



# Ethical Hacking and Countermeasures

Version 6

## Module XIV

### Denial of Service



# Scenario

Henderson, an investigative journalist in the field of Information Security sets up a new security portal called “HackzXposed4u”. This portal claims to expose the activities and identities of all known hackers across the globe.

He plans a worldwide launch on 28<sup>th</sup> March. The portal receives a wide media coverage before its release as this was one of its kind in the world.

Within five minutes of the official launch of the portal, the server crashes thus putting hold to Henderson’s plans.

*What could be the reason for the mishap?*

*Why would anyone want to sabotage the portal?*

## PCWorld

### Botnets Trump Denial of Service Attacks

A survey shows that malware-infected botnet PCs have overtaken denial-of-service attacks as the top security issue facing Internet service providers and others.

Matt Hines, Computerworld

Tuesday, September 18, 2007 02:00 PM PDT

Malware-infected botnet PCs have overtaken denial-of-service attacks as the top security issue facing Internet service providers and other Web infrastructure hosting players, according to a new survey of the organizations.

Arbor Networks published the results of its third-annual Infrastructure Security Report on Monday -- a survey of 75 large ISPs, hosting companies, and other providers -- which found for the first time that botnets currently outrank DoS threats as the most serious concern for the firms.

Tens of millions of PCs are likely infected with botnet programs worldwide, according to survey results, and Arbor researchers said the ISPs they questioned admitted to spending more time and resources battling botnets than ever before.

Infrastructure providers are finding [botnets hard to pin down](#), as the people responsible for controlling the zombie machines are increasingly employing more advanced detection evasion techniques, said Craig Labovitz, chief scientist at Arbor. As they can't accurately gauge the size of the problem, he said, infrastructure providers are afraid they're only scraping the tip of the iceberg in taking on the botnet phenomenon.

"ISPs are spending a lot of time trying to measure, and there's a lot of subjective data, but there are such widely different qualities to the various bots that it's a real challenge to get any strong metrics," Labovitz said. "We are seeing a widening separation between the pros and the amateurs, but as easy as it is to infiltrate and measure the less sophisticated botnets, the pro grade stuff is far more problematic and harder to trace."

By using the same peer-to-peer botnet propagation strategy that has made the so-called [Storm worm](#) a recurring problem in terms of generating subsequent infections, the sophisticated sect of the botnet community is moving forward at a rapid pace, according to Arbor.

In eliminating the need for traditional botnet command and control centers [using P2P techniques](#) to distribute the threats, the attackers have also removed the most efficient place to attempt to take down the attacks, the researcher said.

Source: <http://www.pcworld.com/>

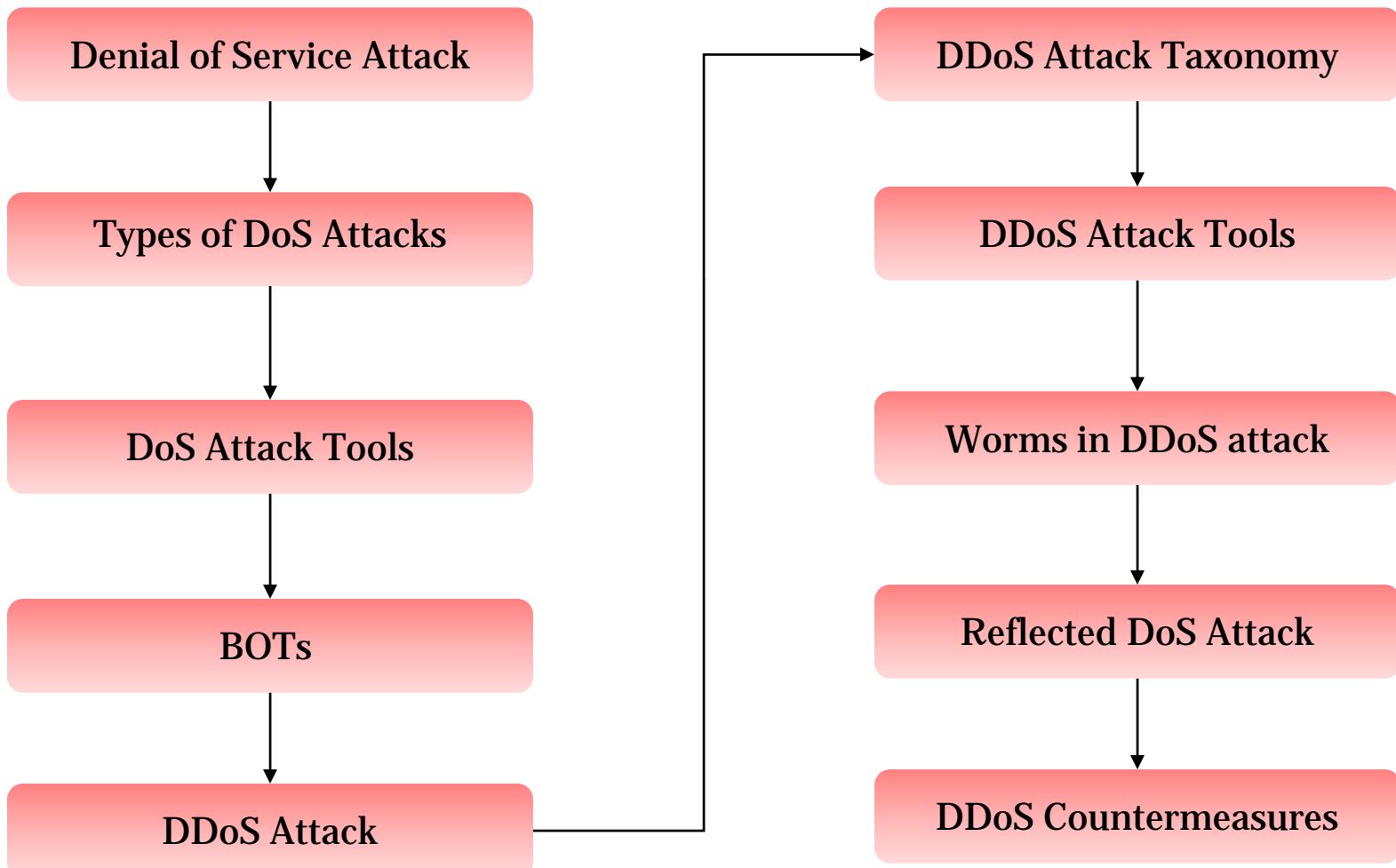


TM

# Module Objective

This module will familiarize you with :

- Denial of Service(DoS) Attack
- Types of DoS Attacks
- Tools that facilitate DoS Attack
- BOTs
- Distributed Denial of Service (DDoS) Attack
- Taxonomy of DDoS Attack
- Tools that facilitate DDoS Attack
- Worms and their role in DDoS attack
- Reflected DoS Attack
- DDoS Countermeasures



# Terminologies

## A Denial of Service (DoS) attack:

- It is an attack through which a person can render a system unusable, or significantly slow it down for legitimate users, by overloading its resources

## A Distributed Denial-of-Service (DDoS) attack:

- On the Internet, a distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system

# Real World Scenario of DoS Attacks

## WordPress.com under a denial-of-service attack

[Blogging News](#) February 21st, 2008

WordPress.com being targeted with a denial-of-service attack



Automattic has confirmed that their blogging service WordPress.com has been facing a DOS attack since the last couple of days.

Due to this, access to the service is affected and some bloggers are unable to check out their accounts and blogs hosted on the servers of the company.

WordPress.com operator Automattic added that the service has been mostly restored by now and they are returning back to normal.

A denial of service attack results in heavy loads on the server which results in crashing of system services delaying access. The company said that their servers were being attacked with spikes of up to 6 gigabits of incoming traffic which resulted in some blogs remaining inaccessible for a couple of minutes.

Source: <http://news.techwhack.com>

Copyright © by **EC-Council**  
All Rights Reserved. Reproduction is Strictly Prohibited



## DoS Attack Cripples Internet Root Servers

The denial-of-service attack hit Tuesday and nearly took down three of the 13 root servers that help manage worldwide Internet traffic.

By Sharon Gaudin, [InformationWeek](#)

Feb. 6, 2007

URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=197003903>

The 13 servers that help manage worldwide Internet traffic were hit Tuesday by a denial-of-service attack that nearly took down three of them.

It was the fiercest attack on the 13 root servers since an October 2002 assault that took down many of the roots that help manage worldwide Internet traffic, according to Ben Petro, a senior VP of NeuStar, which provides clearinghouse services to the [communications](#) and Internet industry. Three of the servers were nearly overloaded by the attack, but they didn't go down, says Petro, who adds that they were in a slowed-down brownout stage.

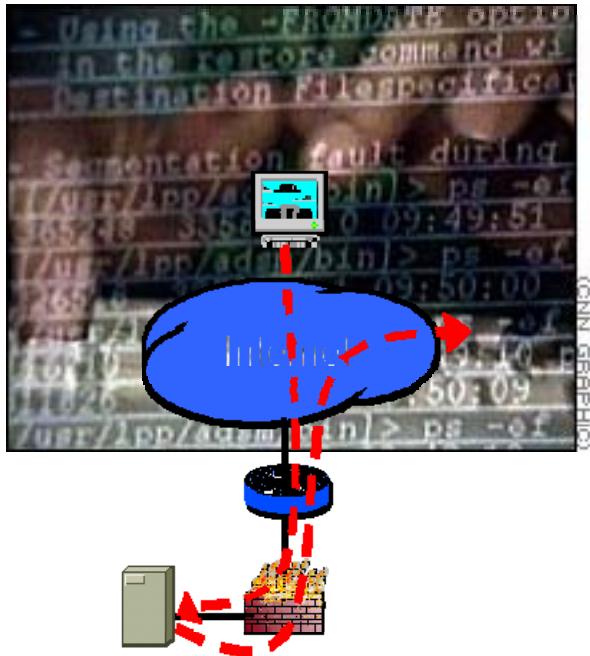
Tuesday's attack nearly matched the 2002 attack in terms of strength but surpassed the old attack in sophistication, Petro says. The servers didn't go down this time because of the significant increase in computing power in the last four years and because the roots' defenses have been heavily beefed up since then.

"If you take down the roots, you take down the Internet," says Petro. "By comparison, if you take down a company, that hurts them. But this is just an attack of a very different scale. When you see someone going after root, it's an attack directly at the [infrastructure](#) of the Internet."

Petro, though, says the Internet was not close to going down Tuesday. He notes that those three servers were heavily strained, but they withstood the attack and the disturbance wasn't noticeably felt around the globe.

Source: <http://www.informationweek.com/>

# What are Denial of Service Attacks



A Denial of Service attack (DoS) is an attack through which a person can render a system unusable, or significantly slow it down for legitimate users, by overloading its resources

If an attacker is unable to gain access to a machine, the attacker will most likely crash the machine to accomplish a denial of service attack

# Goal of DoS

The goal of DoS is not to gain unauthorized access to machines or data, but to prevent legitimate users of a service from using it

Attackers may:

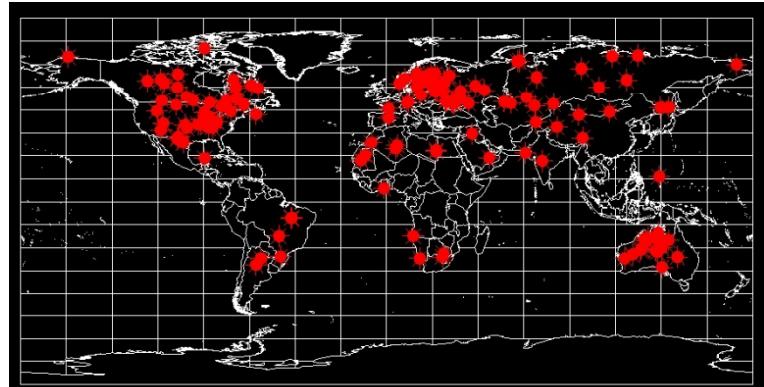
- Attempt to flood a network, thereby preventing legitimate network traffic
- Attempt to disrupt connections between two machines, thereby preventing access to a service
- Attempt to prevent a particular individual from accessing a service
- Attempt to disrupt service to a specific system or person



# Impact and the Modes of Attack

## The Impact:

- Disabled network
- Disabled organization
- Financial loss
- Loss of goodwill



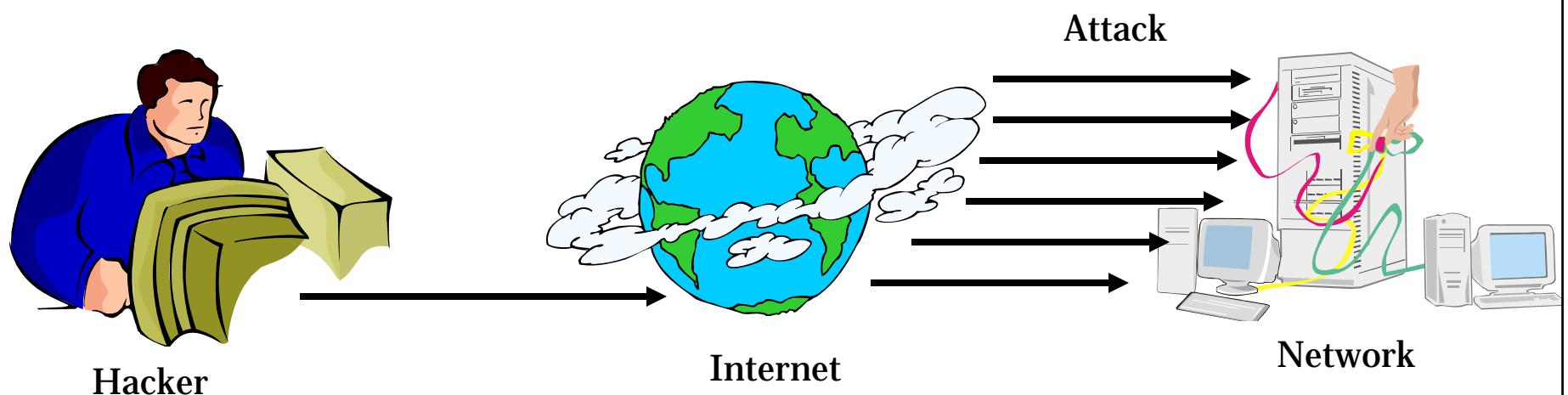
## The Modes:

