Máster Interuniversitario en Seguridad de las TIC (MISTIC)

Identidad Digital – 1er semestre, curso 2019-20

Segunda Prueba de Evaluación Continuada (PEC2)

Recursos

- Para resolver la prueba podéis consultar los materiales de la asignatura que están a la sección de Recursos del aula del campus virtual.
- Para cualquier duda y/o aclaración sobre el enunciado, tenéis que dirigiros al consultor responsable de vuestra aula.
- También podéis consultar fuentes externas.

Formato y fecha de entrega

- Se tiene que entregar la solución en un archivo en **formato PDF**.
- La fecha de entrega es: **2 de enero de 2020, 23:59, AoE (Anywhere on Earth)**
- Las PECs entregadas fuera del plazo establecido no se puntuarán y constarán como no presentadas.

Criterios de valoración

- **Razonad la respuesta en todos los ejercicios e indicar todos los pasos que habéis realizado para obtener la solución.**
- Se valorará la claridad de la información aportada, el estilo comunicativo empleado, y la capacidad de síntesis.
- **Las respuestas sin justificación, que sean una copia de una fuente de información y/o que no contengan las referencias utilizadas, no recibirán ninguna puntuación.**
- Si se detecta una copia de la PEC, esta será evaluada con una D y la incidencia será notificada a la dirección del Máster para actuar en consecuencia.
- El valor de esta PEC es del 40% de la nota global de PECs de la asignatura y, por lo tanto, **corresponde al 16 % de la nota final de la asignatura**.

Nombre y Apellidos:

Ejercicio 1 (2,5 puntos)

Tal como se explica a los materiales del curso, la red Tor es una conocida herramienta que permite anonimizar el tráfico de datos entre dos nodos situados de forma remota en Internet. Una utilidad habitual de esta herramienta es la de esconder la IP de un cliente que se conecta a un cierto servidor Web. No obstante, Tor también permite crear los llamados *hidden services,* los cuales son servidores web ocultos que ofrecen servicios sin hacer pública su localización (el cliente no conoce la IP del servidor web). *The Silk Road*, un mercado virtual de productos ilegales que fue clausurado por el FBI, es un ejemplo claro de servicio oculto.

a) (0.5 puntos) Describe brevemente y expone las diferencias de deep web, dark web y dark net.

b) (0.75 puntos) Compara Epicbrowser con TOR browser. ¿Qué ventajas en privacidad y anonimato ofrecen?

c) (0.75 puntos) Describe y compara los proyectos TOR y Freenet.

d) (0.5 puntos) Que es un TOR relay, describe los distintos tipos y comenta que información sobre la conexión ver cada uno de ellos al usar TOR para acceder a la internet convencional.

Ejercicio 2 (2,5 puntos)

Los estándares para la gestión de identidades federadas definen diversos protocolos de autenticación y autorización, cada uno con distintas particularidades que los hacen más adecuados para una u otra situación. En este ejercicio analizaremos el flujo de comunicaciones y/o mensajes entre cliente, servidor y servicio de autenticación/autorización de algunos de estos protocolos o estándares concretos.

a) (0.75 puntos) Definid y explicad el flujo de comunicaciones y/o mensajes entre cliente, servidor y servicio de autenticación/autorización para el estándar **Security Assertion Markup Language (SAML)**

b) (0.5 puntos) Exponed brevemente las diferencias y similitudes entre SAML y el protocolo CAS usado en la practica2.

c) (0,5 puntos) Definid para qué sirve el estándar **WebAuthn**, recientemente aprobado, i los principios básicos de su funcionamiento.

d) (0.75 puntos) Definid y explicad el flujo de comunicaciones y/o mensajes entre cliente, servidor y servicio de autenticación/autorización para el protocolo de autenticación **Kerberos**

Ejercicio 3 (2,5 puntos)

Cada vez que se accede a una página web, el proveedor de esa web puede hacer uso de mecanismos como galletas (cookies), balizas web (web beacons) o tecnologías similares. Normalmente, estos mecanismos tienen fines publicitarios o de personalización para ofrecer una mejor experiencia de usuario pero en algunos casos pueden suponer un problema de seguridad. En este ejercicio analizaremos algunas de estas técnicas:

a) (0,5 puntos) En la práctica, algunas empresas se dedican a rastrear los hábitos de los usuarios mediante las galletas dichas de “terceros”. Explica cómo funciona este mecanismo de seguimiento y por qué puede afectar duramente a la privacidad de los usuarios.
b) (0,5 puntos) Explica qué es una baliza web (“web beacon” en inglés). Pon un ejemplo y di cuales son los usos más frecuentes.
c) (1,5 punto) Además de las galletas de "terceros", los sitios webs utilizan diferentes técnicas para poder registrar las visitas de los diferentes usuarios y comprender en profundidad sus patrones de uso (por ejemplo, para poder ver qué páginas web son populares, el efecto de las campañas de publicidad en línea etc.).

Instálate el complemento "Ghostery" en tu navegador habitual (está disponible para los navegadores Opera, Firefox, Google Chrome, Safari e Internet Explorer). Para ello, es necesario que visites el sitio web https://www.ghostery.com/try-us/download-browser-extension/. Una vez hecho el ejercicio, lo podrás desinstalar sin ningún problema.

Una vez lo tengas instalado en tu navegador, debes acceder a un conjunto de páginas web y registrar la información sobre los trackers que encontrarás en la extensión en la pestaña “Detailed View”. Debes visitar y documentar:

- 5 páginas web de periódicos o sitios de noticias.
- 6 páginas web de universidades, entre ellas www.uoc.edu, www.urv.cat y www.uab.cat.
- 3 redes sociales.
- 3 tiendas online.

Sois libres de ampliar el número de páginas web visitadas para mejorar los resultados obtenidos.

Una vez recogida toda esta información, comenta los resultados obtenidos. En tu análisis debes comentar, al menos:

- Qué tipo de páginas incluyen mayor seguimiento.
- Todas las páginas del mismo “tipo” incluyen o no el mismo tipo de seguimiento.
- Qué resultados te han sorprendido y cuáles de ellos no te han sorprendido, expón tus razones.

Ejercicio 4 (2,5 puntos)

En las siguientes páginas web se describe el concepto de 'browser fingerprinting':

- https://restoreprivacy.com/browser-fingerprinting/
- https://pixelprivacy.com/resources/browser-fingerprinting/

Leed el contenido de los enlaces y responded a las siguientes preguntas:

a) (0,5 puntos) Explica en qué consiste el "browser fingerprinting" según tus propias palabras y que implicaciones tiene para la privacidad. Puedes complementar la definición con información de otros artículos o de otras páginas web.

b) (1 punto) Utiliza alguno de los proyectos descritos en estas webs (por ejemplo **https://panopticlick.eff.org**) para generar la huella de tres navegadores diferentes (por ejemplo, Chrome, Firefox y Tor Browser). Compara los resultados de los tres navegadores.

c) (0,5 puntos) Explicad cuales creéis que son las medidas más eficaces para combatir el "*browser fingerprinting*", y analiza para cada una su facilidad de uso vs su eficacia.

d) (0,5 puntos) En el siguiente artículo explican cómo se puede hacer *fingerprinting* cuando se usan diferentes navegadores en un mismo ordenador:

- https://arstechnica.com/information-technology/2017/02/now-sites-can-fingerprint-you-online-even-when-you-use-multiple-browsers/

Explica cómo funciona esta técnica y compara sus ventajas/desventajas con las técnicas de *fingerprinting* tradicional.