Propuesta de actividades #CyberCampULPGC para centros educativos

La Escuela de Ingeniería Informática de la Universidad de Las Palmas de Gran Canaria está preparando una serie de talleres prácticos sobre ciberseguridad para el cuso académico 2023/2024. Estas actividades, englobadas dentro del programa #CyberCampULPGC que organizamos en colaboración con el Instituto Nacional de Ciberseguridad (INCIBE), tienen como objetivo sensibilizar en materia de ciberseguridad en los distintos niveles educativos, fortaleciendo y mejorando las capacidades de los participantes en esta materia.

Este documento constituye el catálogo de talleres prácticos que ofrecemos a los centros educativos. Estos talleres están diseñados por profesionales del sector para que los participantes desarrollen competencias digitales en materia de ciberseguridad, de forma dinámica e interactiva, realizando actividades apropiadas para su nivel educativo. Cada taller está descrito con detalle en las siguientes páginas del documento, incluyendo el grupo de edad concreto al que está dirigido:

- **#1:** De mayor quiero ser influencer. Edades entre 6 y 12 años.
- **#2:** Fomentando una navegación segura en el mundo digital. Edades entre 8 y 12 años.
- **#3:** Configuración segura de mi primer móvil. Edades entre 12 y 16 años.
- **#4:** Ciberseguridad a nuestro alcance: securizando nuestro entorno. Edades de 14 años en adelante.
- **#5:** Experiencias de Pentesting – Google Dorking. Edades de 14 años en adelante.
- **#6:** Iniciación al apasionante mundo del OSINT. Edades de 16 años en adelante.
- **#7:** Desmitificando la Deep Web. Edades de 18 años en adelante.
- **#8:** Experiencias de Pentesting – ataques de fuerza bruta. Edades de 18 años en adelante.
- **#9:** Experiencias de Pentesting – gestión de vulnerabilidades. Edades de 18 años en adelante.
- **#10:** Experiencias de Pentesting – password cracking. Edades de 18 años en adelante.
- **#11:** Experiencias de Pentesting – explotación de vulnerabilidades. Edades de 18 años en adelante.
- **#12:** Esquema Nacional de Seguridad – Gobernanza µCeENS. Edades de 18 años en adelante.

Los talleres se celebrarán durante un periodo de seis semanas que comenzará el lunes 16 de octubre de 2023 y concluirá el viernes 24 de noviembre. La duración estimada de todos los talleres será de tres horas. La fecha concreta y el horario de celebración de cada taller se fijarán de mutuo acuerdo con los centros educativos interesados. Todas las actividades se desarrollarán en las instalaciones de la Escuela de Ingeniería Informática en el Campus Universitario de Tafira. El laboratorio destinado a la celebración de los talleres cuenta con 14 puestos de trabajo, por lo que el número máximo de participantes en cada taller será de 28 personas, asumiendo que en cada puesto haya dos personas.

Los talleres serán completamente gratuitos, no supondrán coste alguno para los participantes, aunque los gastos de transporte hasta y desde las instalaciones de la Escuela correrán a cargo de los participantes o de los centros educativos. El tiempo de desplazamiento debe tenerse en cuenta a la hora de acordar el horario de los talleres. De acuerdo con experiencias previas, especialmente cuando los centros organicen el transporte de los participantes, recomendamos celebrar los talleres en turno de mañana en horario de 10:00 a 13:00.

Si tienen interés en participar y quieren concretar la celebración de un taller, deben ponerse en contacto con nosotros en la dirección de correo electrónico cybercamp@ulpgc.es lo antes posible. El número de ediciones de cada taller está limitado y la asignación de fechas se hará por estricto orden de llegada de las solicitudes. Por supuesto, estamos a su disposición para cualquier consulta que quieran realizar.

Estas iniciativas se realizarán en el marco de los fondos del Plan de Recuperación, Transformación y Resiliencia, financiadas por la Unión Europea (Next Generation), el proyecto del Gobierno de España que traza la hoja de ruta para la modernización de la economía española, la recuperación del crecimiento económico y la creación de empleo, para la reconstrucción económica sólida, inclusiva y resiliente tras la crisis de la COVID19, y para responder a los retos de la próxima década.

Taller #1: De mayor quiero ser influencer

Edades: entre 6 y 12 años

Niños, niñas y adolescentes son seguidores habituales de personajes con cierto tirón en Internet, blogueros, youtubers o instagramers entre otros. A veces se ven fascinados por esas profesiones, su fama y reconocimiento, sin ser plenamente conscientes de las circunstancias que rodean a estas personas, el esfuerzo y dedicación necesarios, o los riesgos y problemas a los que se enfrentan.