- Consumption of
  - Scarce, limited, or non-renewable resources
  - Network bandwidth, memory, disk space, CPU time, or data structures
  - Access to other computers and networks, and certain environmental resources such as power, cool air, or even water
- Destruction or Alteration of Configuration Information
- Physical destruction or alteration of network components, resources such as power, cool air, or even water

# Types of Attacks

There are two types of attacks:

- DoS attack
- DDos attack
  - A type of attack on a network that is designed to bring the network down by flooding it with data packets



# DoS Attack Classification

Smurf

Buffer Overflow Attack

Ping of death

Teardrop

SYN Attack



# Smurf Attack

The perpetrator generates a large amount of ICMP echo (ping) traffic to a network broadcast address with a spoofed source IP set to a victim host

The result will be lots of ping replies (ICMP Echo Reply) flooding the spoofed host

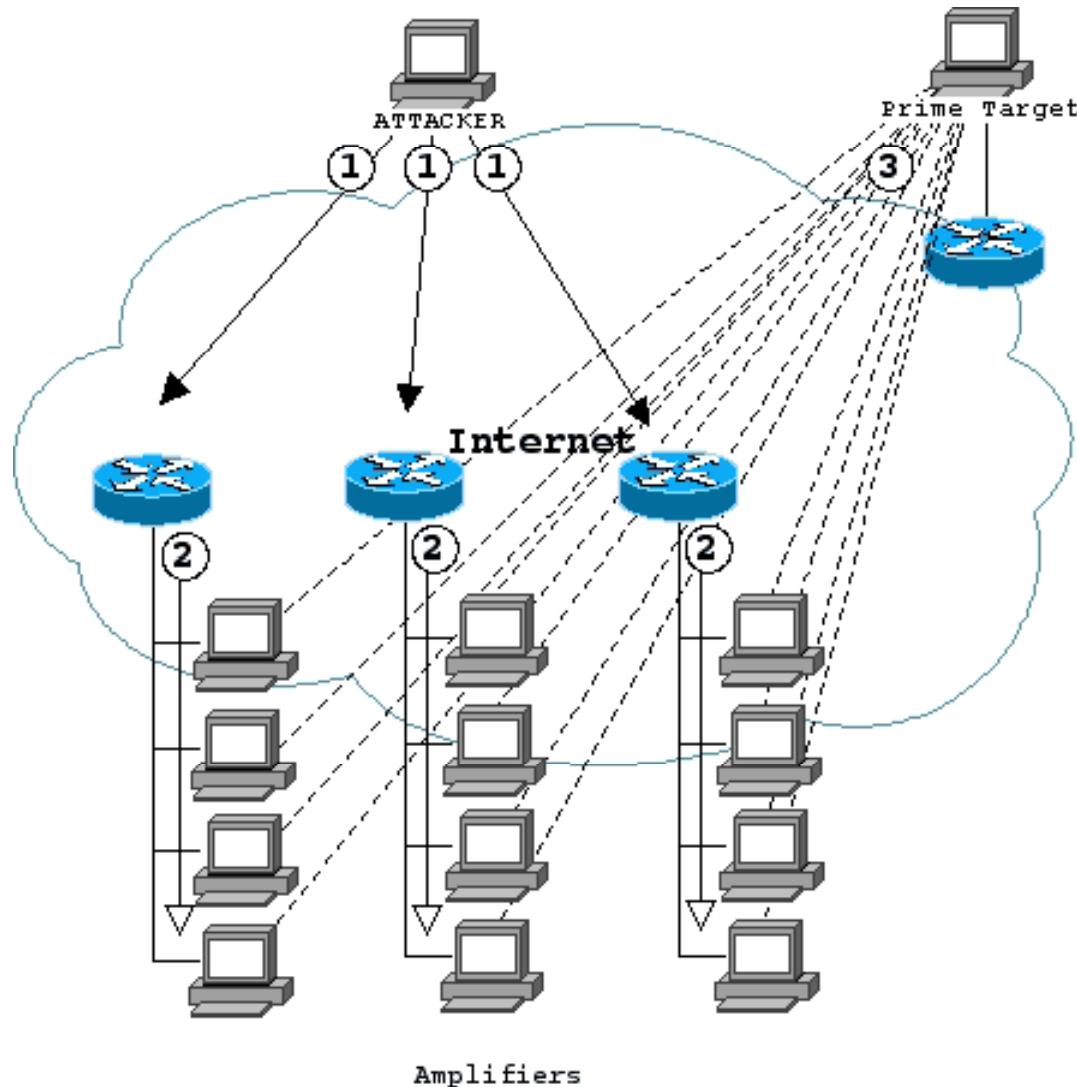
Amplified ping reply stream can overwhelm the victim's network connection

Fraggle attack, which uses UDP echo is similar to the smurf attack

```
ICMP: ----- ICMP header -----  
ICMP:  
ICMP: Type = 8 (Echo)  
ICMP: Code = 0  
ICMP: Checksum = 80CE (should be FB47)  
ICMP: Identifier = 512  
ICMP: Sequence number = 17152  
ICMP: [1472 bytes of data]  
ICMP:  
ICMP: [Normal end of "ICMP header".]  
ICMP:
```



# Smurf Attack



# Buffer Overflow Attack

Buffer overflow occurs any time the program writes more information into the buffer than the space allocated in the memory

The attacker can overwrite the data that controls the program execution path and hijack the control of the program to execute the attacker's code instead of the process code



Sending email messages that have attachments with 256-character file names can cause buffer overflow

# Ping of Death Attack

The attacker deliberately sends an IP packet larger than the 65,536 bytes allowed by the IP protocol

Fragmentation allows a single IP packet to be broken down into smaller segments

The fragments can add up to more than the allowed 65,536 bytes. The operating system, unable to handle oversized packets freezes, reboots, or simply crashes

The identity of the attacker sending the oversized packet can be easily spoofed



# Teardrop Attack

IP requires that a packet that is too large for the next router to handle should be divided into fragments

The attacker's IP puts a confusing offset value in the second or later fragment

If the receiving operating system is not able to aggregate the packets accordingly, it can crash the system

It is a UDP attack, which uses overlapping offset fields to bring down hosts

The Unnamed Attack

- Variation of the Teardrop attack
- Fragments are not overlapping but gaps are incorporated



# SYN Attack

The attacker sends bogus TCP SYN requests to a victim server. The host allocates resources (memory sockets) to the connection

Prevents the server from responding to the legitimate requests

This attack exploits the three-way handshake

Malicious flooding by large volumes of TCP SYN packets to the victim's system with spoofed source IP addresses can cause DoS



# SYN Flooding

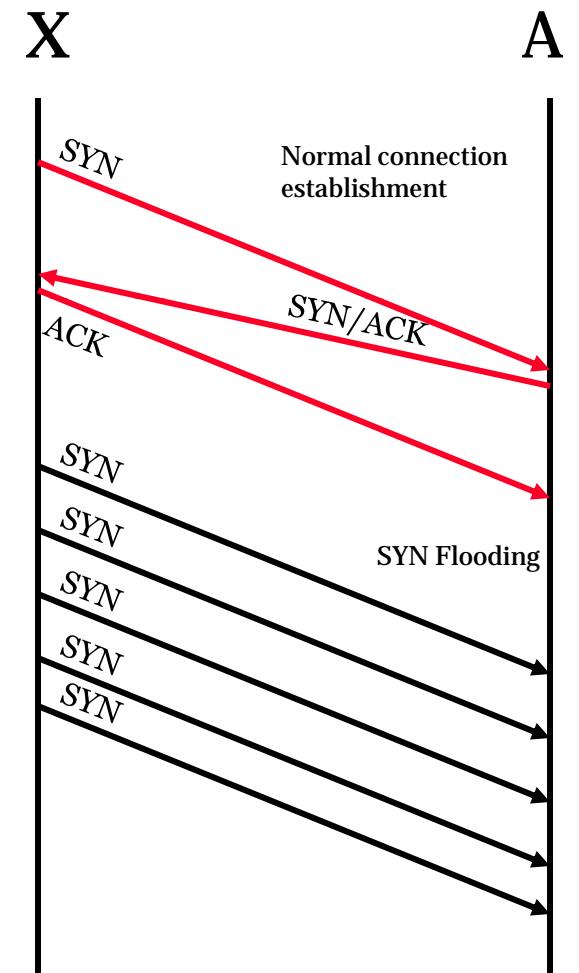
SYN Flooding takes advantage of a flaw in how most hosts implement the TCP three-way handshake

When Host B receives the SYN request from A, it must keep track of the partially-opened connection in a "listen queue" for at least 75 seconds

A malicious host can exploit the small size of the listen queue by sending multiple SYN requests to a host, but never replying to the SYN&ACK

The victim's listen queue is quickly filled up

This ability of removing a host from the network for at least 75 seconds can be used as a denial-of-service attack



# DoS Attack Tools

Jolt2

Bubonic.c

Land and LaTierra

Targa

Blast20

Nemesy

Panther2

Crazy Pinger

Some Trouble

UDP Flood

FSMax



# DoS Tool: Jolt2

Allows remote attackers to cause a denial of service attack against Windows-based machines

Causes the target machines to consume 100% of the CPU time on processing the illegal packets

**Not Windows-specific. Cisco routers and other gateways may be vulnerable**

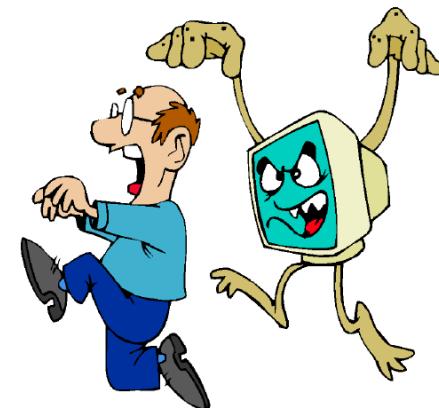


# DoS Tool: Bubonic.c

Bubonic.c is a DoS exploit that can be run against Windows 2000 machines

It works by randomly sending TCP packets with random settings with the goal of increasing the load of the machine, so that it eventually crashes

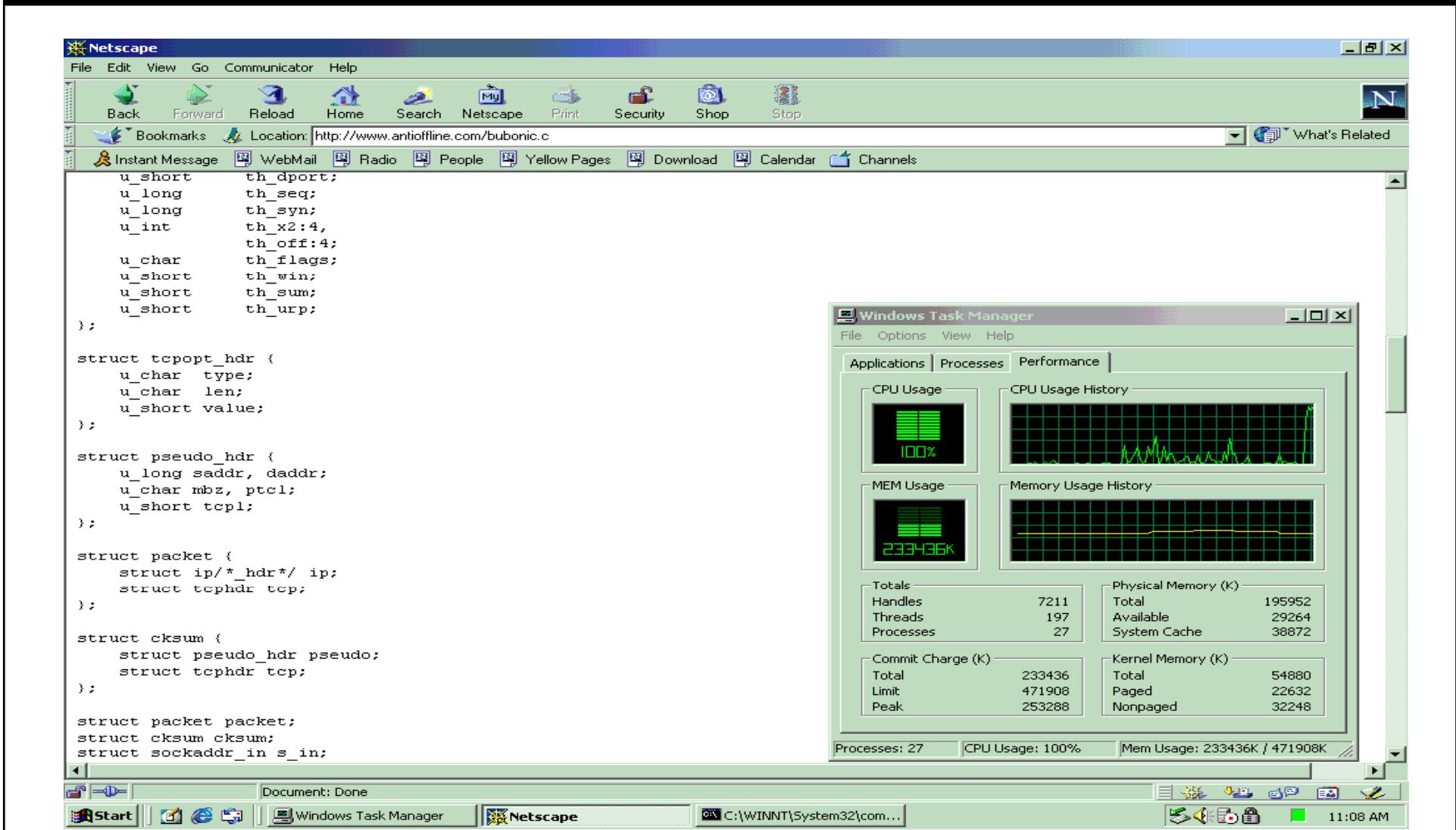
- c: \> bubonic 12.23.23.2 10.0.0.1 100





TM

# Bubonic.c: Screenshot

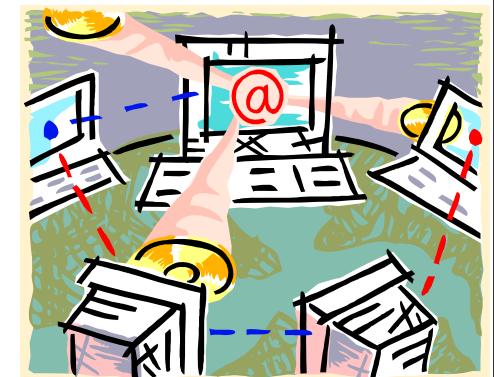


# DoS Tool: Land and LaTierra

IP spoofing in combination with the opening of a TCP connection

Both IP addresses, source, and destination, are modified to be the same—the address of the destination host

