GRANADA

CIENCIA ABIERTA

UNIVERSIDAD DE GRANADA | DEPARTAMENTO DE Didáctica DE LAS Ciencias Experimentales

● Los estudiantes descubrieron las muchas vulnerabilidades existentes en nuestro propio sistema

DISEÑO DE IMAGEN: MODESTO MARTÍNEZ PALENZUELA

Primer concurso de **ciberseguridad** IES Zaidín-Vergeles

EL curso de especialización en Ciberseguridad en Entornos de las Tecnologías de la Información (TIC) fue anunciado por el Ministerio de Educación en verano de 2019. El 7 de abril de 2020 se publica en BOE el título LOE correspondiente. Se trata de una especie de 'master' que viene a cubrir un ámbito tan específico, novedoso y demandado como es el de la ciberseguridad informática. Esta formación, cuya duración es de 720 horas, habilita al alumnado para desempeñar salidas profesionales como pueden ser: experto, auditor, perito forense o consultor en ciberseguridad informática.

"El curso de especialización en ciberseguridad en entornos TIC ha supuesto un reto personal tanto para el alumnado como para el profesorado en cuanto a formación y actualización de conocimientos. Durante el curso 2020-21, el profesorado del curso de especialización, además de impartir la formación, ha recibido formación por medio de tres cursos, capacitados tanto por el centro de formación del profesorado como por empresas específicas del sector", declara José Luis Navarro, profesor de Análisis Forense Informático.

El objetivo era hacer una auditoría a los sistemas de infomática del centro para descubrir errores

Para José Luis Berenguel, profesor de Hacking ético y tutor del grupo, lo más importante es que "este curso de especialización es solo la punta del Iceberg de los conocimientos que debe tener un experto en ciberseguridad o pentester. Son necesarios conocimientos de redes, arquitectura de computadores, programación, protocolos de comunicación y otros muchos que engloban todo el campo de la informática, y que permite a un buen auditor ganarse la vida descubriendo nuevas vulnerabilidades en el software, y para ello se requieren varios años de estudio y experiencia".

En septiembre del curso 2020-2021 se comenzó a impartir en el IES Zaidín-Vergeles el curso de especialización en ciberseguridad. Al final de su preparación, entre el 21 de mayo y el 13 de junio, el alumnado del curso de especialización participó en el primer concurso de ciberseguridad del IES Zaidín-Vergeles. El objetivo del concurso era realizar una auditoría o 'ataque ficticio' a los sistemas de informática del Centro con la intención de descubrir posibles errores, vulnerabilidades y/o fallos de seguridad para posteriormente introducir mejoras que permitan prevenir futuros ciberataques, a la vez que se fomentaba el espíritu investigador y la ética hacker. El alumnado participante se comprometió a minimizar el efecto que podrían tener sus acciones en el normal desarrollo de la actividad de los servidores del centro, y también, en mantener celosamente la privacidad de la información personal que fueran capaces de recabar.

Efrén García Férez (primer premio), Antonio Gallego López (segundo) y Mariano Terrón Torres (tercero) fueron respectivamente los ganadores del concurso del actual curso académico. Además, el alumnado ganador realizó una exposición pública al alumnado y profesorado del Departamento de Informática, en la que explicaron los hallazgos detectados. Cabe destacar, que fueron capaces de:

- Realizar un ataque DOS (*denial of service* o denegación de servicio) a la plataforma educativa Moodle y conseguir que dejara de funcionar.
- Explotar una vulnerabilidad detectada en la plataforma educativa Moodle, la cual permitía robar las *cookies* de sesión del alumnado/profesorado y acceder con sus usuarios.
- Extraer información personal (nombre, apellidos, email) del profesorado, poniendo de manifiesto el riesgo que se corría a un posible filtrado de datos (data leak).
- Determinar los DNI al completo del alumnado y suplantar su identidad en nuestra bolsa de empleo.
- Suplantar la identidad del profesorado en nuestra aplicación de mantenimiento para indagar en los partes ya resueltos y obtener así las credenciales de algunos de los equipos del IES (*data breach*).
- Obtener documentos confidenciales escaneados por el profesorado en la fotocopiadora del Centro.
- Realizar un ataque de amplificación de fuerza bruta contra el blog de noticias basadas en Wordpress.
- Detectar una vulnerabilidad de Wordpress en la web del centro que permitiría a un ciberdelincuente utilizar nuestro hosting para atacar a otras webs (Botnet).

Os contamos algunos secretos de ciberseguridad que los ganadores del concurso han querido compartir con los lectores de Ciencia Abierta:

¿Qué destacarías del curso de especialización?

Antonio: "El curso de especialización aporta una base desde la que poder partir y seguir investigando por tu cuenta; me ha ayudado a ser más autodidacta, lo cual es un valor que es muy importante en este campo".

¿Cuánto tiempo te ha llevado 'asaltar' la web de vuestro IES?