La mayoría de las redes sociales son gratuitas. Esto solo es posible si son capaces de monetizar los datos personales y la información de perfil de los usuarios, fundamentalmente a través de la publicidad. Cuantos más datos personales se expongan en las redes sociales, mayor será el riesgo de que los empleen para dirigir publicidad más personalizada o vender perfiles comerciales.

Las redes sociales son un espacio de comunicación complejo, donde pueden surgir problemas y situaciones de peligro para un menor. Aprender cuales son los riesgos es el primer paso para garantizar su protección. Además, los menores han de moderar la información que publican para evitar la pérdida de privacidad, asegurando el respeto de su propia intimidad y la de los demás.

Por todo ello, en el presente taller se procederá a trabajar conjuntamente con los participantes identificando los distintos riesgos que existen en el uso de las redes sociales y los videojuegos; con el objetivo de concienciar al alumnado y que éste adquiera una serie de competencias que le permitan hacer un uso más seguro de la tecnología.

En la primera parte del taller se procederá a repasar los distintos riesgos asociados al uso de las redes sociales y los videojuegos como pueden ser la suplantación de identidad, el grooming, los bulos y los fraudes, los discursos de odio, etc.

En la segunda parte del taller y para terminar, se procederá a dividir la clase en grupos y se le entregará a cada grupo un juego de cartas relacionadas con la temática con el objetivo final de promover el diálogo abierto y cercano sobre el fenómeno influencer, el uso que hacen los menores de las redes sociales y los riesgos asociados a éstas.

Taller #2: Fomentando una navegación segura en el mundo digital

Edades: entre 8 y 12 años

En esta era digital en constante evolución, es fundamental que los jóvenes adquieran habilidades y conocimientos para navegar de manera segura por Internet. Este taller de ciberseguridad tiene como objetivo empoderar a estudiantes de educación primaria para que se conviertan en usuarios responsables y conscientes de la tecnología. Además, proporcionará a educadores y familias los recursos necesarios para guiarles hacia una experiencia en línea segura y positiva.

Actualmente, los niños desde edades muy tempranas a menudo tienen acceso a dispositivos como tabletas, ordenadores, y smartphones con conexión a internet. Este acceso puede ser beneficioso para el aprendizaje y la creatividad, pero también requiere prestar atención a ciertos aspectos que garanticen un uso seguro y equilibrado de los mismos. Este taller ha sido diseñado para qué los jóvenes de entre 8 y 12 años adquieran habilidades esenciales de ciberseguridad que les servirán para tomar decisiones informadas y responsables en entornos digitales en el presente y en el futuro.

El taller consta de una sesión de 3 horas aproximadamente, en las que se incluye una pausa para desayuno de 20 minutos. Durante el taller se entregará a los estudiantes el material necesario para su desarrollo. También se pondrá a disposición del profesorado una guía de conceptos básicos de ciberseguridad que podrán compartir con las familias.

El taller se llevará acabo de manera interactiva y participativa, utilizando enfoques pedagógicos adaptados a la edad de los estudiantes. La sesión incluirá:

- Actividades prácticas para aprender de manera divertida y atractiva.
- Historias y casos apropiados para la edad.
- Conversaciones guiadas para fomentar la reflexión y el diálogo.
- Materiales didácticos y herramientas para utilizar en el aula.

<u>Módulos del taller:</u>

El taller se dividirá en 6 temáticas principales, centradas en el uso seguro del Internet y las redes sociales. No obstante, el organizador, se reserva el derecho de realizar modificaciones para ajustarlo al perfil del público (teniendo en cuenta la diferencia entre jóvenes de 8 y 12 años) o la evolución de las tendencias en materia de seguridad informática.