This results in sending the packet back to itself, because the addresses are the same

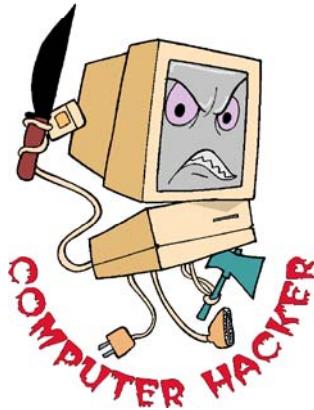


# DoS Tool: Targa



Targa is a program that can be used to run eight different DoS attacks

It is seen as a part of kits compiled for affecting DoS and sometimes even in earlier rootkits



The attacker has the option to either launch individual attacks or try all the attacks until it is successful

Targa is a powerful program and can do a lot of damage to a company's network

# DoS Tool: Blast

Blast is a small, quick TCP service stress test tool that does a large amount of work quickly and can spot potential weaknesses in your network servers

## Example of blasting HTTP servers

```
blast 134.134.134.4 80 40 50 /b "GET /some" /e "url/ HTTP/1.0" /nr /dr /v
```

- Sends 'GET /some\*\*\*\*\*url/ HTTP/1.0' capped by dual LF/CR's

```
blast 134.134.134.4 80 25 30 /b "GET /some" /nr /dr
```

- Sends 'GET /some\*\*\*\*\*' capped by dual LF/CR's

## Example of blasting POP servers

```
blast 134.134.134.4 110 15 20 /b "user te" /e "d" /v
```

- Sends 'user te\*\*\*\*d' capped by a LF/CR

```
blast 134.134.134.4 110 15 20 /b "user te" /e "d" /v /noret
```

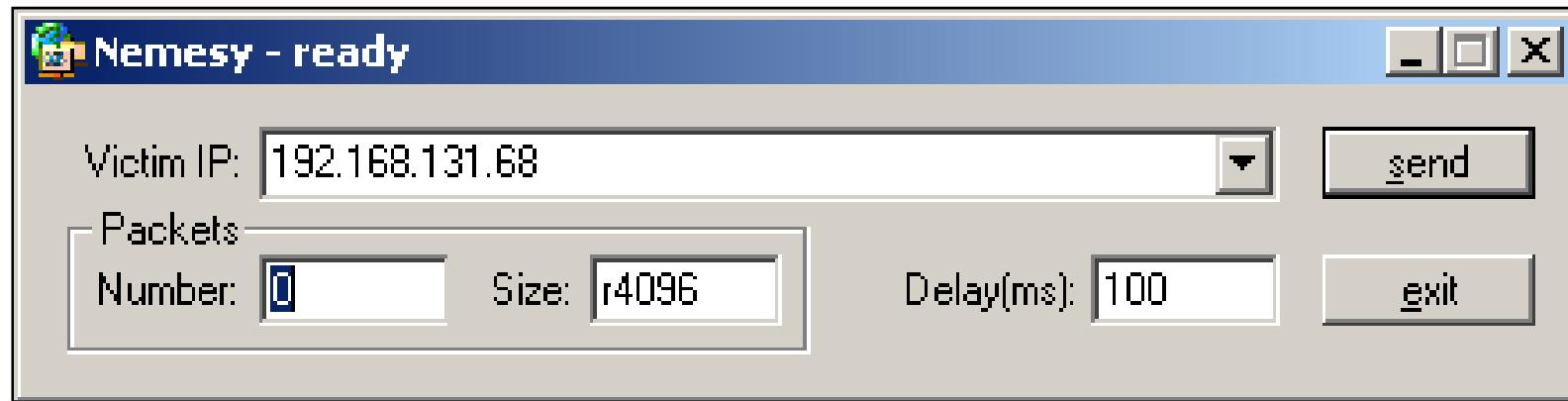
- Sends 'user te\*\*\*\*\*d'



# DoS Tool: Nemesy

Nemesy application generates random packets (protocol, port, etc)

Its presence means that your computer is infected with malicious software and is insecure



# DoS Tool: Panther2

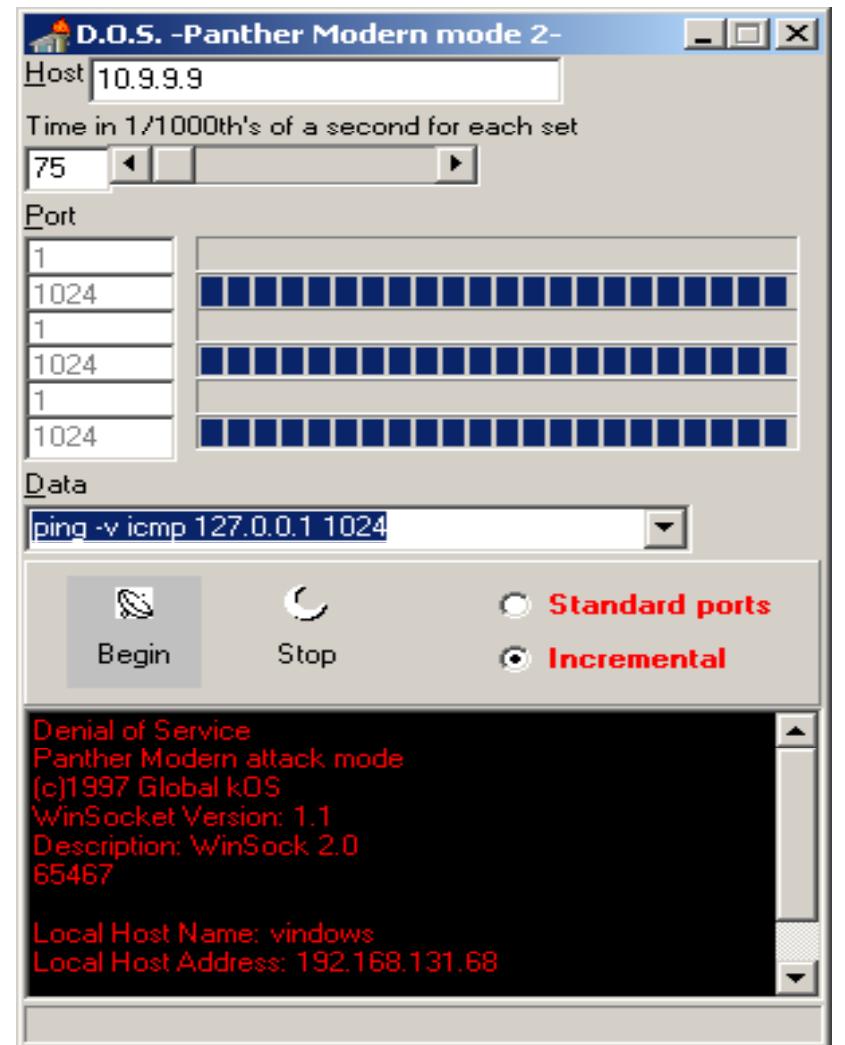
Denial of service UDP-based attack is designed for a 28.8-56k connection

It comes under Flooder category

Flooder:



- A program that overloads a connection by any mechanism, such as fast pinging, causing a DoS attack



# DoS Tool: Crazy Pinger

This tool could send large packets of ICMP to a remote target network

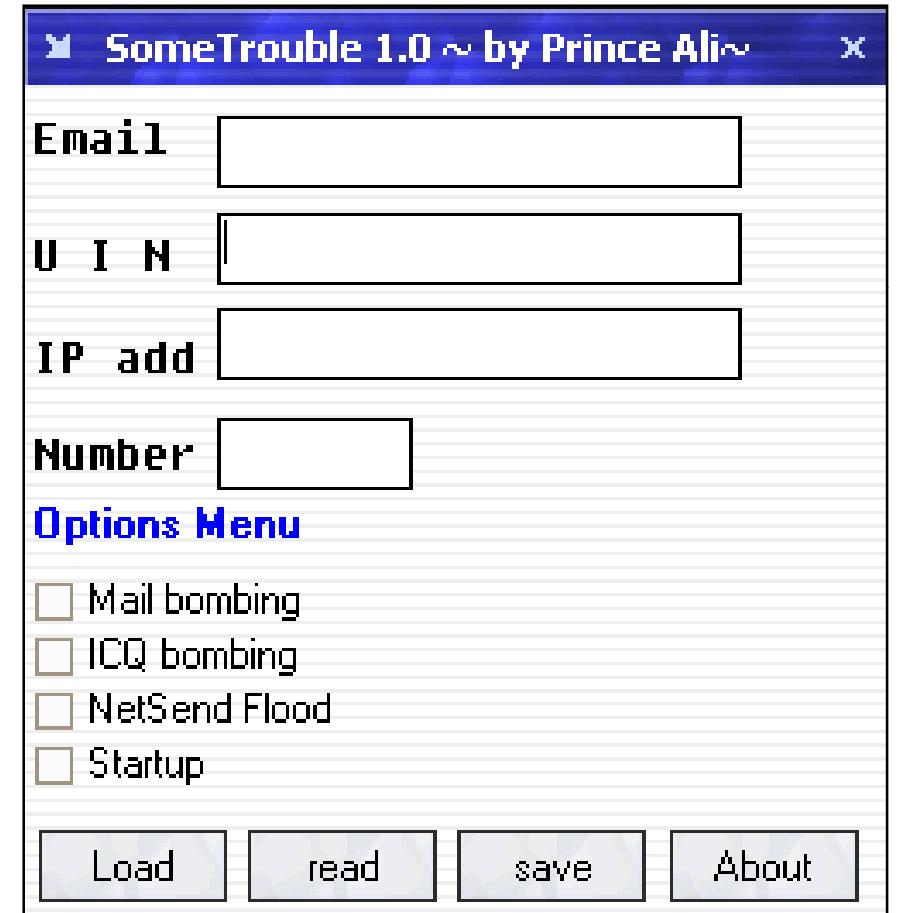


# DoS Tool: SomeTrouble

SomeTrouble is a remote flooder

SomeTrouble is a simple program with 3 remote functions:

- Mail Bomb (Self Resolve for Smtip)
- Icq Bomb
- Net Send Flood



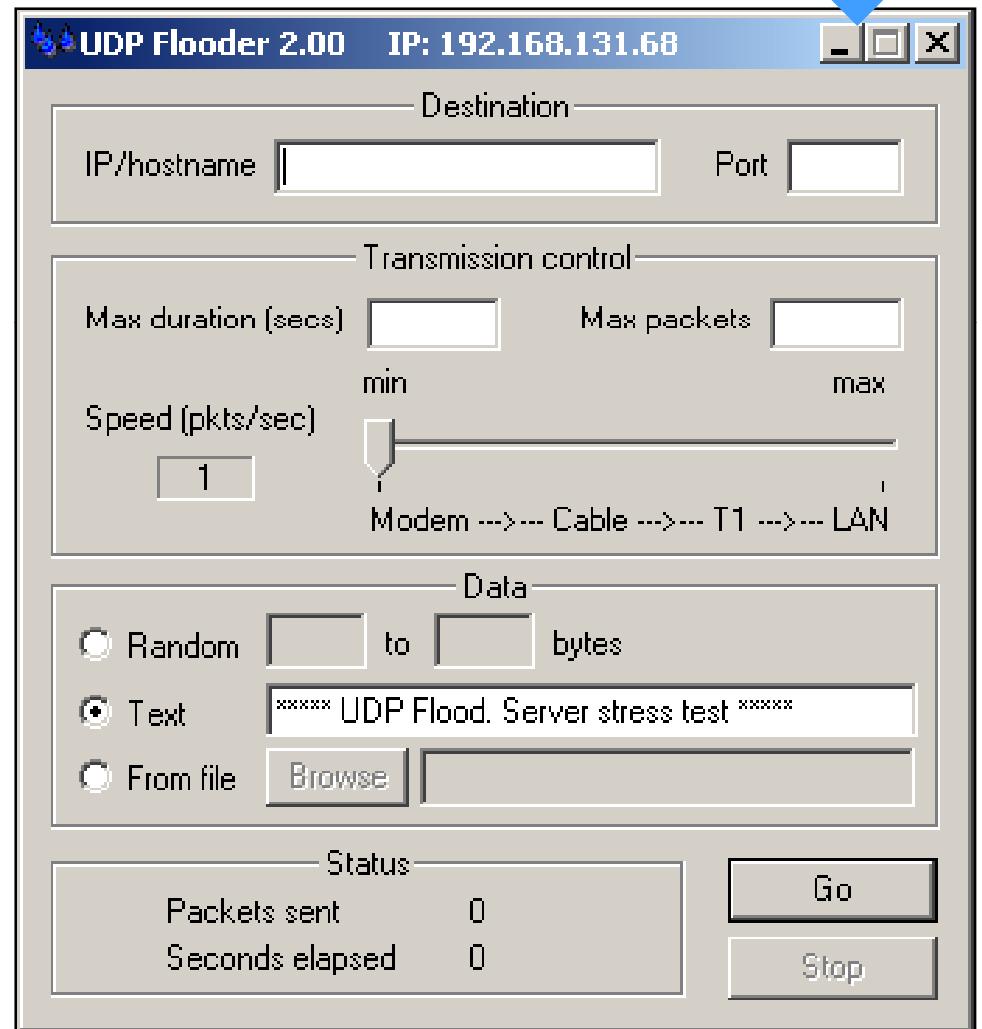


UDPFlood is UDP packet sender

It sends out UDP packets to the specified IP and port at a controllable rate

Packets can be made from a typed text string; a given number of random bytes or data from a file

