Understanding Distributed Denial-of-Service Attacks

Craig Ozancin

Senior Security Analyst

Symantec Product Vulnerability Coordinator

cozancin@symantec.com

Agenda

- The Anatomy of a Denial-of-Service attack
- Distributed Denial-of-Service
- Trends and Factors
- A history in the making
- Distributed Denial-of-Service tools
- Is there an solutions?
- Where can I find more information
- Conclusion
- Questions?

I: The Anatomy of a Denial-of-service Attack

What Is a Denial-of-Service

A Denial-of-Services is when someone or something is prevented from performing a desired task or operation.

Types of Denial-of-Service Attacks

- **Bandwidth Consumption**
  - Flooding a smaller network with data
    - **flooding a 56-kbps network connection from a T1 connection.**
    - **This may actually be legitimate network usage**
  - Using multiple sources to flood a network
- **Resource Starvation (Consuming system resources)**
  - filling Disk/File system
  - memory fully allocated
  - CPU at maximum usage
  - Filling process table

Definitions from “Hacking Exposed”

Types of Denial-of-Service Attacks

- **Programming Flaws**
  - Buffer overflows that cause services to terminate prematurely
  - Memory leaks that can be used to consume system resources
  - Malformed or illegal network packets that cause kernel crashes
- **Routing and DNS Attacks**
  - Manipulation of routing tables to prevent legitimate access (breaking into routers)
  - Manipulation of DNS tables to point to alternate IP addresses

Definitions from “Hacking Exposed”

DoS Attacks Can Strike Anywhere

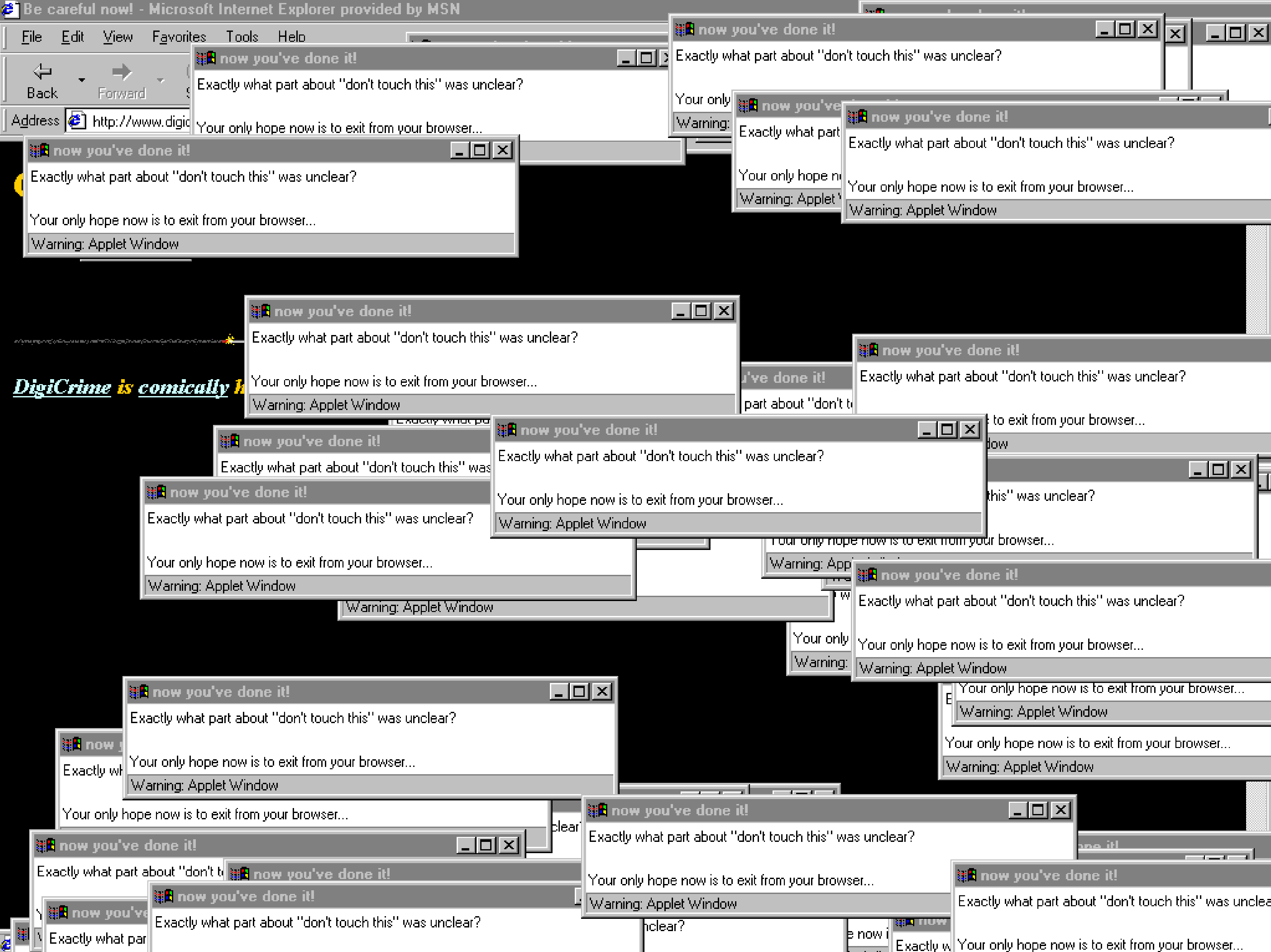
- **Web browsers**
  - The browser becomes unresponsive
  - Continues to open windows (until system resources are exhausted)
- **Individual Services**
  - Disable or crash network services (a buffer overflow can cause a service to crash)
- **The whole system**
  - Resource attacks (file system, process table, memory, …)
- **The whole network**
  - NIS, DNS, …