- *Haciendo un buen uso de Internet (15 – 20 min.)* ¿Por qué nos conectamos a Internet? ¿Qué aplicaciones utilizamos para ello? A menudo usamos Internet para hacer los deberes, aprender, comunicarnos con amigos, etc. Sin embargo, ¿estamos haciendo un buen uso de las distintas plataformas? En esta sección introductoria buscamos comprender los hábitos de los participantes y fomentar un debate que les permita expresarse y reflexionar sobre sus experiencias en línea.
- *Introducción a la ciberseguridad (10 – 15 min.)* Una vez hayamos conocido el uso que le damos a Internet, adentraremos a los estudiantes en los fundamentos básicos de la ciberseguridad. Abordaremos los posibles riesgos y les proporcionaremos información sobre cómo protegerse de manera efectiva en línea.
- *Redes sociales y juegos online (25 min.)* Las redes sociales y los juegos online ofrecen a los jóvenes la oportunidad de conectarse, expresarse y aprender en un entorno virtual, pero también plantean desafíos en términos de privacidad, seguridad y comportamiento en línea (bullying, grooming, etc.). Enseñar a los jóvenes cómo utilizar estas plataformas de manera adecuada les brindará las herramientas para construir relaciones positivas, comunicarse de manera respetuosa con los demás, discernir entre información confiable y falsa, y salvaguardar su privacidad.

- *Descanso (20 min.)*
- *Privacidad y contraseñas (30 – 40 min.)* Aprender a construir contraseñas seguras y robustas y establecer permisos de acceso, es fundamental para la protección de datos personales, y prevención de robo de identidad y otras amenazas cibernéticas. De la misma manera, es crucial comprender entre información personal y privada.
- *Otros peligros en línea y precauciones (20 min.)* En este apartado buscaremos sensibilizar a los jóvenes acerca de los riesgos a los que se pueden enfrentar en línea y motivarlos a buscar asistencia en caso de ataques cibernéticos o ciberacoso. Al alentarlos a solicitar ayuda en caso de encontrarse en estas situaciones, estamos brindándoles la oportunidad de recibir el apoyo esencial para enfrentar y superar tales desafíos de manera rápida y efectiva. Esta pronta intervención no solo contribuye a minimizar el impacto emocional que estas situaciones podrían ocasionar, sino que también promueve su seguridad y bienestar digital.
- *Antivirus (5 min.)* En esta sección hablaremos de la importancia que tiene el antivirus para ayudar a minimizar los riesgos cibernéticos.
- *Actividades para la puesta en práctica lo aprendido (10 – 15 min.)* Al finalizar los distintos bloques, organizaremos otros juegos y actividades interactivas para que el alumnado ponga en práctica lo aprendido. A través de la gamificación, pretendemos reforzar los conceptos y garantizar una mayor retención de estos.

Taller #3: Configuración segura de mi primer móvil

Edades: entre 12 y 16 años

Normalmente, el primer móvil que llega a nuestras manos suele ser un dispositivo nuevo que no ha sido previamente configurado. Si queremos estar protegidos y evitar tener problemas, hemos de configurar de manera segura el teléfono antes de utilizarlo.

Por otro lado, no es extraño que alguno de los primeros teléfonos móviles que tengamos sea un terminal que hayan utilizado anteriormente alguno de nuestros padres o hermanos mayores. Si bien esta es una opción perfectamente válida y razonable, no obstante, conviene que tomemos algunas precauciones en la puesta a punto del dispositivo para evitar posibles riesgos.

En el presente taller se explicarán los consejos más importantes que debes seguir para mejorar la seguridad y la privacidad de tus dispositivos móviles, ya tengas Android o iOS, como, por ejemplo, cómo proteger el dispositivo con un buen mecanismo seguro de desbloqueo o comprobar que está al día con las actualizaciones, además de cómo realizar copias de seguridad, descargar aplicaciones desde tiendas oficiales o añadir una capa extra de seguridad.

Con estos consejos se puede evitar que cualquiera pueda acceder a la información de tu dispositivo al configurar una contraseña robusta, un patrón, tu huella o tu rostro para desbloquear tu dispositivo y activar la verificación en dos pasos de tus aplicaciones. Al descargar aplicaciones desde Play Store o App Store no correrás el riesgo de instalar malware. Si mantienes tu sistema operativo y tus aplicaciones actualizadas, evitarás vulnerabilidades o agujeros de seguridad; y si ocurre una catástrofe o pierdes tu dispositivo, realizar copias de seguridad periódicas te ayudará a no perder tu información para siempre.

En la primera parte del taller se procederá a repasar conjuntamente con el alumnado los distintos riesgos a los que se enfrentan con el uso de los dispositivos móviles y se cerrará la charla con cinco consejos para mejorar la seguridad y privacidad.

En la segunda parte del taller y para terminar, se le entregará a cada uno de los participantes un dispositivo móvil virtual (en el ordenador) y, a modo de práctica, se procederá, paso a paso, a configurar un dispositivo móvil de manera segura. Para ello se contará también con la asistencia del docente y se seguirán las indicaciones y los consejos impartidos en la primera fase de taller.