It is useful for server testing

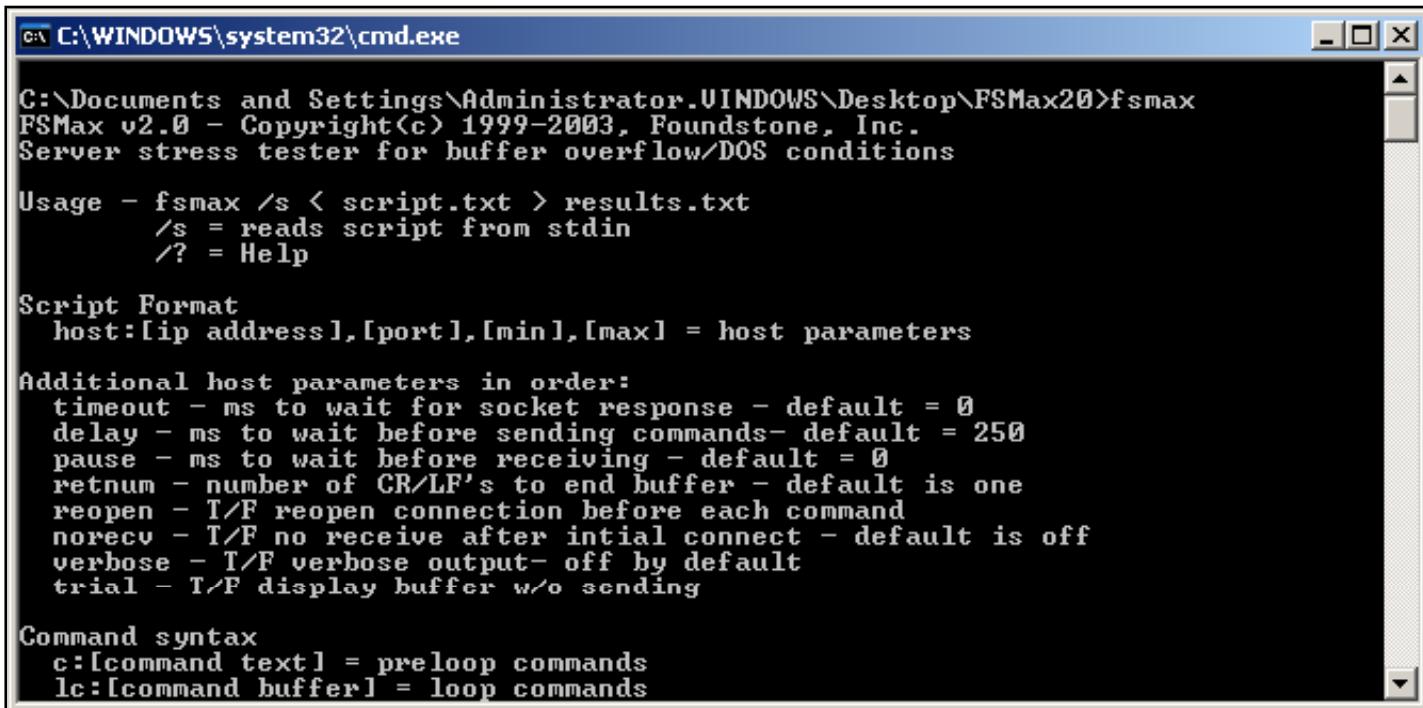


# DoS Tool: FSMax

A scriptable, server stress testing tool

It takes a text file as input and runs a server through a series of tests based on the input

The purpose of this tool is to find buffer overflows of DOS points in a server



C:\WINDOWS\system32\cmd.exe

```
C:\Documents and Settings\Administrator.WINDOWS\Desktop\FSMax20>fsmax
FSMax v2.0 - Copyright(c) 1999-2003, Foundstone, Inc.
Server stress tester for buffer overflow/DOS conditions

Usage - fsmax /s < script.txt > results.txt
        /s = reads script from stdin
        /? = Help

Script Format
  host:[ip address],[port],[min],[max] = host parameters

Additional host parameters in order:
  timeout - ms to wait for socket response - default = 0
  delay - ms to wait before sending commands- default = 250
  pause - ms to wait before receiving - default = 0
  retnum - number of CR/LF's to end buffer - default is one
  reopen - T/F reopen connection before each command
  norecv - T/F no receive after intial connect - default is off
  verbose - T/F verbose output- off by default
  trial - T/F display buffer w/o sending

Command syntax
  c:[command text] = preloop commands
  lc:[command buffer] = loop commands
```

# Bot (Derived from the Word RoBOT)

*IRC* bot is also called *zombie* or *drone*

*Internet Relay Chat* (IRC) is a form of real-time communication over the Internet. It is mainly designed for group (one-to-many) communication in discussion forums called channels

The bot joins a specific IRC channel on an IRC server and waits for further commands

The attacker can remotely control the bot and use it for fun and also for profit

Different bots connected together is called *botnet*

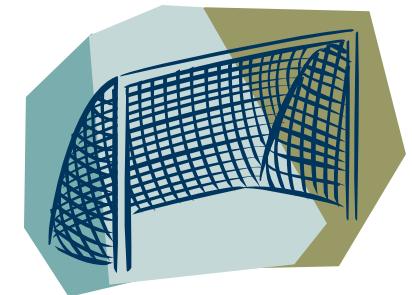


# Botnets

Botnets consist of a multitude of machines

They are used for DDoS attacks

A relatively small botnet with only 1,000 bots has a combined bandwidth that is probably higher than the Internet connection of most corporate systems (1,000 home PCs with an average upstream of 128KBit/s can offer more than 100MBit/s)



# Uses of Botnets

## Distributed Denial-of-Service Attacks

- Botnets are used for Distributed Denial-of-Service (DDoS) attacks

## Spamming

- Opens a SOCKS v4/v5 proxy server for spamming

## Sniffing Traffic

- Bots can also use a packet sniffer to watch interesting clear-text data passing by a compromised machine

## Keylogging

- With the help of a keylogger, it is easy for an attacker to retrieve sensitive information such as online banking passwords

## Spreading new malware

- Botnets are used to spread new bots



TM

# Uses of Botnets (cont'd)

## Installing Advertisement Addons

- Automated advertisement “clicks”

## Google AdSense abuse

- AdSense offers companies the possibility to display Google advertisements on their own website and earn money this way. Botnet is used to click on these advertisements

## Attacking IRC Chat Networks

- These are called “clone” attacks

## Manipulating online polls

- Since every bot has a distinct IP address, every vote will have the same credibility as a vote cast by a real person

## Mass identity theft

- ("phishing mails")



TM

# Types of Bots

## Agobot/Phatbot/Forbot/XtremBot

- The bot itself is written in C++ with cross-platform capabilities and the source code is put under the GPL. Agobot was written by Ago alias Wonk, a young German man who was arrested in May 2004 for computer crime
- Agobot can use NTFS Alternate Data Stream (ADS) and offers Rootkit capabilities like file and process hiding to hide its own presence on a compromised host

## SDBot/RBot/UrBot/UrXBot

- SDBot is written in poor C and also published under the GPL. It is the father of RBot, RxBot, UrBot, UrXBot, and JrBot

## mIRC-based Bots - GT-Bots

- GT is an abbreviation for *Global Threat* and this is the common name used for all mIRC-scripted bots. These bots launch an instance of the mIRC chat-client with a set of scripts and other binaries

# How Do They Infect? Analysis Of Agobot

## Step 1: Mode of Infection

- When first run (Ex: chess.exe), an Agobot usually copies itself to the System directory and will add registry entries to autostart when Windows boot:
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run  
HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices

## Step 2: Massive Spreading Stage

- Agobots are able to spread automatically to other systems using network shares
- It attempts to connect to default administrative shares, such as admin\$, C\$, D\$, E\$ and print\$, by guessing usernames and passwords that may have access to these shares
- Agobot can be also spread by exploiting vulnerabilities in Windows operating systems and third party applications

# How Do They Infect? Analysis Of Agobot (cont'd)

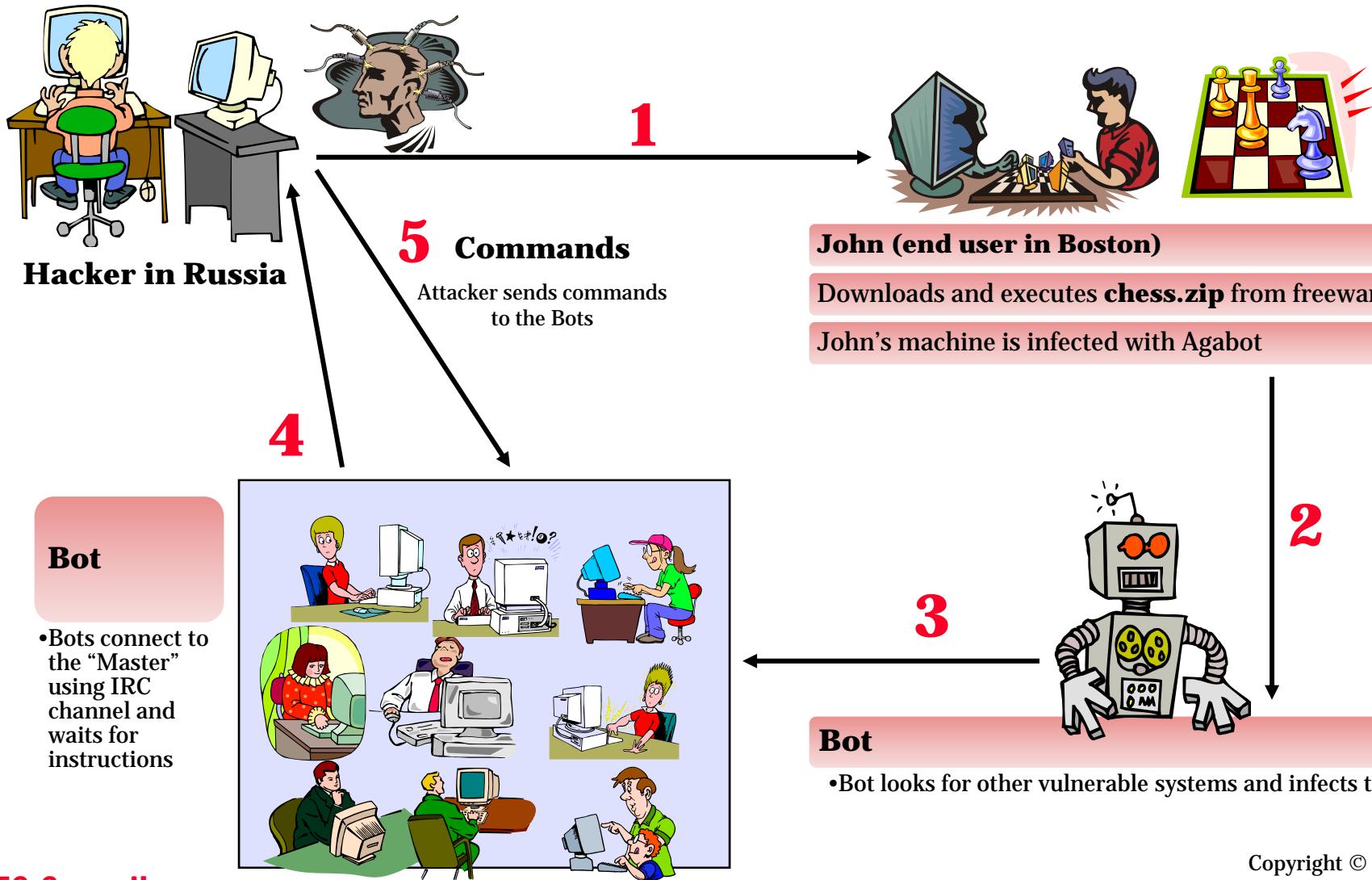
## Step 3: Connect back to IRC

- Agobot's main function is to act as an IRC-controlled backdoor
- It attempts to connect to an IRC server from a pre-defined list and join a specific channel so that the victim's computer can be controlled

## Step 4: Attacker takes control of the Victim's computer

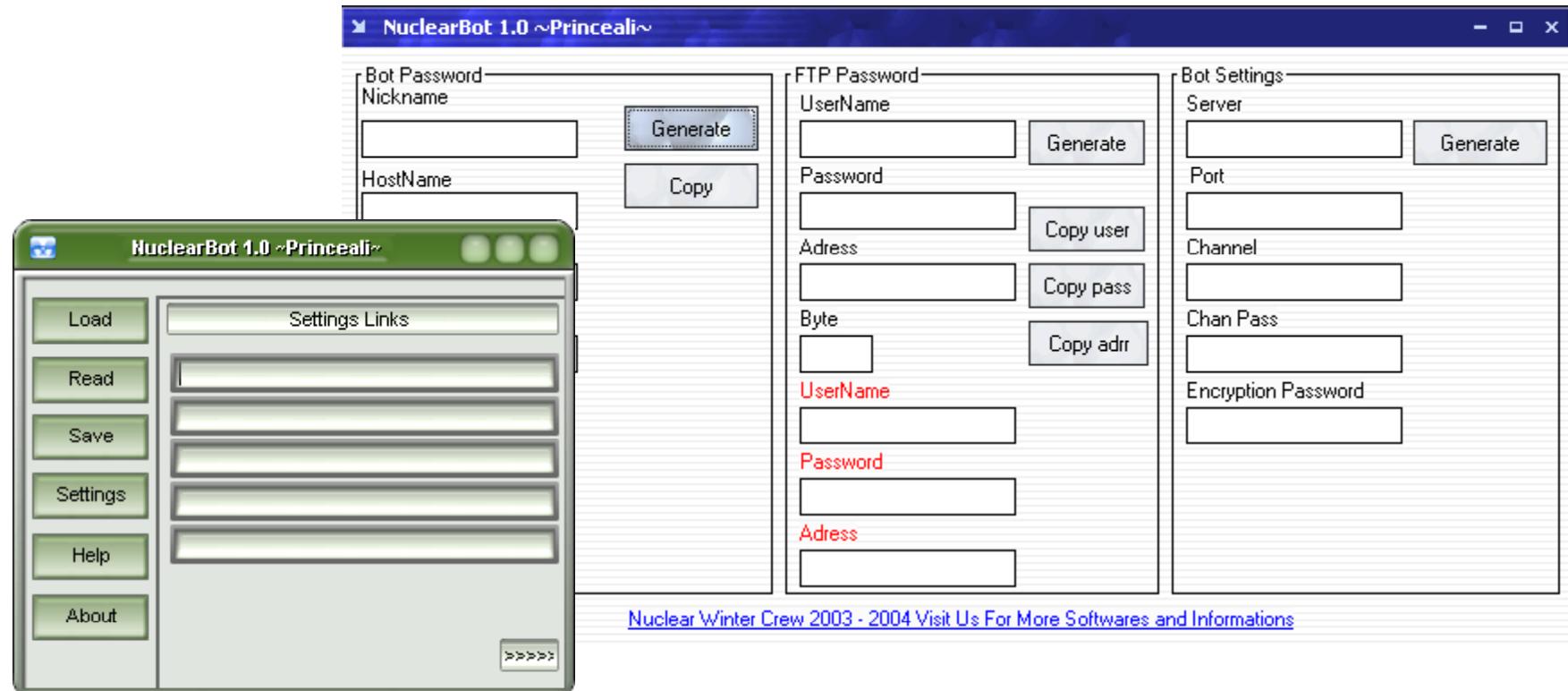
- Downloads and executes files from the Internet
- Retrieves system information such as operating system details
- Executes local files
- Launches DDOS attack on other systems

