

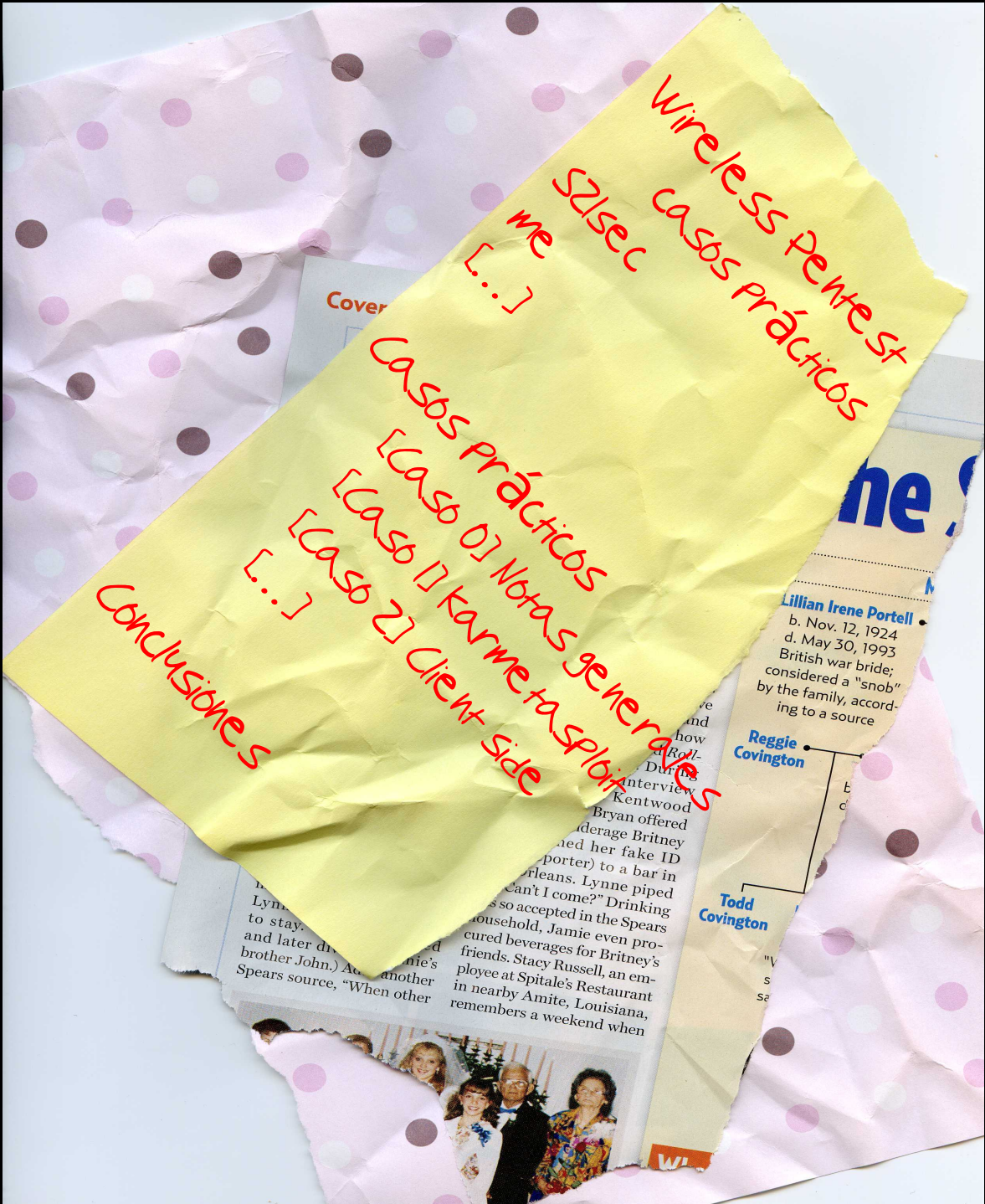
Pentest

wireless

casos prácticos

FRANCISCO CABALLERO CALZADA (FCABALLERO@S21SEC.COM)
S21SEC

La información facilitada en este documento es propiedad del autor, quedando terminantemente prohibido la modificación o explotación de la totalidad o parte de los contenidos del presente documento, sin el consentimiento expreso y por escrito del mismo, sin que en ningún caso la no contestación a la correspondiente solicitud pueda ser entendida como autorización presunta para su utilización.



Wireless Pentest
casos prácticos
S2Sec
me
[...]

Casos Prácticos
[Caso 0] Notas generage
[Caso 1] Karne ta split
[Caso 2] Client Side
[...]

Conclusiones

Lillian Irene Portell
b. Nov. 12, 1924
d. May 30, 1993
British war bride;
considered a "snob"
by the family, accord-
ing to a source

Reggie
Covington

Todd
Covington



S2TSEC

Año 2000 NcN Mallorca

Igor Uruñe,

Mikel Fernández y

Xabier Mitxelena

Gestión Integral de
Seguridad Digital

I+D+i

SOC (Security

Operations Center)

CERT (Center

Emergency Response Team)

Bitácora

Bitácora Horizon

Vigilancia Digital

6 - España

3 - Internacionales

2 - Partners Int.

La seguridad digital del futuro, hoy.