Networks

- **Cause a large amount of network traffic**
- **Connectivity slows to a standstill**
- **Starts dropping packets**
- **Network Information Service (NIS) attack:**
  - Systems using NIS must request user information from the NIS server, one user at a time.
  - This creates a spike in network traffic (not to heavy under normal use).
  - The follow could be used to perform a network DoS:

```
while :
do
    finger bogus-name@system &
done
```

The system power turns off!



now you've done it!

Exactly what part about "don't touch this" was unclear?

Your only hope now is to exit from your browser...

now you've done it!

Exactly what part about "don't touch this" was unclear?

Your only

Warning:

now you've done it!

Exactly what part about "don't touch this" was unclear?

Your only hope now is to exit from your browser...

Warning: Applet Window

now you've

Exactly what part

Your only hope n

Warning: Applet

now you've done it!

Exactly what part about "don't touch this" was unclear?

Your only hope now is to exit from your browser...

Warning: Applet Window

now you've done it!

Exactly what part about "don't touch this" was unclear?

Your only hope now is to exit from your browser...

Warning: Applet Window

u've done it!

part about "don't t

now you've done it!

Exactly what part about "don't touch this" was unclear?

to exit from your browser...

dow

now you've done it!

Exactly what part about "don't touch this" was

now you've done it!

Exactly what part about "don't touch this" was unclear?

Your only hope now is to exit from your browser...

Warning: Applet Window

this" was unclear?

Your only hope now is to exit from your browser...

Warning: App

now you've done it!

Exactly what part about "don't touch this" was unclear?

Your only hope now is to exit from your browser...

Warning: Applet Window

Warning: Applet Window

Your only

Warning:

now you've done it!

Exactly what part about "don't touch this" was unclear?

Your only hope now is to exit from your browser...

Warning: Applet Window

Your only hope now is to exit from your browser...

Warning: Applet Window

Your only hope now is to exit from your browser...

Warning: Applet Window

now you've done it!

Exactly what part about "don't touch this" was unclear?

Your only hope now is to exit from your browser...

Warning: Applet Window

now

Exactly wh

Your only hope now is to exit from your browser...

clear?

now you've done it!

Exactly what part about "don't t

now you've done it!

now you've done it!

Exactly what part about "don't touch this" was unclear?

now you've

Exactly what par

nclear?

e now i

Exactly w

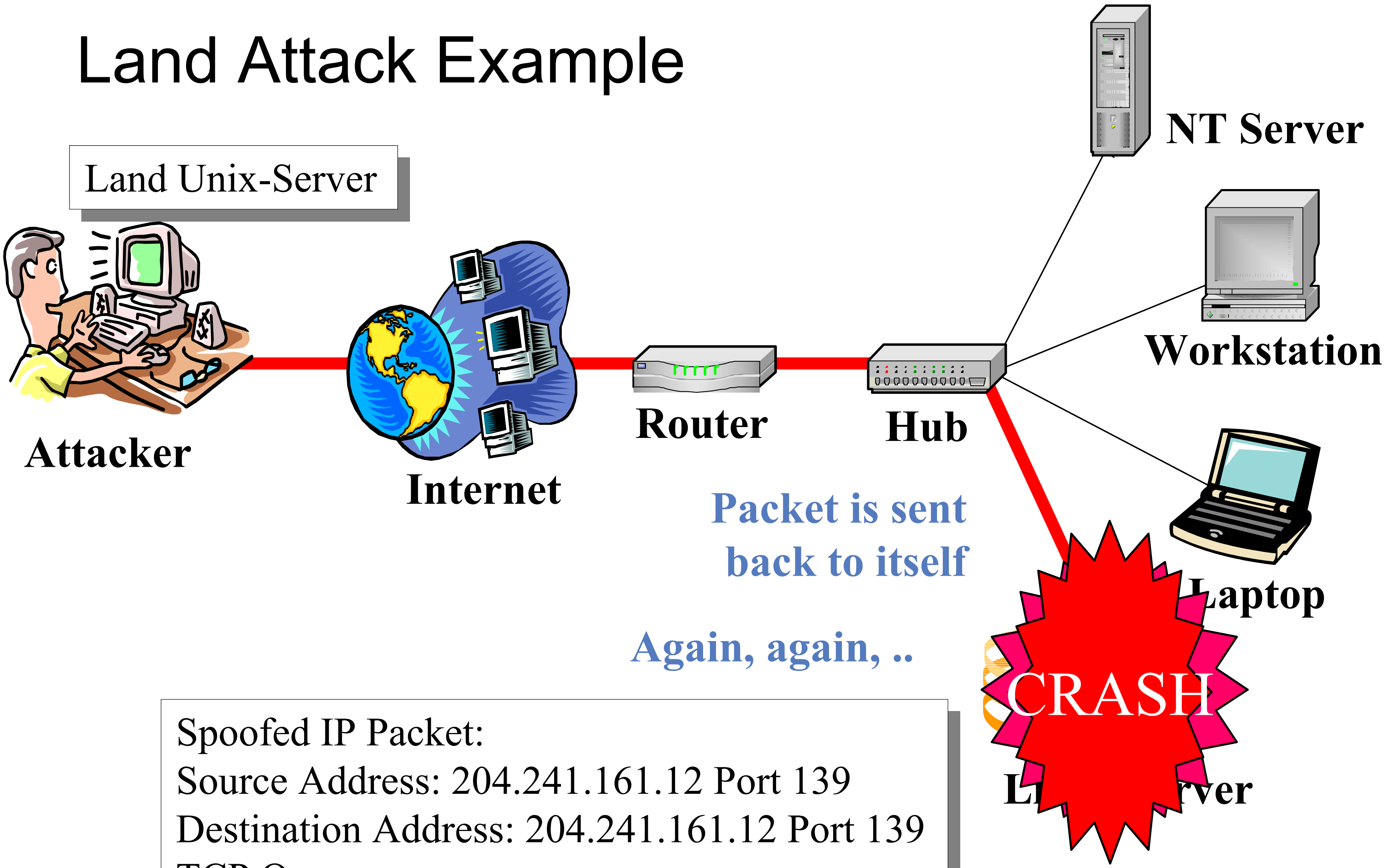
now you've done it!