# How Do They Infect



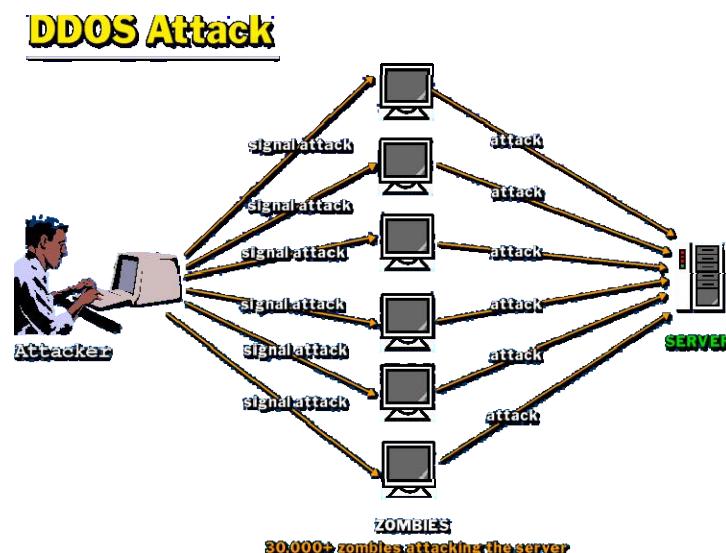
# Tool: Nuclear Bot

Nuclear Bot is a Multi Advanced IRC BOT that can be used for floods, managing, utilities, spread, IRC Related, DDOS Attacks, and so on



# What is DDoS Attack

According to the website, [www.searchsecurity.com](http://www.searchsecurity.com): On the Internet, a distributed denial of service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to the legitimate users





*The Independent Online Poker Authority*

Published on <http://www.pokernews.com/news/2008/02/ddos-attacks-hamper-online-poker-sites.htm>

## DDoS Attacks Hamper Online Poker Sites

February 22, 2008

Haley Hintze



A wave of Distributed Denial of Service (DDoS) attacks targeting major online poker and gambling sites has at times impaired the functionality of several of those major sites in recent days. According to a report at the Shadowserver Foundation, the first tracking entity to report on the attacks, affected poker sites have included Full Tilt Poker, Titan Poker and CD Poker, with the casino-games portion of operations at PartyGaming and Virgin Games also affected.

A DDoS attack impairs a website's capability by attacking its web servers, usually by flooding those servers with traffic from many thousands of different locations at once. One illicit method for implementing a DDoS attack involves the use of remote computers infected with a virus or other latent code; upon activation, these otherwise innocent computers are then incorporated into the "bot net" used in the attacks on the targeted site.

Several of the major sites were reported as being down or as suffering slow response times while the recent attacks were in process, though none of the affected sites have, to date, issued a release on the matter. An examination made by the group (which maintains its watchdog site at shadowserver.org) uncovered a total of 32 different online gambling domains which had been attacked from February 10-18, 2008. An unusual number of the sites were smaller Russian-based (.ru) gambling sites, despite the attacks on the larger entities such as Full Tilt and Titan Poker. All of the above-mentioned sites have, according to the research published by Shadowserver, taken countermeasures designed to combat the attacks being made upon them.

A later report also indicated that the "command and control" server orchestrating the attacks had been taken offline after its "upstream" service provider had been notified, thereby short-circuiting the attacks. Such a solution, of course, does not preclude new attacks from starting from a different, relocated web server.

Source: <http://www.pokernews.com>

**EC-Council**

Copyright © by **EC-Council**  
All Rights Reserved. Reproduction is Strictly Prohibited



TM

# Characteristics of DDoS Attacks

DDoS Attack is a large-scale and coordinated attack on the availability of services of a victim system

The services under attack are those of the “primary victim,” while the compromised systems used to launch the attack are often called the “secondary victims”

This makes it difficult to detect because attacks originate from several IP addresses

If a single IP address is attacking a company, it can block that address at its firewall. If it is 30,000, this is extremely difficult

Perpetrator is able to multiply the effectiveness of the Denial of Service significantly by harnessing the resources of multiple unwitting accomplice computers which serve as attack platforms



TM

# DDOS Unstoppable

DDoS attacks rely on finding thousands of vulnerable, Internet-connected systems and systematically compromising them using known vulnerabilities

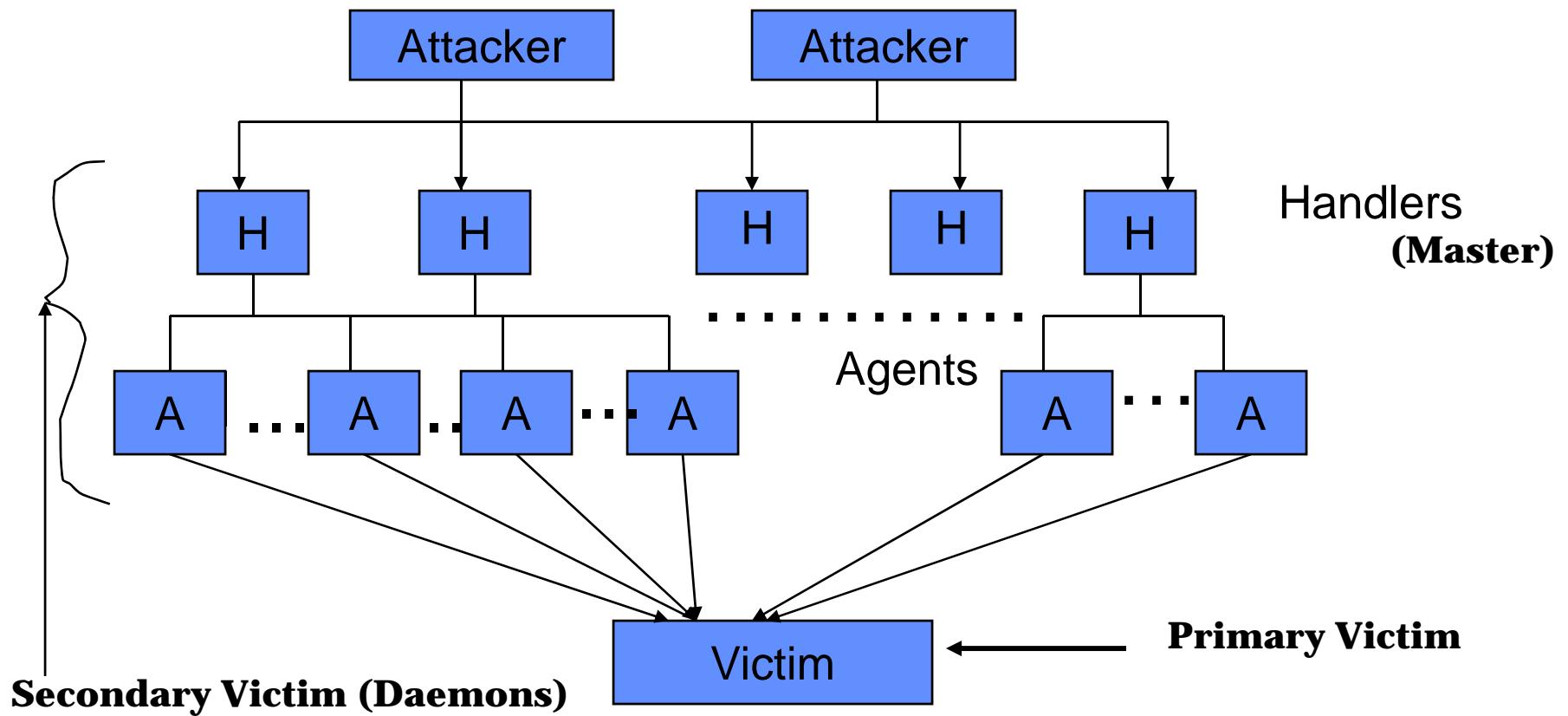
Once the DDoS attack has been launched, it is hard to stop

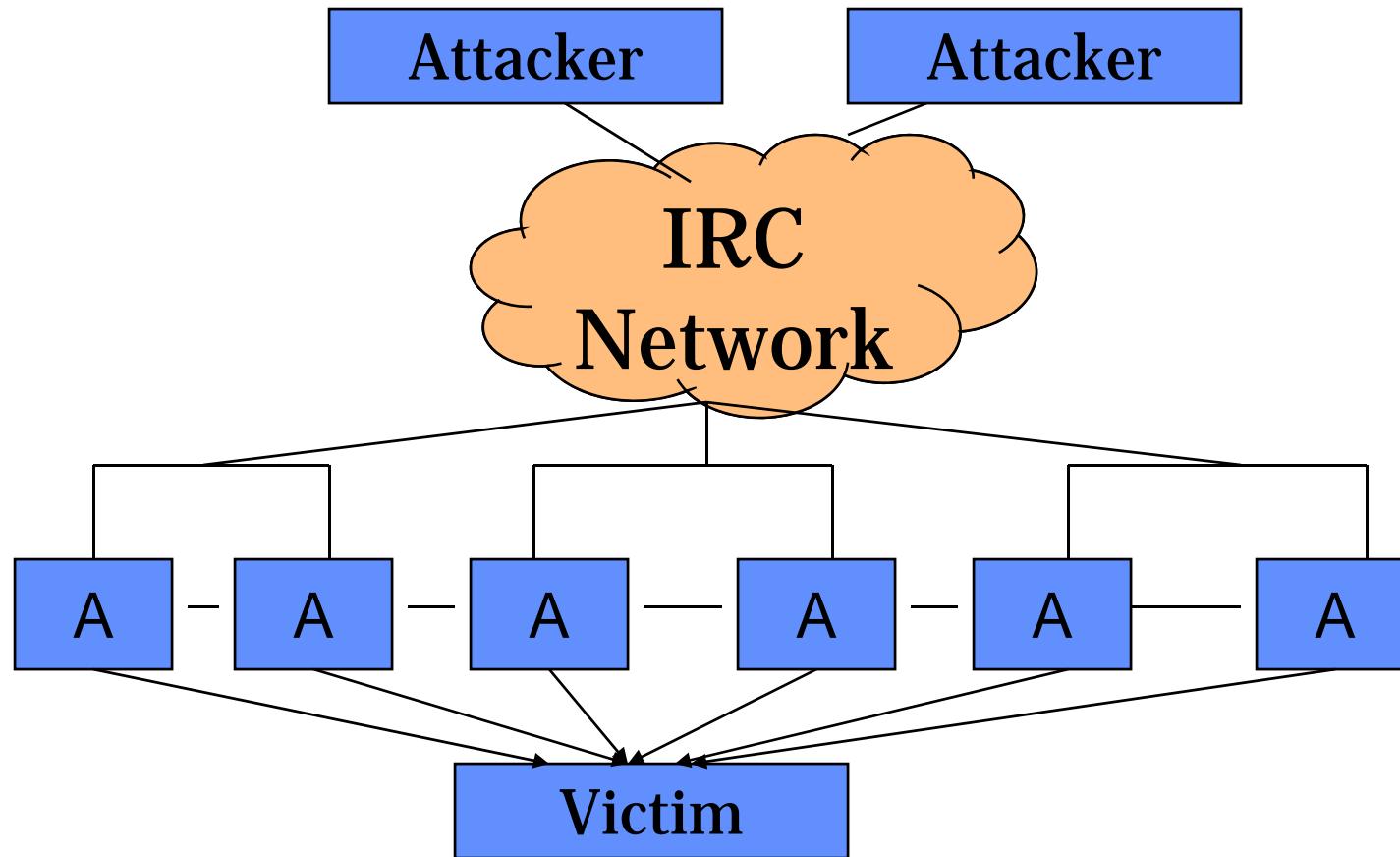
Packets arriving at your firewall may be blocked there, but they may just as easily overwhelm the incoming side of your Internet connection

If the source addresses of these packets have been spoofed, then you will have no way of knowing if they reflect the true source of the attack until you track down some of the alleged sources

