SEGURIDAD INFORMATICA

CLAVE:
No. De Horas/Semana: 3
Duración Semanas: 16
Total de Horas: 48
No. De Creditos: 6
Prerrequisitos: CI7200-T, IA7600-T

OBJETIVOS: Proporcionar al estudiante los conocimientos básicos sobre los conceptos principales de la seguridad informática así como de la aplicación de las técnicas y herramientas adecuadas para preservar la confidencialidad, integridad y disponibilidad de la información y de los sistemas de información.

CONTENIDO SINTETICO:

1. ARQUITECTURA DE SEGURIDAD INFORMATICA.
2. TECNOLOGIA CRIPTOGRAFICA
3. SEGURIDAD EN SERVIDORES
4. CONTROL DE ACCESO Y CORTAFUEGOS
5. ACCESO REMOTO Y REDES PRIVADAS VIRTUALES
6. DETECCION DE INTRUSOS

PROGRAMA DESARROLLADO:

I – ARQUITECTURA DE SEGURIDAD INFORMATICA 8 HRS.

1. Introducción a la seguridad informática.
2. Amenazas y contramedidas.
3. Desarrollo de la arquitectura de seguridad informática.
4. Análisis de riesgos.
5. Políticas, estándares, guías y su clasificación.
6. Desarrollo de la política de seguridad.
7. Aspectos de implementación de políticas de seguridad.
8. Planificación de continuidad del negocio (BCP) y recuperación de desastres (DRP).
9. Fundamentos de la auditoria de seguridad.
10. Adiestramiento en seguridad, educación y certificaciones.

II – TECNOLOGIA CRIPTOGRAFICA 8 HRS.

1. Criptología: Criptografía y criptoanálisis.
2. Criptografía simétrica.
3. Compendio de mensajes.
4. Criptografía de clave pública.

5. Firmas digitales.
6. Administración y distribución de claves simétricas.
7. Sistema de autenticación Kerberos.
8. Certificados digitales. Estándar X.509.
9. Infraestructura de clave pública (PKI).
10. Estándares de clave pública (PKCS, PKIX).
11. Implementación de PKI.

III – SEGURIDAD EN SERVIDORES 8 HRS.

1. Seguridad física.
2. Seguridad en UNIX.
3. Control de acceso y contraseñas. Permisos en directorios.
4. Principio de mínimo privilegio.
5. Aseguramiento de servicios de red en UNIX.
6. Análisis de bitácoras.
7. Seguridad en Windows 2000. Infraestructura de Seguridad.
8. Autenticación en W2K.
9. Configuración segura de W2K. Seguridad de recursos.
10. Registro de eventos de seguridad en W2K.
11. Seguridad de servicios de red en W2K. Seguridad en IIS.

IV – CONTROL DE ACCESO Y CORTAFUEGOS 8 HRS.

1. Ruteo en el protocolo IP.
2. Ruteadores y listas de control de acceso.
3. Filtraje de paquetes. NAT y enmascaramiento.
4. Clasificación de firewalls: Dual Homed Gateway, Screened Host Gateway, Screened Subnets.
5. Diseño de DMZ.
6. Criterios de certificación de cortafuegos ITSEC, CC, AISEP e ICSA.
7. Niveles de aseguramiento Ex y EALx.
8. Implementaciones de cortafuegos.
9. Cortafuegos y pruebas de penetración.
10. Pruebas de penetración con ISS, Nessus, SARA.

V – ACCESO REMOTO Y REDES PRIVADAS VIRTUALES.
8 HRS.

1. Protocolos de autenticación criptográfica. Protocolos de clave pública.
2. Protocolos de seguridad de la capa de aplicación. SSH.
3. Protocolos de seguridad de la capa de transporte. SSL/TLS.
4. Seguridad en redes inalámbricas. WTLS y WAP.
5. Protocolos de seguridad de la capa de enlace: PPTP, L2TP.
6. Protocolos de seguridad de la capa de red. IPSec.
7. Redes privadas virtuales e Internet.
8. Implementación de redes privadas virtuales.

VI – DETECCION DE INTRUSOS 8 HRS.

1. Sistemas detectores de intrusos: basados en host y basados en red.
2. Técnicas de detección de intrusiones.
3. Verificación de integridad.
4. Análisis de tráfico.
5. Sistemas actuales de detección de intrusos.
6. Detección activa. *Honeypots*.
7. Respuesta a incidentes.
8. Técnicas de informática forense.
9. Recursos: CERT, CIRT, etc.