ABOUT ME

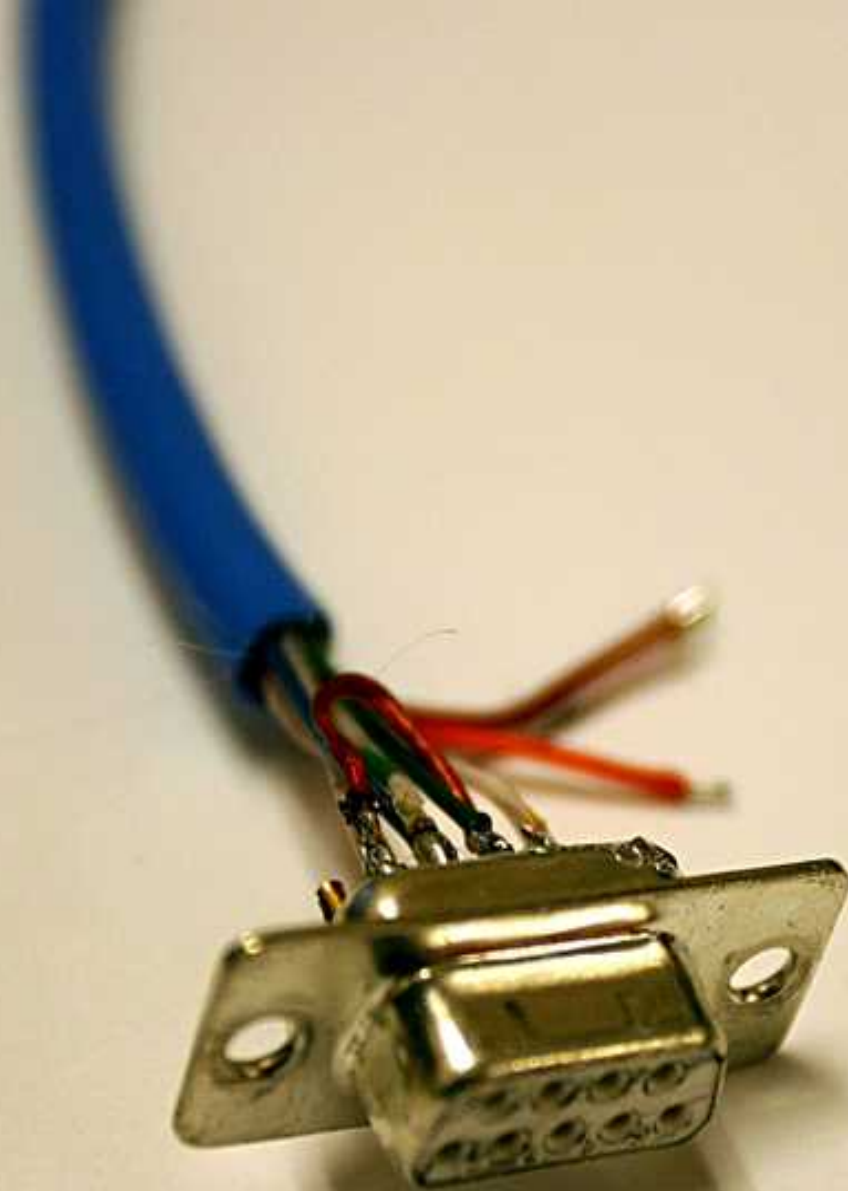
Senior Security Auditor
Director Técnico SZIsec MX
Inter. Support Manager AR

Aster Sistemas de Control
DDTel
Coiffure Hispania

Wireless Pentest
Análisis Forense
APW Pentest
Internal/External Pentest
Reverse Engineering

México
Argentina
USA
Israel
Portugal

Zazen
Aikido
Atletismo
Fútbol



CASOS PRÁCTICOS

CASOS: NOTAS GENERALES

Chipset

Permiso

Tiempo

Ganas

- Linux en muchos casos -

CASOS: notas generales

Redes abiertas

SSID oculto

ACLs

Portales cautivos

Cifrado WEP

Cifrado WPA/WPA2

CASOS: notas generales

WPACracker (400 CPUs...
diccionario 135mills palabras)

WPA

Wlan_XXXX

Jazztel_XXXX

Casos 1 y 2: notas

Antenas

Amplificador de señal

Tarjetas de alta potencia

Caso 1: karma Metasploit

Módulo/plugin de Metasploit (karma.rc)

(Metasploit: framework de explotación de vulnerabilidades)

Fake AP

Obtención de información

Caso 18: karmetasploit

Sniffing y detección de clientes buscando AP

Activación modo monitor

Activación IP Forward

Configuración Rogue AP

Configuración IP rogue AP

Configuración DHCP Server

Caso IC: karmetasplit

Redirección de paquetes

entrantes y salida hacia Internet

karmetasplit

]...[cookies, info, datos, shell,]...[

Caso 2: Client side

Sniffing y detección de clientes buscando AP

Activación modo monitor

Probe request de los clientes (identificación)

Activación IP Forward

Configuración Rogue AP

Configuración IP rogue AP

Configuración DHCP Server

Caso 28 Client Side

Redirección de paquetes

entrantes y salida hacia Internet

Sniffing

SSLstrip

Caso 2C Client side

Windows XP

(HLM/Software/Microsoft/WZCSV/C/Parameter/
Interfaces/<interface wireless guid>)

Windows Vista/7 (ProgramData/Microsoft/
Wlansvc/Profiles/Interface/<interface guid>)

Linux (/etc/wpa_supplicant/wpa_supplicant)

CONCLUSIONES

¿Son seguras vuestras redes?



Preguntas