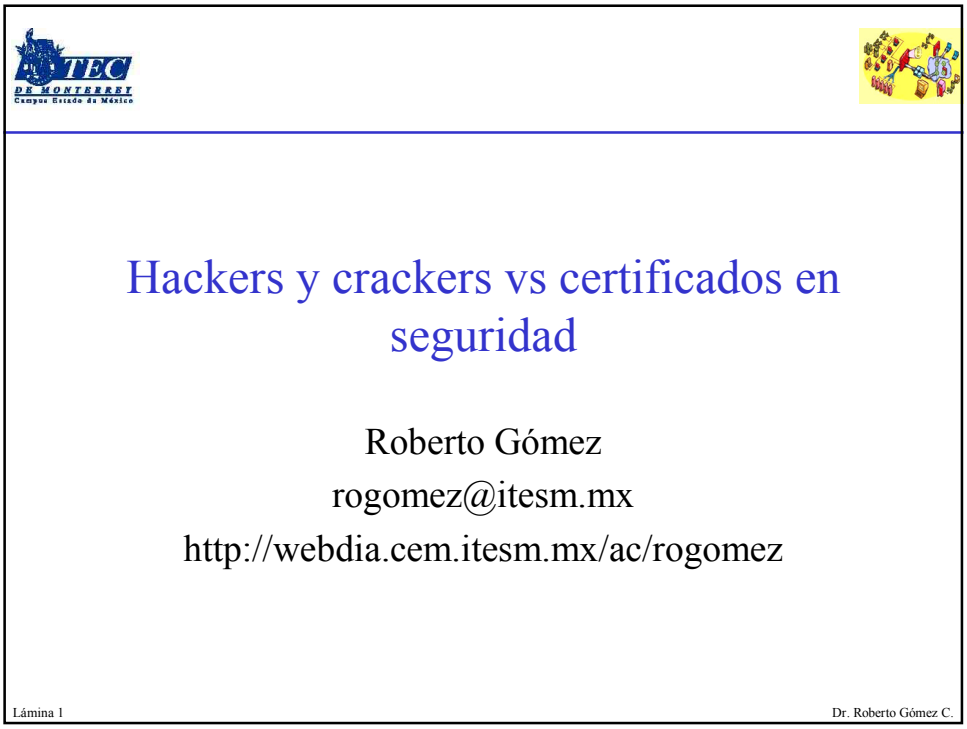
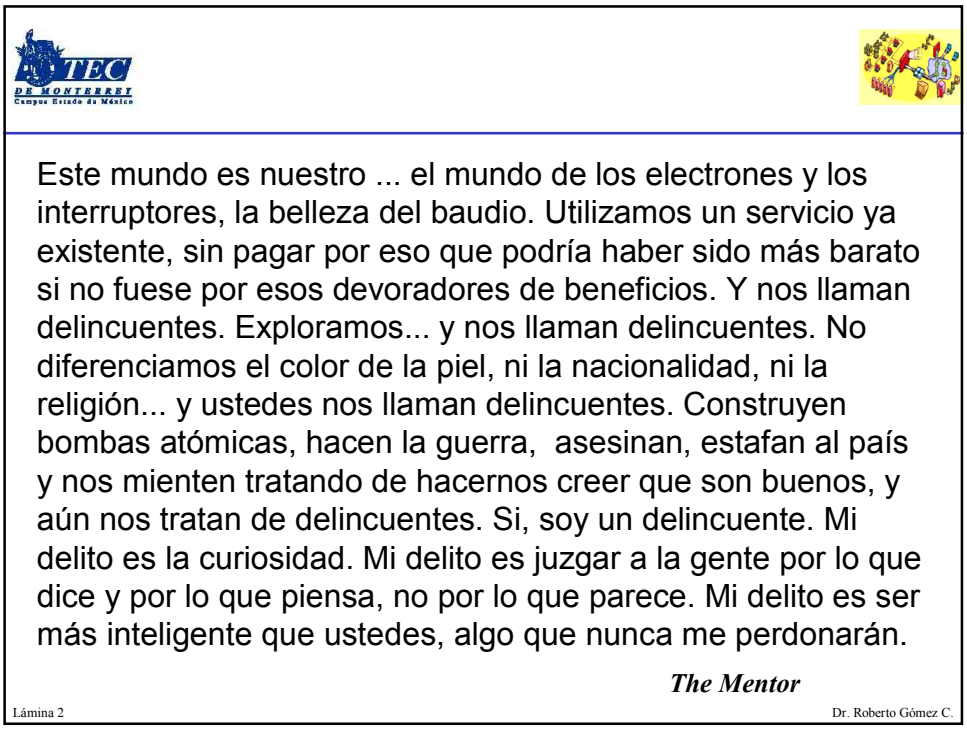


Hackers y crackers vs certificados en seguridad

Roberto Gómez
rogomez@itesm.mx
http://webdia.cem.itesm.mx/ac/rogomez

Lámina 1 Dr. Roberto Gómez C.