The sheer volume of sources involved in DDoS attacks makes it difficult to stop

# Agent Handler Model



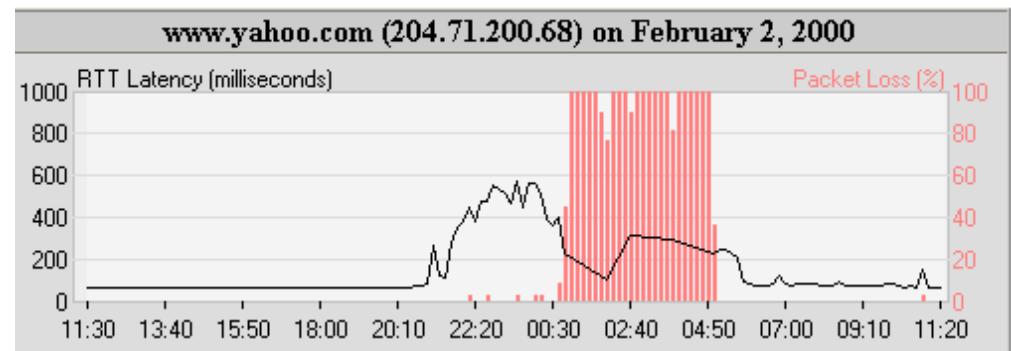


## Bandwidth depletion attacks

- Flood attack
- UDP and ICMP flood

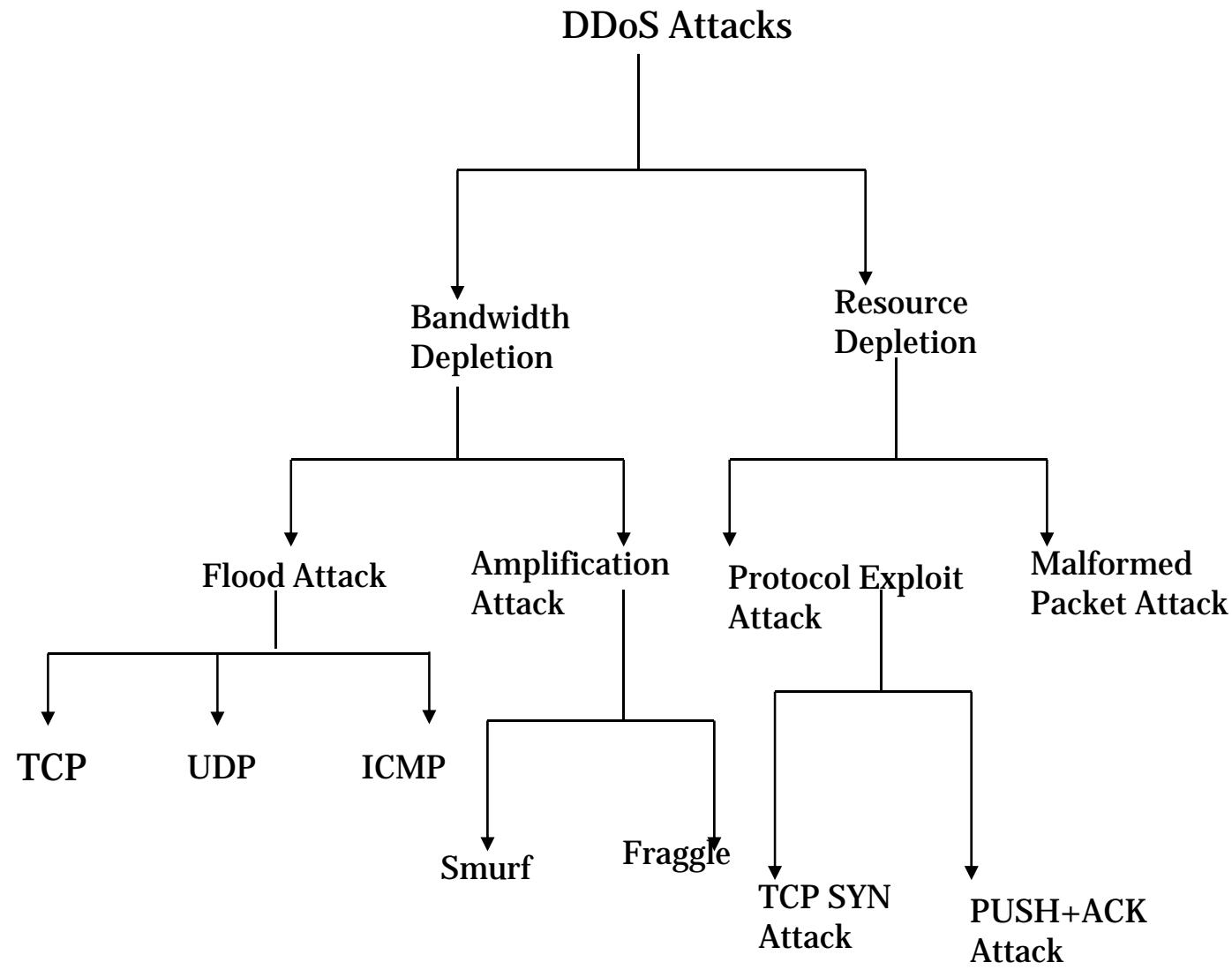
## Amplification attack

- Smurf and Fraggle attack

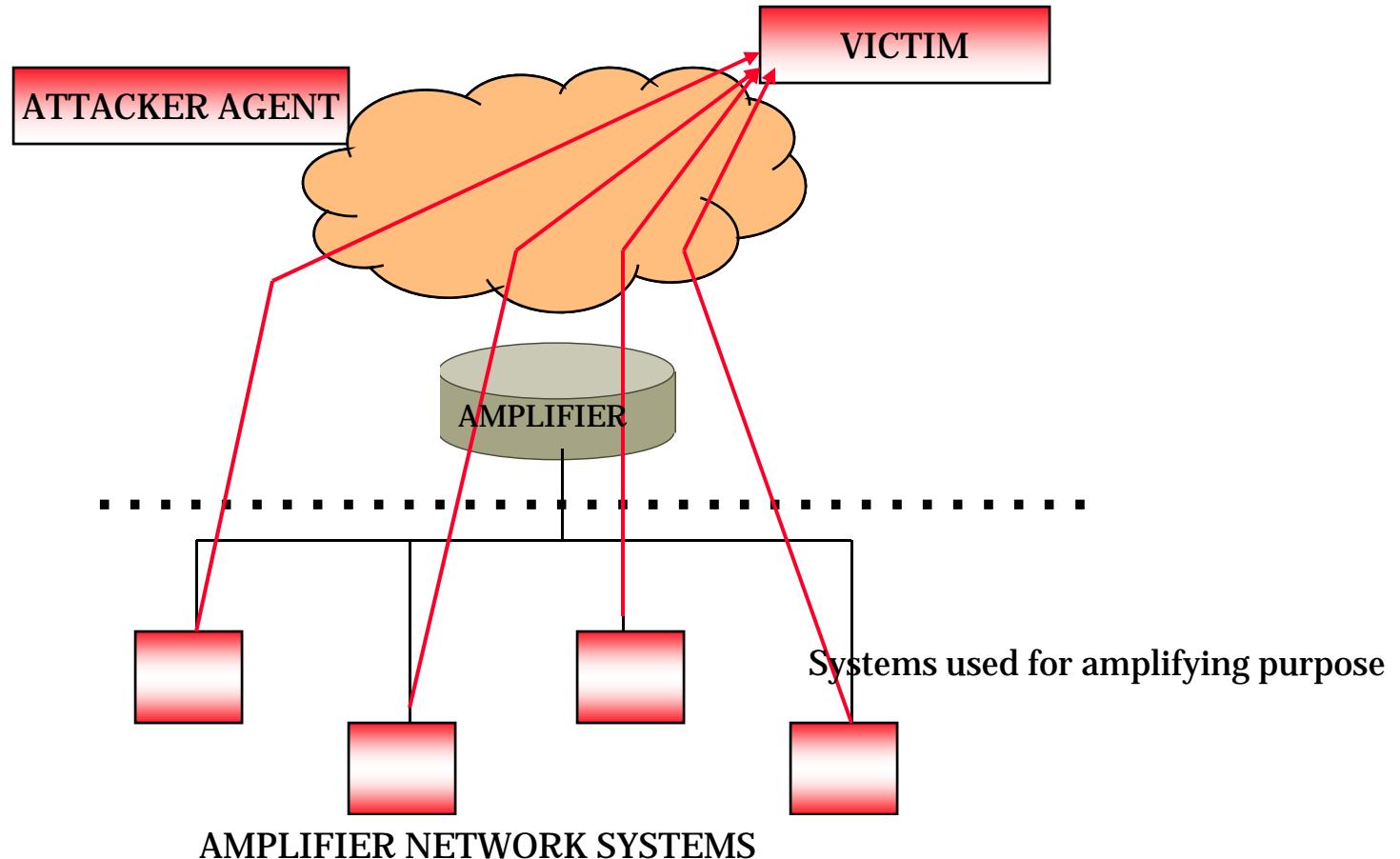


Source: <http://www.visualware.com/whitepapers/casestudies/yahoo.html>

# DDoS Attack Taxonomy



# Amplification Attack





TM

# Reflective DNS Attacks

A Hacker would typically use a botnet to send a large number of queries to open DNS servers

These queries will be "spoofed" to look like they come from the target of the flooding and the DNS server will reply to that network address

It is generally possible to stop the more-common bot-delivered attack by blocking traffic from the attacking machines, which are identifiable

But blocking queries from DNS servers brings problems in its wake. A DNS server has a valid role to play in the workings of the Internet

Blocking traffic to a DNS server could also mean blocking legitimate users from sending e-mail or visiting a Web site

A single DNS query could trigger a response that is as much as 73 times larger than the request



# Reflective DNS Attacks Tool: ihateperl.pl

ihateperl.pl is a small, yet effective, DNS-based reflective attack

It uses a list of predefined DNS servers to spoof the requests of name resolution by the targeted host

As an example, the script uses google.com as the host being resolved by the target, which can be changed to any domain name - example  
[www.xsecurity.com](http://www.xsecurity.com)

To use the tool, simply create a list of open DNS servers, specify the target IP address, and set the count of requests to send

- \$ perl ihateperl.pl
- Usage: ./ihateperl.pl <target IP> <loop count>



TM

# News

## Scientology website shielded against DDoS attack

By [John Leyden](#)

Published Monday 28th January 2008 18:09 GMT

**Updated** The Church of Scientology has restored its website to normal after a campaign of denial of service attacks prompted it to use DDoS mitigation service Prolexic.

Web sites associated with the Church of Scientology were intermittently unavailable last week after an internet group calling itself Anonymous declared war on the controversial organisation.

Anonymous justified its actions by alleging the Church of Scientology has misused copyright and trademark law in censoring criticism against the church. The campaign was sparked off by the church's attempts to remove a promotional video featuring Scientologist Tom Cruise from YouTube. The clip shows a video from Cruise's Freedom Medal ceremony from late 2004 in which the actor speaks with (frankly scary) intensity about the responsibilities of being a Scientologist. After the Church of Scientology lodged a copyright infringement complaint, YouTube pulled the video, but the material has since resurfaced on Gawker.com.

As well as directing sympathisers to use denial of service software, Anonymous is calling on its members to make nuisance calls, host Scientology documents the Church claims as protected by copyright, and fax black pages to the Church's fax machines in an effort to waste ink. Longer established critics of Scientology have criticised the actions of Anonymous as counterproductive.

Source: <http://www.theregister.co.uk>

Copyright © by **EC-Council**

All Rights Reserved. Reproduction is Strictly Prohibited



TM

# DDoS Tools

Tribe Flood Network (TFN)

TFN2K

Shaft

Trinity

Knight

Mstream

Kaiten

## Warning

These are classic outdated tools and is presented here for proof of concept ( You will not be able to find the source code for these tools on the Internet). It is presented in this module so that the students are encouraged to view the source code of these tools to understand the attack engineering behind them.

Classic tools presented for proof of concept

# DDoS Tool: Tribal Flood Network

Provides the attacker with the ability to wage both bandwidth depletion and resource depletion attacks

TFN tool provides for UDP and ICMP flooding, as well as TCP SYN, and Smurf attacks

The agents and handlers communicate with ICMP\_ECHO\_REPLY packets. These packets are harder to detect than UDP traffic and have the added ability of being able to pass through firewalls

Classic tool presented for proof of concept





# Tribal Flood Network: Screenshot

The screenshot shows a Windows Notepad window titled "td.c - Notepad". The window contains the source code for a C program named "td.c". The code is a daemon for the Tribal Flood Network, developed by Mixter in 1999. The code includes headers for config.h, tubby.h, control.h, sync.c, udp.c, and icmp.c. It defines a main function that initializes buffers for IP and ICMP headers, creates a raw socket, and handles signal handlers for SIGHUP, SIGTERM, and SIGCHLD. A loop reads from the socket into the buffer.

```
/* td.c - tribe flood network daemon
(c) 1999 by Mixter - PRIVATE */

#include "config.h"
#include "tubby.h"
#include "control.h"
#include "sync.c"
#include "udp.c"
#include "icmp.c"

int
main (int puke, char **fart)
{
    char buf[1024], target[1024], answer[1024];
    struct iphdr *ip = (struct iphdr *) buf;
    struct icmphdr *icmp = (struct icmphdr *) (buf + sizeof (struct iphdr));
    char *p = (buf + sizeof (struct iphdr) + sizeof (struct icmphdr));
    int lsock, i, whereami, port4syn = 0;

    if (geteuid ())
        exit (-1);
    strcpy (fart[0], HIDE_ME);
    lsock = socket (AF_INET, SOCK_RAW, 1);
    close (0);
    close (1);
    close (2);
    if (fork ())
        exit (0);

    signal (SIGHUP, SIG_IGN);
    signal (SIGTERM, SIG_IGN);
    signal (SIGCHLD, SIG_IGN);

    while (1)
    {
        i = read (lsock, buf, 1024);
    }
}
```



TM

# DDoS Tool: TFN2K



Based on the TFN architecture with features designed specifically to make TFN2K traffic difficult to recognize and filter

Remotely executes commands, hides the true source of the attack using IP address spoofing, and transports TFN2K traffic over multiple transport protocols including UDP, TCP, and ICMP

UNIX, Solaris, and Windows NT platforms that are connected to the Internet, directly or indirectly, are susceptible to this attack

