SEMILLERO DE SEGURIDAD DE LA INFORMACIÓN

Objetivo General:

Investigar sobre los avances de la seguridad de la información con el fin de identificar problemáticas y aportar soluciones.

Objetivos específicos:

1. Estudiar de forma continua el estado del arte en seguridad de la información en cada una de sus áreas.
2. Realizar prácticas para apropiar el conocimiento
3. Identificar fallas o falencias de seguridad de la información
4. Proponer soluciones a los problemas identificados
5. Poner en marcha las propuestas

Problemática

En seguridad de la información la premisa es que “No existe la seguridad al cien por ciento” ya que cualquier sistema es vulnerable y susceptible de ser atacado, por lo tanto la seguridad no debe ser considerada como una actividad puntual sino como un proceso en constante revisión.

METODOLOGÍA

1. Reuniones presenciales quincenales
2. Creación de foros, seminarios, talleres, laboratorios, retos y actividades lúdicas (*gamification*) orientados a la apropiación y difusión del conocimiento sobre seguridad de la información; asistencia a eventos: cursos, diplomados, certificaciones, etc. En cada actividad realizada se generará la documentación correspondiente.
3. Temáticas: Metodologías, estándares, buenas prácticas, pruebas de penetración (recolección de información, análisis de vulnerabilidades, explotación, post explotación, reportes), password attacks, Wireless attack, Shell scripting, Ataques web (XSS Y SQL INJECTION ), computación forense.

ESTADO ACTUAL DEL SEMILLERO

Actualmente nos estamos reuniendo cuatro horas semanales, dos horas los martes y dos horas los viernes con el fin de captar personas interesadas en participar, replicando las sesiones. Se han hecho sesiones informativas y prácticas, contamos con un logo y algún material propio y otro recopilado, así como una cuenta en Gmail para el envío de comunicaciones y el uso de google drive para edición de documentos de forma conjunta, así como una cuenta en Mega (<https://mega.co.nz>) a modo de repositorio. Igualmente se abrió una página web (<http://sophia.javeriana.edu.co/~paez-r/GIS/>) para hacer difusión del material informativo y darle visibilidad al semillero.

INTEGRANTES

Rafael V. Páez Méndez (Tutor)

|  |  |  |  |
| --- | --- | --- | --- |
| Luis Montaño | 5 | 1913661062 | luis.montano@javeriana.edu.co |
| Miguel Urquijo | 7 | 1026581501 | urquijom@javeriana.edu.co |
| Andres Rodriguez | 1 | 1026588457 | andresssss10@gmail.com |
| Carlos José Manrique Ramírez | 8 | 1110546336 | manrique.carlos@javeriana.edu.co |
| Andrés Rincon | 5 | 1019097939 | arinconp@javeriana.edu.co |
| Camilo Andrés Oviedo Lizarazo | 7 | 1018473407 | oviedo-c@javeriana.edu.co |
| Oscar Alejandro Moreno Galeano | 5 | 1015461950 | oscarmoreno@javeriana.edu.co |
| Juan Manuel Joya López | 3 | 1020811521 | juanmajoya@gmail.com |
| Javier Felipe Vasquez Roldan | 7 | 1015456333 | jfvr@outlook.com |
| José Camilo Villagrán Gutiérrez | 7 | 1022397121 | jvillagran@javeriana.edu.co |
| Ivan Dario Sandoval Acosta | 2 | 98050961125 | sandoval.i@javeriana.edu.co |
| Javier Camilo Mendoza | 9 | 1032444916 | mendoza.javier@javeriana.edu.co |
| Andres Felipe Chia Avila | 5 | 1023946708 | pipechia11@gmail.com |

PROPUESTA PARA EL SEMESTRE 2015-3

Problemática: Actualmente las personas tienen acceso a diferentes sistemas de información, Internet y redes sociales, en donde la seguridad no es un factor que se ha tenido en cuenta desde el principio, por lo que se debe sensibilizar al usuario de la importancia la información que maneja y que puede tener consecuencias negativas sobre una organización, una comunidad e incluso a la propia persona, si no tiene en cuenta unas recomendaciones mínimas de seguridad. Los riesgos no son sólo lógicos al perder confidencialidad, integridad y disponibilidad de la información, sino que podrían ser físicos al revelar información sobre ubicación, actividades y/o transacciones realizadas por una persona. Por lo tanto es necesario tener estrategias claras para que los usuarios adopten buenas prácticas de seguridad. Una de las técnicas que se utilizan para lograr este objetivo es la utilización de juegos (*gaming*), de manera que de forma divertida, el usuario apropie conocimientos y los ponga en práctica, con el fin de superar la barrera natural de la resistencia al cambio y sin imponer comportamientos que no serían bien acogidos por los usuarios.

Objetivo General

Generar material lúdico para transmitir buenas prácticas en seguridad de la información a los usuarios utilizando *gamification*.

Objetivos específicos

1. Identificar los conocimientos y las buenas prácticas que se quieren reforzar en los usuarios sobre seguridad de la información
2. Identificar las estrategias para reforzar los conocimientos (Mecánica, dinámica y componentes de la actividad)
3. Desarrollar e implementar las estrategias