

The logo for BAICOM networks is centered on a dark blue rectangular background. The word "BAICOM" is written in a bold, white, sans-serif font. Below it, the word "networks" is written in a lighter blue, lowercase, sans-serif font.

BAICOM
networks

Hacking Network Security Seminar

Agosto de 2005

www.baicom.com

Presentación Institucional

BAICOM networks S.A. es una empresa joven que se ha posicionado en un mercado extremadamente competitivo merced a su experiencia en el campo de las Telecomunicaciones e Informática y a la construcción de una relación de confianza para con sus clientes.

Tenemos una fuerte especialización en Seguridad Informática y servicios profesionales basados en soluciones de código abierto.

Algunas de las empresas que confían en nosotros son:



Agenda

1. Seguridad Informática en el mundo

- Historia
- Puntos relevantes
- Situación actual

2. Estadísticas

- Evolución de incidentes publicados
- Evolución de vulnerabilidades

3. Administración de la Seguridad Informática

- Organización y reportes

4. Metodologías de Security Assessment y Penetration Test

- Information Gathering
- Análisis
- Ataques y Penetraciones
- Covering Tracks
- Consolidación

5. Productos y Servicios BAICOM networks

- Security
- IT & Networking
- Consulting

Historia

- Durante los años noventa, la tecnología tuvo el salto mas grande, y fue el período en el cual las empresas mas invirtieron en tecnología
- El concepto de seguridad informática no estaba instalado
- Las empresas fueron volcando sus procesos de core sobre distintas tecnologías
- Pasando la segunda mitad de los años noventa se comenzaron a descubrir vulnerabilidades sobre los sistemas instalados ...

Fuente: Ernst & Young – 2004 Global Security Survey

Puntos relevantes

- El 90% de las organizaciones afirman que la seguridad sobre sus sistemas de información es de vital importancia para alcanzar sus objetivos generales.
- El 78% las organizaciones afirman que la reducción de riesgos es el principal objetivo de los gastos en Seguridad Informática.

Sin embargo ...

- Una de cada tres organizaciones consideran que no es adecuada su capacidad para:
 - Determinar si sus sistemas son vulnerables
 - Responder a incidentes de seguridad
- Sólo una de cada tres organizaciones aseguran que cumplen con regulaciones de seguridad.
- Más de la mitad de las organizaciones coinciden en que las restricciones presupuestarias son el principal obstáculo para implementar un programa efectivo de seguridad informática.

Fuente: Ernst & Young – 2004 Global Security Survey

Puntos relevantes (cont.)

Las mayores implicancias de la Seguridad Informática se pueden resumir en los siguientes puntos:

- A pesar de la generalizada visión sobre la criticidad de una evaluación de riesgos, sólo el 27% de las empresas considera que “los resultados de una evaluación de seguridad de la información” se encuentra entre los tres factores más influyentes.
- La tecnología es el imán más poderoso para conseguir fondos dentro de las organizaciones. De estas inversiones, lo invertido en Seguridad Informática aparenta ser extremadamente bajo comparado con tecnología.
- Los virus y los “troyanos” son las principales preocupaciones de seguridad y continúan captando la mayor atención de los medios y el público.

Fuente: Ernst & Young – 2004 Global Security Survey

Situación Actual

El 52 % de las empresas reconocen haber sufrido interrupciones inesperadas o no programadas de sus sistemas críticos de negocio.

- Se producen aproximadamente 200 incidentes diarios de gravedad en el mundo
- El 90% de las empresas del mundo son víctimas de ataques informáticos contra sus redes
- El 70% de los ataques provienen desde Internet
- Se detectaron 1220 nuevas vulnerabilidades en lo que va del año
- Aparece el concepto de “Managed Security”
- Aparecen los SSP (Security Service Provider)

“En 2004 los ataques provocaron pérdidas de entre 40.000 y 50.000 M de dólares”

Evolución de incidentes publicados

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**

Fuente: CERT

Evolución de vulnerabilidades

Vulnerabilities reported 1995-1999

| Year | 1995 | 1996 | 1997 | 1998 | 1999 |
|-----------------|------|------|------|------|------|
| Vulnerabilities | 171 | 345 | 311 | 262 | 417 |

2000-2005

| Year | 2000 | 2001 | 2002 | 2003 | 2004 | 1Q,2005 |
|-----------------|-------|-------|-------|-------|-------|---------|
| Vulnerabilities | 1,090 | 2,437 | 4,129 | 3,784 | 3,780 | 1,220 |

Total vulnerabilities reported (1995-1Q,2005): **17,946**

Fuente: CERT

Organización y Reportes

Se analiza con que frecuencia las organizaciones proporcionan al Directorio o entidad equivalente un informe sobre el estado de la seguridad de la información o incidentes de seguridad.

