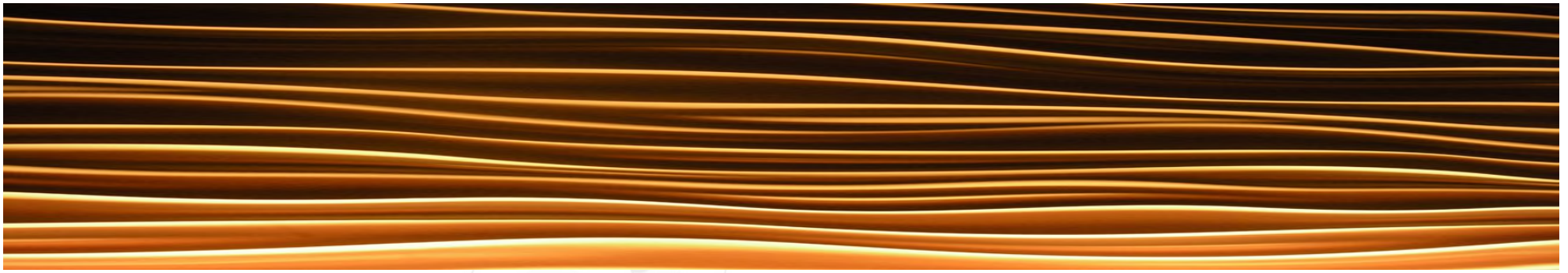


Beholder

Nelson Murilo
nelson(at)pangeia.com.br

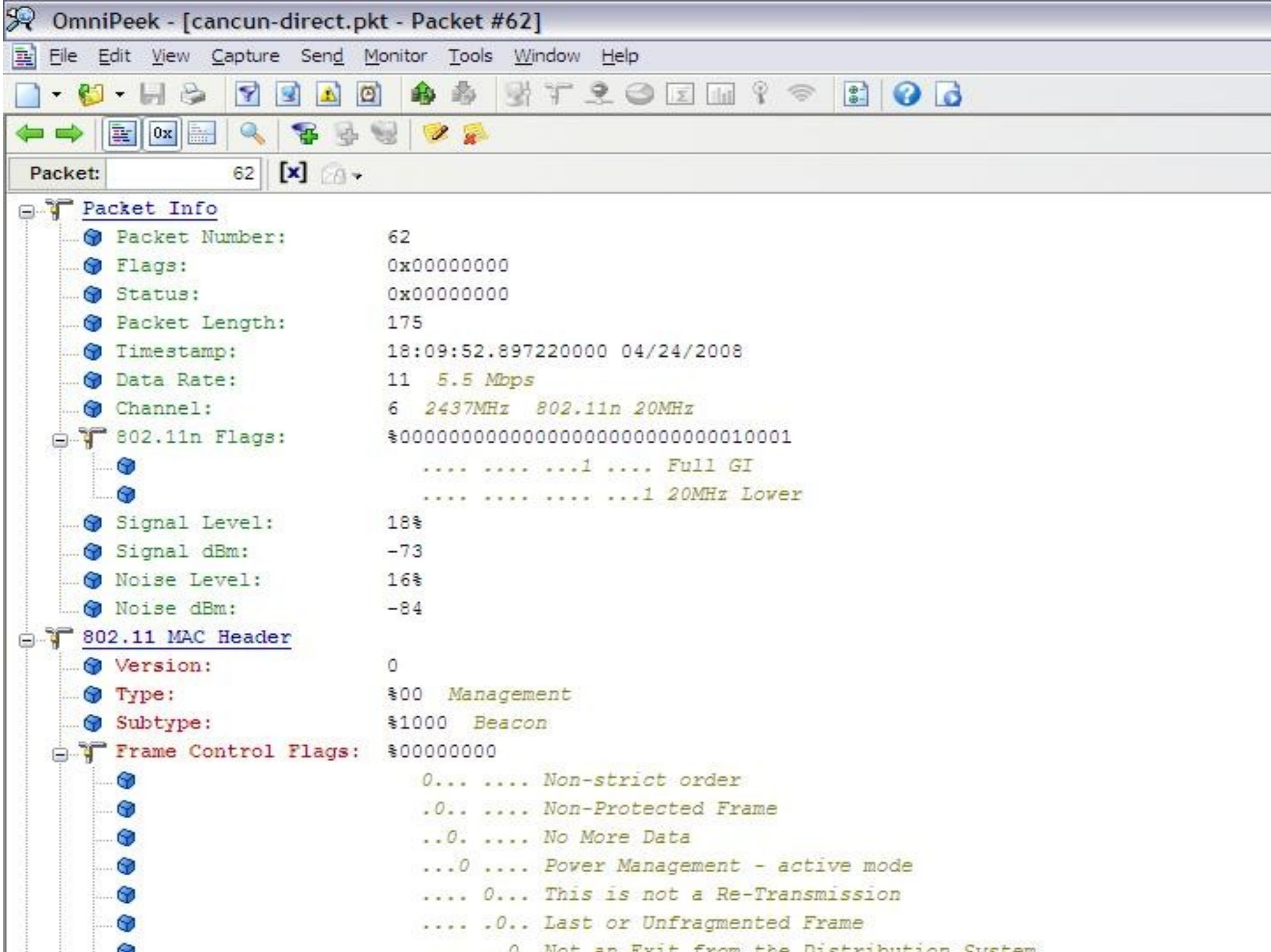
Agenda

- Motivação
- Conceitos
- Características
- Estrutura da ferramenta
- Tipos de detecção
- O que o Beholder não faz
- Cenários
- Demo

Motivação

- Observação das deficiências dos atuais WIDS
- Análise do código do wireless-tools
- Vislumbre que algo útil poderia ser feito
- Falar na DefCon

BEACONS


OmniPeek - [cancun-direct.pkt - Packet #62]
File Edit View Capture Send Monitor Tools Window Help
Packet: 62
Packet Info
Packet Number: 62
Flags: 0x00000000
Status: 0x00000000
Packet Length: 175
Timestamp: 18:09:52.897220000 04/24/2008
Data Rate: 11 5.5 Mbps
Channel: 6 2437MHz 802.11n 20MHz
802.11n Flags: %00000000000000000000000000010001
....1 .... Full GI
....1 20MHz Lower
Signal Level: 18%
Signal dBm: -73
Noise Level: 16%
Noise dBm: -84
802.11 MAC Header
Version: 0
Type: %00 Management
Subtype: %1000 Beacon
Frame Control Flags: %00000000
0... .... Non-strict order
.0.. .... Non-Protected Frame
..0. .... No More Data
...0 .... Power Management - active mode
.... 0... This is not a Re-Transmission
.... .0.. Last or Unfragmented Frame

802.11 Beacons

Podem esconder informações importantes

Packet: 62 [x]

- Cisco Proprietary
  - Element ID: 133
  - Length: 30
  - OUI: 00-0
  - Value: 0x00
  - AP Name: AP11-
