

Servidores seguros

Presentación

Gustavo Romero López

Updated: 18 de octubre de 2024

Ingeniería de Computadores, Automática y Robótica

Información básica:

web: <https://pccito.ugr.es/~gustavo/ss>
profesor: Gustavo Romero López
email: gustavo@ugr.es
despacho: 2D33: 2ª planta, nº 33
teléfono: 958 24 08 21
telegram: @gustavo_ugr

Antecedentes

Tecnología y Organización de Computadores - 1º curso, 2º semestre.



Estructura de Computadores - 2º curso, 1º semestre.



Arquitectura de Computadores - 2º curso, 2º semestre.



Ingeniería de Servidores - 3º curso, 1º semestre.



Arquitectura de Sistemas
- 3º curso, 2º semestre.



Arquitectura y Computación de Altas
Prestaciones - 3º curso, 2º semestre.

1. Seguridad en protocolos de transporte.
 - 1.1 Túneles SSH. Túneles SSL: Seguridad en protocolos de transporte (SSL/TLS). Túneles HTTP.
 - 1.2 Redes Privadas Virtuales (VPN - Virtual Private Network). Descripción, tipos VPN Microsoft, OpenVPN.
 - 1.3 Seguridad en redes inalámbricas. WPA-PSK, WPA utilizando servidores Radius. Herramientas de análisis wireless. Análisis de tráfico. Vulnerabilidades WEP.
2. Seguridad en aplicaciones.
 - 2.1 Análisis de vulnerabilidades y Detección de ataques.
 - 2.2 PKI (Public Key Infrastructure). Certificados. OpenSSL.
 - 2.3 Seguridad en aplicaciones: apache, imap,...
 - 2.4 Seguridad en sistemas de objetos distribuidos
3. Control de acceso al servidor.
 - 3.1 IDS: Detección de intrusos. Ataques.
 - 3.2 Seguridad perimetral: Tcpwrapper, Iptables,...
 - 3.3 Autenticación: Kerberos, LDAP, PAM,...
 - 3.4 Seguridad: SE-Linux.
 - 3.5 Seguridad en sistemas de ficheros

División del temario

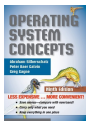
- ① Seguridad en protocolos de transporte.
 - ① Túneles SSH, Túneles SSL: Seguridad en protocolos de transporte (SSL/TLS). Túneles HTTP.
 - ② Redes Privadas Virtuales (VPN - Virtual Private Network). Descripción, tipos VPN Microsoft, OpenVPN.
 - ③ Seguridad en redes inalámbricas. WPA PSK, WPA utilizando servidores Radius. Herramientas de análisis wireless. Análisis de tráfico. Vulnerabilidades WEP.
- ② Seguridad en aplicaciones.
 - ① Análisis de vulnerabilidades y Detección de ataques.
 - ② PKI (Public Key Infrastructure). Certificados, OpenSSL.
 - ③ Seguridad en aplicaciones: apache, mysql,...
 - ④ Seguridad en sistemas de objetos distribuidos
- ③ Control de acceso al servicio.
 - ① IDS: Detección de intrusiones. Ataques.
 - ② Seguridad perimetral: Tcpwrapper, Iptables,...
 - ③ Autenticación. Kerberos, LDAP, PAM,...
 - ④ Seguridad. SELinux.
 - ⑤ Seguridad en sistemas de ficheros

Seguridad en sistemas operativos y aplicaciones

1. Entorno de seguridad
2. Seguridad en sistemas operativos
3. Control de acceso a los recursos
4. Modelos formales de seguridad
5. Criptografía básica
6. Autenticación
7. Software de explotación
8. Ataques desde dentro
9. Software malicioso
10. Defensa



Modern Operating Systems. Fourth Edition. Andrew S. Tanenbaum. Prentice Hall. 2014.



Operating System Concepts. Ninth Edition. Abraham Silberschatz, Peter B. Galvin, Greg Gagne. Wiley. 2010.



Computer Systems. A Programmer's Perspective. Second Edition. Randal E. Bryant, David R. O'Hallaron. Pearson. 2011.

<https://www.cert.org>

<https://cve.mitre.org>

<http://www.exploit-db.com>

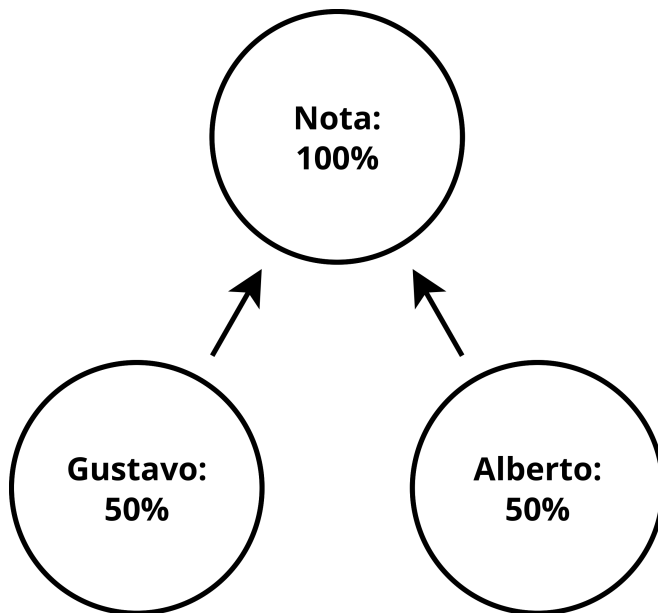
<https://www.incibe.es>

Fuente: **DuckDuckGo**

- ⊙ CSO
- ⊙ TechBeacon
- ⊙ HP
- ⊙ Infosec

Fuente: **Google**

- ⊙ TripWire
- ⊙ Digital Guardian
- ⊙ Security Magazine
- ⊙ Secutiry Trails



Evaluación continua: test diarios $\longrightarrow$ nota $\in [0 \cdots 10]$