Rede Nacional de Ensino e Pesquisa - RNP
Centro de Atendimento a Incidentes de Segurança - CAIS
30 de Junho de 2007

GTS Grupo de Trabalho em Segurança

# Caixa de Ferramentas do Auditor Wi-Fi

**Ronaldo Vasconcellos**


## Sumário

- Caixa de Ferramentas
- Software
- Hardware
- Combinações

## Caixa de Ferramentas

- Conjunto de software e hardware ideais
- Bom custo/benefício
- Linux, Windows
- Sugestões de hardware
- Merchandising Linksys não é intencional

## Caixa de Ferramentas (2)

### HARDWARE

- Dell D620 Pre-configuredLaptop
- Nokia N800 Internet Tablet
- 5 Wireless NIC Cards
- 5 Antennas • Spectrum Analyzer
- 2.4 GHz Jammer • Access Points • Garmin Portable GPS
- WiFi Finder

### SOFTWARE

- Air Defense Mobile
- OmniPeek Personal
- NetScanTools Pro
- 'The Network Toolkit'
- Wireshark w/AirPcap
- WiFi Hopper
- KF Sensor Honeypot
- Custom Linux Attack Scripts
- Backtrack V.2.0 Suite of Tools

## Caixa de Ferramentas (3)

- CWNP Kit HotLabs WLSAT (25/04/07)
  - Wireless LAN Security Assessment Toolkit
  - $6,995 USD = Dell Latitude D620, XP Pro, BackTrack, software, 5 NIC, treinamento
  - Interessante, mas caro e sem alguns itens úteis.
  - http://www.hotlabs.org/wlsat
  - O assunto da apresentação é um “Poor Man’s WLSAT”

## Software

- BackTrack 2.0
  - Live CD Linux
  - Kismet, Aircrack-ng (WEP PTW), Wicrawl, Karma, Airpwn, coWPAtty e várias outras ferramentas 802.11 prontas para usar

## Software (2)

- VMware
  - Limitador: apenas interfaces USB
  - Carrega BackTrack de um arquivo ISO9660
  - Menu “VM > Removable Devices”
  - Chipset Ralink
    - Kismet: sources rt2400, rt2500, rt8180
    - Linksys WUSB54G (~$50 USD)

CAIS

## Software (3)

- VMware (2)

1-11

+


14


+

WIDS

KISMET

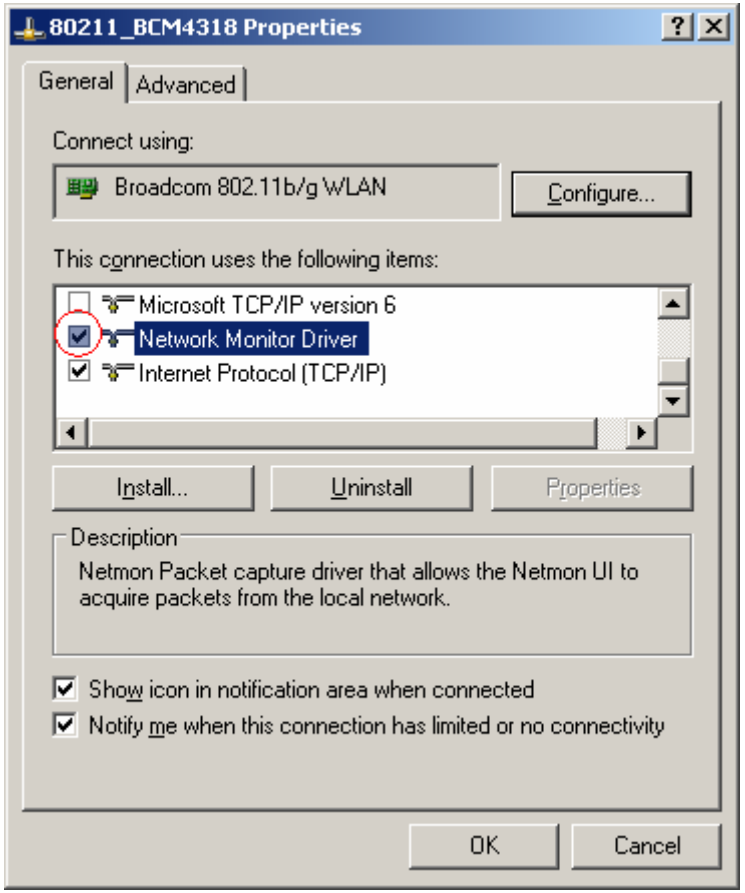
## Software (4)

- Windows Vista + Microsoft Network Monitor (netmon)

**http://connect.microsoft.com**
**http://blogs.technet.com/netmon/**

```
What's new in Network Monitor 3.1
(15/06/2007)

Ability to capture wireless 802.11
frames in monitor mode, and scan
across 802.11 physical layers and
channels on Windows Vista
```