  - Number of clients: 3
  - Value: 0x000025
- Vendor Specific
  - Element ID: 221 *Vendor Specific - Cisco*
  - Length: 6
  - OUI: 00-40-96
  - Data: (3 bytes)
- Vendor Specific
  - Element ID: 221 *Vendor Specific - Cisco*
  - Length: 5
  - OUI: 00-40-96
  - Version: 3
  - CCX Version: 3
- Vendor Specific
  - Element ID: 221 *Vendor Specific - Cisco*
  - Length: 22
  - OUI: 00-40-96
  - Data: (19 bytes)
- WMM
  - Element ID: 221 *WMM*
  - Length: 24
  - OUI: 00-50-F2

Número de clientes conectados

Hidden ESSID

File Edit Settings Help

scan
channel 6

Network device ath0 Refresh
Driver type Other

40 bit crack breadth: 3
128 bit crack breadth: 2

C	BSSID	Name	WEP	Last Seen	Last IV	Chan	Packets	Encrypted	Interesting	Unique	PW: Hex	PW: ASCII
	00:07:40:4D:1A:5C	Homenet54		Fri Apr 21 20:23:39 2006	00:00:00	3	542	0	0	0		
	00:09:5B:66:3D:0E	NETGEAR	Y	Fri Apr 21 20:23:23 2006	00:00:00	11	2	0	0	0		

Enable bridging to wired LAN

Enable SSID broadcast

Apply Cancel

File Edit Settings

scan
channel 6

Network device ath0 Refresh
Driver type Other

40 bit crack breadth: 3
128 bit crack breadth: 2

C	BSSID	Name	WEP	Last Seen	Last IV	Chan	Packets	Encrypted	Interesting	Unique	PW: Hex	PW: ASCII
	00:07:40:4D:1A:5C	Homenet54		Fri Apr 21 20:14:18 2006	00:00:00	3	266	0	0	0		
	00:09:5B:66:3D:0E	.....	Y	Fri Apr 21 20:13:58 2006	00:00:00	11	1	0	0	0		

