CASO PRÁCTICO 2 – ASPECTOS ÉTICOS DE LA CIBERSEGURIDAD

CONTEXTO

Es imprescindible que tengáis la capacidad de emitir juicios críticos sobre situaciones que pueden ser ambiguas o éticamente discutibles. Sobre todo, a partir del curso próximo cuando comencéis a adquirir competencias en seguridad ofensiva.

FORMA DE TRABAJAR

En equipos de cuatro personas (dos parejas), yo os asigno un tema. Cada pareja dentro del equipo tiene que argumentar a favor de una posición diferente (una a favor del SI, otra a favor del NO). Esto son dos bloques del entregable: a favor, en contra. Y hay que trabajar un tercer bloque con unas conclusiones. Los argumentos tienen que basarse en una fase de documentación (lecturas, charlas, vídeos, noticias, etc.). Por lo tanto, es necesario que incluyáis una sección de Bibliografía completa y actualizada en el entregable, que consiste justo en esta Bibliografía y en un vídeo en el que expongáis los tres bloques ya comentados.

TEMAS

1. Hack back (identificar el origen de un ciberataque y contra-atacar, legítima defensa).
   https://www.theregister.com/2019/08/27/nato_repeats_article_5_cyber_attack_bombast_again/
2. Enseñanza de seguridad ofensiva desde el bachillerato (CTFs, bug bounties, ejercicios gamificados, etc.).
   https://www.business-live.co.uk/technology/students-recruited-ethical-hacking-boost-22061760
3. Inclusión del hacking ético como delito en la legislación.
   https://www.legaltoday.com/practica-juridica/derecho-penal/penal/delito-de-hacking-y-comentario-de-sentencia-2021-04-16/
4. Full disclosure de vulnerabilidades (publicación de nuevas vulnerabilidades en redes sociales e Internet de manera masiva: see something, say something).
   https://www.theregister.com/2021/09/24/apple_zeroday/
5. Pago de rescates para desmontar mafias de ransomware o que alquilan botnets.
   https://apnews.com/article/technology-joe-biden-europe-business-government-and-politics-cd21d84b5fd070421f871610b40e91d0
6. Exigencia de responsabilidades a los proveedores que alojan o almacenan materiales ilegales (material de hacking, pornografía infantil, etc.).
   https://portswigger.net/daily-swig/insider-phd-hacking-education-channel-suspended-from-youtube-for-severe-guideline-violations
   https://www.nytimes.com/2021/08/05/technology/apple-iphones-privacy.html
7. Puertas traseras en productos criptográficos (para poder investigar crímenes si es necesario, por ejemplo).
   https://www.cloudwards.net/encryption-backdoors/