Taller #4: Ciberseguridad a nuestro alcance: securizando nuestro entorno

Edades: de 14 años en adelante

Este taller de Ciberseguridad tiene como objetivo acercar a los participantes una serie de conceptos fundamentales de ciberseguridad. Se llevará a cabo a través de módulos dedicados y de ejercicios prácticos, buscando que los asistentes aprendan a identificar y prevenir amenazas comunes como el phishing, asegurar sus equipos y dispositivos móviles, proteger sus cuentas en línea y correos electrónicos, y entender las tecnologías inalámbricas para realizar conexiones seguras. Además, se promoverá una reflexión ética sobre el papel de los hackers y la responsabilidad en línea. Se pretende capacitar a las personas asistentes para protegerse en el ciberespacio y fomentar una cultura de ciberseguridad informada y responsable.

Módulos del taller:

- *Introducción a la Ciberseguridad.* En este primer módulo se introducirán conceptos básicos de ciberseguridad como el modelo de "Seguridad por Capas" y la "tríada CID". Posteriormente se hará una exposición de las amenazas más comunes y del impacto de un ciberataque exitoso. Se finalizará el módulo hablando sobre cómo introducirse a nivel profesional en la ciberseguridad.
- *Información en fuentes abiertas (OSINT).* En este módulo se hablará de los peligros relacionados con la sobreexposición de nuestra vida en internet y sobre cómo puede ser utilizada en nuestra contra.
- *Seguridad en equipos de escritorio.* Exploraremos las mejores prácticas para una navegación segura. Por otra parte, exploraremos el uso de antivirus y se enumerarán diferentes tipos de malware.
- *Seguridad en el correo electrónico.* Aprenderemos a identificar y prevenir ataques de phishing, comprendiendo cómo detectar correos electrónicos maliciosos y proteger nuestra información personal.
- *Seguridad de las cuentas online.* Hablaremos sobre los principales métodos que existen para acceder a nuestras cuentas de manera ilícita y aprenderemos a cómo crear contraseñas robustas y a configurar un sistema de autenticación adicional.
- *Protección de los dispositivos móviles.* Aprenderemos sobre qué implicaciones existen al descargar aplicaciones de terceros aplicando una buena gestión de sus ajustes y permisos.
- *Tecnologías inalámbricas.* Aprenderemos a cómo protegernos en entornos wifi y qué consecuencias puede tener el conectarnos a redes públicas. Introduciremos el concepto de "Red Privada Virtual" (VPN) y en qué escenarios nos es de utilidad.
- *Ser un hacker o un ciberdelincuente.* Para finalizar el taller, reflexionaremos sobre la responsabilidad de ser un hacker o un ciberdelincuente. Abordaremos las posibles implicaciones morales y éticas del hacking creando conciencia sobre el impacto de nuestras acciones en el entorno digital.

Prácticas a realizar por el alumnado:

- Uso avanzado de buscadores para obtener información sensible.
- Uso de herramientas de ingeniería social y de análisis de malware.
- Analizar cabeceras de correo electrónico y llevar cabo la suplantación de remitentes.
- Comprobación de cuentas comprometidas mediante herramientas web.
- Revisión de buenas prácticas en smartphones.
- Instalación de aplicaciones móviles para auditoria WiFi.

Taller #5: Experiencias de Pentesting – Google Dorking

Edades: de 14 años en adelante

Google *Dorks* o *Dorking*, también conocido como Google *Hacking* es una técnica que consiste en aplicar la búsqueda avanzada de Google para conseguir encontrar en Internet información concreta a base de ir filtrando los resultados con operadores conocidos como *Dorks*, que son símbolos que especifican una condición. Por ejemplo, si ponemos en nuestro texto de búsqueda las dobles comillas ("texto"), buscará información que coincida exactamente con el texto, es decir, si buscamos "OSI", nos devolverá el contenido que concuerde exactamente con ese término. A lo largo de este taller te enseñaremos cómo te puede ser útil.

El Google *Dorking* se utiliza para encontrar información oculta que de otro modo sería inaccesible a través de una búsqueda normal en Google. Los *Dorks* de Google pueden revelar información delicada o privada sobre los sitios web y las empresas, organizaciones y personas que los poseen y manejan. Dependiendo de los parámetros utilizados para la búsqueda, los resultados cambiarán, pero podría ser posible identificar información de todo tipo como, por ejemplo:

- Credenciales: usuarios y contraseñas de tus cuentas.
- Contenido audiovisual: fotos y vídeos.
- URLs privadas.
- Documentación sensible: DNI, números de teléfono, otros carnets.
- Información bancaria: números de cuenta o tarjetas.
- Correos electrónicos.
- Acceso a cámaras de seguridad.