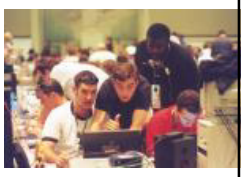
Este mundo es nuestro ... el mundo de los electrones y los interruptores, la belleza del baudio. Utilizamos un servicio ya existente, sin pagar por eso que podría haber sido más barato si no fuese por esos devoradores de beneficios. Y nos llaman delincuentes. Exploramos... y nos llaman delincuentes. No diferenciamos el color de la piel, ni la nacionalidad, ni la religión... y ustedes nos llaman delincuentes. Construyen bombas atómicas, hacen la guerra, asesinan, estafan al país y nos mienten tratando de hacernos creer que son buenos, y aún nos tratan de delincuentes. Si, soy un delincuente. Mi delito es la curiosidad. Mi delito es juzgar a la gente por lo que dice y por lo que piensa, no por lo que parece. Mi delito es ser más inteligente que ustedes, algo que nunca me perdonarán.

The Mentor

Lámina 2 Dr. Roberto Gómez C.

El Hacker: La Vieja Guardia

- Origen del término a finales de los 60.
- Programador con alto dominio de su profesión, capaz de solucionar problemas a través de hacks (segmentos de código muy ingenioso).
- Verdaderos conocedores de la tecnología de cómputo y telecomunicaciones (85-93).
- La búsqueda del conocimiento siempre fue su fuerza impulsora.



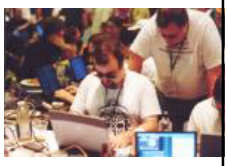
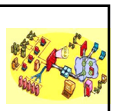


Lámina 3
Dr. Roberto Gómez C.

Los origines...



- Trazan sus antecesores espirituales a la élite de las universidades técnicas, especialmente M.I.T. y Stanford en los sesenta.
- Las raíces genuinas del moderno hacker underground
  - se pueden buscar de forma más exitosa en un tipo de movimiento hippy anarquista particularmente oscuro conocido como los yippies
- Yippies tomaron su nombre de un partido de ficción el "Youth International Party"
  - yippies más activos eran Abbie Hoffman y Jerry Rubin

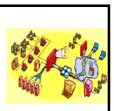
Lámina 5 Dr. Roberto Gómez C.

El cracker

- Aquella persona que en forma persistente realiza intentos hasta obtener acceso a sistemas computacionales.
- Una vez logrado el acceso produce daños a los recursos del sistema atacado.
- No necesariamente tiene el mismo nivel de conocimientos que el hacker.

Lámina 6 Dr. Roberto Gómez C.

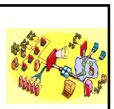
Los phreakers



- Aquella persona que en forma persistente realiza intentos hasta obtener acceso a sistemas telefónicos privados.
- Una vez logrado el acceso produce daños a los recursos del sistema atacado, o se beneficia del mismo.

Lámina 7

Otro concepto de Phreakers



- Es el más "doloroso"
- Persona que busca realizar actividades ilegales para enriquecerse, o bien destruir por puro terrorismo
- También se incluyen las personas que revientan sistemas de televisión, cada vez más en auge con las televisiones privadas, vía satélite y por cable

Lámina 8
Dr. Roberto Gómez C.

Los ¨Script-kidies¨

- Gente con la capacidad de buscar un programa en la red y ejecutarlo.
- No hay una meta fija.
- Necesidad de pertenencia, aunque sea al *inframundo*.
- No hay preocupación por las consecuencias reales de sus actos.
- Se sienten muy ¨cool¨.

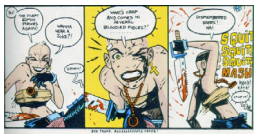
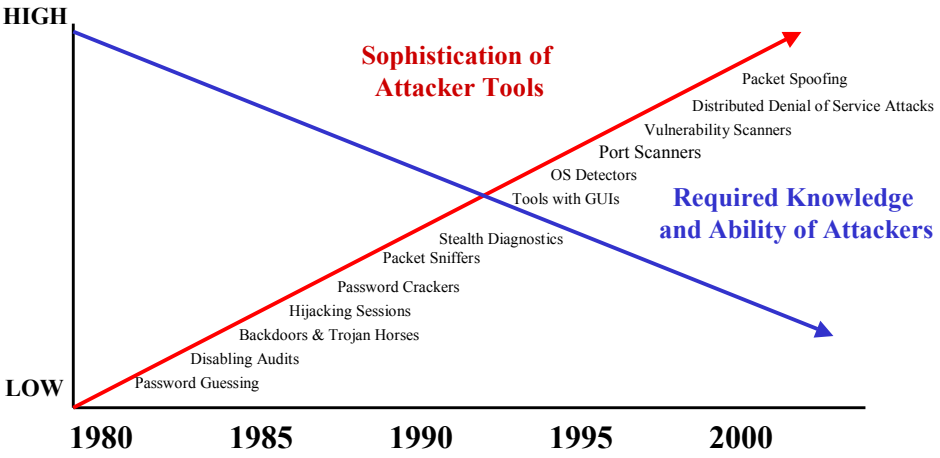


Lámina 9 Dr. Roberto Gómez C.