Exactly what part about "don't touch this" was uncle

Your only hope now is to exit from your browser...

Land Attack Example

Land Unix-Server

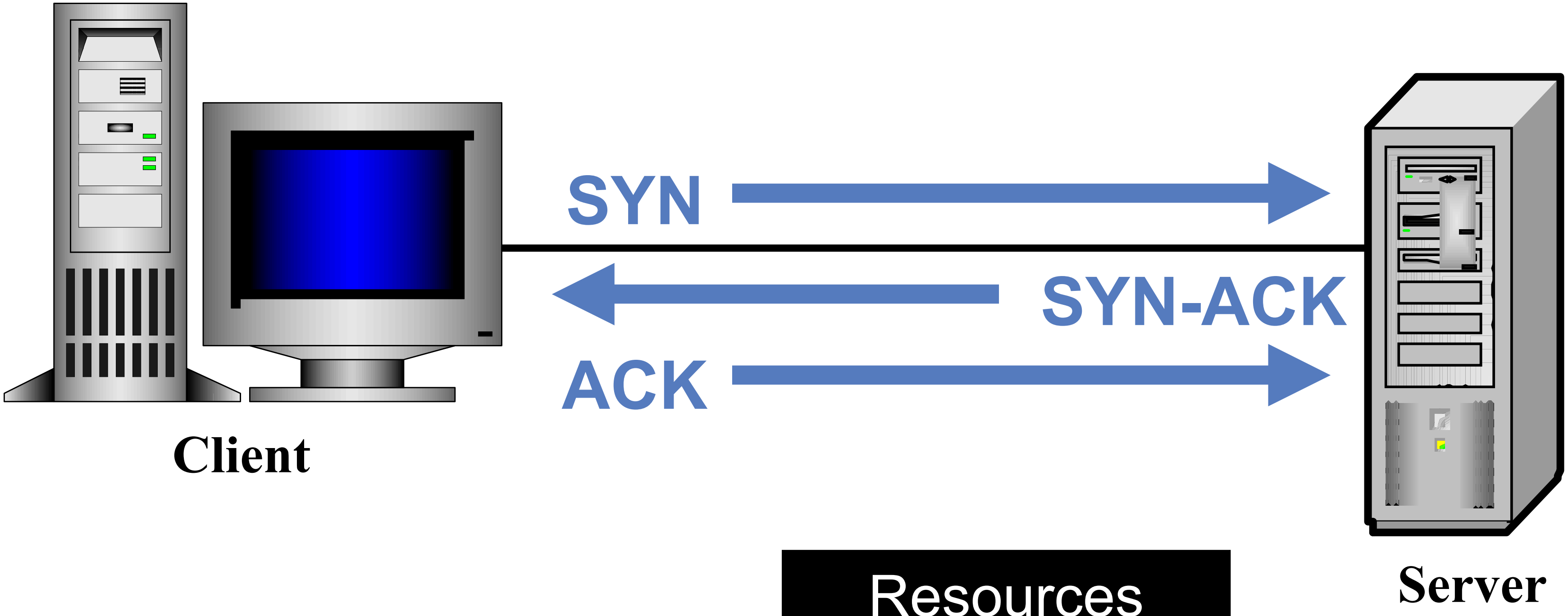


Packet is sent back to itself

Again, again, ..

