

Attack the [*own*] Network so you`ll survive

Who Am I

- Founder echo.or.id, e-rdc.org, ubuntulinux.or.id
- A Bandwidth hunter
- Security TroubleMaker since 2000
- Not a Celebrity
- y3dips@REMOVEUPPERCASEecho.or.id

Network?

- So, what is Network?
- A collection of host computers together with the subnetwork or internetwork through which they can exchange data.
- **Internet**, very popular term in network

Issue

- Spoofing
- Sniffing
- Tunneling
- Denial Of Service/ Botnets

Why attacking?

“The best defense is a good offense”

<http://www.answers.com/topic/attack-is-the-best-form-of-defence>

Brief History

- TCP/IP is more than 30 years
- Create without security considerations, eg: FTP, TELNET, SMTP, POP3
- Weakness Lies on IP layer, no auth and encryption

Spoofing

- Spoof = Masquerade - rfc4949
- Is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage — wikipedia

Spoofing Example

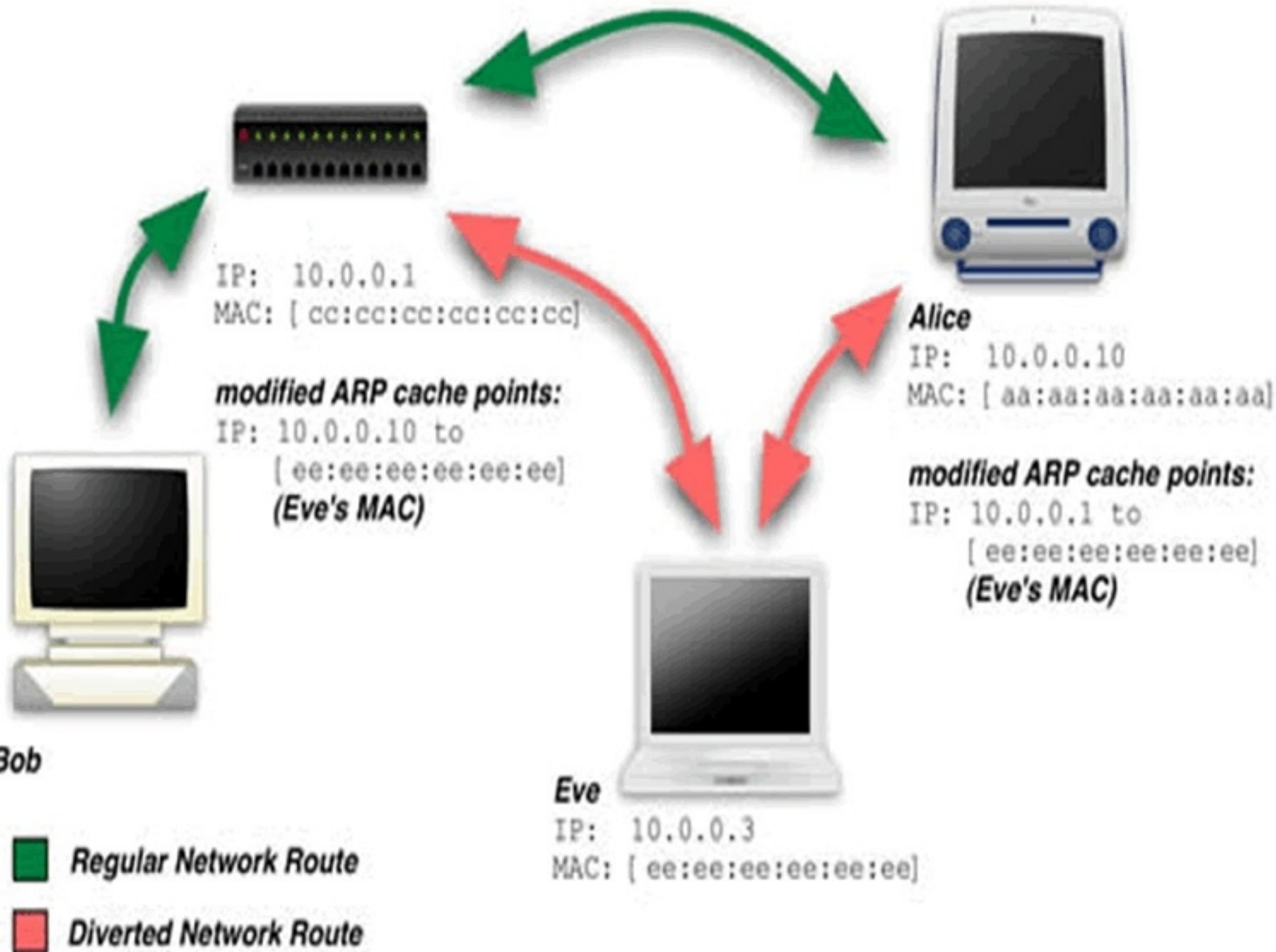
- IP spoofing, e.g: modify source address