External Threats: Hacker Tool Explosion

Recent Web Search for "Hacker Tools" returned over 2100 hits

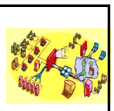


I get scanned dozens of times everyday. Less than 20% of those scans are US based

ISS User

Lámina 10 Dr. Roberto Gómez C.

Los Lammers



- Individuo sin muchos conocimientos, aunque un poco más elevados que los mortales, pero claramente inferiores a los de un hacker.
- Se hacen pasar por hackers
- Termino bastante despectivo
- Se les reconoce por su costumbre de presumir en los chats de conocimientos, normalmente técnicas que aunque al conjunto de los usuarios puedan parecer asombrosas, son más viejas que el arca de Noé y su uso no implica conocimientos de alto nivel.

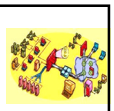
Lámina 11 Dr. Roberto Gómez C.

Algunos intentos de sofisticación

- Escribir con k
  - "kasi" da pena al leerlos
- Escribir minúsculas y mayúsculas
  - EsTo TiPo De TiPoGrAfIa Ya No EsTa De MoDa Y yA nO sE uSa
- Lenguaje "elite"
  - sustituir letras por números
  - 3ST0 S3RI4 UN 3J3MPLO D3 DICH0 L3NGU4J3

Lámina 12 Dr. Roberto Gómez C.

Newbies

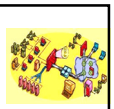


- Joven usuario que está comenzando y decide aprender siguiendo las reglas sin romper nada.
- No son peligrosos porque prefieren asesorarse y normalmente acaban siendo hackers
- En cierto modo un newbie es un "aprendiz" de un hacker.

Una madrecita Aprendiendo a "Hackear".

Lámina 13
Dr. Roberto Gómez C.

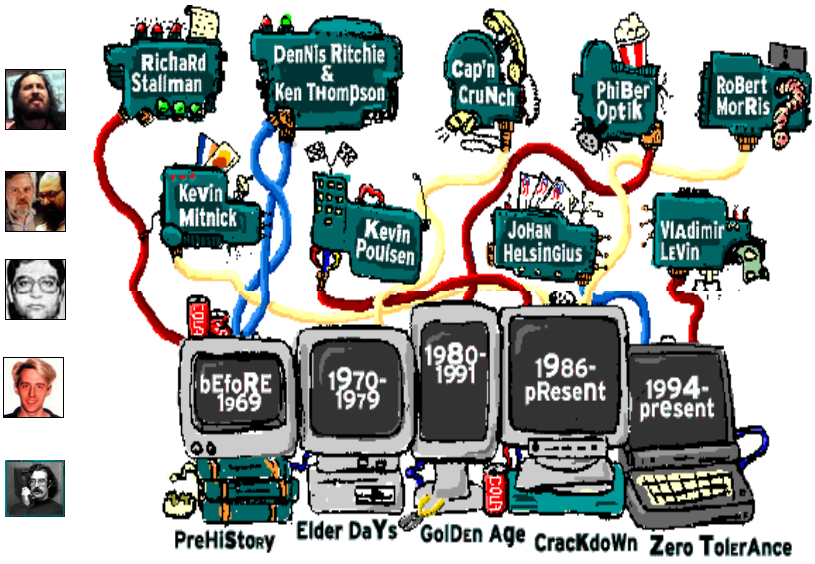
El Hacker: ¿cómo lo ven el resto de los usuarios?



- ¿Qué es eso?
- Eso pasa solo en las películas.
- Así como los de ¨The Net¨
- Yo soy hacker.
- Yo apenas sé como se usa una computadora.
- Bill Gates se va a encargar de ellos.

Lámina 14
Dr. Roberto Gómez C.

El hall de la fama de los hackers



www.discovery.com/area/technology/hackers/hackers.html

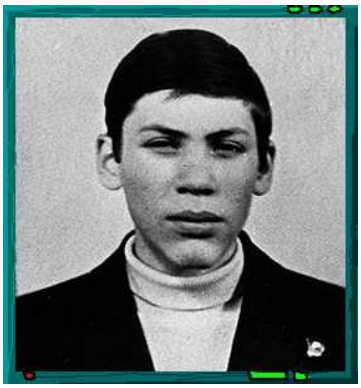
¿Qué hicieron?

- Kevin Poulsen
  - En 1990 Poulsen tomo control de todas las líneas telefonicas que llegaban a la estación de radio de Los Angeles KII-FM para ganar un concurso.
- Johan Helsingius
  - Opersaba el más fomoso remailer anónimo a nivel mundial, llamado penet.fi, hasta que lo cerro en Septiembre de 1996
- Phiber Optik (Mark Abene)
  - Inspiro cientos a adolescentes en el país para “estudiar” los trabajos internos del sistema telefónico nacional de USA.
- Cap Crunch (John Draper)
  - Averiguo la forma de realizar llamadas telefónicas gratis usando un silbato de plastico que encontró en una caja de cereales

El hacker Kevin Mitnick

Lámina 17
Dr. Roberto Gómez C.