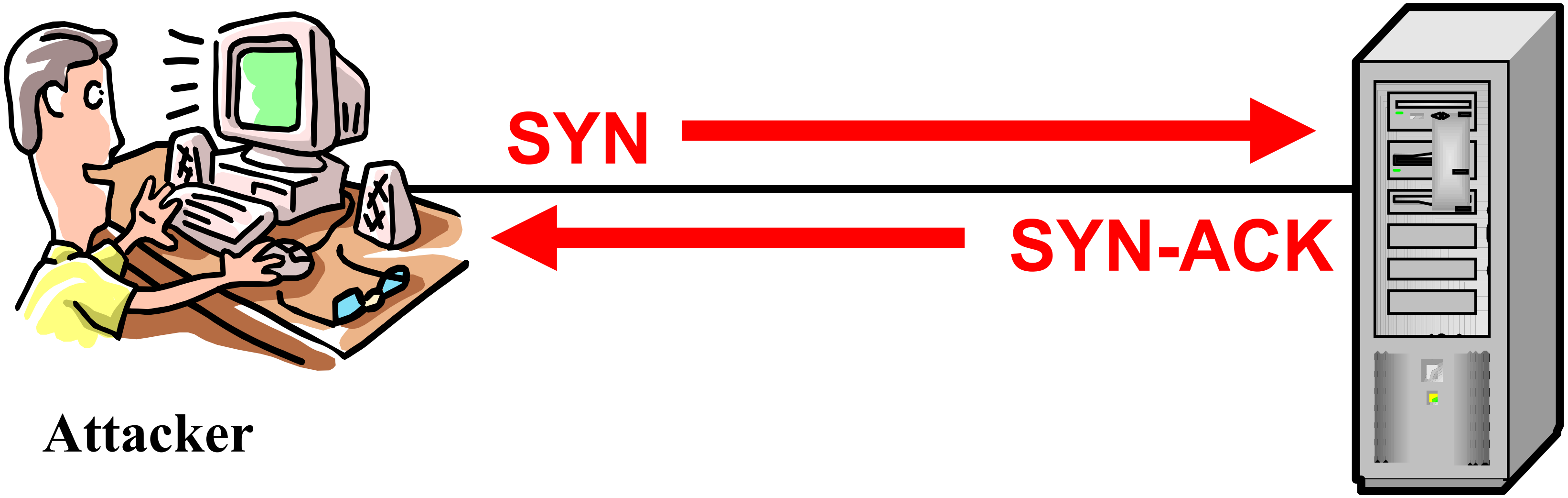
Spoofed IP Packet:
Source Address: 204.241.161.12 Port 139
Destination Address: 204.241.161.12 Port 139
TCP Open