Classic tool presented for proof of concept



TM

# TFN2K: Screenshot

```
td.c - Notepad
File Edit Format Help

/*
 * Tribe FloodNet - 2k edition
 * by Mixter <mixter@newyorkoffice.com>
 *
 * td.c - tribe flood server
 */
/*
 * This program is distributed for educational purposes and without any
 * explicit or implicit warranty; in no event shall the author or
 * contributors be liable for any direct, indirect or incidental damages
 * arising in any way out of the use of this software.
 */
#include "tribe.h"

extern int fw00ding, nospoof, port4syn, psize;
extern unsigned long myip;
extern void security_through_obscurity (int);

void tribe_cmd (char, char *, char **);

int
main (int argc, char **argv)
{
    char buf[BS], clear[BS];
    struct ip *iph = (struct ip *) buf;
    struct tribe *tribeh = (struct tribe *) clear;
    int isock, tsock, usock, i;
    char *p = NULL, *data = (clear + sizeof (struct tribe));
    fd_set rfds;

    isock = socket (AF_INET, SOCK_RAW, ICMP);
    tsock = socket (AF_INET, SOCK_RAW, TCP);
    usock = socket (AF_INET, SOCK_RAW, UDP);

    if (geteuid () >
```

# DDoS Tool: Shaft

Shaft is a derivative of the Trin00 tool which uses UDP communication between handlers and agents

Shaft provides statistics on the flood attack. These statistics are useful to the attacker to know when the victim's system is completely down and allows the attacker to know when to stop adding zombie machines to the DDoS attack. Shaft provides UDP, ICMP, and TCP flooding attack options

One interesting signature of Shaft is that the sequence number for all TCP packets is 0x28374839

Classic tool presented for proof of concept





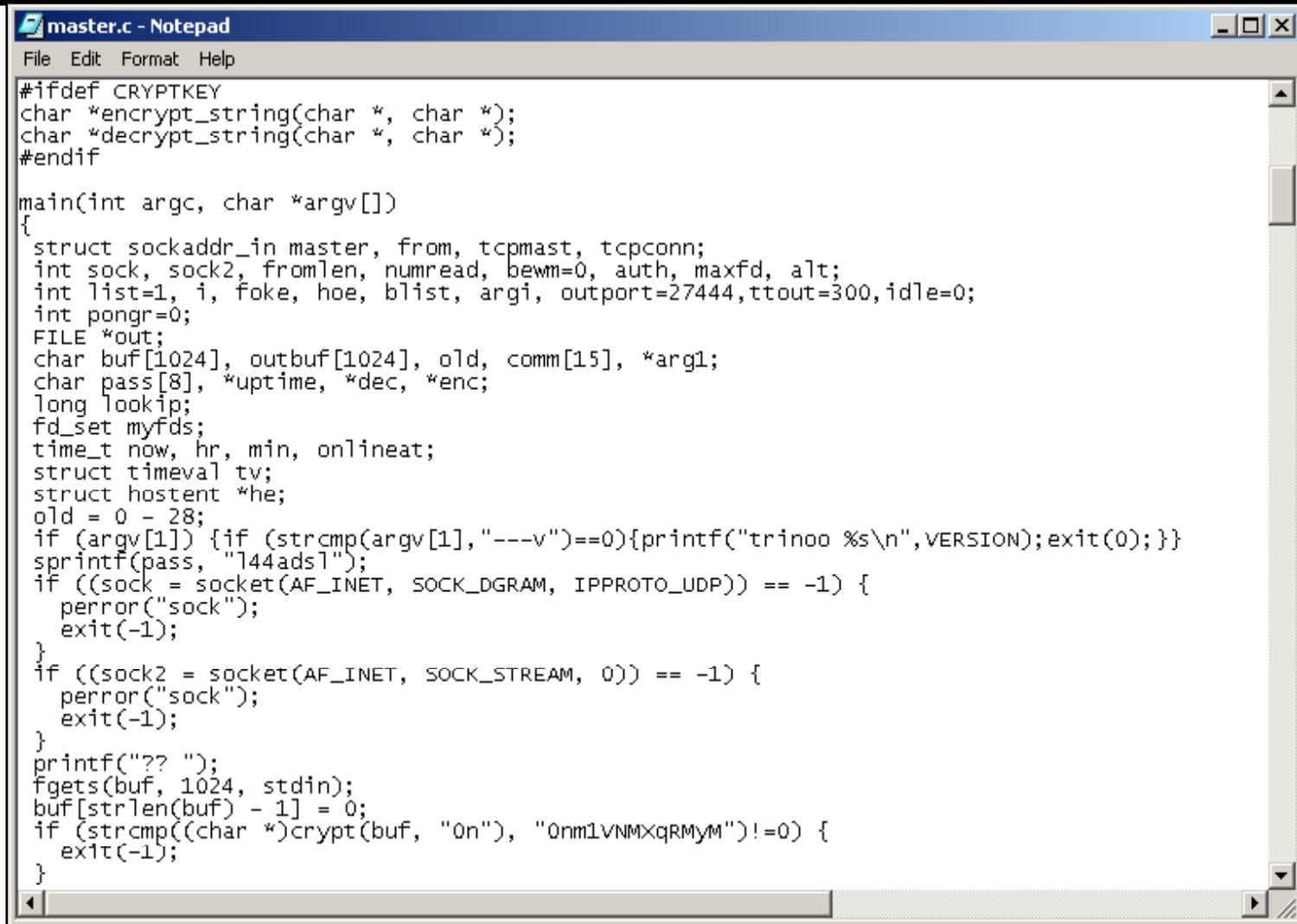
Trinity appears to use port 6667 primarily and also has a backdoor program that listens on TCP port 33270

Trinity has a wide variety of attack options including UDP, TCP SYN, TCP ACK, and TCP NUL packet floods as well as TCP fragment floods, TCP RST packet floods, TCP random flag packet floods, and TCP established floods

It has the ability to randomize all 32 bits of the source IP address

Classic tool presented for proof of concept

# Trinity: Screenshot



The screenshot shows a Windows Notepad window titled "master.c - Notepad". The code displayed is a C program named "master.c". The code includes a section for encrypting and decrypting strings, defines a main function that handles socket communication, and includes logic for handling command-line arguments and performing crypt operations.

```
#ifndef CRYPTKEY
char *encrypt_string(char *, char *);
char *decrypt_string(char *, char *);
#endif

main(int argc, char *argv[])
{
    struct sockaddr_in master, from, tcpmast, tcpconn;
    int sock, sock2, fromlen, numread, bewm=0, auth, maxfd, alt;
    int list=1, i, foke, hoe, blist, argi, outport=27444, ttout=300, idle=0;
    int pongr=0;
    FILE *out;
    char buf[1024], outbuf[1024], old, comm[15], *arg1;
    char pass[8], *uptime, *dec, *enc;
    long lookip;
    fd_set myfds;
    time_t now, hr, min, onlineat;
    struct timeval tv;
    struct hostent *he;
    old = 0 - 28;
    if (argc[1]) {if (strcmp(argv[1], "--v") == 0){printf("trinoo %s\n", VERSION);exit(0);}}
    sprintf(pass, "144ads1");
    if ((sock = socket(AF_INET, SOCK_DGRAM, IPPROTO_UDP)) == -1) {
        perror("sock");
        exit(-1);
    }
    if ((sock2 = socket(AF_INET, SOCK_STREAM, 0)) == -1) {
        perror("sock");
        exit(-1);
    }
    printf("?? ");
    fgets(buf, 1024, stdin);
    buf[strlen(buf) - 1] = 0;
    if (strcmp((char *)crypt(buf, "On"), "Onm1VNMXqRMym") != 0) {
        exit(-1);
    }
}
```



## Knight:

- IRC-based DDoS attack tool that was first reported in July 2001
- It provides SYN attacks, UDP Flood attacks, and an urgent pointer flooder
- Can be installed by using a Trojan horse program called Back Orifice
- Knight is designed to run on Windows operating systems

## Kaiten:

- Another IRC-based DDoS attack tool
- Is based on Knight, and was first reported in August of 2001
- Supports a variety of attacking features. It includes code for UDP and TCP flooding attacks, for SYN attacks, and a PUSH + ACK attack
- It also randomizes the 32 bits of its source address

Classic tools presented for proof of concept

# DDoS Tool: Mstream

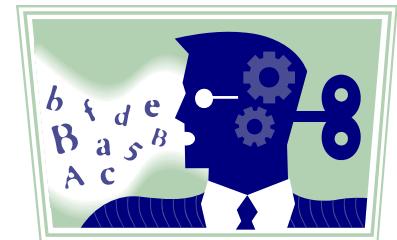
Uses spoofed TCP packets with the ACK flag set to attack the target

Mstream tool consists of a handler and an agent portion, much like previously known DDoS tools such as Trinoo

Access to the handler is password protected

The apparent intent for 'stream' is to cause the handler to instruct all known agents to launch a TCP ACK flood against a single target IP address for a specified duration

Classic tool presented for proof of concept





TM

# How to Conduct a DDoS Attack

## **Step 1:**

- Write a virus that will send ping packets to a target network/websites

## **Step 2:**

- Infect a minimum of (30,000) computers with this virus and turn them into “zombies”

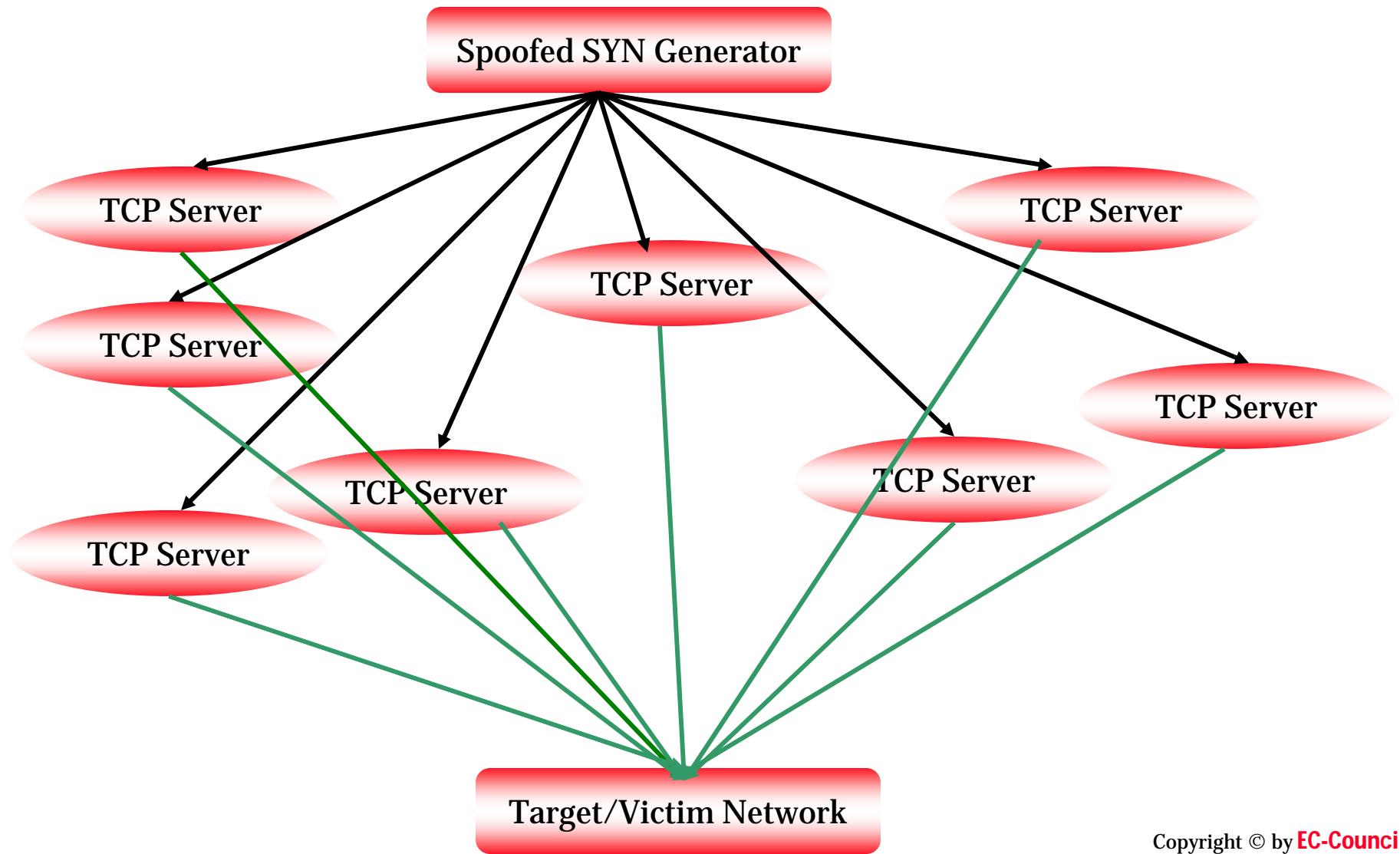
## **Step 3:**

- Trigger the zombies to launch the attack by sending wake-up signals to the zombies or activated by certain data

## **Step 4:**

- The zombies will start attacking the target server until they are disinfected

# The Reflected DoS Attacks



# Reflection of the Exploit

TCP three-way handshake vulnerability is exploited



The attacking machines send out huge volumes of SYN packets but with the IP source address pointing to the target machine

Any general-purpose TCP connection-accepting Internet server could be used to reflect SYN packets

For each SYN packet received by the TCP reflection server, up to four SYN/ACK packets will generally be sent