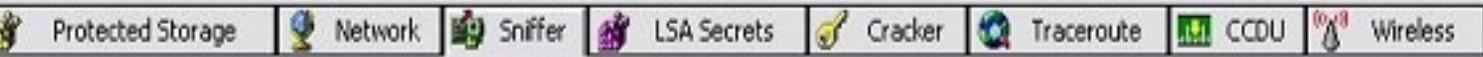
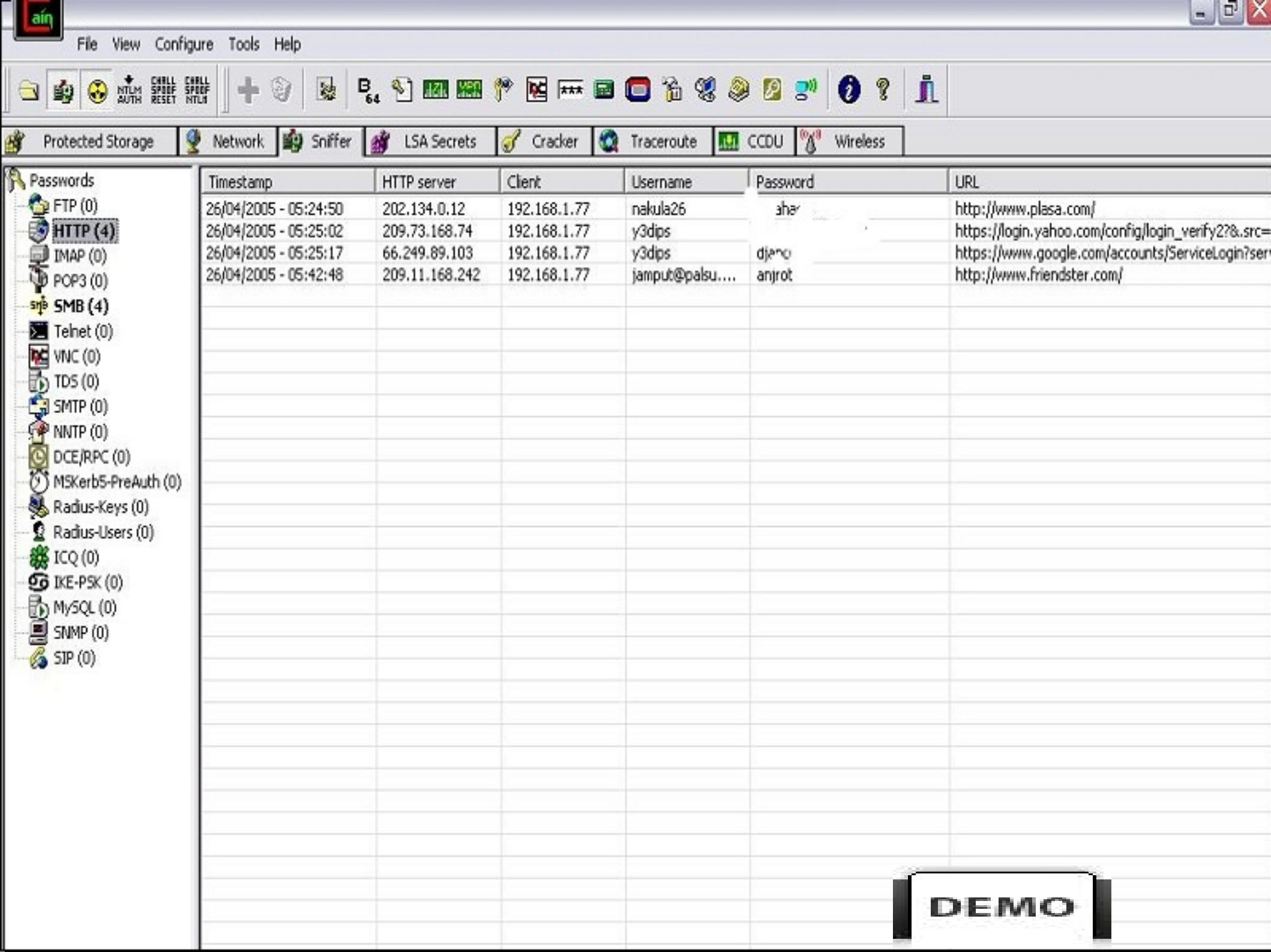
A common misconception is that "IP spoofing" can be used to hide your IP address while surfing the Internet, chatting on-line, sending e-mail, and so forth. This is generally **not true**. Forging the source IP address causes the responses to be misdirected, meaning you cannot create a normal network connection. - iss.net