Connection Oriented 3-Way Handshake



Resources
Allocated

Beginning of a Syn-flood Attack



SYN

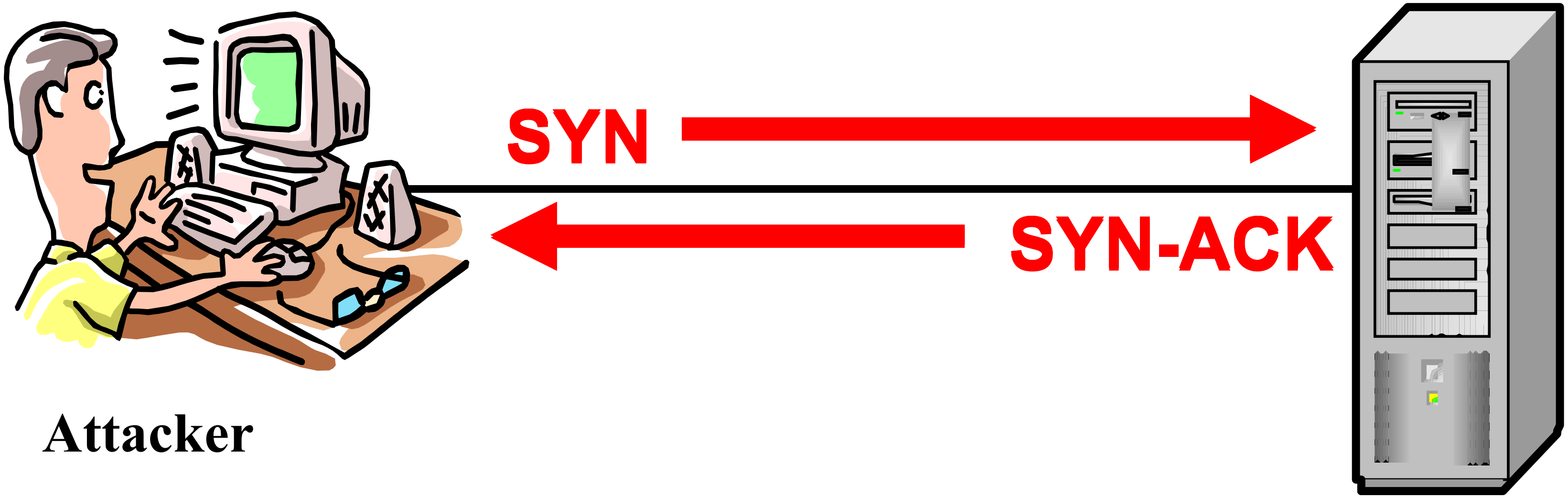
SYN-ACK

Attacker

Server

Resources

The Complete Syn-flood



SYN

SYN-ACK

Attacker

Server

No

More

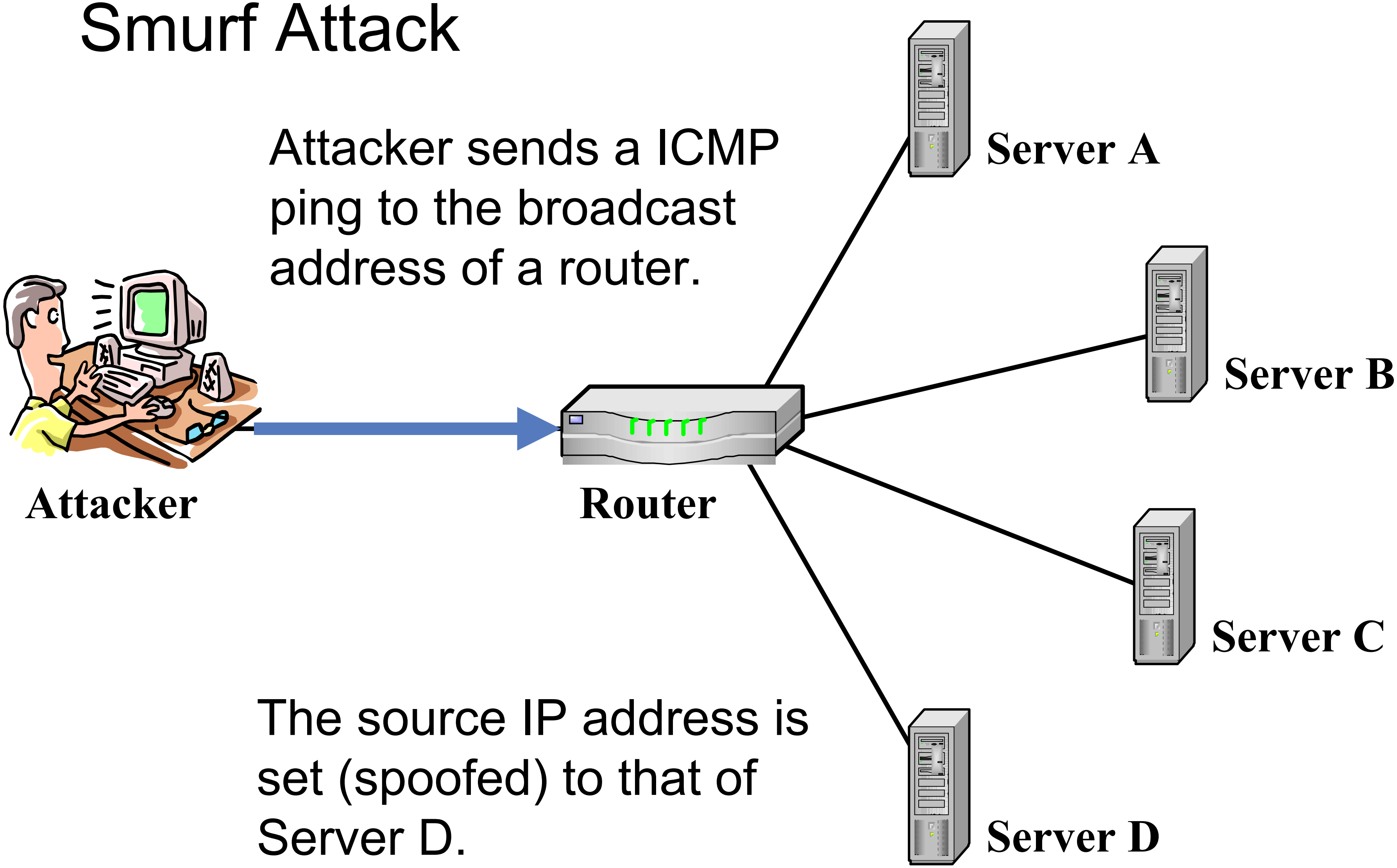
Resources

Evidence of SYN Flood

- **Look for too many connections in the state “SYN_RECEIVED” may indicate an attack**
  - SunOS
    - — **netstat -a –f inet**
  - FreeBSD
    - — **netstat -s |grep “listenqueue overflows”**
  - Windows
    - — **netstat –a**
  - Linux
    - — **netstat –a**