Vladimir Levin (Russian Hacker).



Hacked the City Bank $ 10,000,000

Lámina 18
Dr. Roberto Gómez C.

Algunos otros

- Steve Wozniak
- Tsutomu Shimomura
- Linus Torvalds

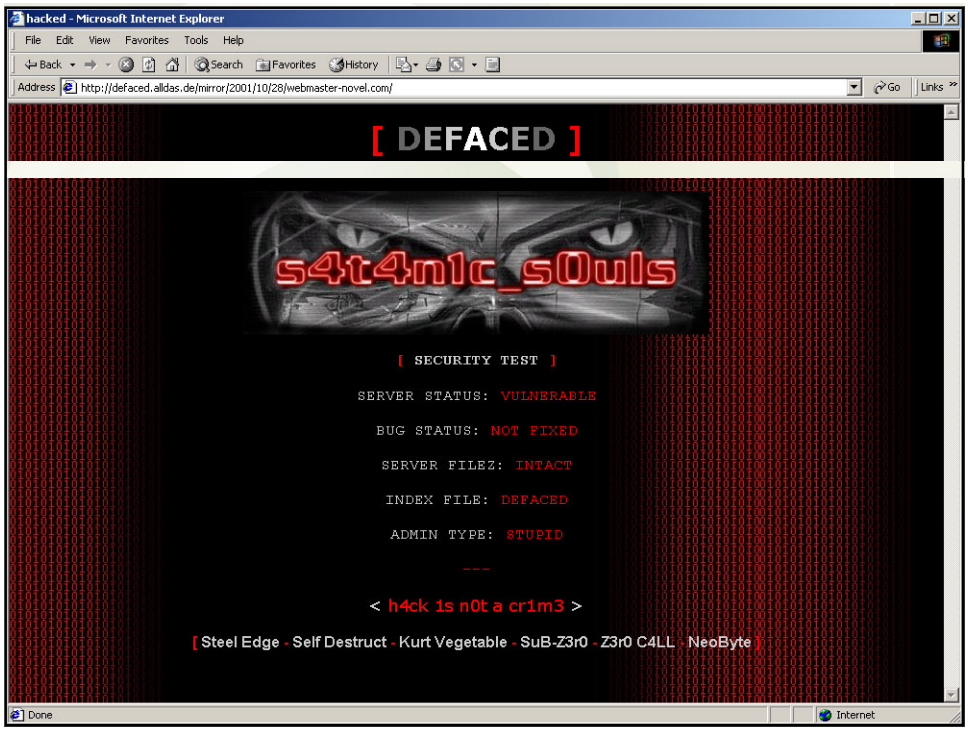


Lámina 19
Dr. Roberto Gómez C.

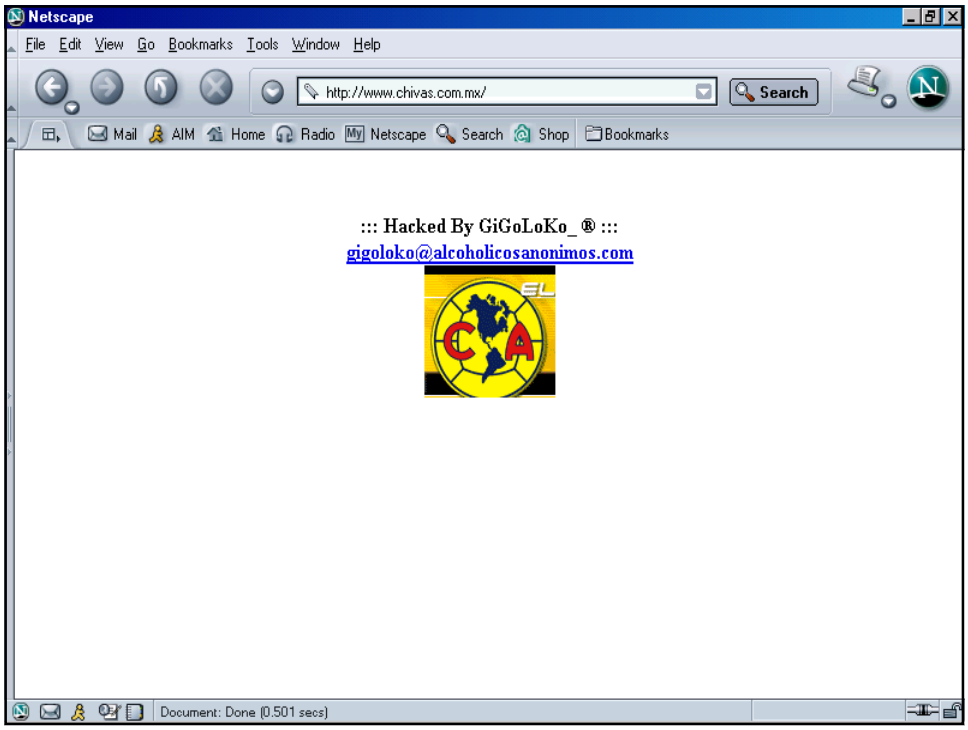
¿Que motiva a un hacker?