Las empresas de seguridad prueban el *Dorking* para entender mejor cómo alguien podría abordar el hackeo de los sistemas. O bien, las empresas pueden utilizar los *Dorks* de Google para encontrar información que pueda aprovecharse en las estrategias de SEO y de marketing de resultados. En definitiva, el uso de *hacks* de Google ayuda a las empresas y a los usuarios a ver exactamente qué tipo de información pueden encontrar los demás sobre ellas (y así saber cuánta información tiene uno expuesta en internet).

Por todo ello, en el presente taller, y haciendo uso del navegador Google; los participantes aprenderán a realizar búsquedas avanzadas en Google, con el objetivo de enumerar diferentes activos del objetivo, buscar versiones vulnerables de dichos activos, conocer datos de interés e incluso encontrar fugas de información del objetivo en cuestión e información sensible de usuarios. Para la realización del taller los participantes dispondrán de un equipo con conexión a Internet y acceso al buscador de Google.

Taller #6: Iniciación al apasionante mundo del OSINT

Edades: de 16 años en adelante

La Inteligencia de Fuentes Abiertas (OSINT) se refiere a la recopilación y el análisis de información obtenida de fuentes de acceso público. Su aplicación abarca desde la identificación de amenazas y la investigación criminal hasta la evaluación de riesgos empresariales y la obtención de información competitiva. En lo referente a la ciberseguridad se pueden ver casos prácticos en los que se necesite descubrir datos sensibles sobre una persona o empresa o descubrir activos que no deberían estar accesibles desde Internet.

Los participantes se iniciarán en un taller totalmente práctico mediante herramientas concretas de distinta índole que son ampliamente usadas de forma profesional en auditorías de seguridad dentro de la fase de "Reconocimiento de Información Inicial".

Módulos del taller:

- *¿Qué es OSINT?* Profundizaremos en el concepto de OSINT y por qué es especialmente relevante en el Pentesting (Test de Penetración) como en una metodología para poder aplicarlo de forma eficiente.
- *Uso de herramientas OSINT.* Instalaremos y utilizaremos más de trece herramientas dedicadas al OSINT que nos permitirán obtener información y datos que ya de por sí podrían ser incluso reportados como un incidente de seguridad.

Practicas a realizar por el alumnado:

- Uso de herramientas OSINT:
    - Búsqueda de versiones de tecnologías web.
    - Exportación y análisis de metadatos.
    - Búsqueda de activos IP.
    - Uso avanzado de buscadores.
    - Enumeración de activos SMB.
    - Búsqueda avanzada de datos personales y de interés.

Taller #7: Desmitificando la Deep Web

Edades: de 18 años en adelante

En el imaginario colectivo, cuando se habla de la Deep Web se le suele relacionar con el mundo del cibercrimen, pero no muchos saben que también es un entorno de gran utilidad. Algunos usuarios la utilizan para proteger su anonimato y salvaguardar su privacidad, ya sea para fines legítimos como la comunicación segura, la investigación académica o el intercambio de información en entornos de comunicaciones restrictivas.

Los participantes de este taller descubrirán cómo acceder a este tipo de redes, cómo funcionan, qué tienen de mito y qué de realidad, cuáles son sus orígenes y qué se puede encontrar en ellas.

Módulos del taller:

- *¿Qué es la Deep Web?* Profundizaremos en qué es y cómo funciona la Deep Web, más en concreto la red TOR, entendiendo su mecánica principal, comparándola con otras herramientas como por ejemplo VPNs y cuestionando su principal característica, que es el anonimato.
- *Buceando en la Deep Web.* Tendremos la oportunidad de probar numerosas herramientas dedicadas al uso e investigación de la Deep Web con el propósito de reforzar los conocimientos adquiridos en el módulo anterior mediante una serie de prácticas.