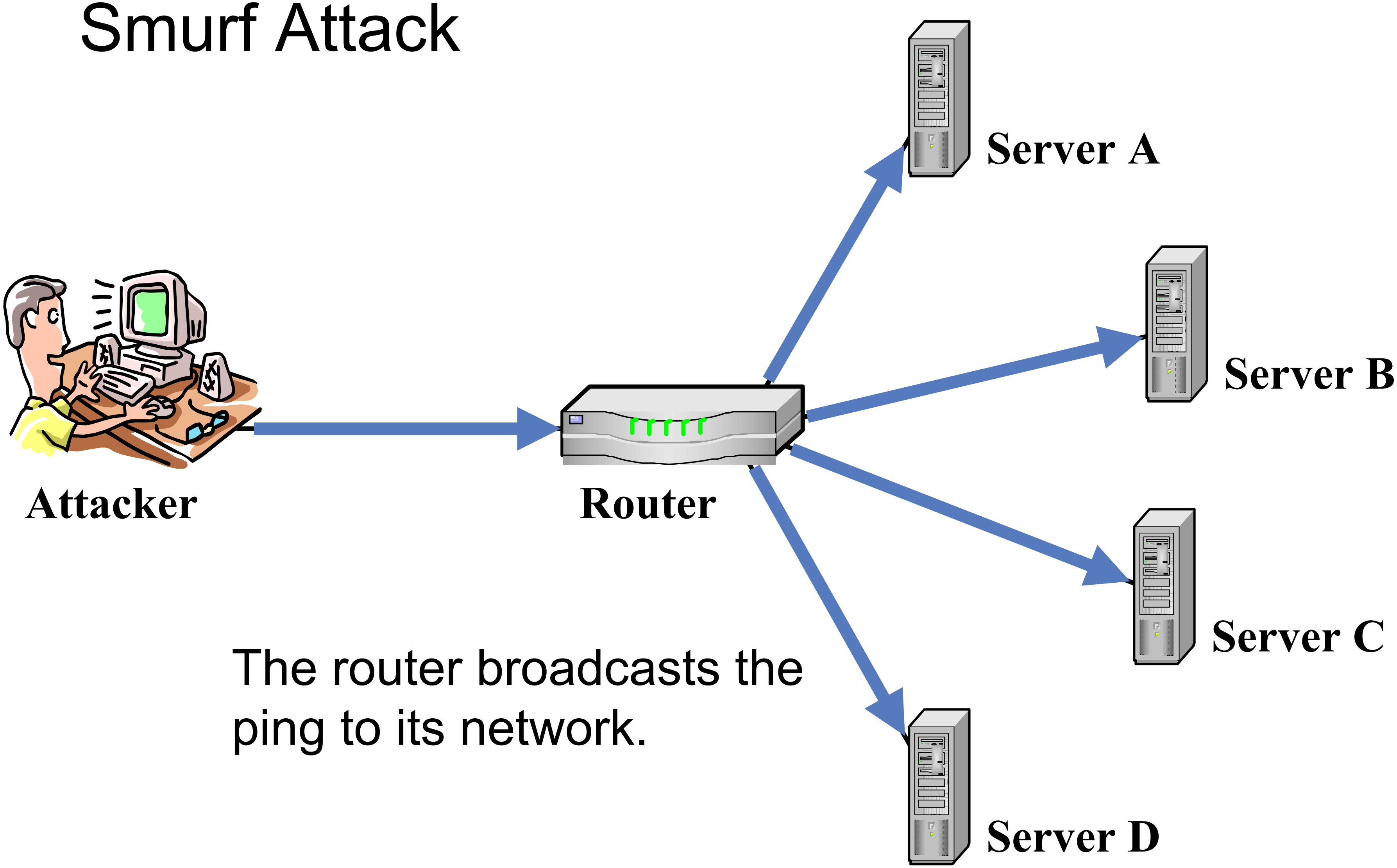
Smurf Attack

Attacker sends a ICMP ping to the broadcast address of a router.



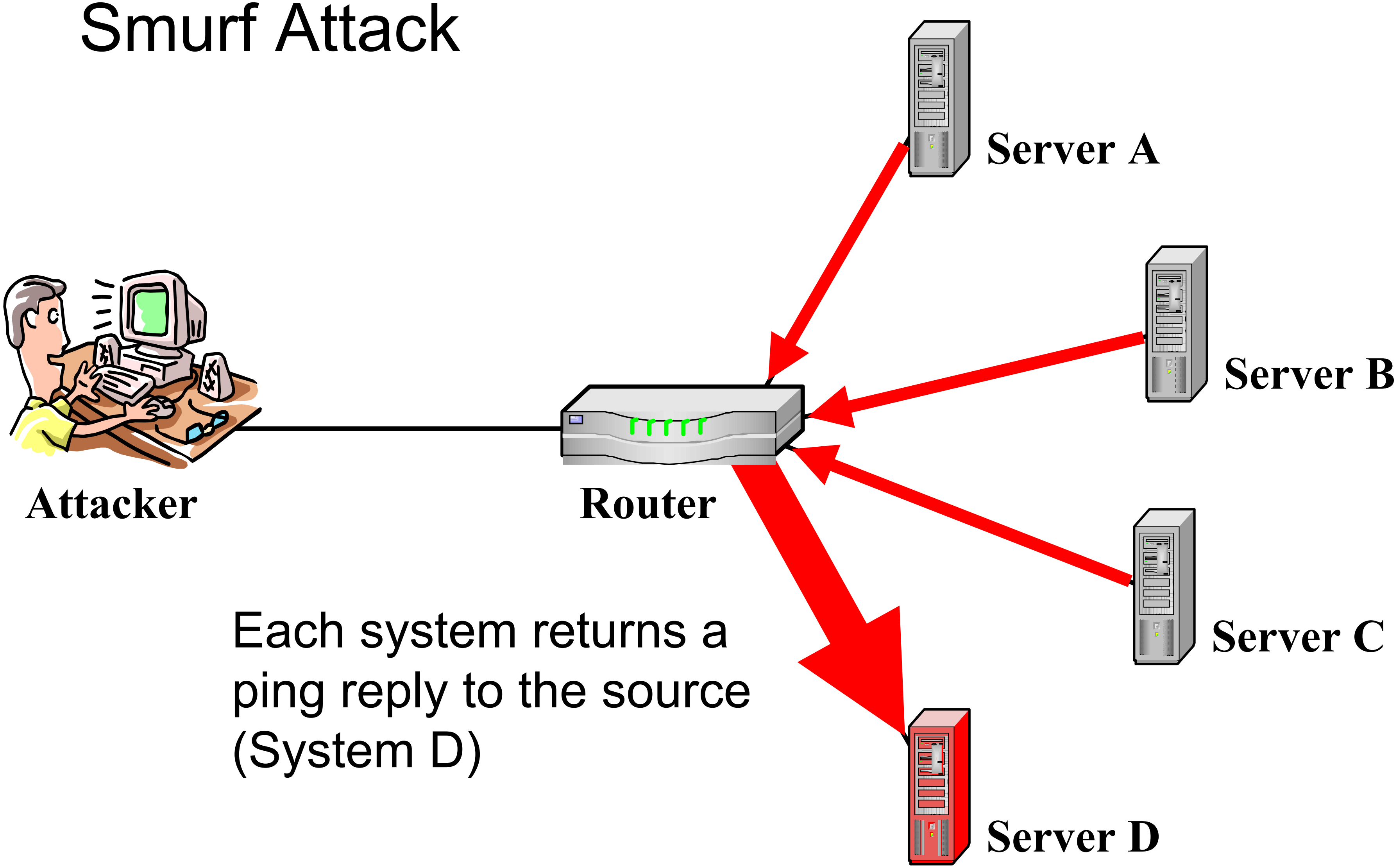
The source IP address is set (spoofed) to that of Server D.

