SyPeR - Trabajo Práctico 1

Conceptos básicos, autenticación, e identidad

1. ¿Cuál es la diferencia entre *seguridad* y *privacidad*?
2. Defina y relacione los conceptos de *vulnerabilidad*, *amenaza* e *incidente*.
3. ¿A qué se hace referencia con el concepto de *"seguridad en capas"* y *"zero trust"*? ¿Considera que están relacionados?
4. Busque noticias sobre algún incidente de seguridad de la información de público conocimiento. Identifique cuál fue el bien afectado, qué error permitió el problema y qué se podría haber realizado para evitar el mismo.
5. Analice los riesgos introducidos en una organización por el uso de redes sociales y mensajería instantánea. Relacione con ingeniería social y ciberinteligencia. Dé al menos un ejemplo que se haya judicializado.
6. ¿Qué medidas de seguridad toma en cada uno de los siguientes casos?:
    - Al usar una computadora de la Sala de PC de la Facultad.
    - Al conectarte a una red inalámbrica pública.
    - Cuando te solicitan información personal por algún medio (telefónico / redes sociales / correo electrónico).
    - Al caminar por la calle, respecto a tus pertenencias personales.
    - Al realizar pagos con tarjeta de crédito/débito en un comercio físico.
    - Al realizar pagos con tarjeta de crédito/débito mediante e-commerce.
7. Suponiendo que usted pierde (o le sustraen) su notebook y/o su celular:
    a. Enumere qué información confidencial se vería expuesta en caso de no haber adoptado medidas de prevención adecuadas.
    b. ¿Qué medidas podría haber adoptado para evitar la pérdida de confidencialidad de la información?
    c. ¿Qué medidas podría haber adoptado para evitar la pérdida de disponibilidad de la información?
    d. Evalúe qué información relevante sería irrecuperable.
8. Descargue la máquina virtual Linux de la cátedra y utilice el acceso físico al sistema para poder ingresar al mismo. Una vez logrado esto, configure una contraseña al usuario **core** que será el usuario que deberá utilizar sobre dicha VM.
9. Gestión de accesos y privilegios. Definir y describir brevemente los siguientes conceptos:
    a. IAM
    b. PAM
    c. PIM
    d. IGA
    e. BYOI
    f. Password Less
    g. Factores de autenticación (tres)
    h. MFA
    i. SSO
    j. OTP
    k. Framework AAA
10. La pirámide de la CIA, ¿es igual en ambientes IT que en OT? Justificar.
11. Relacionar Ingeniería Social con Inteligencia Artificial. Dar ejemplos donde la autenticación se vea afectada.

12. 

Suponga que trabaja en el área de Ciberseguridad para *SyPeR Company*, una empresa mediana ubicada en la Ciudad Autónoma de Buenos Aires, Argentina.
La empresa se encarga de desarrollar software a medida para otras empresas. Los clientes de *SyPeR Company* otorgan ocasionalmente accesos (limitados) a algunas de sus plataformas.

Se pide realizar un documento normativo a modo de “reglas” que deben aplicar para el ciclo de vida de contraseñas. Considerar la creación, uso (y uso compartido), rotación, inteligencia de ciberamenazas.

Las normas creadas deben poder ser auditadas correctamente, es decir, bajo una auditoría se debe poder comprobar que lo que esté documentado realmente se cumpla.

El documento no debe tener más de 3 carillas.

Ayuda: Documentos del CIS y NIST pueden ser útiles.