BIBLIOGRAFIA

UNIDAD I

1. Michael Whitman, Herbert Mattord, *Principles of Information Security*, Course Technology, 1st edition, 2002.
2. Thomas R. Peltier, *Information Security Policies, Procedures and Standards: Guidelines for Effective Information Security Management*, CRC Press, 1st Edition, 2001.
3. Thomas R. Peltier, *Information Security Risk Analysis*, Auerbach Publications, 1st Edition, 2001.
4. Micki Krause, Harold F. Tipton, *Information Security Management Handbook*, Fourth Edition, Volume I, Auerbach Publications, 1999.
5. Jack Killmeyer Tudor, *Information Security Architecture: An Integrated Approach to Security in the Organization*. CRC Press, 2000.
6. Christopher King, Ertem Osmanaglu, Curtis Dalton, *Security Architecture: Design, Deployment and Operations*, McGraw Hill Osborne Media, 1st Ed. 2001.
7. Scott Barman, *Writing Information Security Policies*, QUE, 1st Edition, 2001.
8. Jay Ramachandran, *Designing Security Architecture Solutions*, John Wiley & Sons, 1st edition, 2002.
9. Jon William Toigo, *Disaster Recovery Planning: Strategies for Protecting Critical Information Assets*, Prentice Hall, 3rd ed, 2002.
10. Eric Maiwald, William Seiglen, *Security Planning and Disaster Recovery,* Mc Graw-Hill Osborne Media, 2002.
11. Floyd Piedad, Michael Hawkins, *High Availability: Design, Techniques and Processes*, Prentice Hall, 1st edition, 2000.
12. Evan Marcus, Hal Stern, *Blueprints for High Availability: Designing Resilient Distributed Systems*, John Wiley & Sons, 1st edition, 2000.

UNIDAD II

1. Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, John Wiley & Sons, 2nd Ed, 1995.
2. Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

3. William Stallings, *Cryptography and Network Security: Principles and Practice*, Prentice Hall, 3rd Edition, 2002.
4. Niels Ferguson, Bruce Schneier, *Practical Cryptography*, John Wiley & Sons, 1st edition, 2003.
5. Douglas Stinson, Cryptography: Theory and Practice, 2nd Edition, Chapman & Hall, 2nd edition, 2002.
6. Charlie Kaufman, Radia Perlman, Mike Speciner, *Network Security: Private Communications in a Public World*, Prentice Hall, 2nd Edition, 2002.
7. William Stallings, *Network Security Essentials*, Prentice Hall, 2nd Edition, 2002.
8. Andrew Nash, Bill Duane, Derek Brink, Celia Joseph, *PKI: Implementing and Managing E-Security*, Mc Graw Hill Osborne Media, 2001.
9. Carlisle Adams, Steve Lloyd, *Understanding PKI: Concepts, Standards and Deployment Considerations*, Addison Wesley Professional, 2nd edition, 2002.
10. Jalal Feghhi, Peter Williams, *Digital Certificates: Applied Internet Security*, Addison-Wesley, 1998.

UNIDAD III

1. Simson Garfinkel, Alan Schwartz, Gene Spafford, *Practical Unix & Internet Security*, O'Reilly & Associates, 3rd edition, 2003.
2. Scott Mann, Ellen L. Mitchell, Mitchell Krell, *Linux System Security: The Administrator's Guide to Open Source Security Tools*, Prentice Hall PTR, 2nd edition, 2002.
3. Bob Toxen, *Real World Linux Security*, Prentice Hall PTR, 2nd edition, 2002.
4. Peter H. Gregory, *Solaris Security*, Prentice Hall PTR, 1st edition, 1999.
5. Phillip Cox, Tom Sheldon, *Windows 2000 Security Handbook*, McGraw Hill Osborne Media, 1st edition, 2000.
6. Roberta Bragg, *Windows 2000 Security*, QUE, 1st edition, 2000.
7. Ed Bott, Carl Siechert, *Microsoft Windows Security Inside Out for Windows XP and Windows 2000*, Microsoft Press, 2002.
8. Stefan Norberg, *Securing Windows NT/2000 Servers for the Internet*, O'Reilly & Associates, 1st edition, 2000.
9. Chris Weber, Gary Bahadur, *Windows XP Professional Security*, McGraw Hill Osborne Media, 2002.
10. Marty Jost, Michael Cobb, *IIS Security*, McGraw Hill Osborne Media, 1st edition, 2002.