Hidden ESSID

```
23:05:16.386193 Beacon () [1.0 2.0 5.5 11.0 6.0 12.0 24.0 36.0
Mbit] ESS CH: 11

23:05:16.488612 Beacon () [1.0 2.0 5.5 11.0 6.0 12.0 24.0 36.0
Mbit] ESS CH: 11

23:05:17.321039 Beacon (Homenet54) [1.0 2.0 5.5 11.0 Mbit] ESS
CH: 3

23:05:17.629271 Beacon (Homenet54) [1.0 2.0 5.5 11.0 Mbit] ESS
CH: 3
```

Características

Características

Escrito em C Ansi

Detecta mudanças de AP (ESSID, MAC, Canal, Modo, etc.)

Grandes variações de nível de sinal

Suporte ao uso de syslog (sensores)

...

Características


Your
karma
is leaking.

Karma

KARMA includes patches for the Linux MADWifi driver to allow the creation of an 802.11 Access Point that responds to any probed SSID. So if a client looks for 'linksys', it is 'linksys' to them (even while it may be 'tmobile' to someone else). Operating in this fashion has revealed vulnerabilities in how Windows XP and MacOS X look for networks, so clients may join even if their preferred networks list is empty.

Oferece DHCP
Captura de POP3/FTP credenciais
Redireciona tráfego HTTP para um servidor malicioso

Karma com esteróides

KARMA + MetaSploit3 + Aircrack-ng == KarmaSploit

MadWifi patch substituido por Aircrack-ng tools

Facilidade para criação de novos exploits

Integração com a vulnerabilidade do DNS (DK)

Novos exploits são imediatamente disponíveis assim que incorporados ao Metasploit.


```
/h[a4@](([c<](k)|(\|<)))|((k)|(\|<))|(x))\s+\
((d)|([t\+]h))[3ea4@]\s+p[l1][a4@]n[3e][t\+]/i
```


POWER
CHARGE
GNXT

Coisas ele NÃO faz

Colocar interface em modo promíscuo

Colocar interface em modo monitor

Quebrar chave WPA/WEP

Detectar falhas de rede em cliente ou AP

Desafios

Simples de instalar, usar e manter

De fácil entendimento e contribuição

Problemas

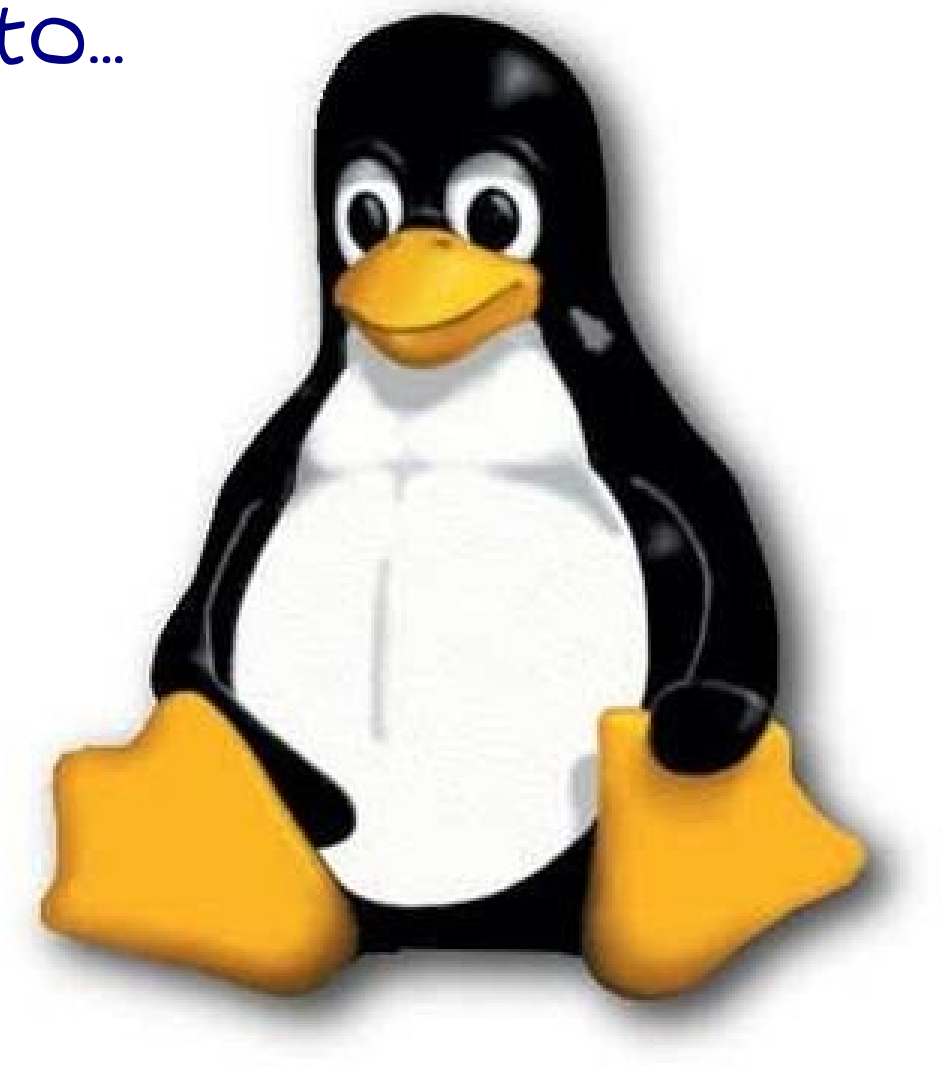
Diferentes interfaces tem tempos de varredura distintos