- El 36% de los consultados reportan incidentes de seguridad al directorio al menos trimestralmente, mientras que,
- El 12% realizan los reportes en forma semestral
- El 38% lo hacen anualmente o aún menos
- El 14% nunca reportó al directorio

Fuente: Ernst & Young – 2004 Global Security Survey

Metodologías de SA y PT

Information Gathering

Networking information

Se basa en buscar y descubrir como esta armada la red y sus direcciones IP publicas y privadas

- ✓ Estructura de la red
- ✓ Gateways
- ✓ Firewalls
- ✓ Saltos

firewalk / traceroute / mtr / ping

Fingerprinting

Buscamos patrones del stack TCP/IP o de alguna respuesta de la red para identificar el Sistema Operativo

- ✓ Características propias del Sistema Operativo
- ✓ Análisis de comportamiento del Sistema Operativo

nmap / p0f / scapy / queso

Information Gathering (cont.)

Advanced fingerprinting

Identificación de servicios según protocolo y respuestas

- ✓ Análisis de tráfico de servicios (Ej. banner grabbing)

scapy / spike / nmap

Port scanning

De esta manera se identifican los servicios activos y que ports están habilitados en el firewall

- ✓ Protocolos: tcp y udp
- ✓ Tipos de escaneos

nmap (+ flags)

Information Gathering (cont.)

Vulnerability scanning

Chequeo rápido contra base de vulnerabilidades, sin descartar nada.

nessus / retina

Ingeniería Social

Búsqueda de información sensible o no sensible.

- ✓ Llamadas telefónicas
- ✓ Google
- ✓ Web Corporativa (nombres, teléfonos, emails, cargos, etc.)
- ✓ Intranet

whois / nic

Análisis

Sistema Operativo y servicios

Se determinan, en los casos que sean posibles, que Sistemas Operativos se corre, junto con que servicios.

- ✓ Detección de NAT (Uso de DMZ)
- ✓ Configuraciones

También en este punto se prueban funciones específicas del servicio y su respuesta ante las distintas variantes de un protocolo

(Ej: DNS: zone transfer, cache poisoning, ttl)

scapy / p0f

Análisis (cont.)

Versiones Vulnerables

Según los datos obtenidos previamente, se analizan vulnerabilidades búsqueda y validación de versiones vulnerables (99 %)
misconfigurations (ej. mysql y samba)

- ✓ Bugs conocidos
- ✓ Bugs desconocidos
 - Zero days
 - Reserching propio

nessus / retina / cve / nvd (ex-icat) / propias

Ataques y Penetraciones

Denial of Service (DoS)

Se intenta saturar un servicio para bloquearlo. Depende del protocolo y servicio que pruebas se realizan.

- ✓ TCP Syn flood
- ✓ Análisis de posible impacto

tools propias

Exploits

Una vez determinado un servicio vulnerable se procede a su explotación

- ✓ Testing de exploits (lab, virtual machines)
- ✓ Introducción de exploits (local o remoto)
- ✓ Ejecución de código arbitrario
- ✓ Análisis del comportamiento post-exploiting

metasploit / packetstorm

Ataques y Penetraciones (cont.)

Privilege Escalation

Si es necesario el exploiting se divide en dos etapas, ganar una shell de usuario no privilegiado y luego explotar nuevamente para lograr acceso administrador o root.

Por lo general, existen muchas vulnerabilidades locales, lo cual amplía el panorama de ataque. (Ej. kernel, servicios win32 system, sendmail)

Brute Forcing

Cuando no se encontraron vulnerabilidades (o no se conocen) se procede a un ataque de fuerza bruta. Generalmente las pruebas son USER / PASS

- ✓ Servicios factibles a ataques de diccionario (ssh mysql telnet imap smb cisco ldap mssql nntp vnc socks cvs)
- ✓ Sistemas con autenticación en general
- ✓ /etc/passwd
- ✓ SAM (win32)

hydra / john the ripper

Una vez dentro...