Smurf Attack



The router broadcasts the ping to its network.

Smurf Attack

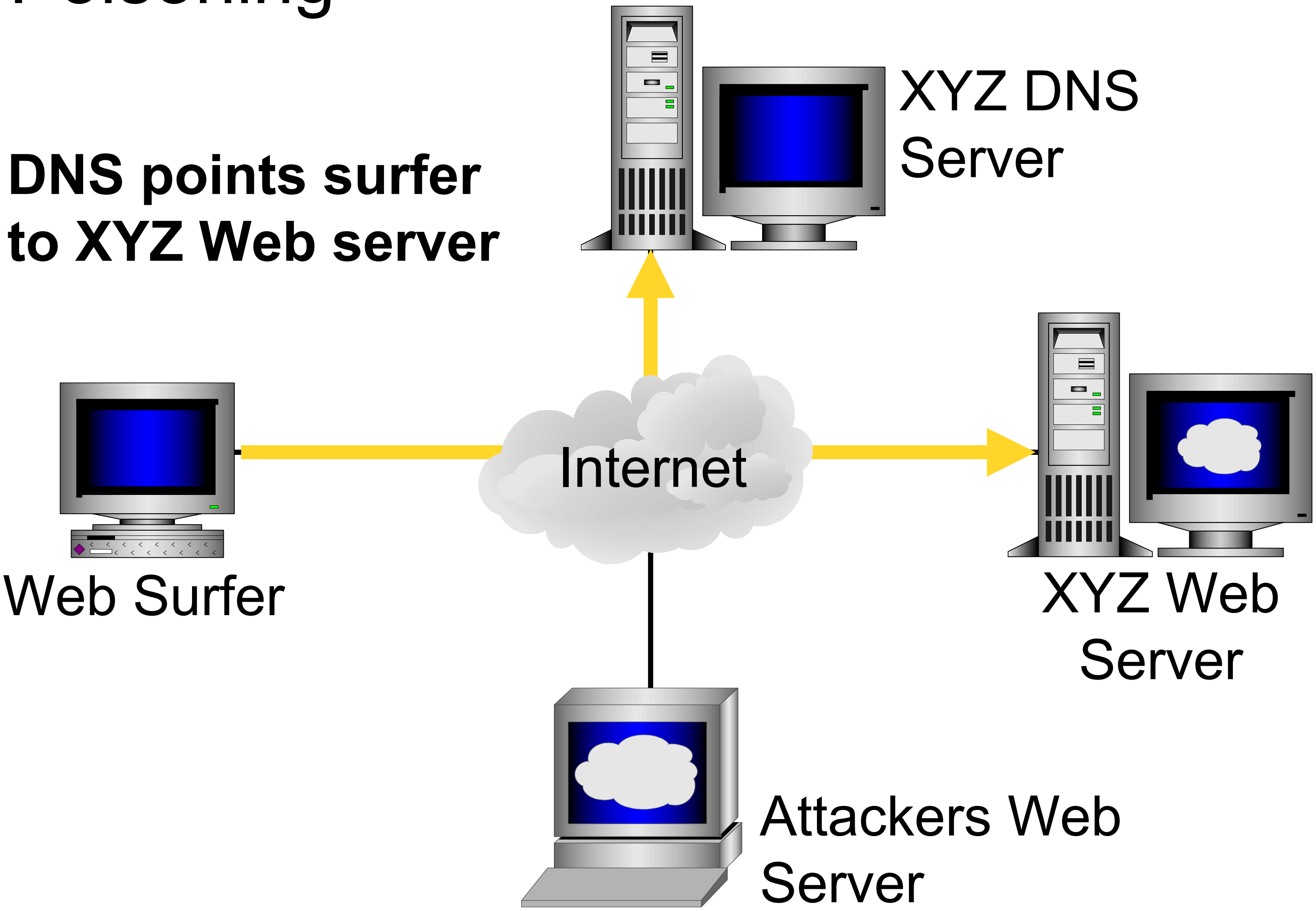


Each system returns a ping reply to the source (System D)