Practicas a realizar por el alumnado:

- Instalación de TorProject. Descarga, instalación y uso de un navegador web que permite el acceso a la red TOR, crucial para el acceso a la Deep Web.
- Acceso a HiddenWiki. Acceso al portal web por excelencia dentro de la Deep Web, donde pueden encontrarse numerosas páginas web de diversa índole y dudosa legalidad.
- Uso de distribución de linux TAILS. Uso de la conocida distribución de permite navegar por la red TOR con un mayor nivel de anonimato que la que se consigue usando únicamente un navegador web.
- Búsquedas en la Darknet. Acceso a determinados portales web en la Deep Web que permiten hacer búsquedas para encontrar determinadas páginas.
- Uso de Darkdump. Uso de herramientas para la recolección de enlaces de páginas de la Deep Web.
- Uso de DeepDarkCTI. Uso de herramientas de inteligencia sobre ciberamenazas relacionadas con la Deep Web.
- Montaje de servidor web en TOR. Tutorial sobre como montar un servidor web básico accesible de forma “anónima” desde la red TOR.

Taller #8: Experiencias de Pentesting – ataques de fuerza bruta

Edades: de 18 años en adelante

Este tipo de ataque consiste en automatizar los procesos de autenticación sobre un determinado servicio o aplicación con la finalidad de ir probando posibles combinaciones de contraseñas o usuario/contraseña hasta averiguar las credenciales de acceso de algún usuario privilegiado. Para mantener seguras nuestras contraseñas y las de la organización en la que trabajamos, debemos realizar pruebas de Pentesting de forma rutinaria para revelar los puntos débiles. En una prueba de Pentesting se replica de manera controlada el ataque para determinar posibles debilidades en los sistemas de la organización; en este caso, el objetivo será comprometer las credenciales de la organización mediante los ataques de fuerza bruta.

Dependiendo de la tipología de la infraestructura, es posible que existan mecanismos de protección contra este tipo de ataques que interrumpen la conexión si detectan que se están realizando un número de peticiones determinado en un intervalo de tiempo. En estos casos, es necesario comprobar, durante las fases de enumeración y escaneo, si existe algún sistema de protección que actúe de esta manera, con la finalidad de ajustar la intensidad con la que se realizan las pruebas para intentar que pasen desapercibidas.

En este tipo de técnicas, las probabilidades de éxito de localizar credenciales válidas dependen, en gran medida, de la utilización de un buen diccionario de posibles contraseñas para probar. Además, la utilización de un buen diccionario limita el número de peticiones que se van a realizar y reduce el tiempo necesario para localizar las contraseñas.

Por todo ello, en el presente taller, y haciendo uso de la distro Kali Linux y las herramientas “Medusa”, “Ncrack”, “Hydra”, “Patator”, etc. los participantes procederán a ejecutar distintos ataques de fuerza bruta contra varios servicios (ssh, mysql, telnet, etc.) para concienciar en la importancia de tener credenciales robustas y el doble factor de autenticación.

En concreto se realizarán hasta tres tipos de ataque:

- *Diccionario.* Un fichero con contraseñas es cargado en una herramienta que se ejecuta contra la cuenta de un usuario legítimo.
- *Fuerza Bruta.* Se generan todas las posibles combinaciones de caracteres en una longitud de contraseña determinada para luego ejecutarse contra la cuenta de un usuario legítimo.
- *Basados en Regla.* Se generan combinaciones teniendo en cuenta cierta información preliminar que se ha obtenido del usuario legítimo.

Para la realización del taller, los participantes dispondrán de dos máquinas virtuales que han sido previamente configuradas: una máquina virtual (Kali Linux) con todas las herramientas necesarias para el seguimiento del taller y una máquina virtual (Win7) que será contra la que se realizarán las correspondientes pruebas.

Taller #9: Experiencias de Pentesting – gestión de vulnerabilidades

Edades: de 18 años en adelante

El hacking ético incluye el uso de herramientas de hacking, trucos y técnicas para identificar vulnerabilidades y así asegurar la seguridad del sistema. El hacking ético simula las técnicas usadas por los atacantes para verificar la existencia de vulnerabilidades explotables en un sistema de información. Los hackers éticos realizan la búsqueda de vulnerabilidades en las organizaciones con el permiso de las autoridades competentes. El objetivo es descubrir vulnerabilidades en los sistemas de las organizaciones para que puedan ser parcheadas antes de que se produzca un ataque real.

Una evaluación de vulnerabilidades (*vulnerability assessment* en inglés), es un procedimiento que ayuda a las organizaciones a estimar su exposición a las amenazas informáticas. A medida que los hackers hacen que el mundo digital sea cada vez más peligroso, cada vez más organizaciones intentan identificar sus vulnerabilidades en relación con phishing, malware, ataques de DDoS y otras amenazas.

Las evaluaciones de vulnerabilidad se realizan utilizando herramientas de escaneo estándar además de pruebas manuales. La realización de escaneos de vulnerabilidad ayudará a garantizar que cualquier vulnerabilidad existente en su sistema sea identificada y tratada inmediatamente, reduciendo el riesgo o la exposición de la organización a un nivel aceptable.