It degrades the performance of the aggregation router

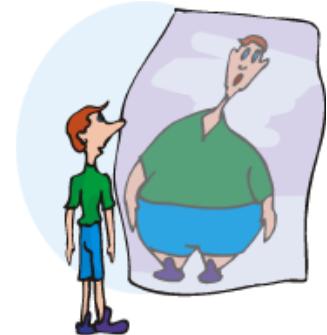
# Countermeasures for Reflected DoS

Router port 179 can be blocked as a reflector

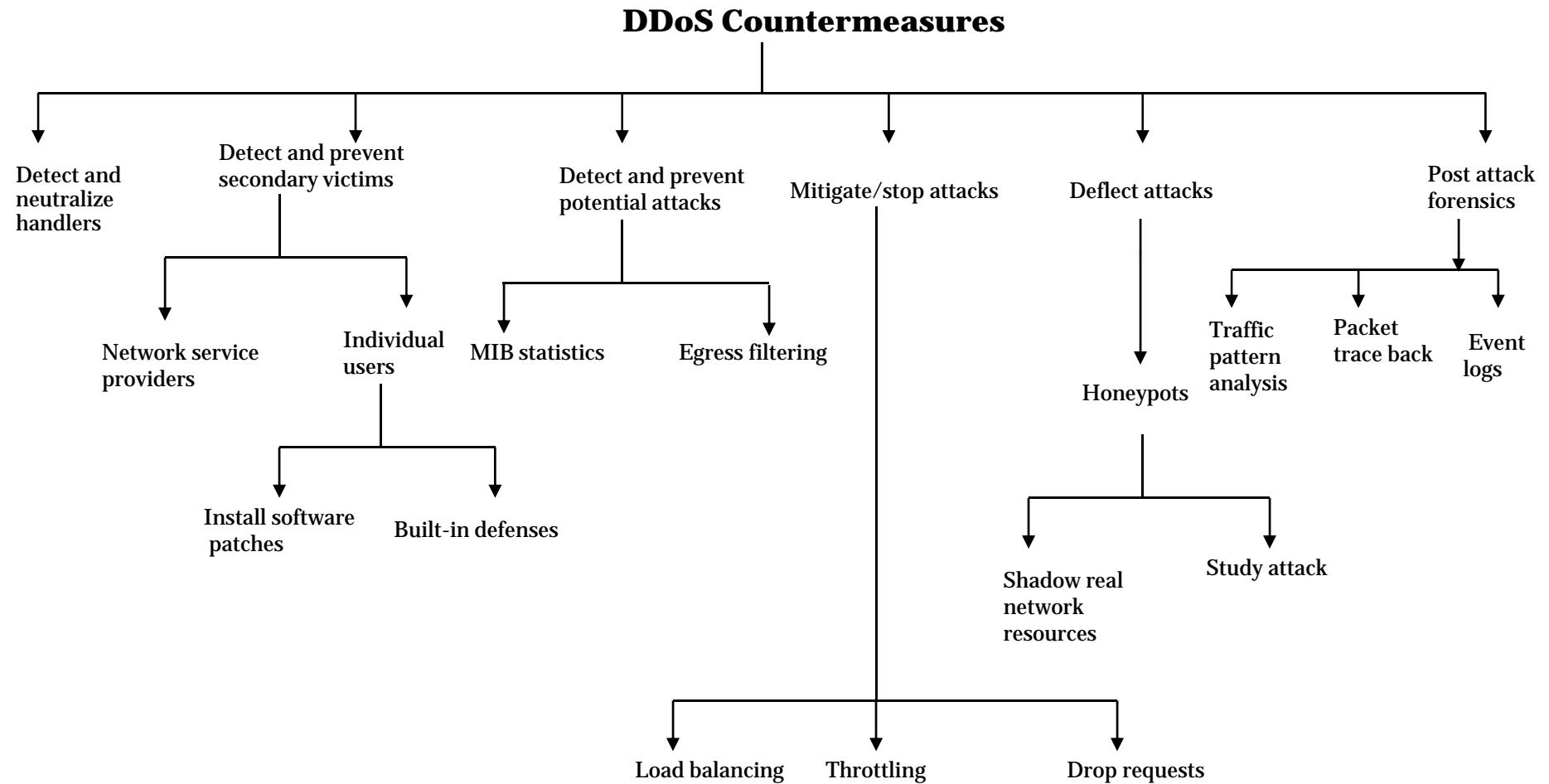
Blocking all inbound packets originating from the service port range will block most of the traffic being innocently generated by reflection servers

ISPs could prevent the transmission of fraudulently addressed packets

Servers could be programmed to recognize a SYN source IP address that never completes its connections



# DDoS Countermeasures



Three essential components:

Preventing secondary victims and detecting and neutralizing handlers

Detecting or preventing the attack, mitigating or stopping the attack, and deflecting the attack

The post-attack component which involves network forensics





TM

# Preventing Secondary Victims

A heightened awareness of security issues and prevention techniques from all Internet users

Agent programs should be scanned for in the systems

Installing anti-virus and anti-Trojan software, and keeping these up-to-date can prevent installation of the agent programs

Daunting for the average “web-surfer,” recent work has proposed built-in defensive mechanisms in the core hardware and software of computing systems

# Detect and Neutralize Handlers

Study of communication protocols and traffic patterns between handlers and clients or handlers and agents in order to identify network nodes that might be infected with a handler

There are usually few DDoS handlers deployed as compared to the number of agents. So neutralizing a few handlers can possibly render multiple agents useless, thus thwarting DDoS attacks



## Egress filtering

- Scanning the packet headers of IP packets leaving a network

There is a good probability that the spoofed source address of DDoS attack packets will not represent a valid source address of the specific sub-network

Placing a firewall or packet sniffer in the sub-network that filters out any traffic without an originating IP address





TM

# DoSHTTP Tool

DoSHTTP is a powerful HTTP Flood Denial of Service testing software for windows

It includes URL verification, HTTP Redirection, and performance monitoring

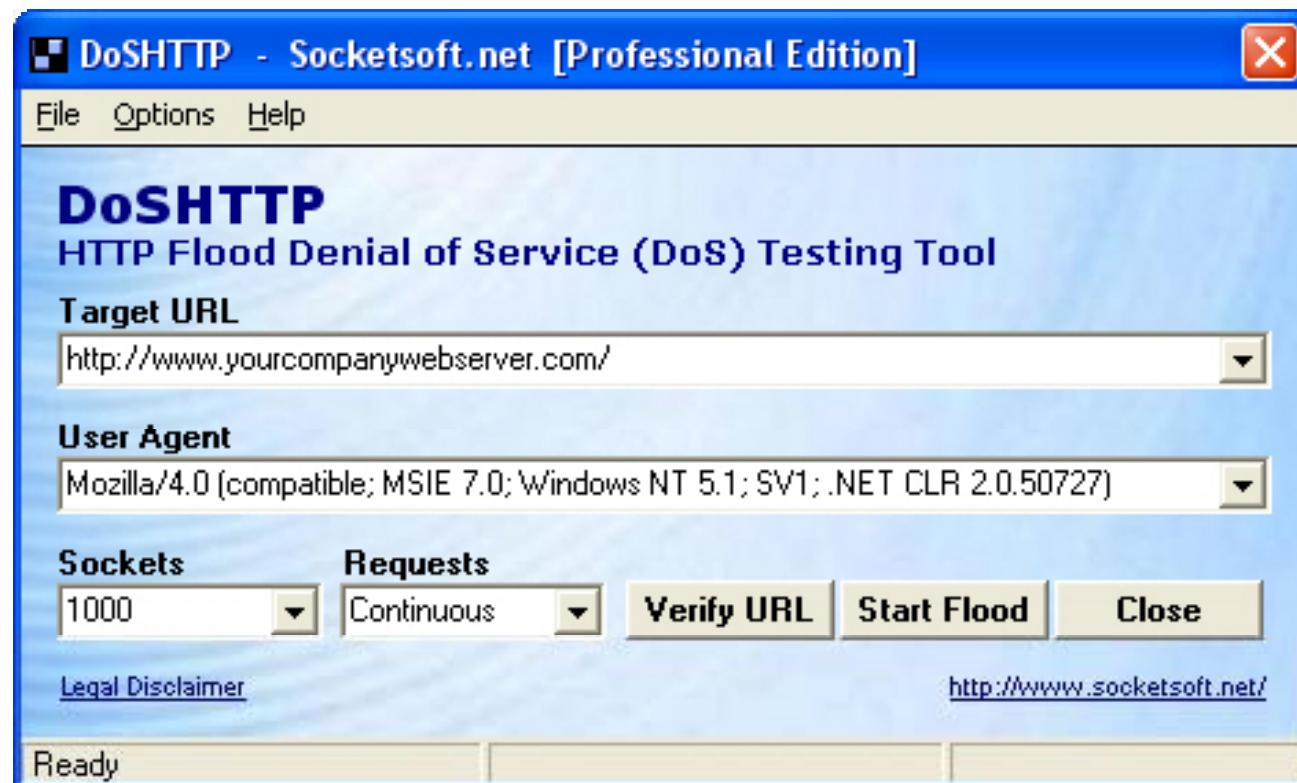
It makes use of multiple asynchronous sockets for performing an effective HTTP Flood

It can function in multiple clients simultaneously to emulate DDOS attack

The features of DDOS are:

- It allows customized User Agent header fields
- It allows user defined Socket and Request settings
- For the target URL's, it supports numeric addressing

# DoSHTTP Tool: Screenshot



# Mitigate or Stop the Effects of DDoS Attacks

## Load Balancing

- Providers can increase bandwidth on critical connections to prevent them from going down in the event of an attack
- Replicating servers can provide additional failsafe protection
- Balancing the load to each server in a multiple-server architecture can improve both normal performances as well as mitigate the effect of a DDoS attack



## Throttling

- This method sets up routers that access a server with logic to adjust (throttle) incoming traffic to levels that will be safe for the server to process



# Deflect Attacks

## Honeypots

- Systems that are set up with limited security act as an enticement for an attacker
- Serve as a means for gaining information about attackers by storing a record of their activities and learning what types of attacks and software tools the attackers used



KFSensor

File View Scenario Help

127.0.0.1 - Main Scenario

TCP

- 2 Death, Trojan - Recent Activity
- 21 FTP - Recent Activity
- 22 SSH - Recent Activity
- 23 Telnet - Recent Activity
- 25 SMTP - Error
- 53 DNS - Recent Activity
- 80 HTTP MS IIS - Error
- 110 POP MS - Error
- 999 WinSatan
- 1024 NetSpy, T...
- 1080 WinGate
- 1433 MS SQL Server
- 2023 Hack City
- 5000 Socket32 - Error
- 6912 Sht Heep, T...
- 6969 GateCrasher, Tr...**
- 6970 GateCrasher, Tr...

Ready

Edit Scenario

Name: Main Scenario

Domain Name: fakewebsiteattack.com

Name	Active	Protocol	Port	Sensor Bind	Severity	Action	Sim Server
Death, Trojan	True	TCP	2		Medium	Close	
FTP	True	TCP	21		Medium	SimBanner	FTP MS
SSH	True	TCP	22		Medium	ReadAndClose	
Telnet	True	TCP	23		High	SimStdServer	Telnet
SMTP	True	TCP	25		High	SimStdServer	SMTP
DNS	True	TCP	53		Medium	ReadAndClose	
HTTP MS IIS	True	TCP	80		Medium	SimBanner	HTTP MS IIS
POP MS	True	TCP	110		Medium	SimBanner	POP MS
WinSatan	True	TCP	999		Medium	ReadAndClose	
NetSpy, Trojan	True	TCP	1024		Medium	Close	
WinGate	True	TCP	1080		Medium	ReadAndClose	
MS SQL Server	True	TCP	1433		Medium	ReadAndClose	
Hack City Ripper...	True	TCP	2023		Medium	ReadAndClose	
Socket32	True	TCP	5000		Medium	ReadAndClose	
Sht Heep, Trojan	True	TCP	6912		Medium	Close	
GateCrasher, Tr...	True	TCP	6969		Medium	ReadAndClose	
GateCrasher, Tr...	True	TCP	6970		Medium	ReadAndClose	
Hack Office Arm...	True	TCP	8879		Medium	ReadAndClose	
HTTP MS IIS	True	TCP	9133		Medium	SimBanner	HTTP MS IIS
HTTP Apache	True	TCP	9732		Medium	SimBanner	HTTP Apache
SunHive_Telnet	True	TCP	10985		Medium	Close	

Change All... Active Add... Edit... Delete OK Cancel Help

## Traffic pattern analysis

- Data can be analyzed—post-attack—to look for specific characteristics within the attacking traffic

This characteristic data can be used for updating load balancing and throttling countermeasures

DDoS attack traffic patterns can help network administrators to develop new filtering techniques for preventing it from entering or leaving their networks



# Packet Traceback

Packet Traceback allows back tracing the attacker's traffic and possibly identifying the attacker

Additionally, when the attacker sends vastly different types of attacking traffic, this method assists in providing the victim's system with information that might help develop filters to block the attack

Event Logs:

- It keeps logs of the DDoS attack information in order to do a forensic analysis, and to assist law enforcement in the event the attacker does severe financial damage





TM

# What Happened Next

Jason Springfield, an Ethical Hacker whom Henderson knew, was called to investigate the case. Jason checks the network performance. Shocked to find the evidence of huge Sync attacks, Jason is forced to believe that the attack was one kind of distributed denial of service attack using spoofed IPs.

Large number of computers connected on the Internet played the role of zombie machines, and all were directed towards the “HackzXposed4u” portal. The web server was subjected to a large number of requests which made it unstable thereby crashing the system.



# Summary

DoS attacks can prevent legitimate users from using the system by overloading the resources

It can result in disabled network, disabled organization, financial loss, and loss of goodwill

Smurf, Buffer overflow, Ping of death, Teardrop, SYN, and Tribal Flow Attacks are some of the types of DoS attacks; and WinNuke, Targa, Land, and Bubonic.c are some of the tools used to achieve DoS

A DDoS attack is an attack in which a multitude of compromised systems attack a single target

Countermeasures include preventing secondary victims, detecting and neutralizing handlers, detecting or preventing the attack, mitigating or stopping the attack, and deflecting the attack



TM

DEAR, I THINK YOU'RE  
SPENDING WAAAAAY  
TOO MUCH TIME ON  
THE INTERNET.

I.COM  
AM.COM  
NOT.COM



© 2000 Randy Glasbergen. [www.glasbergen.com](http://www.glasbergen.com)



TM

Certified Ethical Hacker

Copyright 2005 by Randy Glasbergen.  
[www.glasbergen.com](http://www.glasbergen.com)



**"To protect our network against computer viruses,  
our IT Department has issued a ban on any use of  
e-mail attachments. For further details, please  
refer to the attached document."**