

Seguridad en *nix y OpenSSH

Boris J. Quiroz Q.
Director de Tecnologías
Substance.
boris{at}substance.cl



Donde no hay seguridad nadie puede romperla.

RMS

Agenda

Introducción a la Seguridad.

SSH y OpenSSH.

Vulnerabilidades de OpenSSH.

El *problema* de Debian.

Buenas prácticas.

Introducción a la Seguridad

Seguridad física + Seguridad lógica
Problema humano.



Esa cosa llamada SSH

Integridad y confidencialidad.

Diversos tipos de autenticación.

AAA

OpenSSH

Encripta toda la transmisión.

Permite crear túneles.

Port Forwarding.

Inseguro

Métodos de autenticación.

Passwd.

Claves públicas. (*)

Keyboard-interactive.

GSSAPI.

Vulnerabilidades de OpenSSH

Configuraciones por *default*.

Suplantación de identidad.

Autenticación básica.

0-day exploit.

Julio de 2009

Fáciles de prevenir. *Para el que sabe*

Claves públicas (*)

Criptografía simétrica

Vulnerable al acceso físico

Únicas e irrepetibles (?)

RSA y DSA

```
boris[at]bitch:~$ cat ~/.ssh/id_rsa.pub
```

```
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA vLZNSFY37GVI2PbC5XpGqFH8JF/  
2TgmzzU1qEEA4vwBJuGrPJn01O9nDyxnYJsqq6wljo6TpAGtUS5GZg+ETe/RyrG5  
yDZ51cWfvRg0bXm0IKuzWv04+p5ESmzfAVKtDtJ+6yVApRK2RwJGLS4sPDZpYx  
HcNOCIPbtX8m1ej23zm3Gc3UynmWBKc8XKjPoDR/BLIU87DwZd7KGId+F4HGHB  
MtvkcerrJ3Sa43ZMi88PT0vcuGC/PZYt83FLXoi2HvjB6H7gfx7VdwlikVgfoUcW9aZ0x  
OwC185Y6feVEGBmCns5cNCaNjyGY21xLQVy27S3VYzdUSI9VJ11ACZIXGXw==  
boris@bitch
```

Entonces...

¿Qué método usar?
¿Cuál es más seguro?

El problema de Debian

Luciano Bello (AR).

Predicción de un número aleatorio.

Cualquier materia criptográfico.

SSH (RSA y DSA), OpenVPN, X.509,
DNSSEC, SSL/TLS.

DSA-1571-1.

Buenas prácticas

Seguridad **no** invasiva.

Deshabilitar servicios en desuso.

hosts.allow && hosts.deny.

Sistema **siempre** up-to-date.

Modificar puertos de acceso.

Portknocking.

Certificados digitales.

Conclusiones

Un solo método de autenticación no es suficiente.

Seguridad amigable con el usuario.

No sacamos nada con asegurar los extremos.

Jornadas Regionales de Software Libre

Encuentro de nivel mundial.

MozCamp Hispano.

Auspiciado por INACAP.

www.jornadasregionales.org



¿Preguntas?

boris{at}substance.cl

<http://www.substance.cl>

<http://boris.insert-coin.org>

http://twitter.com/cereal_bars