Por todo ello, en el presente taller, y haciendo uso de la distro Kali Linux y herramientas open source; los participantes procederán a ejecutar evaluaciones de vulnerabilidad internas y de aplicación. En la evaluación interna se procederá a escanear toda la infraestructura (entorno de prueba) para la búsqueda de vulnerabilidades y en la evaluación de aplicación se procederá a realizar un escaneo sobre una App Web para la búsqueda de vulnerabilidades de una aplicación en particular.

Para la realización del taller, los participantes dispondrán de una máquina virtual (Kali Linux) con todas las herramientas necesarias para el seguimiento del taller y un entorno de prueba (infraestructura y App Web) que será contra el que se realizarán las correspondientes pruebas para detectar vulnerabilidades. Las fases de la evaluación serán las siguientes: preparación (elegir el target y las herramientas adecuadas), identificación (lanzar las correspondientes automatizadas y, en su caso, pruebas manuales), análisis (análisis de las vulnerabilidades detectadas), evaluación (evaluar el riesgo de explotación de las vulnerabilidades encontradas teniendo en cuenta el contexto en cada organización) y reporte (documentar las vulnerabilidades encontradas).

Taller #10: Experiencias de Pentesting – password cracking

Edades: de 18 años en adelante

La técnica del password cracking consiste en intentar utilizar los hashes de las contraseñas para averiguar las contraseñas en texto claro. La mayoría de estos ataques prosperan debido a la debilidad de las contraseñas utilizadas o a que son fáciles de usar. Para mantener seguras nuestras contraseñas y las de la organización en la que trabajamos, debemos realizar pruebas de Pentesting de forma rutinaria para conocer el nivel de robustez del cifrado. En una prueba de Pentesting se replica de manera controlada el ataque para determinar posibles debilidades en los sistemas de la organización; en este caso, el objetivo serña comprometer el encriptado de las credenciales.

Por definición, un hash no se puede revertir a su contraseña en texto claro, la única manera de averiguar la contraseña inicial con la que se generó ese hash consiste en probar posibles combinaciones de contraseñas y aplicar el mismo algoritmo de hash empleado por el protocolo de hashing utilizado para almacenar la contraseña. En caso de que los hashes coincidan, significará que habremos averiguado la contraseña, ya que generará el mismo hash.

Existen varias aplicaciones que pueden realizar cracking de distintos tipos de hashes, pero en el presente taller trabajaremos con las más utilizadas debido a la cantidad de algoritmos de hashes que soportan, la posibilidad de paralelismo o las capacidades de utilizar procesamiento GPU para realizar los cálculos de hashing.

Por todo ello, en el presente taller, y haciendo uso de la distro Kali Linux y herramientas open source, los participantes procederán a ejecutar ataques de password cracking (descifrado de hashes) para entender el concepto de “cifrado de contraseña” y concienciar en la importancia de tener credenciales robustas.

En concreto las herramientas que se utilizarán:

- *John the ripper.* Es una herramienta de cracking de contraseñas. Existen dos versiones, la versión normal y la versión jumbo o community, que soporta muchos más algoritmos de hashing para realizar el proceso de cracking. Además, soporta paralelización de procesos, pudiendo indicar el número de núcleos de CPU que se le asignan al proceso de cracking.
- *Hashcat.* Es una herramienta de cracking de contraseñas. Soporta muchos más algoritmos de hashing que John para realizar el proceso de cracking, lo cual la dota de mayor versatilidad. Además, soporta el uso de procesamiento GPU, utilizado en las tarjetas gráficas, mucho más rápido que el uso de procesadores CPU convencionales.

Para la realización del taller, los participantes dispondrán de dos máquinas virtuales que han sido previamente configuradas: una máquina virtual (Kali Linux) con todas las herramientas necesarias para el seguimiento del taller y una máquina virtual (Win7) que será contra la que se realizarán las correspondientes pruebas para obtener y descifrar sus hashes.

Taller #11: Experiencias de Pentesting – explotación de vulnerabilidades

Edades: de 18 años en adelante

Tras la identificación de vulnerabilidades en los servicios identificados en las fases descritas en las Experiencias de Pentesting anteriores (ver tallleres #5, #8, #9 y #10), el siguiente paso es explotarlas con el objetivo de mostrar el riesgo real de la vulnerabilidad. Un exploit es un software o técnica que permite explotar o aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo. La explotación es una fase vital en la ejecución de un test de intrusión, ya que nos permite evaluar el riesgo real de la vulnerabilidad, tanto en información obtenida como en la posibilidad de saltar o pivotar hacia otros sistemas.

