

## Sample *Snort* Signature


```
alert tcp $EXTERNAL_NET any -> $HOME_NET 139
  flow:to_server,established
  content:"|eb2f 5feb 4a5e 89fb 893e 89f2|"
  msg:"EXPLOIT x86 linux samba overflow"
  reference:bugtraq,1816
  reference:cve,CVE-1999-0811
  classtype:attempted-admin
```

## Sample *Snort* Signature

- ```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS
  $HTTP_PORTS
  (msg:"WEB-CGI finger access";
  flow:to_server,established;
  uricontent:"/finger"; nocase;
  reference:arachnids,221;
  reference:cve,1999-0612;
  reference:nessus,10071;
  classtype:attempted-recon;
  sid:839; rev:7;)
```

## Snort Botnet Command-and-Control Rule

- alert ip \$HOME\_NET any ->
   
[206.59.139.195,207.114.175.51,207.126.115.205,207.126.115.219,207.12
   
6.162.236,207.126.162.237,207.150.167.55,207.162.194.151,207.179.120.
   
238,207.182.240.68,207.192.72.43,207.192.72.99,207.192.73.110,207.210.
   
208.16,207.44.152.199,207.44.180.227,207.44.184.225,207.45.69.69,208.1
   
00.20.83,208.100.20.90,208.100.23.100,208.100.38.15,208.110.65.135,208
   
.110.69.227,208.111.34.13,208.111.35.75,208.127.19.151,208.146.35.105,
   
208.146.35.106,208.167.236.6,208.167.237.120,208.185.80.72,208.185.80.
   
74,208.185.80.85,208.185.80.87,208.185.81.205,208.185.81.237,208.185.8
   
1.243,208.185.82.128,208.185.92.26,208.185.92.31,208.20.225.248,208.27
   
.69.193,208.51.40.10,208.51.40.2,208.53.146.4,208.53.146.6,208.53.148.1
   
11,208.53.148.254,208.53.148.8,208.53.150.43,208.53.150.44,208.53.163.
   
194,208.53.172.67,208.53.175.92,208.53.181.86,208.67.249.244,208.68.94
   
.62,208.72.157.63,208.77.191.41] any
   
(msg:"ET DROP Known Bot C&C Server Traffic (group 5) ";
   
reference:url,www.shadowserver.org; threshold: type limit, track by\_src,
   
seconds 3600, count 1; classtype:trojan-activity; sid:2404004; rev:1660;)



[MarketPlace](#) [About](#) [Services](#) [FAQ](#) [Blog](#) [Contacts](#)

Home page > Current bids

**Sign In**

Username

Password

[Sign in](#)

New user? [Sign up here](#)

**News**

**PRESS RELEASE** 03/07/2007

Finally a Marketplace Site for Security Research

Current bids
MarketPlace history

4 items found, displaying all items. Page 1

| Code        | Time to live | Title                                       | System          | Offer type            | Bid                     |
|-------------|--------------|---------------------------------------------|-----------------|-----------------------|-------------------------|
| ZD-00000007 | 9d 13h 26m   | Local Linux kernel memory leak              | Linux           | Bidding               | 600€ 1 bid(s)           |
| ZD-00000005 | 9d 13h 26m   | Yahoo! Messenger 8.1 remote buffer overflow | Windows XP      | Bidding               | 2,000€ 0 bid(s)         |
| ZD-00000004 | 9d 13h 26m   | Squirrelmail GPG Plugin Command Execution   | Web application | Bidding<br>Buy now at | 600€ 1 bid(s)<br>1,750€ |
| ZD-00000008 | 10d 13h 26m  | MKPortal SQL injection                      | Web application | Bidding<br>Buy now at | 500€ 0 bid(s)<br>800€   |

**Current bids**

4 items found, displaying all items. Page 1

| Code        | Time to live | Title                                       | System          | Offer type            | Bid                     |
|-------------|--------------|---------------------------------------------|-----------------|-----------------------|-------------------------|
| ZD-00000007 | 9d 13h 26m   | Local Linux kernel memory leak              | Linux           | Bidding               | 600€ 1 bid(s)           |
| ZD-00000005 | 9d 13h 26m   | Yahoo! Messenger 8.1 remote buffer overflow | Windows XP      | Bidding               | 2,000€ 0 bid(s)         |
| ZD-00000004 | 9d 13h 26m   | Squirrelmail GPG Plugin Command Execution   | Web application | Bidding<br>Buy now at | 600€ 1 bid(s)<br>1,750€ |
| ZD-00000008 | 10d 13h 26m  | MKPortal SQL injection                      | Web application | Bidding<br>Buy now at | 500€ 0 bid(s)<br>800€   |