Efrén: "Desde la primera toma de contacto hasta terminar el reporte de la, aproximadamente unas 50 horas. Es un trabajo que requiere de tiempo, habilidades y dedicación".

¿Es posible 'hackear' cualquier web?

Efrén: "Pienso que sí, aunque no en un periodo de tiempo aceptable. No sólo páginas web, además Internet, entendido como toda la red, se ha puesto en peligro varias veces, tan solo no ha tenido repercusiones por la rápida actuación de las organizaciones encargadas de arreglarlo. El tiempo es un factor principal a tener en cuenta. El avance de las tecnologías y el hardware hacen que aquello que era seguro hace un tiempo se vuelva vulnerable. Para crackear una contraseña en 2008 se necesitarían meses, cuando ahora tardaríamos cuestión de minutos. Debemos tomar la seguridad como una probabilidad, no una medida, ya que nada es seguro al cien por cien. Pensar que algo es completamente seguro además genera una falsa sensación de confianza que constituye un peor remedio".

¿Qué piensas del nivel de seguridad de las instituciones, organismos y empresas españolas?

Antonio: "Sólo tenemos que leer las noticias sobre ciberataques para ver como está. Por ejemplo, da mucho que pensar que el SE-

JOSÉ LUIS NAVARRO GALINDO

PE sea atacado debido a que usan servicios ya anticuados, con vulnerabilidades reportadas hace tiempo y no reparadas; tampoco disponían de ningún *backup* reciente y tuvieron que recurrir a páginas externas para recuperarse. En general, las instituciones españolas tienen un bajo nivel en ciberseguridad; se tiene la percepción de que un informático sirve y puede hacer todo a la vez y es un gran error".

¿Cuáles suelen ser las vulnerabilidades más comunes?

Antonio: "Hay vulnerabilidades muy comunes que son las que suelen explotar los ciberdelincuentes. Si consultamos el Top OWASP 2021 (es el top de vulnerabilidades ordenadas estadísticamente) nos damos cuenta de que tenemos las más frecuentes son: inyecciones de comandos, seguidas de autenticaciones rotas, ataques XSS y, por último, filtraciones (*leaks*). Cuando se exponen datos sensibles podemos ser víctimas de un posible ataque que alguien vaya a aprovecharse de una vulnerabilidad, hasta que se demuestra con consecuencias catastróficas".

José Luis Berenguel
Tutor del grupo

"Este curso es sólo la punta del iceberg de lo que ha de conocer un experto en ciberseguridad"

que, sobre todo si la empresa que ha sufrido la filtración no ha cambiado las credenciales expuestas".

Efrén: "Hay una lista de vulnerabilidades más frecuentes, pero creo que depende en gran medida de la organización. Por ejemplo, hay muchas instituciones públicas que pueden ser vulnerables a SQLi, *exploits* y otras simples resueltas años atrás, pero que todavía no se han corregido por la dejadez y falsa confianza. Siempre parece imposible

EFE

Los ganadores del concurso junto al autor del artículo.

¿A la hora de navegar, qué pautas de seguridad recomendáis a un usuario normal?

Antonio: "Yo creo que la primera y fundamental es navegar siempre bajo el protocolo HTPPS ya que nos garantiza que la información viaja cifrada. Tampoco debemos conectarnos nunca a una Wi-Fi abierta, sobre todo en sitios públicos, ya que puede ocurrir que los ciberdelincuentes estén 'escuchando' la información privada que nosotros consultamos. Otro consejo es utilizar contraseñas fuertes y robustas, esto es, evitar utilizar nuestro nombre en y añadirle un par de números y símbolos. Por último, recomiendo tener mucho cuidado con los correos que nos llegan a nuestro buzón de entrada, los ciberdelincuentes intentarán hacerse pasar por alguien de confianza (*phishing*);ante la más mínima duda recomiendo borrar dicho correo y, por supuesto, evitar pinchar en ningún enlace que pueda contener".

Efrén: "El mayor peligro siempre se encuentra en los usuarios, ya que la mayoría veces caemos en trampas relacionadas con la ingeniería social, como por ejemplo, supuestos programas que limpian tu equipo de virus, aunque en realidad no haya alguno. Si se trata solo a la hora de navegar, considero que lo que más debemos tener en cuenta es nuestra privacidad, preguntarnos si realmente nuestros datos, tanto el contenido público en redes sociales como contraseñas privadas, podrían tener un impacto negativo sobre nosotros. Actualmente los datos de los usuarios son el recurso más valioso de la red, y el uso que se le da por terceros puede no ser de nuestro agrado. Además, diariamente hay brechas de organizaciones grandes donde se exponen públicamente o venden en subastas nuestros datos como pueden ser contraseñas, fechas de nacimiento y dirección, entre otras. Cambiar las contraseñas habitualmente es un consejo simple y eficaz".

▸**José Luis Navarro Galindo.** Doctor en Informática. Profesor de Sistemas y Aplicaciones Informáticas en el IES Zaidín-Vergeles.