Driver Madwifi faz cache de Beacons recebidos

Ter menos dependências possível

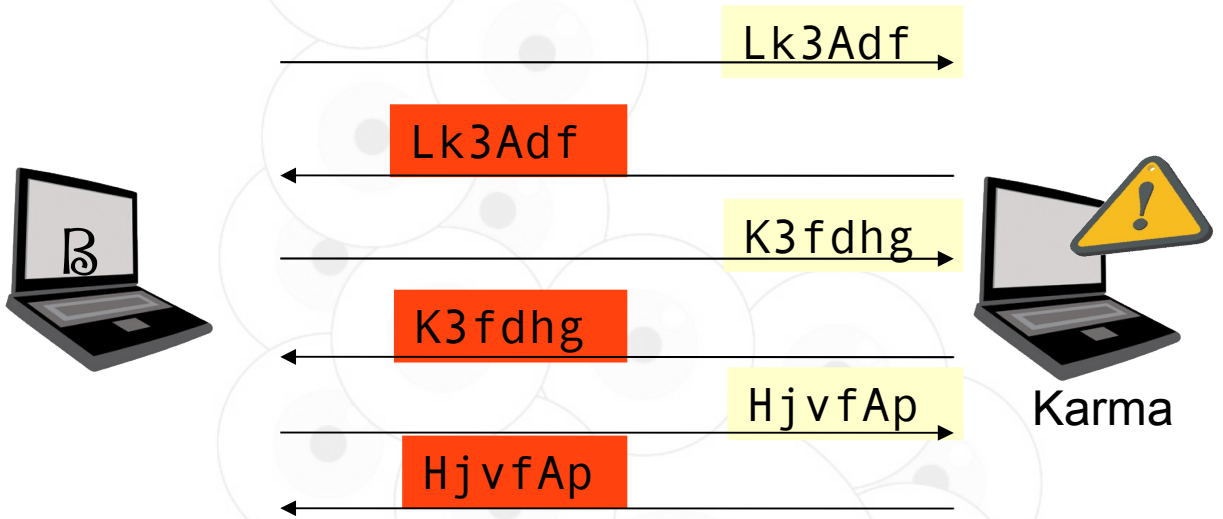
Disponibilidade

Por enquanto...



Futuro?