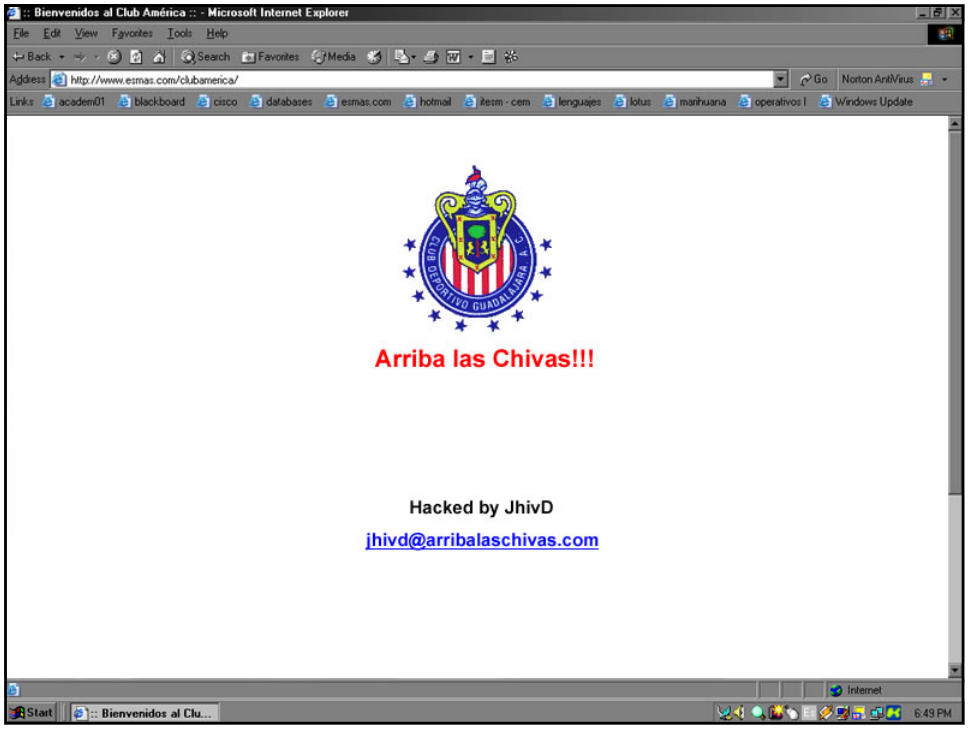
- Hacktivists
- State sponsored
- Industrial Espionage

Lámina 20
Dr. Roberto Gómez C.


hacked - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://defaced.alldas.de/mirror/2001/10/28/webmaster-novel.com/
[DEFACED]
s4t4n1c_s0uls
[SECURITY TEST]
SERVER STATUS: VULNERABLE
BUG STATUS: NOT FIXED
SERVER FILEZ: INTACT
INDEX FILE: DEFACED
ADMIN TYPE: STUPID

< h4ck 1s n0t a cr1m3 >
[Steel Edge - Self Destruct - Kurt Vegetable - SuB-Z3r0 - Z3r0 C4LL - NeoByte]
Done
Internet


Netscape
File Edit View Go Bookmarks Tools Window Help
http://www.chivas.com.mx/
Search
Mail AIM Home Radio Netscape Search Shop Bookmarks
::: Hacked By GiGoLoKo_ ® :::
gigoloko@alcoholicosanonimos.com
Document: Done (0.501 secs)


:: Bienvenidos al Club América :: - Microsoft Internet Explorer
Arriba las Chivas!!!
Hacked by JhivD
jhivd@arribalaschivas.com


H.i.S saving the world and owning your b0x - Netscape
O único homem que não comete erros é o que nunca faz nada...
Não tenha medo de errar, contanto que não cometa duas vezes o mesmo erro.
A continuidade da vida no planeta e a sobrevivencia da propria humanidade depedem do meio ambiente. A preservação do meio ambiente tem que fazer parte do cotidiano de todas as pessoas. Então, todo dia deve ser dia do meio ambiente
H.i.S
Fazendo sua parte
Thank: ModProb3, StaMaster, nandaF., ADMIM cool and GreenPeace
Fuck: American explorers of Brazillian florests

Defaced pages

- Primero fue attrition
  - http://www.attrition.org
- Después fue alldas
  - http://defaced.alldas.de/
- Ahora es:
  - http://www.zone-h.org/defacements/onhold

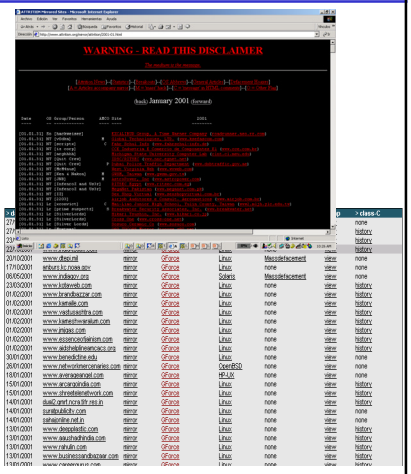


Lámina 25
Dr. Roberto Gómez C.