Covering Tracks

Se intenta borrar los rastros de todo ataque o intrusión realizada. Esto se hace solamente a pedido del cliente y a veces para probar sus propios sistemas.

Logs

- ✓ Archivos estándar
- ✓ Servicios
- ✓ Historiales (accounting)
- ✓ /var/log/* lastlog wtmp utmp .bash_history ...

IDS

- ✓ Identificación de ataque y eliminación del log
- ✓ Generación de ruido (muchas alarmas en celulares)
- ✓ Comportamientos "normales"
- ✓ Encoding shellcodes (no usar NOPs)

Covering Tracks (cont.)

Integrity Check

- ✓ Detección
- ✓ Actualización

Otros

- ✓ Terminales dev/tty
- ✓ Registros físicos (posibles impresiones)

Consolidación

Se intenta seguir escalando a otros servicios, y facilitar la tarea entrando de forma directa, sin la necesidad de repetir los ataques.

Sniffing

- ✓ Tráfico de toda la red
- ✓ Capturar passwords en texto plano

pop / imap / smb / ...

tcpdump / ethercap / kismet (wifi) / ethereal

Backdoors

Distintos niveles de complejidad

- ✓ Sockets
- ✓ Hiding process
- ✓ Covered channels
- ✓ User y kernel mode

Consolidación (cont.)

Rootkits

- ✓ Comandos más comunes
 - ls / netstat / ps / ...
 - Una manera de evitar chequeos de md5 periódicos

adobe (LKM)

Keyloggers

- ✓ Capturar información sensible

Ej: <http://people.baicom.com/~agramajo/misc/myread.c>

Ejemplos

Explotando bugs en Win32

- ✓ Plataforma
 - Windows 2000 SP3
 - Sin patches
 - Recién instalado
- ✓ Scanning rápido
- ✓ Utilizar un framework de exploits open source
 - Metasploit
 - RPC bug
Microsoft RPC DCOM MSO3-026
 - VNC injection

Ejemplos (cont.)

Descubriendo un bug en Win32

- ✓ Warftpd 1.65
 - Fuzzer
 - Debugger
 - Creación del exploit
 - Shellcodes

Para seguir investigando...

Herramientas

- ✓ Metasploit <http://www.metasploit.org>

Repositorios de bugs / exploits / vulns

- ✓ <http://www.frsirt.com/> (ex k-otik)
- ✓ <http://www.packetstormsecurity.org/>
- ✓ <http://cve.mitre.org/cve/>
- ✓ <http://www.securiteam.com/>
- ✓ <http://icat.nist.gov/>
- ✓ <http://www.osvdb/>

Listas de correo

- ✓ Full-Disclosure
- ✓ Vulnwatch
- ✓ SANS
- ✓ Vuln-Dev
- ✓ Repositorio de listas: <http://archives.neohapsis.com/>

Productos y Servicios

BAICOM networks

Security

Servicios

- ✓ BAICOM Security Assessment
- ✓ BAICOM Penetration Test
- ✓ BAICOM Forensics Analysis
- ✓ BAICOM Security Policies
- ✓ BAICOM Source Code Audit
- ✓ BAICOM Detect Anomaly Behavior
- ✓ BAICOM Managed Security

Security

Productos

- ✓ BAICOM Firewall
- ✓ BAICOM VPN Concentrator
- ✓ BAICOM IDS

IT & Networking

Productos

- ✓ HotSpot Integrated Solution (HIS)
- ✓ Proxy Server & Content Filtering
- ✓ Perimetral Networking Box
- ✓ Mail Server Solution
- ✓ Backup Server

Servicios

- ✓ MAB Servers
- ✓ MAG Networking & Security

Consulting

Servicios

- ✓ Análisis de Negocios
- ✓ Reducción de Costos
- ✓ Gerenciamiento de Proyectos
- ✓ Tercerización de Servicios
- ✓ Desarrollo de Aplicaciones
- ✓ Capacitaciones, Cursos y Workshops

Consultas y Preguntas

Muchas Gracias