- Combine with DDOS attack

Spoofing Example

- ARP Spoofing
- Send 'fake' or 'spoofed', ARP messages to an Ethernet LAN. These frames contain false MAC addresses, confusing network devices (e.g switches)
- Monkey In the Middle Attack with Cain
- Cain, ettercap, nemesis, dsniff





- Protected Storage
 - Network
 - Sniffer
 - LSA Secrets
 - Cracker
 - Traceroute
 - CCDU
 - Wireless
- Passwords
- FTP (0)
 - HTTP (4)**
 - IMAP (0)
 - POP3 (0)
 - SMB (4)
 - Telnet (0)
 - VNC (0)
 - TDS (0)
 - SMTp (0)
 - NNTP (0)
 - DCE/RPC (0)
 - MSKerberos-PreAuth (0)
 - Radius-Keys (0)
 - Radius-Users (0)
 - ICQ (0)
 - IKE-PSK (0)
 - MySQL (0)
 - SNMP (0)
 - SIP (0)

Timestamp	HTTP server	Client	Username	Password	URL
26/04/2005 - 05:24:50	202.134.0.12	192.168.1.77	nakula26	aha	http://www.plasa.com/
26/04/2005 - 05:25:02	209.73.168.74	192.168.1.77	y3dips		https://login.yahoo.com/config/login_verify2?&.src=
26/04/2005 - 05:25:17	66.249.89.103	192.168.1.77	y3dips	djemo	https://www.google.com/accounts/ServiceLogin?ser
26/04/2005 - 05:42:48	209.11.168.242	192.168.1.77	jampub@palsu....	anjrot	http://www.friendster.com/

DEMO

Sniffing

- "*wiretapping*"
- Capturing and examining the data packets carried on a LAN - rfc4949
- Objectives : Capture credential data through network (password, files, video sound, etc)
- Hub (passive) v.s Switch (active)
- Wireshark (ethereal), ettercap, tcpdump
- MITM, Combine with spoofing

Tunneling

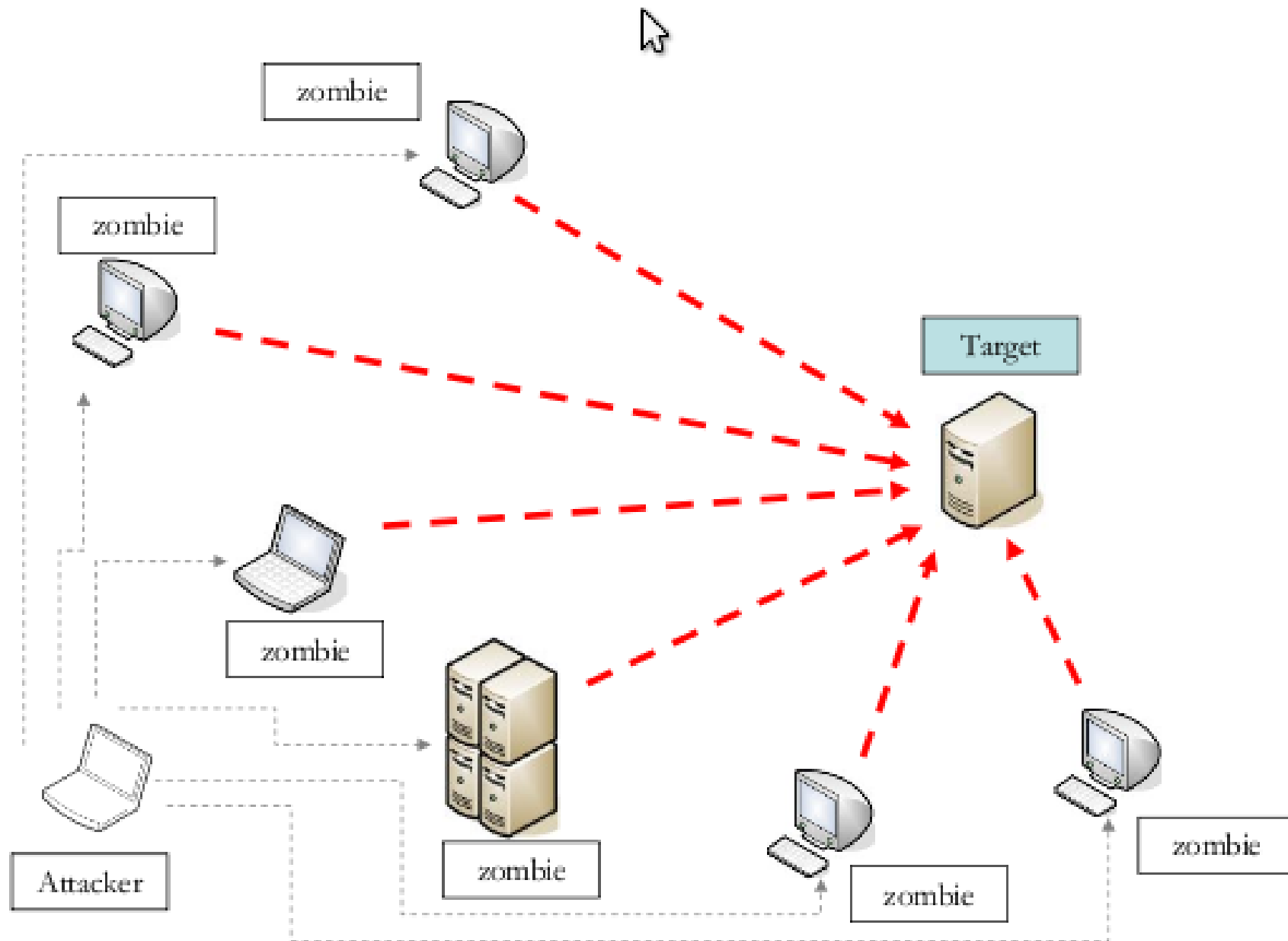
- Tunnel is A communication channel created in a computer network by encapsulating (i.e., layering) a communication protocol's data packets in (i.e., above) a second protocol that normally would be carried above, or at the same layer as, the first one. - rfc4949
- Http, ssh, dns, icmp
- Ssh `foo@doo -D port`

