Seguridad de Sistemas Informáticos. Examen de Teoría Enero 2023

Nombre y Apellidos:

UO:

1) La empresa a la que he entrado a trabajar ha sido atacada, y me han dado un log de conexiones que estoy seguro de que no ha sido alterado. En la fecha y hora del ataque hay un enorme nº de conexiones de la IP 192.168.10.15, y el responsable de IT de mi empresa me dice que es una IP rusa. ¿Crees que es posible que esa IP sea de Rusia? Si crees que es posible que lo sea, ¿cómo lo averiguarías? *(1 punto)*

2) Mi jefe me autoriza a hacer un escaneo con `nmap` a la red de mi empresa y me encuentro con un servicio `http` en el puerto 59345 de una de las máquinas. He preguntado, pero nadie sabe qué hace ahí o a quien pertenece. ¿A qué crees que puede deberse la existencia de este servicio `http` misterioso? *(1 punto)*

Seguridad de Sistemas Informáticos. Examen de Teoría Enero 2023

Nombre y Apellidos:

UO:

3) Explica qué tendría que hacer yo para que alguien pudiera enviarme mensajes cifrados que sólo yo pudiera leer, en base a los conceptos de criptografía que hemos visto en teoría *(1 punto)*

4) Cómo verificarías que un software que te has descargado no ha sido alterado respecto a cuando su autor lo publicó (asume que el autor te proporciona los datos necesarios para hacerlo, la pregunta es respecto al procedimiento para hacerlo que seguirías) *(1 punto)*

Seguridad de Sistemas Informáticos. Examen de Teoría Enero 2023

Nombre y Apellidos:

UO:

5) Ha llegado un auditor que quiere decirnos cómo implantar la ISO 27001 en nuestra empresa, y le comentas que todas las máquinas de la empresa tienen aplicados y verificados todos los controles de seguridad de los *CIS Benchmarks* correspondientes a su SO. El auditor dice que eso no sirve para cumplir nada del estándar ISO 27001, y que tenemos que volver a empezar. ¿es cierto? ¿por qué? *(1 punto)*

6) En la SNI (*Secure Network Infraestructure*) propuesta en clase, ¿qué elementos forman la intranet de administración? Enumera y explica en 2 líneas máximo cada uno *(1 punto)*

Seguridad de Sistemas Informáticos. Examen de Teoría Enero 2023

Nombre y Apellidos:

UO:

7) DMZ (*Demilitarized zone*). Explica qué es y para qué se usa *(1 punto)*

8) Autorización (*AuthZ*). ¿Qué es? Formas de implementarla *(1 punto)*

Seguridad de Sistemas Informáticos. Examen de Teoría Enero 2023

Nombre y Apellidos:

UO:

9) *SQL Injection*. *Explica qué es* *(1 punto)*

10) *GTFOBins*. Explica qué son y cómo funcionan *(1 punto)*