Detecção de Karma



Cenários
Alerta APs desaparecidos (RegEx)

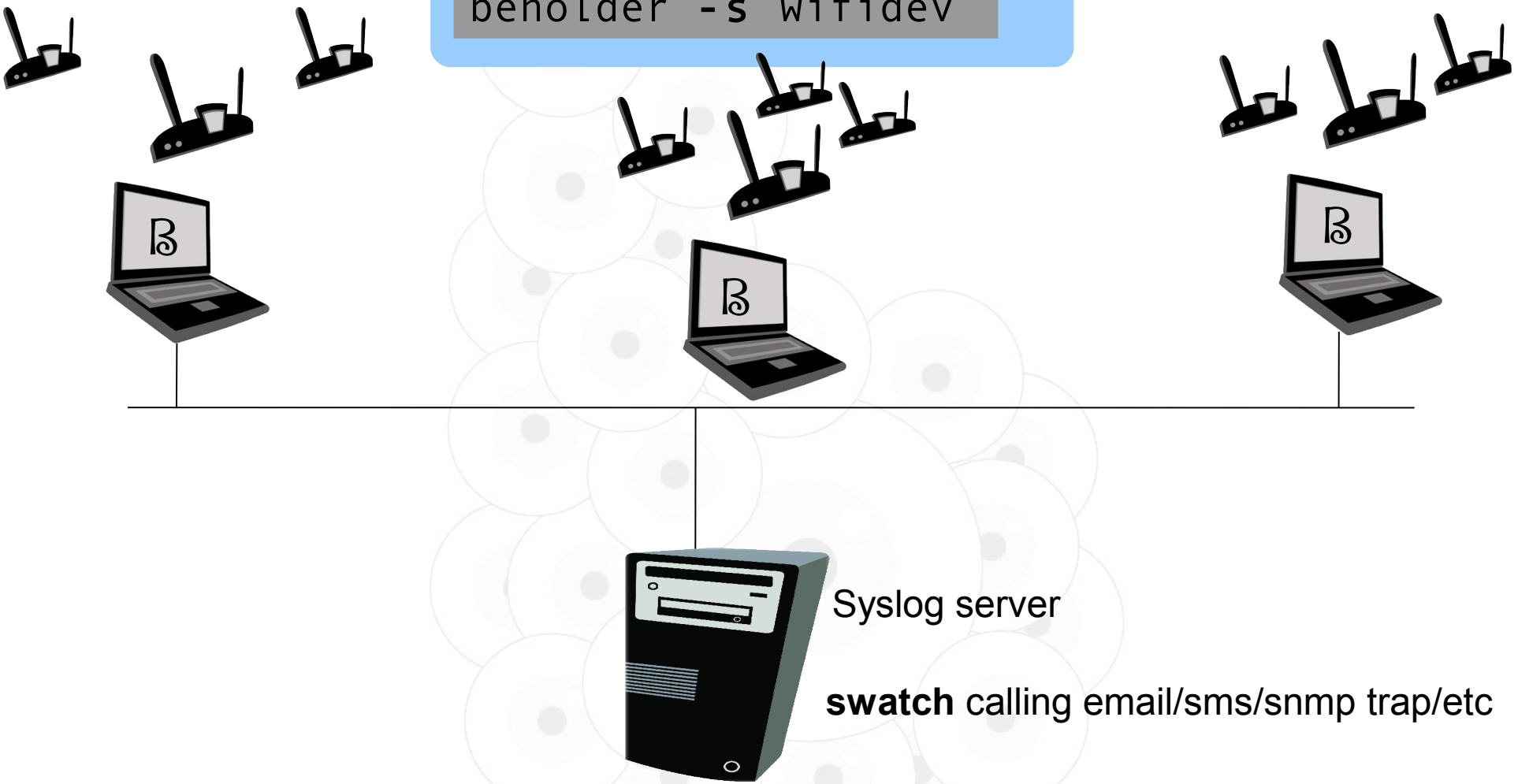
```
beholder -m “mynets” wifidev
```

Cenários
Verificação de essids similares (RegEx)

```
beholder -r “myne[t7]s.*” wifidev
```

Cenários
Grandes ambientes

```
beholder -s wifidev
```



Syslog server

swatch calling email/sms/snmp trap/etc

Let me see the code

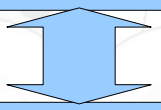
Números

```
$ wc -l *.[ch]
   807 beholder.c
  2169 iwlib.c
   603 iwlib.h
   773 wireless.h
  4352 total
```

Let me see the code

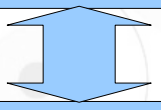
BEHOLDER Código

Detecções, Regex, Etc.



