

Seguridad en los Sistemas de Información

Dr. Manuel Sánchez Rubio

Presentación de la asignatura

Presentación de la asignatura.

- ✓ **Asignatura. Seguridad en los Sistemas de Información.**
 - **Prof. Manuel Sánchez Rubio, me presento...**



@sanchezrum



<https://www.linkedin.com/in/sanchezrum>

Presentación de la asignatura.

- ✓ **Asignatura. Seguridad en los sistemas de Información**



<https://www.flickr.com/photos/alancleaver/4121423119>

Presentación de la asignatura.

✓ Asignatura. Seguridad en los sistemas de Información

- Temario

15 semanas -> 12 temas ... tranquilos

Tema 1. Una perspectiva global de la seguridad

Tema 2. Criptografía y criptoanálisis clásicos

Tema 3. Criptografía simétrica

Tema 4. Criptografía asimétrica

Tema 5. Ataques en redes

Tema 6. Arquitecturas de seguridad

Tema 7. Técnicas de protección de sistemas

Tema 8. Desarrollo de código seguro

Tema 9. Botnets y spam

Tema 10. Auditoría y ataques Web

Tema 11. Malware y código malicioso

Tema 12. Análisis forense



Presentación de la asignatura.

- ✓ Asignatura. Seguridad en los sistemas de Información



SCADA



... y más

Presentación de la asignatura.

- ✓ Asignatura. Seguridad en los sistemas de Información
 - Trabajos y actividades a desarrollar.



<https://www.flickr.com/photos/morrosko/12823524005/in/photostream/>

Presentación de la asignatura.

- ✓ **Asignatura. Seguridad en los sistemas de Información**
 - **Trabajos y actividades a desarrollar.**
 - **Actividad Individual (semana 3) ... ¡hoy!**
Delitos informáticos en fuentes abiertas
 - **Actividad Grupal (semana 5)**
Vectores de ataque
 - **Laboratorio (semana 11)**
Misión: reconocimiento

Presentación de la asignatura.

- ✓ **Asignatura. Seguridad en los sistemas de Información**
 - **Trabajos y actividades a desarrollar.**

- **Presentación.**
- **Extensión libre.**
- **Bibliografía.**



En formato pdf



<https://flic.kr/p/7PTtv>

Presentación de la asignatura.

- ✓ Asignatura. Seguridad en los sistemas de Información
 - Exámenes ¿Qué temario entra?, ¿Cuál no?
...acotaciones en clases de refuerzo



Presentación de la asignatura.

✓ Asignatura. Seguridad en los sistemas de Información

- Exámenes ... en principio
- Tipo test: 10 preguntas
 - Cada pregunta vale 0.2
 - Pregunta no contestada o mal contestada vale 0
- Preguntas de desarrollo (2)
 - Cada pregunta vale 4 puntos
 - Extensión máxima 1 folio
- Tiempo máximo: 2 horas

Presentación de la asignatura.

- ✓ Asignatura. Seguridad en los sistemas de Información
 - Ejemplo de pregunta de examen

La técnica diseñada para capturar información personal mediante la modificación del servidor de DNS, se conoce con el término:

- a.- Smishing.*
- b.- Dnsing.*
- c.- Pharming.*
- d.- Phishing.*

Presentación de la asignatura.

✓ Asignatura. Seguridad en los sistemas de Información

- Ejemplo de pregunta de examen

Pharming (recordando...)

; fichero mi_dominio.com

```
MI_DOMINIO.COM.      IN      SOA   DNS_1.MIDOMINIO.COM. (
                        Postmaster.MI_DOMINIO.COM.
                        941022001   ; Número de serie
                        86400       ; Actualizar cada 24 horas
                        7200        ; Reintentar cada 2 horas (si error)
                        2592000     ; Expira a los 30 días
                        345600      ; TTL por defecto, 4 días
                        )
MI_DOMINIO.COM.      IN      NS    DNS_1.MIDOMINIO.COM
MI_DOMINIO.COM.      IN      NS    DNS_2.MIDOMINIO.COM

MI_DOMINIO.COM.      IN      MX     10    MAIL_1.MIDOMINIO.COM
MI_DOMINIO.COM.      IN      MX     20    MAIL_2.MIDOMINIO.COM

DNS_1                 IN      A      172.66.1.15
DNS_2                 IN      A      172.66.1.67
MAIL_1                IN      A      172.66.1.5
MAIL_2                IN      A      172.66.1.18
                      IN      TXT     WWW, FTP sobre mail_2
                      IN      HINFO    SUN UNIX

WWW                   IN      CNAME    MAIL_2
FTP                   IN      CNAME    MAIL_2
```

; fin de fichero mi_dominio.com

Presentación de la asignatura.

- ✓ **Asignatura. Seguridad en los sistemas de Información**
 - **Ejemplo de pregunta de examen a desarrollar**

Fases del plan de respuesta a incidentes:

- 1. Respuesta inmediata**, para evitar males mayores, como reconfigurar automáticamente las reglas de los cortafuegos o inyectar paquetes de RESET sobre conexiones establecidas.
- 2. Investigación**, para recolectar evidencias del ataque que permitan reconstruirlo con la mayor fidelidad posible.
- 3. Recuperación**, para volver a la normalidad en el menor tiempo posible y evitar que el incidente se repita de nuevo.
- 4. Creación de informes**, para documentar los datos sobre los incidentes y que sirvan como base de conocimiento con posterioridad, para posibles puntos de mejora y como información para todos los integrantes de la organización. De manera adicional, se hacen necesarios los informes por posibles responsabilidades legales que pudieran derivarse.

Presentación de la asignatura.

- ✓ **Asignatura. Seguridad en los sistemas de Información**
 - **TFG: dos tipos**

1.- Mis propuestas.



2.- Si algo os ha gustado, es vuestro.

Presentación de la asignatura.

- ✓ **Asignatura. Seguridad en los sistemas de Información**
 - **Bibliografía recomendada**

*Sánchez, M. (2020) “Redes de computadores”, Ed. UAH, Junio 2020
ISBN/ISSN:978-84-18254-07-9*

*BARRERA, S. (2017) “Claves de la investigación en redes sociales”, Ed.
Círculo Rojo, Marzo 2017. ISBN: 978-84-9160-000-8*

*Casas, E (2017) "La Red Oscura", Ed La Esfera de los Libros", Enero 2017.
ISBN 978-8490608777*

*Casas, E (2017) "Las andanzas de un Policía Tecnológico, Ed. Palabras de
Agua, Octubre 2017. ISBN 978-8494654978*

Presentación de la asignatura.

Intercambio de opiniones.



www.unir.net