## Software (5)

- Outras alternativas com Windows
  - Combinação de hardware, software e driver ideais
    - Mais adiante
  - Cygwin

## Hardware

- Objetivos
  - minimizar quantidade de equipamento
  - bom custo/benefício
  - maximizar compatibilidade com ferramentas
  - modo monitor vs. modo infrastructure


## Hardware (2)

- NIC
  - Chipsets imprescindíveis
    - Atheros
    - Prism 2.5
  - Drivers/módulos Linux
    - MadWifi
    - HostAP

CAIS

## Hardware (3)

- NIC (2)
  - Senao NL-2511CD Plus EXT2 Prism 2.5 (~$60 USD)
    - PCMCIA
    - 802.11b apenas
    - 200mW
    - antena interna, conector para antena externa (2x MMCX)
    - EIRP com antena direcional de 8dBi: 1.6W

## Hardware (4)

- NIC (3)
  - Ubiquiti SRC (AR5004) (~$130 USD)
    - Cardbus 802.11a/b/g
    - 300mW (b/g) e 100mW (a)
    - antena interna, conector antena externa (2x MMCX)
    - EIRP com antena direcional de 8dBi: 2.4W

## Hardware (5)

- NIC (4)
  - "Meu notebook já tem uma NIC WLAN, não quero/posso comprar um cartão PCMCIA/Cardbus"
    - Sem problemas, você ainda pode brincar.
  - Principais interfaces embutidas
    - Broadcom (Compaq, HP, Acer)
      - Linux: bcm43xx, ndiswrapper
    - Intel/Centrino
      - Linux: ipw2100, ipw2200, ipw3945

## Hardware (6)

- NIC (5)
  - "Não quero usar Linux"
  - Chipset Atheros
    - Modo Monitor em Windows 2000 / XP / Vista
    - Captura associada com Aircrack-ng (sem injeção)
    - AR5001, AR5002, AR5004, AR5005 e AR5006
    - Drivers Peek (www.wildpackets.com)

## Hardware (7)

- Extras
  - Antena direcional e GPS
    - 9dBi (LANPoynt YAGI-A0003), cabo pigtail LMR-100
    - GPS USB (Modelo BU-303)
  - Wardriving, Warwalking, War[whatever]
  - Mapas
    - NetStumbler, Kismet/GPSD + Google Earth (niquille.com/kismet-earth/)

CAIS

## Hardware (8)

- Extras (2)
  - WAP como agente remoto
  - OpenWrt
  - Versões de hardware específicas
    - Linksys: WRT54GL (4M Flash 16M RAM), WRTSL54GS (8/32 com **USB**)
    - Buffalo: WHR-HP-G54 (4/16), WHR-G54S (4/16)
  - Kismet
    - Arquitetura cliente-servidor
    - Drones

## Hardware (9)

- Extras (3)
  - AirPcap
    - Integração com Wireshark (“ex-Ethereal” ou “Éter Rial”)
    - A partir de $198 USD

## Hardware (10)

- Extras (4)
  - Wi-Spy
    - Analisador de Espectro barato
      - $99 USD → $199 USD (2007)
      - Wi-Spy 2.4x com conector externo ($399 USD)


CAIS

## Hardware (11)

- Extras (5)
  - Tablet Nokia 770
    - Suporte a Kismet (capture source “nokia770”)

## Informações de Contato

Centro de Atendimento a Incidentes de Segurança – CAIS

cais@cais.rnp.br - http://www.rnp.br/cais

Ronaldo Castro de Vasconcellos
GIAC GAWN SSP-DRAP
ronaldo@cais.rnp.br

# Contato com o CAIS: Notificação de Incidentes

Incidentes de segurança envolvendo redes conectadas ao backbone da RNP podem ser encaminhadas ao CAIS através de:

1. *E-mail*: **cais@cais.rnp.br**.

   Para envio de informações criptografadas, recomenda-se o uso da chave PGP pública do CAIS, disponível em: **http://www.rnp.br/cais/cais-pgp.key**

2. *Web*: Através do Formulário para Notificação de Incidentes de Segurança, disponível em: **http://www.rnp.br/cais/atendimento_form.html**

***Inoc-DBA:***

Para entrar em contato com o CAIS através da hotline INOC-DBA (Inter-NOC Dial-By-ASN): INOC-DBA: 1916*800

***Atendimento Emergencial:***

Contatos emergenciais fora do horário comercial (09:00 - 18:00) devem ser feitos através do telefone: **(61) 226-9465**.

***Alertas do CAIS***

O CAIS mantém a lista **rnp-alerta@cais.rnp.br**. Assinatura aberta à comunidade atuante na área. Inscrições através do formulário disponível em:

**http://www.rnp.br/cais/alertas**