Seguridad en Telecomunicaciones

PROFESORES

Cátedras: Alberto Castro, Rodrigo Werlinger

Agenda primera clase (1)

- Revisión objetivos y contenidos del curso
- Horario
- Bibliografía
- Evaluaciones
- Test diagnóstico

Agenda primera clase (2)

- La problemática global
- Tendencias
- Estadísticas
- Seguridad por niveles
- Estándares para empresas
- Certificaciones para profesionales
- Un ejemplo típico

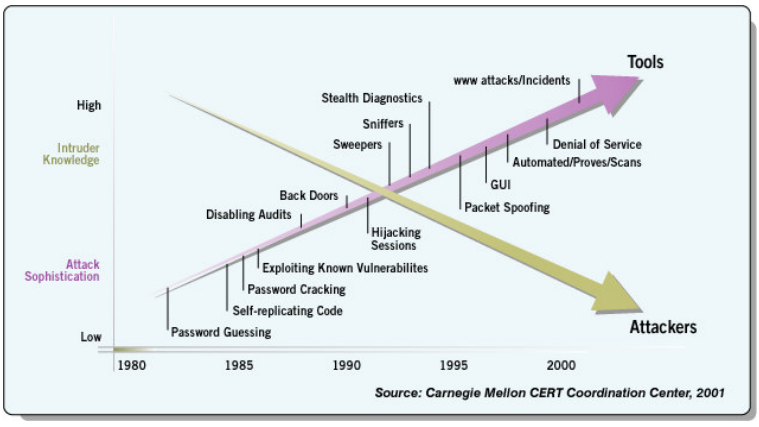
La problemática global

- Seguridad no sólo se refiere a protegerse de hackers
- Se debe abarcar la seguridad en su conjunto: fisica, desarrollo de aplicaciones, plataformas, etc

Tendencias (1)

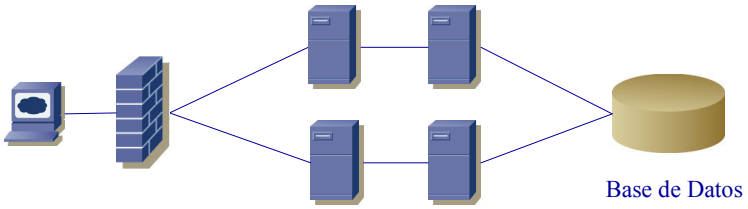
- Los negocios han aumentado su nivel de dependencia en los procesos computacionales
- Se espera una mayor interoperabilidad entre los sistemas
- La sofisticación de los ataques computacionales ha aumentado (no todos se hacen públicos)

Tendencias (2)



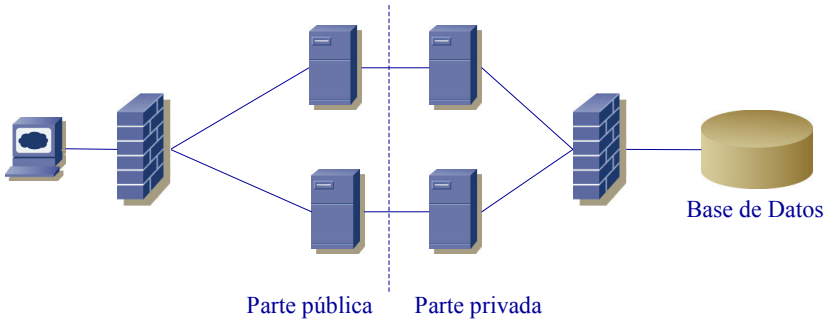
Tendencias (3)

•Modelo antiguo (dos capas)



Tendencias (4)

•Aparecen nuevos niveles o capas de protección (tres capas)

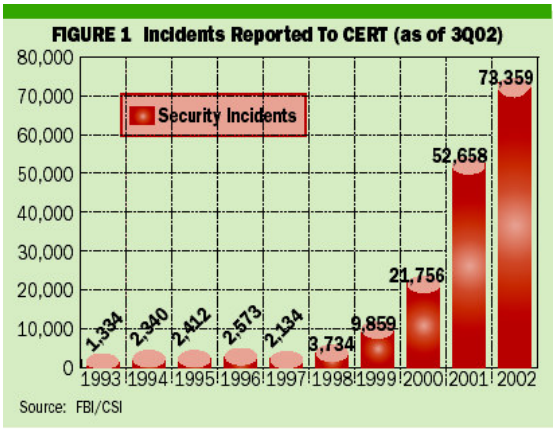


Tendencias (5)

- La seguridad del sistema debe condiderar todo el ambiente. El sistema es tan débil como su capa más débil
- La programación da énfasis a la funcionalidad.
- Pueden haber distintas arquitecturas (LAN-WAN-WEB), pero los conceptos de seguridad se mantienen

Estadísticas (1)

- Incidentes reportados
- ¿Qué significa CERT?