## 1 day of "crud" seen at ICSI (155K times)

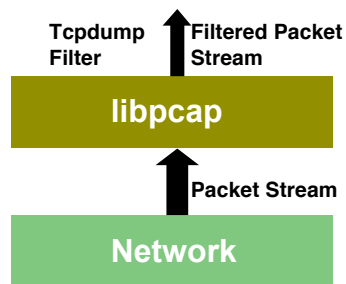
|                                   |                           |                                     |                            |
|-----------------------------------|---------------------------|-------------------------------------|----------------------------|
| active-connection-reuse           | DNS-label-len-gt-pkt      | HTTP-chunked-multipart              | possible-split-routing     |
| bad-ident-reply                   | DNS-label-too-long        | HTTP-version-mismatch               | SYN-after-close            |
| bad-RPC                           | DNS-RR-length-mismatch    | illegal-%-at-end-of-URI             | SYN-after-reset            |
| bad-SYN-ack                       | DNS-RR-unknown-type       | inappropriate-FIN                   | SYN-inside-connection      |
| bad-TCP-header-len                | DNS-truncated-answer      | IRC-invalid-line                    | SYN-seq-jump               |
| base64-illegal-encoding           | DNS-len-lt-hdr-len        | line-terminated-with-single-CR      | truncated-NTP              |
| connection-originator-SYN-ack     | DNS-truncated-RR-rdlength | malformed-SSH-identification        | unescaped-%-in-URI         |
| data-after-reset                  | double-%-in-URI           | no-login-prompt                     | unescaped-special-URI-char |
| data-before-established           | excess-RPC                | NUL-in-line                         | unmatched-HTTP-reply       |
| too-many-DNS-queries              | FIN-advanced-last-seq     | POP3-server-sending-client-commands | window-recision            |
| DNS-label-forward-compress-offset | fragment-with-DF          |                                     |                            |

## How Bro Works

**Network**

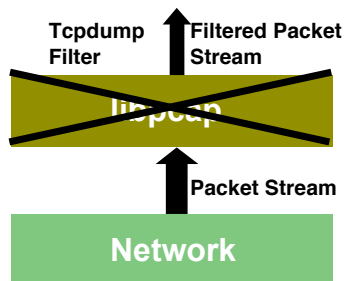
- Taps 10G fiber link passively, sends up a copy of all network traffic.

## How Bro Works



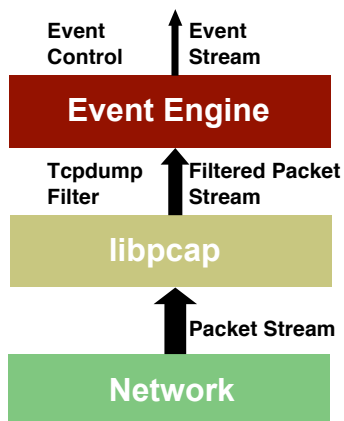
- Kernel filters down high-volume stream via standard *libpcap* packet capture library.

## How Bro Works



- ~~• Kernel filters down high-volume stream via standard *libpcap* packet capture library.~~
- Originally: 100X gain
- Recently: 10X gain
  - Must analyze more applications in traffic
- Today: **no gain**
  - Must analyze traffic that is trying to **hide** by *using other ports*
  - E.g., **Skype**
  - E.g., **botnet** command-and-control over IRC

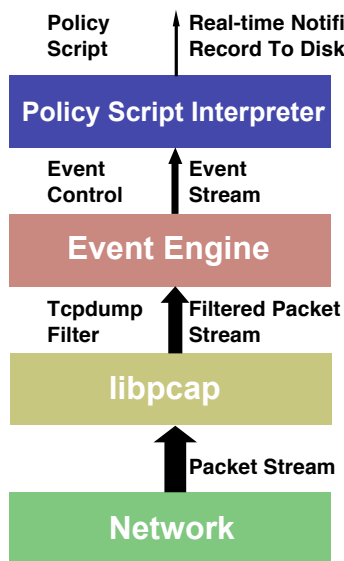
## How Bro Works



- “Event engine” distills filtered stream into high-level, *policy-neutral* events reflecting underlying network activity

- E.g., connection\_attempt, http\_reply, user\_logged\_in
- These span a [range of semantic levels](#)
- Currently about 300 different types

## How Bro Works



- “Policy script” processes event stream, incorporates:

- Context from past events
- Site’s particular policies

# How Bro Works