Metasploit es una plataforma avanzada de código abierto para desarrollar, probar y utilizar código de explotación escrito en Ruby. Contiene herramientas de desarrollo orientadas a explotar vulnerabilidades. Los frameworks estandarizan la sintaxis de uso de exploit y proporcionan capacidades dinámicas de código shell. Esto significa que, para cada exploit en el framework, se pueden seleccionar diferentes payloads, como una bind shell, una reverse shell, descarga y ejecución de Shell codes, etc.

Este framework cuenta con más de 1000 exploits para diferentes plataformas y arquitecturas. Aún así, Metasploit es mucho más que una simple colección de exploits, también es una base sólida que se puede aprovechar y personalizar fácilmente para satisfacer las necesidades de un auditor. Por ello, es una de las herramientas de auditoría de seguridad más útiles disponibles gratuitamente para los profesionales de la seguridad en la actualidad. Desde una amplia gama de exploits de grado comercial y un amplio entorno de desarrollo de exploits, hasta herramientas de recopilación de información de red y complementos de vulnerabilidad web, Metasploit Framework proporciona un entorno de trabajo realmente impresionante.

Por todo ello, en el presente taller, y haciendo uso de la distro Kali Linux y el framework de Metasploit, se procederá a explotar una serie de vulnerabilidades con el objetivo de conseguir un comportamiento indeseado del objetivo. En concreto, se explotarán vulnerabilidades conocidas del sistema operativo Windows, lo que le permitirá a los participantes tomar el control de la máquina objetivo. Uno de los exploits que se utilizarán es el conocido como Ethernal Blue; desarrollado por la NSA. Fue filtrado por el grupo de hackers The Shadow Brokers el 14 de abril de 2017 y fue utilizado en el ataque mundial de ransomware con WannaCry del 12 de mayo de 2017.

Para la realización del taller, los participantes dispondrán de una máquina virtual (Kali Linux) con todas las herramientas necesarias para el seguimiento del taller y un entorno de prueba (máquina objetivo con vulnerabilidades conocidas) que será contra el que se realizarán las correspondientes pruebas para explotar vulnerabilidades.

Taller #12: Esquema Nacional de Seguridad – Gobernanza µCeENS

Edades: de 18 años en adelante

El Esquema Nacional de Seguridad es una Ley de obligado cumplimiento para las Administraciones Públicas y sus proveedores de servicios tecnológicos. Para ello, se establecen una serie de medidas que garantizan la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, permitiendo el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

El esquema establece la política de seguridad en la utilización de medios electrónicos y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de los sistemas de información, los servicios y su información.

µCeENS es una metodología innovadora que nos brinda el proceso completo para obtener la adecuación y la correspondiente Certificación de Conformidad en el ENS, de acuerdo a un Perfil de Cumplimiento (PCE), que se complementa con los servicios de seguridad proporcionados por las herramientas del CCN-CERT, todo ello automatizado en las herramientas de Gobernanza INES y AMPARO.

Estas herramientas han sido desarrolladas por el CCN-CERT para poner a disposición de las entidades públicas y privadas herramientas de apoyo para la Adecuación al ENS, la obtención y gestión de las Declaraciones o Certificaciones de Conformidad con el ENS y la gestión de las correspondientes evidencias que, junto al resto de soluciones del ecosistema de herramientas del CCN-CERT, contribuyen a la Gestión Continua de la Ciberseguridad.

En cuanto a las funcionalidades de las herramientas mencionadas:

- *INES.* Esta plataforma permite la recogida de información organizada, delegada y supervisada de forma continua a lo largo de todo el año, de tal manera que cada organización puede acceder, completar o consultar sus datos en cualquier momento y ver su evolución.
- *AMPARO.* Se trata de una solución que incorpora diversas funcionalidades para facilitar los procesos de auditoría de conformidad, evaluando automáticamente la adecuación del sistema y facilitando la gestión de la Certificación de Conformidad.

El objetivo del presente taller es explicar cómo la metodología µCeENS posibilita que los sistemas de información de organizaciones con limitaciones para abordar por sí solas el proceso de adecuación puedan obtener la Certificación de Conformidad en el Esquema Nacional de Seguridad (ENS) en base a un Perfil de Cumplimiento Específico (PCE).