Estadísticas (2)

http://www.cert.org/stats/cert_stats.html#vulnerabilities

Number of incidents reported
1988-1989

Year	1988	1989
Incidents	6	132

1990-1999

Year	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999
Incidents	252	406	773	1,334	2,340	2,412	2,573	2,134	3,734	9,859

2000-2003

Year	2000	2001	2002	2003
Incidents	21,756	52,658	82,094	137,529

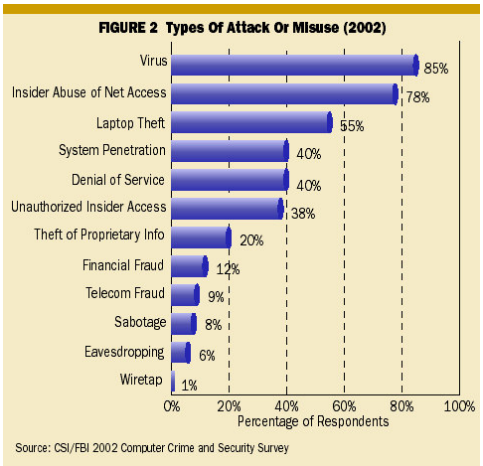
Total incidents reported (1988-2003): **319,992**

Please note that an incident may involve one site or hundreds (or even thousands) of sites. Also, some incidents may involve ongoing activity for long periods of time.

Estadísticas (3)

- Tipos de ataque reportados

http://www.cybercrime.gov/CSI_FBI.htm

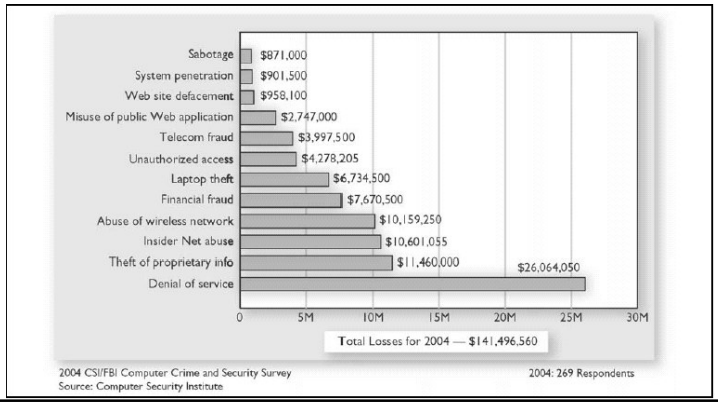


Estadísticas (4)

•Perdidas monetarias por tipo de ataque

http://www.cybercrime.gov/CSI_FBI.htm

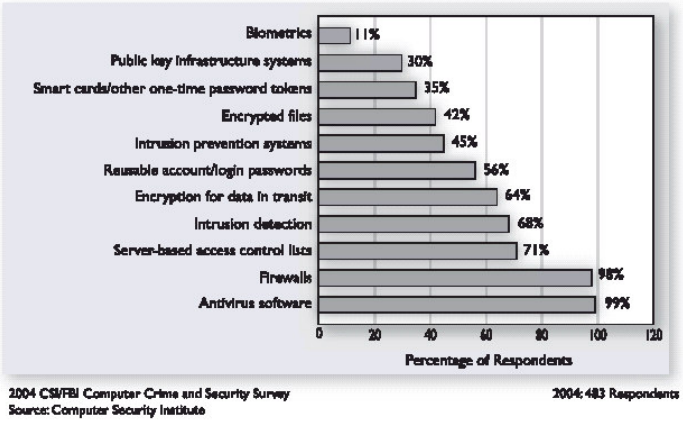
494 computer security practitioners in: U.S. corporations, government agencies, financial institutions, medical institutions, and universities



Estadísticas (5)