UNIDAD IV

1. Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman, *Building Internet Firewalls*, O'Reilly & Associates, 2nd edition, 2000.
2. Keith Strassberg, Gary Rollie, Richard Gondek, *Firewalls: The Complete Reference*, McGraw Hill Osborne Media, 1st edition, 2002.
3. Thomas Akin, *Hardening Cisco Routers*, O'Reilly & Associates, 1st edition, 2002.
4. Jeff Sedayao, *Cisco IOS Access Lists*, O'Reilly & Associates, 2001.
5. Richard A. Deal, *Cisco PIX Firewalls*, McGraw Hill Osborne Media, 2002.
6. Bill McCarthy, *Red Hat Linux Firewalls*, John Wiley & Sons, 1st Edition, 2002.

7. Robert Ziegler, *Linux Firewalls*, QUE, 2nd Edition, 2001.
8. Dameon D. Welch-Abernathy, *Essential Checkpoint Firewall-1: An Installation, Configuration and Troubleshooting Guide*, Addison-Wesley, 1st Edition, 2002.
9. Zubair Alexander, *Microsoft ISA Server 2000*, Sams, 1st Edition, 2001.

UNIDAD V

1. Daniel J. Barrett, Richard Silverman, *SSH, The Secure Shell: The Definitive Guide*, O'Reilly & Associates, 1st edition, 2001.
2. John Viega, Matt Messier, Pravir Chandra, *Network Security with OpenSSL*, O'Reilly & Associates, 1st edition, 2002.
3. Stephen A. Thomas, *SSL & TLS Essentials: Securing the Web*, John Wiley & Sons, 2000.
4. Eric Rescola, *SSL and TLS: Designing and Building Secure Systems*, Addison Wesley Professional, 1st edition, 2000.
5. Ruixi Yuan, W. Timothy Strayer, *Virtual Private Networks: Technologies and Solutions*, Addison-Wesley Pub., 1st edition, 2001.
6. Naganand Doraswamy, *IPSEC: The New Security Standard for the Internet, Intranets and Virtual Private Networks*, Prentice Hall PTR, 1st edition, 1999.
7. Carlton Davis, *IPSec: Securing VPNs*, Mc-Graw Hill Osborne Media, 2001.
8. Thaddeus Fortenberry, *Windows 2000 Virtual Private Networking*, QUE, 1st edition, 2000.
9. Oleg Kolesnikov, Brian Hatch, *Building Linux Virtual Private Network*, QUE, 1st edition, 2002.
10. Merritt Maxim, David Pollino, *Wireless Security*, Mc Graw Hill Osborne Media, 1st edition, 2002.

UNIDAD VI

1. Stephen Northcutt, Judy Novak, *Network Intrusion Detection*, QUE, 3rd Edition, 2002.
2. Rebecca Gurley Bace, *Intrusion Detection*, QUE, 1st Edition, 1999.
3. Mark Cooper, Stephen Northcutt, Matt Fearnow, Karen Frederick, *Intrusion Signature and Analysis*, QUE, 1st Edition, 2001.
4. Rafeeq Rehman, *Intrusion Detection with SNORT: Advanced IDS Techniques Using SNORT, Apache, MySQL, PHP and ACID,* Prentice Hall PTR, 1st edition, 2003.
5. Paul E. Proctor, *Practical Intrusion Detection Handbook*, Prentice Hall PTR, 1st edition, 2003.
6. Earl Carter, Rick Stiffler, *Cisco Secure Intrusion Detection System*, Cisco Press, 1st edition, 2001.
7. Lance Spitzner, *Honeypots: Tracking Hackers*, Addison Wesley Professional, 2002.
8. Warren G. Kruse II, Jay G. Heiser, *Computer Forensics: Incident Response Essentials*, Addison-Wesley Pub, 1st edition, 2001.
9. Richard Forno, Kenneth R. Van Wyk, *Incident Response*, O'Reilly & Associates, 2001.

10. E. Eugene, Russell Shumway, *Incident Response: A Strategic Guide to Handling System and Network Security Breaches*, QUE, 1st edition, 2002.

Metodología de enseñanza-aprendizaje:

Revisión de conceptos, análisis y solución de problemas en clase:	(X)
Lectura de material fuera de clase:	(X)
Ejercicios fuera de clase (tareas):	(X)
Investigación documental:	(X)
Elaboración de reportes técnicos o proyectos:	(X)
Prácticas de laboratorio en una materia asociada:	( )
Visitas a la industria:	( )

Metodología de evaluación:

Asistencia:	(X)
Tareas:	(X)
Elaboración de reportes técnicos o proyectos:	(X)
Exámenes de Academia o Departamentales	(X)