IWLIST Código

Beacons, WiFI interface



Hardware

Let me see the code

Estrutura

- Varredura inicial
- Loop infinito
  - Detecção de jamming
  - Detecção de AP/AD-Doc
  - Detecção de anomalias
    - Mudanças Mac, Channel, mode, etc.
    - Detecta APs com nomes similares
    - Detecta APs desaparecidos
  - Envia requisições de assoc. randômicas
  - Verifica resposta de karma

Let me see the code

Implementação de REGEX:

Duas funções

Compilar:

```
int regcomp(regex_t *preg, const char *regex, int cflags);
```

Comparar:

```
int regexec(regex_t *preg, const char *strings, size_t nmatch,,
regmatch_ pmatch[], int eflags);
```

Let me see the code

Deteção do Karma

```
char *karma_trap(int skfd, const char *dev){
   struct iwreq wrq;
   [...]
   char essid[KARMA_TRAP_LEN] = "XXXXXX";
   [...]
   // Create a random ESSID
   mktemp(essid);
   wrq.u.essid.pointer = (caddr_t) essid;
   [...]
// Set random ESSID
   if(iw_set_ext(skfd, dev, SIOCSIWESSID, &wrq) < 0)
   [...]
  // Get random ESSID
   if(iw_get_ext(skfd, dev, SIOCSIWESSID, &wrq) < 0)
```

Let me see the code

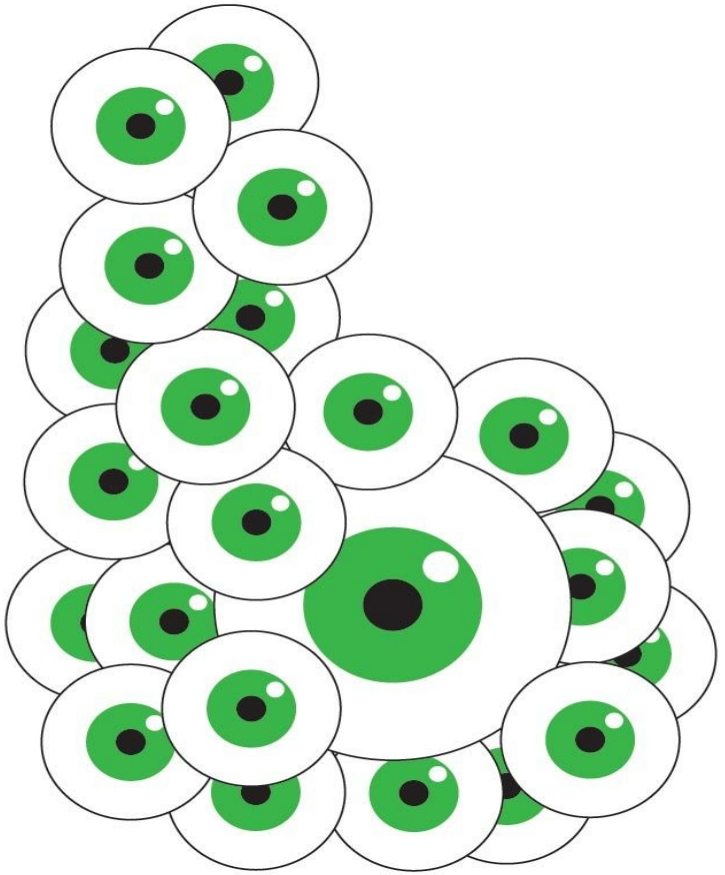
Detecção de jamming

```
while (ap_temp)
{
        if (!wscan_init) /* AP table empty */
        {
           jam++;

           if (jam == 3) // if table empty after 3 seq scanning
           {
              print_out(slog, "ALERT: Danger, Will Robinson!
Jamming device detected\n");
              break;
           }
        }
  }
```

Demo?

Pegue um grátis



http://www.beholderwireless.org

http://ysts.org

english evento a

You Sh0t the

agend

17 de n

patr

Keynote Speaker
David "H1kari" Hulton

Uma Breve Folksonomia(*) dos Hackers
Adriano Cansian

Point of Sales Hacking
Nicholas J. Percoco

Auditores vs. Auditados:
Francisco Milagres

Keynote Speaker
Emmanuel Goldstein

Segurança da Informaçao X Economia
Anderson Ramos

Most people knows about pen-test strategy, but miss tactical
Wendel Guglielmetti Henrique

Sharing my Mic with a (pop)Star and a Little Bit More of Cold Boot Attacks
Bruno Goncalves de Oliveira

beholder