•Tipos de tecnología de seguridad usados

http://www.cybercrime.gov/CSI_FBI.htm



Estadísticas (6)

http://www.sans.org/top20/#ports

•Top Vulnerabilities to Windows Systems

W1 Internet Information Services (IIS)
W2 Microsoft SQL Server (MSSQL)
W3 Windows Authentication
W4 Internet Explorer (IE)
W5 Windows Remote Access Services
W6 Microsoft Data Access Components (MDAC)
W7 Windows Scripting Host (WSH)
W8 Microsoft Outlook and Outlook Express
W9 Windows Peer to Peer File Sharing (P2P)
W10 Simple Network Management Protocol (SNMP)

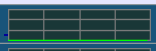
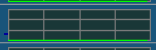
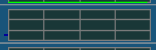
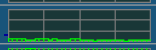
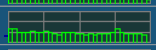
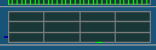
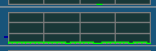
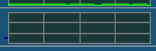
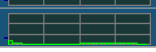
Top Vulnerabilities to UNIX Systems

U1 BIND Domain Name System
U2 Remote Procedure Calls (RPC)
U3 Apache Web Server
U4 General UNIX Authentication Accounts with No Passwords or Weak Passwords
U5 Clear Text Services
U6 Sendmail
U7 Simple Network Management Protocol (SNMP)
U8 Secure Shell (SSH)
U9 Misconfiguration of Enterprise Services NIS/NFS
U10 Open Secure Sockets Layer (SSL)

Estadísticas (7)

•http://isc.incidents.org/trends.php?isc=8af6d812f4f877285ed8ba446f123fea

Top 10 Ports

Service Name	Port Number	30 day history	Explanation
dabber	9898		[trojan] Dabber Worm backdoor
sasser-ftp	5554		[trojan] Sasser Worm FTP Server
Reserved	1023		
netbios-ns	137		NETBIOS Name Service
microsoft-ds	445		Win2k+ Server Message Block
epmap	135		DCE endpoint resolution
ms-sql-s	1433		Microsoft-SQL-Server
ms-sql-m	1434		Microsoft-SQL-Monitor
radmin	4899		Remote Administrator default port
mydoom	3127		W32/MyDoom, W32.Novarg.A backdoor

Estadísticas (8)

•http://isc.incidents.org/trends.php?isc=8af6d812f4f877285ed8ba446f123fea

Top 10 Source IPs

IP Address	Hostname	Targets Attacked	Reports Received	Last Report
212.170.136.19	212-170-136-19.cac.campus-party.org	136848	266902	2004-07-29
203.129.64.230	-none-	135488	149059	2004-07-30
212.38.234.235	-none-	66632	131699	2004-07-29
64.215.244.3	-none-	67038	67046	2004-07-30
67.120.60.213	adsl-67-120-60-213.dsl.lsan03.pacbell.net	65890	115807	2004-07-29
24.225.204.83	host-24-225-204-83.patmedia.net	65532	196243	2004-07-29
217.94.177.160	pD95EB1A0.dip.t-dialin.net	65524	125872	2004-07-29
210.226.247.66	ns7.pdf-factory.co.jp	65356	124729	2004-07-29
62.138.203.74	-none-	65190	65193	2004-07-29
205.251.238.169	wiley-173-13359.roadrunner.nf.net	65208	65210	2004-07-29

Seguridad por niveles

Capa de comunicación	Dispositivo ejemplo	Protocolo
Aplicación	Servidor WEB	SSL
Red	Router	IPSec, NAT
Enlace de datos	Switch	L2TP
Física	Repetidor	TEMPEST

•Tarea: Averiguar que es L2TP y TEMPEST

Estándares para empresas (1)

- Norma BS7799 (www.securityauditor.net)
  - Alcance: es una norma que se divide en dos partes:
    1. BS7799: 1 entrega recomendaciones de buenas prácticas para la empresa.
    2. BS7799: 2 especifica criterios para cumplir las buenas prácticas
  - Abarca 10 tópicos de seguridad
- Estándar ISO 17799
  - Alcance: se enmarca dentro de BS7799:1
  - Se está a la espera de la segunda parte del estándar para certificación

Estándares para empresas (2)

- Otros estándares:
  - Cobit (www.isaca.org)
  - COSO (www.coso.org)
  - Estándares privados

