|  |  |  |
| --- | --- | --- |
| **CLAVE 742** |  | **CICLO** |
| **SISTEMAS OPERATIVOS** |  | **SEPTIMO** |

|  |  |  |
| --- | --- | --- |
| **HORAS FRENTE A DOCENTE**  **56** | **HORAS INDEPENDIENTES**  **40** | **CRÉDITOS**  **6** |

|  |
| --- |
| **OBJETIVO**  Adquirir un visión nueva de lo que es la seguridad informática, ubicarse detrás del programa de aplicación y sobre el hardware. Analizar los principios de la seguridad y estudiar las distintas filosofías existentes. Interiorizar dentro de los sistemas informáticos con la finalidad de poder conocer los distintos ámbitos de la seguridad informática y los requerimientos que esta con lleva, resolver los problemas comunes con ingeniera social en espera de que el alumno logre aprender los conceptos detallados en el programa. |

|  |
| --- |
| **TEMAS Y SUBTEMAS**  **UNIDAD I. ¿Qué es un hacker?**   1. Que es un hacker? 2. Tipos de hacker 3. Sistemas Operativos 4. Conceptos basicos de Networking 5. Instalacion de entornos virtuales 6. Conociendo VMware 7. Corriendo sistemas operativos simultaneamente 8. Creando maquinas virtuales 9. Configuracion NAT y Bridged 10. Instalacion de diferentes OS para pruebas 11. Instalacion de entorno Apache, php y mysql en Windows 12. Instalacion de Perl 13. Instalacion de Phyton 14. Comandos de consola cmd y terminal   **UNIDAD II. Hackeo y Defensa de Paginas Web**   1. Information Gathering 2. Frameworks de explotacion via Browser 3. Ataques XSS (Cross Site Scripting) 4. Ataques de ejecucion remota 5. Elaboracion de exploits con Phyton 6. Herramientas de escaneo de vulnerabilidades 7. Shells PHP 8. Remote File Inclusion 9. Wargames 10. Cross Site Request Forgery 11. Ataques de estres DoS   **UNIDAD III. Man in the Middle**   1. Definicion MITM 2. ARP Poisoning 3. Interceptar datos via Browser 4. Modificacion de Cabezeras 5. Interceptar datos de un binario 6. Ataques de red local 7. Atacando a Windows 7 desde BackTrack 8. Atacando a BackTrack desde Windows 7 9. Credential Harvesting 10. Ataques automatizados   **UNIDAD IV. Metasploit**   1. Armitage 2. Social Engineering ToolKit 3. Vectores de Ataque 4. Hacking Mysql Servers con metasploit 5. Hacking XAMPP con metasploit 6. Brute Force al ssh de iPhone/ipad/ipodTouch   **UNIDAD V. SQL Injection**   1. Inyección SQL . ¿Qué es? 2. Factores que propician esta vulnerabilidad 3. Instalación de la herramienta SQL MAP 4. Instalación de Phyton (Windows) 5. Conociendo la herramienta SQL MAP 6. Conociendo a nuestro objetivo 7. Nmap Scanner 8. Whois 9. Obtención de Mails mediante script en phyton 10. Obtención de Datos de Mysql 11. Obtención de Usuarios 12. Buscando el Panel de Administración 13. Instalando el Entorno grafico de “SQL-Map”   **UNIDAD VI. Android Hacking**   1. Consola de Metasploit 2. búsqueda de módulos y exploits para Android 3. Creación de un “.Apk” infectado para su instalación en un sistema Android 4. Instalación del “.Apk” (intervención del usuario) 5. Explotación Local y Remota 6. Acceso local al dispositivo 7. Manejo de la sesión “meterpreter” en el Dispositivo infectado 8. Conociendo las cámaras de fotografía del dispositivo 9. Tomando fotografías con el Dispositivo (cámara frontal y delantera) 10. Robo de información , fotografías , bd de whatsapp (en caso de tener) 11. Explotación Remota 12. Conociendo nuestra infraestructura (proveedor de servicio , Modem , Velocidad de conexión) 13. Conociendo el Servicio No-ip + creación y configuración de nuestro modem 14. Explotación 100% remota. |
|  |

|  |
| --- |
| **ACTIVIDADES DE APRENDIZAJE**  **Frente a Docentes**   * El método general de trabajo es el de clases teórico-prácticas que propicien la participación y el trabajo grupal. * Se aplicara un sistema de trabajo en donde se acompañara el desarrollo de los contenidos principales a través de clases expositivas a cargo del docente. * Clases prácticas: presentación de seguridad informática manejo de terminal con los comandos básicos. * Problemas de seguridad clásicos, manejo de programas de seguridad informática * Resolución de ejercicios de situaciones comunes * Películas y/o videos de acorde al temario * El docente propondrá lectura y se formara un debate con la temática del tema investigado.   **Independientes**   * Desarrollo de investigaciones en internet * Resolución de cuestionarios * Desarrollo de proyecto de investigación |

|  |
| --- |
| **CRITERIOS Y PROCEDIMIENTOS DE EVALUACIÓN Y ACREDITACIÓN**   * Aplicación de tres exámenes parciales y un final * Presentación de las investigaciones * Presentación de las practicas realizadas en laboratorio * Presentación de los cuestionarios teoricos |

|  |
| --- |
| **BIBLIOGRAFÍA**   * GABRIEL BACA URBINA, INTRODUCCION A LA SEGURIDAD INFORMATICA * JULIAN METCALFE, ¿QUE ES LA SEGURIDAD INFORMATICA? * Ester Chicano Tejada, Gestión de incidentes de seguridad informática. |

|  |
| --- |
| **PERFIL DEL CATEDRÁTICO**   * Licenciatura en sistemas computacionales, ciencias de la computación y áreas a fines |