un hacker había violado la seguridad precisamente a través del hoyo que el parche pretende tapar.

Por todo lo anterior, un esquema que permita instalar (en forma automática y masiva en todos los nodos de la UDLA) las herramientas de seguridad producidas en este trabajo es una necesidad inmediata. De nada sirve producir herramientas si éstas no se usan.

Otro gran factor para que las medidas de seguridad sean exitosas es su penetración en la comunidad en general, que formen ya parte de su forma de trabajo.