- Tarea: elaborar un resumen de los estándares Cobit y COSO

Certificaciones para profesionales (1)

- CISSP: Certified Information Systems Security professional (www.cccure.org)
  - Aborda 10 tópicos de seguridad
    - Administración de seguridad
    - Seguridad Física
    - Seguridad en Telecomunicaciones
    - Control de acceso
    - Criptografía
    - Arquitectura y modelos de seguridad
    - Recuperación ante desastres y continuidad del negocio
    - Leyes, Investigación y ética
    - Desarrollo de sistemas y aplicaciones
    - Seguridad de Operaciones

Certificaciones para profesionales (2)

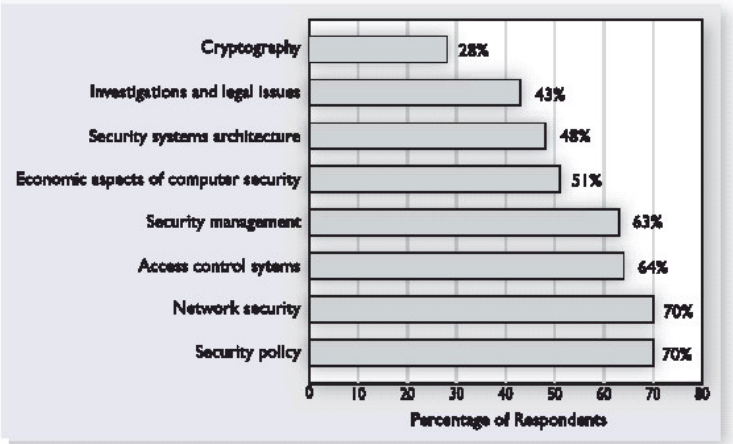
https://www.isc2.org, www.isaca.org, www.giac.org

ABCP - Associate Business Continuity Professional
CBCP - Certified Business Continuity Professional
CCSA - Certification in Control Self-Assessment
CFCE - Certified Forensic Computer Examiner
CFE - Certified Fraud Examiner
CIA - Certified Internal Auditor
CISA - Certified Information Systems Auditor
CISM - Certified Information Security Manager
CISSP - Certified Information Systems Security Professional
CISSP - ISSAP - CISSP, Information Systems Security Architecture Professional
CISSP - ISSEP - CISSP, Information Systems Security Engineering Professional
CISSP - ISSMP - CISSP, Information Systems Security Management Professional
CIW Security - Certified Internet Webmaster Security Analyst
CPP - Certified Protection Professional
CSA - Control Self-Assessment
CWNA - Certified Wireless Network Administrator
CWSP - Certified Wireless Security Professional
G7799 - GIAC Certified ISO-17799 Specialist
GCFA - GIAC Certified Forensic Analyst
GCFW - GIAC Certified Firewall Analyst
GCIA - GIAC Certified Intrusion Analyst
GCIH - GIAC Certified Incident Handler
GCSC - GIAC Certified Security Consultant
GCUX - GIAC Certified UNIX Security Administrator
GCWN - GIAC Certified Windows Security Administrator
GISF - GIAC Information Security Fundamentals
GSAE - GIAC IT Security Audit Essentials
GSEC - GIAC Security Essentials Certification
GSLC - GIAC Security Leadership Certification
GSNA - GIAC Systems and Network Auditor
IAM - NSA Infosec Assessment Methodology
MBCP - Master Business Continuity Professional
PCI - Professional Certified Investigator
PSP - Physical Security Professional
SSCP - Systems Security Certified Practitioner
Security+
TICSA - TruSecure ICSA Certified Security Associate
TICSE - TruSecure TICSE Certified Security Expert

Tarea: ¿qué certificaciones consideraría como parte de un programa de capacitación para personal técnico a cargo de un ISP (internet Service Provider)?

Certificaciones para profesionales (3)

Una referencia



2004 CSI/FBI Computer Crime and Security Survey
Source: Computer Security Institute

2004: 480 Respondents

Un ejemplo típico

- Aparece el aviso de un parche para servidores
- Se aplica el parche (4 horas) y los servidores experimentan problemas de desempeño.
- Se desintalan los parches (2 horas)
- Los servidores son atacados y toma 10 horas recuperarlos, pues algunos respaldos no funcionaron.
- Se libera un parche del parche
- Se libera un nuevo parche (distinto al anterior) que afecta a los servidores...