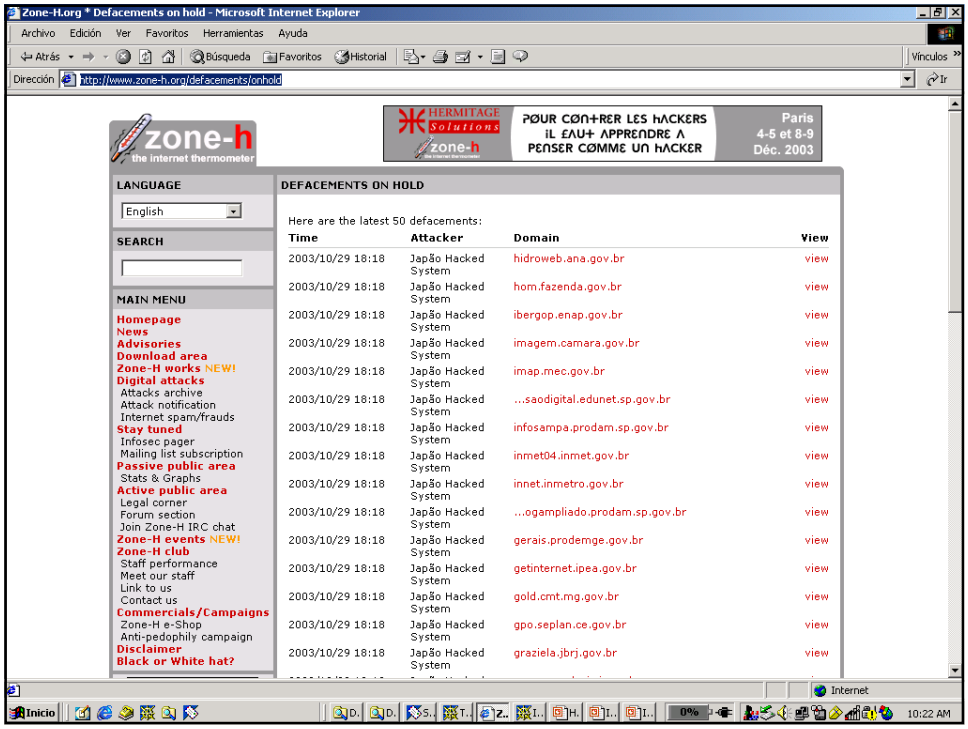
Attrition Decision

One of the most predominant sections of Attrition has been the defacement mirror. What began as a small collection of web site defacement mirrors soon turned into a near 24/7 chore of keeping it up to date. In the last month, we have experienced single days of mirroring over 100 defaced web sites, over three times the total for 1995 and 1996 combined. With the rapid increase in web defacement activity, there are times when it requires one of us to take mirrors for four or five hours straight to catch up. Add to that the scripts and utilities needed to keep the mirror updated, statistics generated, mail lists maintained, and the time required for basic functionality is immense. A "hobby" is supposed to be enjoyable. Maintaining the mirror is becoming a thankless chore.

During this time, we have struggled to keep up various other sections of Attrition that have been a core part of the site. As the mirror grew and began to consume more resources, the other sections have found themselves on the backburner and rarely updated. In essence, what was once a hobby site run in spare time for fun has turned into a beleaguring second job. A job that comes with more headache, complaints, criticisms, slander and attacks than productive output or reward. In two years we have turned away countless computer security work that could have been fulfilled by a number of us. The abuse and ignorance we deal with from defacers and defacement victims is staggering, and some of that abuse spills over into actual attacks. Attrition has been taken down more than once by massive denial of service attacks which have inconvenienced our generous upstream provider, hundreds of other colo customers, and thousands of dialup customers, making our job even more difficult.

With that, the mirror will no longer be maintained. We've served our time.

Lámina 26
Dr. Roberto Gómez C.

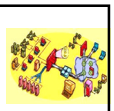


Algunos grupos

- Chaos Computer Club
- Cult of the Dead Cow
- DC2600.org
- AntiOffline removing the Dot in Dot.com
- The gethohackers
- DARK CLAW
- LoD
- ¿Y en México?
  - Raza Mexicana
  - Aztlan Klan
  - Cucaracha Hackers Team

Lámina 28 Dr. Roberto Gómez C.

