**Ejercicio 1**

**1. ¿Qué es el malware? ¿Para qué se utiliza?**

Un malware es un software maligno cuyo propósito es alterar las funciones de toda clase de equipos electrónicos como el ordenador, el móvil y la tablet, incluso, terminan por dañar el sistema operativo por completo.

Se utiliza para robar información a la gente y sacar dinero por ello.

**2. ¿Cómo los hackers ganan dinero según el documental?**

Primero hay alguien que se encarga de crear el software maligno, después infectando los equipos de la gente, robarles la información a los usuarios, y estos revenden la información a otros grupos especializados en lavar el dinero para conseguirlo “limpiamente”

**3. ¿Cómo te podría un hacker robar el dinero a ti?**

Haciendo phishing a través del correo electrónico y SMS.

Suplantan la identidad de nuestro banco, mandándonos un correo electrónico o un SMS haciéndose pasar por ellos. Y buscan que entremos al enlace para que iniciemos sesión con nuestros datos y también pueden indicarnos que debemos actualizar nuestros datos. Y es ahí donde ya nos pueden robar.

**4. ¿Cómo se infecta con un virus un ordenador? En el documental explican un ejemplo con una floristería, descríbelo**

Tienen una herramienta que les permite infectar miles de paginas web de las que usamos normalmente, con visitar la pagina web esa ya quedaríamos infectados.

**5. Explica como hacía dinero butterfly.**

Una persona desarrolló un software maligno y se promocionaba en su pagina web con las tarifas de sus servicios en las que si lo contratabas, él controlaba los ordenadores de terceros, sacaba información y lanzaba ataques.

**6. Explica cómo hace en el vídeo un ataque para controlar el ordenador de un tercero.**

El atacante genera un correo electrónico que va a tener un contenido atractivo para la victima que a su vez este contiene un software maligno, lo que le dará acceso al atacante al ordenador, una vez que lo recibe la victima lo descarga y le da error de que el archivo esta corrupto. En ese momento el atacante ya tiene acceso al ordenador y a todos los documentos que haya en el ordenador.

**7. ¿Cuánta cantidad de información existente en Internet aparece en Google?**

La parte de internet que es accesible a todo el mundo es de un 20% de todo Internet. El 80% restante se conoce como el internet profunda como la deep web, que es donde se comercializa con todo (troyanos, tarjetas de crédito robadas)

**8. ¿Qué es el ataque de denegación de servicio?**

Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad con la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema atacado.

**9. ¿Qué beneficios puede sacar una empresa con este tipo de ataque?**

Hacer ataques DoS a la competencia para colapsar sus servidores y que los clientes no puedan visitar su pagina web en días, semanas o meses y tú como empresa poder beneficiarte de esa caída de servidores atrayendo a los clientes a tu negocio.

**10. ¿Por qué los hackers van un paso por delante de los policías? ¿Qué ventajas legales**

**tienen los hackers?**

El anonimato o la dificultad de identificación y de localización porque puede estar muy cerca o muy lejos.

Los hackers aprovechan las ausencias de fronteras en internet a la hora de cometer el delito, la policía tiene limitaciones territoriales a la hora de hacer justicia.

**11. ¿Cómo funciona eltimo de las cartas nigerianas? ¿Qué tiene que ver con la informática?**

Lanzan campañas masivas de spam en todo el mundo salvo en el país donde van a cometer la estafa.

**12. Explica qué es el phishing ¿Cómo funciona?**

Es un ataque informático de ingeniería social que usa medios de comunicación digitales, como el correo electrónico, para engañar y estafar a las personas.

**13. ¿Cómo los delincuentes ganan dinero con el phishing?**

Engañan a la victima con un correo electrónico que parece legítimo y es ahí donde le piden que inicie sesión y actualice los datos, entonces los hackers aprovechan y le roban toda la información que la victima les ha proporcionado y pueden acceder a sus cuentas bancarias para robarles todo el dinero.

**14. Explica qué trabajo hace un mulero.**

Un mulero bancario es una persona que ha sido engañada con pruebas de ingeniería social (generalmente un phishing) para recibir transferencias que provienen de fraudes electrónicos y mover ese dinero a sitios “seguros” como Western Union para los delincuentes.

**15. Explica cómo funciona el virus de la guardia civil.**

Te llega un mensaje de la policía alertándote de que tu ordenador esta secuestrado por visitar páginas de pornografía infantil o descargas ilegales y te pide 100€ para desbloquear el equipo.

Además, una de sus variantes, puede hacer que active la webcam del ordenador y es entonces ahí donde se ve a la persona que esta manipulando el ordenador y que esta cometiendo delitos.

Si el usuario pagaba la multa de los 100€ el ordenador seguía bloqueado, mientras que la policía buscaba información para identificar al usuario.

**16. ¿Por qué crees que el Bitcoin es importante para la delincuencia por Internet?**

Porque es la moneda que mas cuesta identificar y rastrear el origen y procedencia o la tendencia al alza de su valor

**17. Si te convirtieses en un hacker, ¿Qué técnica usarías para ganar dinero? ¿Y cómo lo harías?**

Brechas de seguridad en la página web de una empresa.

Robar toda la información de la base de datos y extorsionar a la empresa para que pague