MUIInf
Máster Oficial Universitario en
Ingeniería Informática
muiinf.webs.upv.es

Test 2 RSE
24 de enero de 2017

UNIVERSITAT POLITÈCNICA DE VALÈNCIA
etsinf

Nombre:..... Apellidos:.....

1. **La sigla PKI indica:**
   - [x] Una combinación de elementos para la ejecución de operaciones criptográficas
   - [ ] Un método de encriptación basado en clases privadas
   - [ ] Un método de encriptación basado en clases publicas/privadas
   - [ ] Un algoritmo de generación de claves hash

2. **En criptografía, la generación de números aleatorios:**
   - [ ] No debe generar números repetidos.
   - [ ] No debe ser predecible por el usuario.
   - [x] No debe ser predecible por el atacante.
   - [ ] Deben utilizar información generada por los humanos.

3. **¿Qué es un certificado X509?**
   - [ ] Un fichero que contiene fundamentalmente una clave pública junto con la identidad de su propietario.
   - [x] Un fichero que contiene fundamentalmente una clave pública junto con la identidad del propietario firmado por una entidad certificadora PKI.
   - [ ] Un fichero con la clave pública, la identidad del propietario, la firma de una entidad certificadora y la clave privada de la CA firmante.
   - [ ] Nada de lo anterior.

4. **Que es una lista de revocación:**
   - [ ] El conjunto de todos los certificados emitidos por una CA que han caducado.
   - [ ] El conjunto de los certificados emitidos por una CA que han sido robados.
   - [x] La lista de certificados emitidos por una CA que deben ser invalidados.
   - [ ] La lista de certificados que nuestro navegador (o sistema) no acepta.

5. **En los algoritmos de cifrado simétrico:**
   - [x] la clave de cifrado se utiliza también para descifrar.
   - [ ] volviendo a cifrar el ciphertext se obtiene el plaintext.
   - [ ] la clave privada se utiliza para cifrar y la secreta para descifrar.
   - [ ] la clave privada se utiliza para cifrar y la publica para descifrar.

6. **La criptografía de clave pública:**
   - [ ] Es más rápida que la de clave privada.
   - [ ] Es más rápida que la de clave secreta.
   - [ ] Es más rápida que la de resúmenes.
   - [x] Se puede utiliza para intercambiar claves secretas.

7. Los algoritmos de hash se utilizan para:

- [ ] En el proceso de firmado digital.
- [ ] En la generación de certificados x509
- [ ] La gestión de las passwords en servidores
- [x] Todas las anteriores.

8. Que es la Perfect Forward Secrecy (PFS)?

- [ ] Una técnica puramente de encriptación y no de decriptación
- [ ] Una técnica rápida de encriptación en clave simétrica
- [x] Una versión mejorada de la encriptación en clave publica
- [ ] Una técnica de encriptación que además comprime la información

9. Cual es la opción de seguridad mejor para wifi

- [ ] MAC filtering
- [ ] WEP
- [ ] IEEE 802.1x
- [x] WPA/WPA2

10. Que es un "Zero day attacks"?

- [ ] Los ataques en la instalación de un sistema
- [x] Una nueva vulnerabilidad para la cual no se crearon todavía parches o revisiones
- [ ] Los primeros ataques del día
- [ ] Los ataques iniciales en un servidor web

11. ¿Que es una Demilitarized Zone (DMZ)?

- [x] Una zona segura que se ubica entre la red interna de una organización y una red externa
- [ ] Una zona sin sistemas de seguridad
- [ ] Una sección de un sistema de información de acceso restringido
- [ ] Una técnica para evitar el pishing

12. Cual es el uso de Application layer gateway (ALG) en los firewalls?

- [x] Controlar si se debe permitir o denegar el tráfico al servidor de aplicación
- [ ] Un Gateway para optimizar la ejecución de las aplicaciones
- [ ] Bloquear todas las aplicaciones entrantes
- [ ] Bloquear todo el trafico basado en UDP

13. Para protegerse de un Advanced Persistent Threat (APT)...

- [ ] Es suficiente utilizar un firewall
- [x] Hay que utilizar software especifico (p.ej., IDPS)
- [ ] Es suficiente con utilizar VLANs
- [ ] Es suficiente con utilizar VPNs

14. Mobile Device Management (MDM)

- [ ] Permite la gestión de la movilidad de los smartphones
- [x] Permite el uso personal y profesional seguro de un mismo smartphones
- [ ] Permite ahorrar gastos de gestión de los smartphones
- [ ] Permite utilizar varias operadoras de telefonía

15. A que se refiere el Network Foresincs

- [x] El estudio de los ataques recibidos para determinar las causas
- [ ] Estudio de la robustez de las protecciones frente ataques de una red
- [ ] Análisis de las prestaciones (p.ej., throughput) de una red empresarial
- [ ] Análisis de la previsión de carga de trabajo de una red empresarial

16. Que es el 5G

- [ ] La próxima evolución de las redes de telefonía celular
- [ ] Indica las nuevas tecnologías de red inalámbricas basadas en mmWave
- [ ] La próxima evolución de las redes basadas en fibra
- [x] Ninguna de las anteriores

17. ¿Que son las SDN (Software Defined Network)?

- [ ] Un nuevo tipo de middleware para la gestión de redes empresariales
- [x] Una nueva forma centralizada de controlar los dispositivos de red (switches, …)
- [ ] Una tecnología para la programación de servicios en red (basados en cloud)
- [ ] Una tecnología para el diseño de redes corporativas

18. ¿Que ventajas tiene el uso de OAuth?

- [x] Permite reducir el numero de contraseñas que un usuario tiene que recordar
- [ ] Es una forma de autenticación más segura
- [ ] Es una técnica de AAA
- [ ] Es tipo de firewall basado en la delegación del control

19. RADIUS es …

- [x] Un protocolo para el AAA
- [ ] Un tipo de firewall
- [ ] Un algoritmo de encriptación
- [ ] Un protocolo de encaminamiento

20. Wi-Fi utiliza IEEE 802.1X para…

- [ ] Encriptar las comunicaciones
- [ ] Establecer la velocidad de los enlaces
- [x] Otorgar el acceso a un AP
- [ ] Integrarse con redes 4G