Un ejemplo de conversación



#25 por ThA_CroW 21/9/2003

kiuvo banda? ya deberian de dejarse de lameradas y ponerse a trabajar ya ke se supone ke pagar tanta lana por este evento ke segun yo pienso ke deberia de ser gratis o ke? no ke muy hackers?

#14 por SoylalradeDios 18/9/2003

los de hackersoft y hakim.ws si son hackers la mayoria, y organizan sus reuniones sin cobrar para enseñar sus conocimientos en hack por eso preguntaba si iban a dar alguna ponencia como representantes de la escene en mexico, ellos si han hackeado servers importantes

#32 por ArPhAnEt_X 24/9/2003

pus komo ya dijo napa...no kreo ke esto sea kompetencia y al igual ke el yo tambien llevo amigos ke kieren aprender... lo ke dice la ira de dios pues kreo ke no todos en hackersoft sabemos mucho o por lo menos yo... pero lo ke si tenemos en hackersoft, es ganas de avanzar, aprender y kompartir todo esto con mas gente y esto es a lo ke muchos les hace falta y no estankarce kon lo ke ya esta deskubierto, sino deskubrir mas y enseñar a mas dejando el elitismo a un lado.

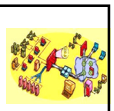
Lámina 29 Dr. Roberto Gómez C.

Otros términos relacionados

- Wracker
  - programas shareware o freeware
- Carding
  - reventar o emular tarjetas de crédito
  - Copy-hackers o Copy-crakers
  - skimming
- Wares
  - intercambio programas comerciales pirateados
- Sneaker
  - espía informático por excelencia

Lámina 30 Dr. Roberto Gómez C.

Más términos relacionados



- Snuffer
  - variante sneaker, limitado a averiguar claves de acceso a sistemas y descubre errores y agujeros en programas
- Corsarios
  - ya no se habla, ya no existen en ningún país
  - comprobar efectividad programas de una empresa y sobre todo los de la competencia
- Bucaneros
  - sin tener conocimientos especiales, recogen programas pirateados y los revenden para enriquecerse con ello
- Rider
  - estaba en alguna de las categorías anteriores pero actualmente trabaja en el campo legal

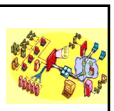
Lámina 31 Dr. Roberto Gómez C.

¿Y cómo los diferencio?

- Títulos académicos
  - licenciatura
  - maestría
  - doctorado
- Certificaciones
  - CISSP
  - SSCP
  - CISA
  - CISM
  - CISMP
  - SCP
  - BS7799-LA

Lámina 32 Dr. Roberto Gómez C.

Las opciones académicas



- Diplomados
  - ITESM-CEM
  - UNAM
  - y otros
- Cursos aislados en programas de maestría y licenciatura
- Ninguna institución a nivel nacional (latinoamerica??) ofrece una opción en seguridad informática
- Varias universidades americanas y europeas ofrecen maestrías en el área de seguridad informática.

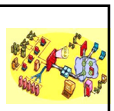
Lámina 33 Dr. Roberto Gómez C.

Universidades relacionadas

- University of Sheffield
  - http://www.shef.ac.uk
- Ecole Ingenieur Télécom Paris - ENST Ecole nationale
  - Mastere Sécurité des systèmes informatiques et des réseaux
  - http://www.enst.fr/3e-cycle-msc-masteres/masteres/ssir.php
- University Purdue
  - Center for Education and Research in Information Assurance and Security, or CERIAS
  - http://www.cerias.purdue.edu/
- The George Washington University
  - Master of Arts in the arts in the field of Criminal Justice Computer Fraud Investigation
  - http://www.gwu.edu

Lámina 34 Dr. Roberto Gómez C.

Otras dos más...



- Carnegie Mellon University.
  - Information Networking Institute (INI)
  - http://www.ini.cmu.edu/
  - Master of Science in Information Networking
  - Master of Science in Information Security Technology and Management
- Capitol College
  - Master of Science in Network Security
  - restricted by the United States Department of Commerce to U.S. citizens and permanent residents
  - http://www.capitol-college.edu/academics/grad/msns.html

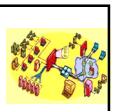
Lámina 35 Dr. Roberto Gómez C.

CISSP

- No es una asociación, es el título que ostenta el profesional certificado
  - Certified Information Systems Security Professional
- Ser CISSP es un privilegio que se debe ganar y mantener
- Otorgado por la $(ISC)^2$
  - International Information Systems Security Certification Consortium
  - Organismo independiente
  - Creado para realizar la certificación de profesionales en seguridad informática

Lámina 36 Dr. Roberto Gómez C.

CBK del CISSP



- Access Control Systems & Methodology
- Telecommunications & Network Security
- Security Management Practices
- Applications & Systems Development Security
- Cryptography
- Security Architecture & Models
- Operations Security
- Business Continuity Planning (BCP) & Disaster Recovery Planning (DRP)
- Law, Investigations & Ethics
- Physical Security

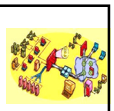
Lámina 37 Dr. Roberto Gómez C.