DOS

- The prevention of authorized access to a system resource or the delaying of system operations and function — rfc4949
- Famous POD, synflood, new attack (actually old, <http://it.slashdot.org/article.pl?sid=08/10/01/0127245>)
- DDOS attack
- BotNet

DOS attacker 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



DDoS Topology

CNN.com.technology > computing

Editions | myCNN | Video | Audio | **Headline News Brief** | Feedback

INSURGENCY on the internet in-depthreports ←

[Main Page](#) | [Bracing for Cyberwar](#) | [Hacking Primer](#) | [Scenes from the 'Hacker Underground'](#) | [Hacking: Two Viewpoints](#) | [Timeline](#) | [Gallery](#) | [News Archive](#) | [Discussion](#) | [Related Sites](#)

'Mafiaboy' faces up to 3 years in prison

April 19, 2000
Web posted at: 5:33 p.m. EDT (2133 GMT)

By D. Ian Hopper
CNN Interactive Technology Editor

(CNN) --Under Canadian law, "Mafiaboy" faces a maximum of three years in jail if convicted in February's denial of service attacks.



The Royal Canadian Mounted Police and the U.S. Federal Bureau of Investigation announced Wednesday that a 15-year-old boy who lives in the Montreal area was charged Monday with two counts of "mischief to data" in connection with the denial of service attack on CNN.com in February.

Since he is a minor, his name has not been released. Instead, authorities have referred to him only by his online handle, "Mafiaboy."

As opposed to the United States, where individual states can criminally prosecute suspects, in Canada all criminal law is federal.

✖ INTERACTIVE
[Check here to see how a denial of service attack works.](#)

CNN.com NewsNet

CNN Sites

Search

CNN.com

Find

TECHNOLOGY

TOP STORIES

[Consumer group: Online privacy protections fall short](#)

[Guide to a wired Super Bowl](#)

[Debate opens on making e-commerce law consistent](#)

(MORE)

CNN.com

TOP STORIES

[More than 11,000 killed in India quake](#)

[Mideast negotiators want to continue talks after Israeli elections](#)

(MORE)

money BUSINESS

[Playing for Iraq's jackpot](#)

[Coke & smoke bite Dow](#)

- MAINPAGE
- WORLD
- U.S.
- WEATHER
- BUSINESS
- SPORTS
- TECHNOLOGY** ↓
- computing
- personal technology
- SPACE
- HEALTH
- ENTERTAINMENT
- POLITICS
- LAW
- CAREER
- TRAVEL
- FOOD
- ARTS & STYLE
- BOOKS
- NATURE
- IN-DEPTH
- ANALYSIS
- LOCAL

EDITIONS:
[CNN.com Europe](#)
[change default edition](#)

MULTIMEDIA:
[video](#)
[video archive](#)
[audio](#)
[multimedia showcase](#)
[more services](#)

E-MAIL:
Subscribe to one of our news e-mail lists.
Enter your address:

DISCUSSION:
[chat](#)
[feedback](#)

Survive

“Security is a process, not a product”

Survive (cont`d)

- Firewall, IDS, IPS just a tool
- Educate the user
- Implement the Best policy
- Regularly Audit

**Thanks All.
Q&A ?**