SSCP

- Especialista Certificado de Seguridad de Sistemas
  - Systems Security Certified Practitioner
- Diseñada para personas que aplican los principios de seguridad de la información, procedimientos, estándares y guías de una organización.
  - proporcionar soporte de la infraestructura de la seguridad
  - security enforcer
  - la persona no solo entiende su posición, sino también tiene un conocimiento de experto de la seguridad informática, como funciona y como es aplicada

Lámina 38 Dr. Roberto Gómez C.

CBK del SSCP



- Access Controls
- Administration
- Audit and Monitoring
- Risk, Response and Recovery
- Cryptography
- Data Communications
- Malicious Code/Malware

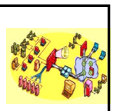
Lámina 39 Dr. Roberto Gómez C.

CISA

- Certified Information Systems Auditor
- En un principio dominio exclusivo de auditores de IT
- Administrada por la ISACA (Information Systems Audit and Control Association & Foundation)
  - fundada en 1969
- Certificación CISA tiene desde 1978
- En 2002 se contaba con unos 28,000 personas con dicha certificación.
- Dominios coinciden con CISSP
  - más enfocado a los procedimientos del negocio que a la tecnología
- Varios CISSP optan por ganar su CISA

Lámina 40 Dr. Roberto Gómez C.

Áreas CISA



- Management, planning and organization of IS
- Technical infrastructure and operational practices
- Protection of information assets
- Disaster recovery and business continuity
- Business application system development, acquisition, implementation and maintenance
- Business process evaluation and risk management
- The IS audit process

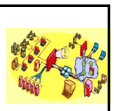
Lámina 41 Dr. Roberto Gómez C.

CISM

- ISACA acaba de diseñar la certificación CISM
  - Certified Information Security Manager
- Certificación reconoce el conocimiento y experiencia de un administrador de seguridad IT
- Debido a que es nuevo, pasa por un periodo de "apadrinamiento"
  - aquellos que puedan demostrar ocho años de experiencia en el área de seguridad informática puede obtener la certificación sin realizar examen alguno
  - periodo abierto hasta el 31 diciembre 2003
- Después periodo será necesario presentar examen.
- Primer examen será ofrecido en Junio 2004

Lámina 42 Dr. Roberto Gómez C.

Global Information assurance certifications



- SANS Institute ofrece una serie de certificaciones bajo el programa GIAC
  - Global Information Assurance Certification
- Certificaciones GIAC están dirigidas principalmente a practicantes
  - system administrators, network engineers
  - existen algunas apropiadas para administradores
- GIAC Information Securtiy Officer (GISO)
  - certificación tipo “entry-level” que incluye conocimientos de threats, riesgos y best practices.
- GSEC
  - certificación de nivel intermedio de conocimiento básico de seguridad tanto para practicantes como administradores.

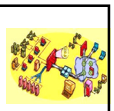
Lámina 43 Dr. Roberto Gómez C.

Otras certificaciones

- Puestos IT managers o IT security managers solicitan otro tipo de certificaciones como
  - Microsoft Certified Systems Engineer (MCSE)
  - CISCO: CCNA, CCNP, etc
- Certificaciones productos
  - ISS: Internet Security Scanner
  - Symantec
  - Network Associates
  - TCSEC certification
    - Trusted Computer Systems Evaluation Criteria

Lámina 44 Dr. Roberto Gómez C.

Mas certiciaciones



- Certificación SCP
  - http://www.securitycertified.net
  - Security Certified Network Professional (SCNP) and
  - Security Certified Network Architect (SCNA).
- CISMP
  - Certificate in Information Security Management Principles (UK)
- BS7799-LA
- ISM - Information Assesment Methodology
  - NSA, USA

Lámina 45 Dr. Roberto Gómez C.

Beneficios certificaciones

- Estudio Certification Magazine sugiere que certificaciones de alto nivel como CISSP son recompensadas de mejor forma.
  - estudio de 1,000 respuestas en el 2002 indicó que aquellos que obtuvieron su certificación CISSP recibieron un aumento promedio de $7,140 en 2001 comparado con 3,487 para otras certificaciones
- De acuerdo a InfoSecurity en agosto 2002 los salarios promedio de los profesionales en IT disminuyeron en un 5.5%
  - aquellos en seguridad IT se incrementaron en un 3.1 %

Lámina 46 Dr. Roberto Gómez C.

Hackers vs CISSP

THE CISSP
aka
Why The Infosec
INDUSTRY IS
A
FUCKING JOKE

Lámina 47
Dr. Roberto Gómez C.

¿Conclusiones?

Lámina 48
Dr. Roberto Gómez C.


Gracias por su atención
Hackers y crackers vs certificados en seguridad
Roberto Gómez
rogomez@itesm.mx
http://webdia.cem.itesm.mx/ac/rogomez
Lámina 49
Dr. Roberto Gómez C.