DNS Attacks (Domain Name Service)

- **DNS is used to equate a human readable system name to a numeric IP address**
  - My.Domain.Com = 12.208.5.23
  - Your.Domain.Com = 12.208.6.87
- **Program and design flaws have allowed the DNS server information to be poisoned with incorrect data**

DNS Poisoning



DNS points surfer to XYZ Web server

XYZ DNS Server

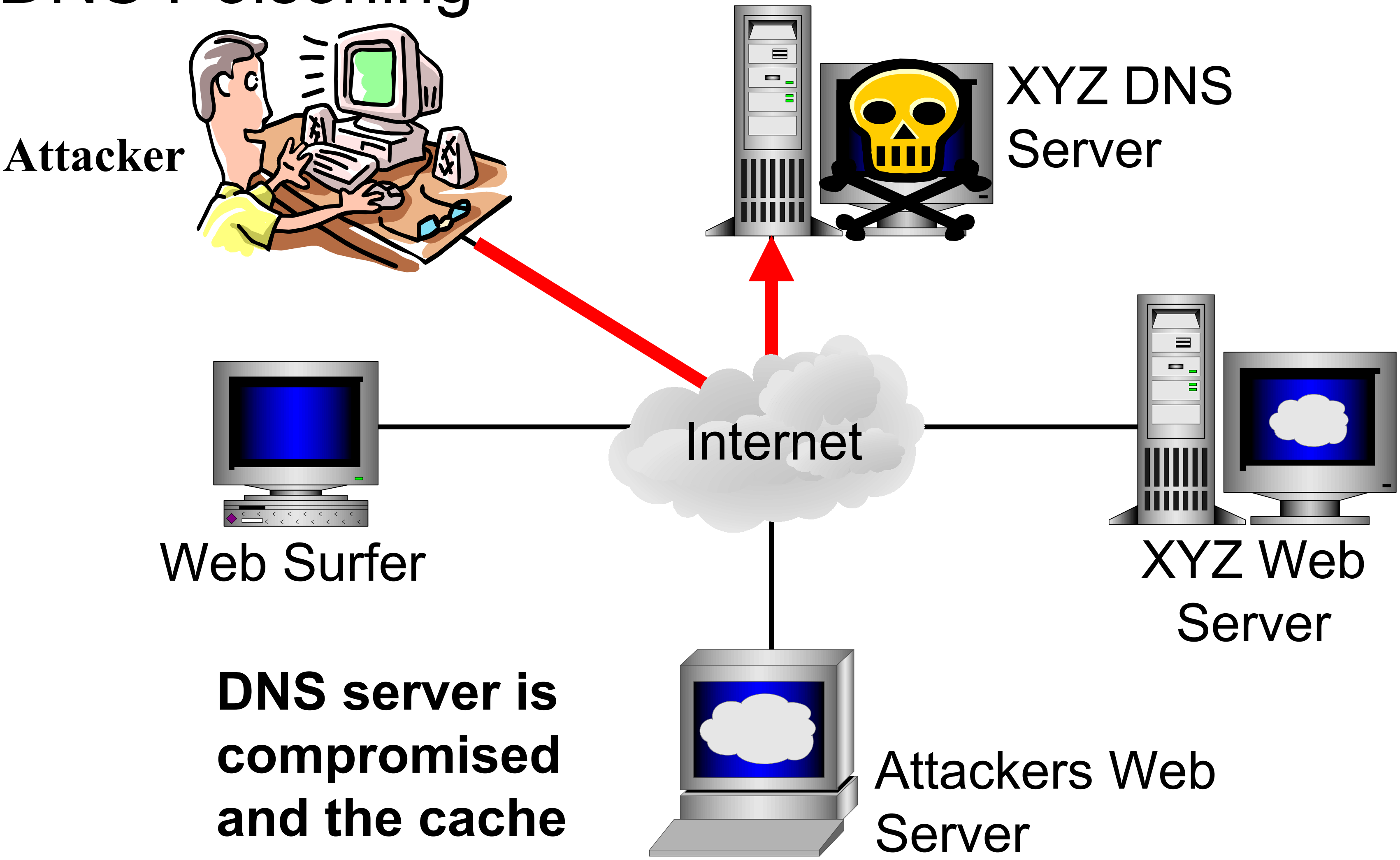
Internet

Web Surfer

XYZ Web Server

Attackers Web Server

DNS Poisoning



Attacker

XYZ DNS Server

Internet

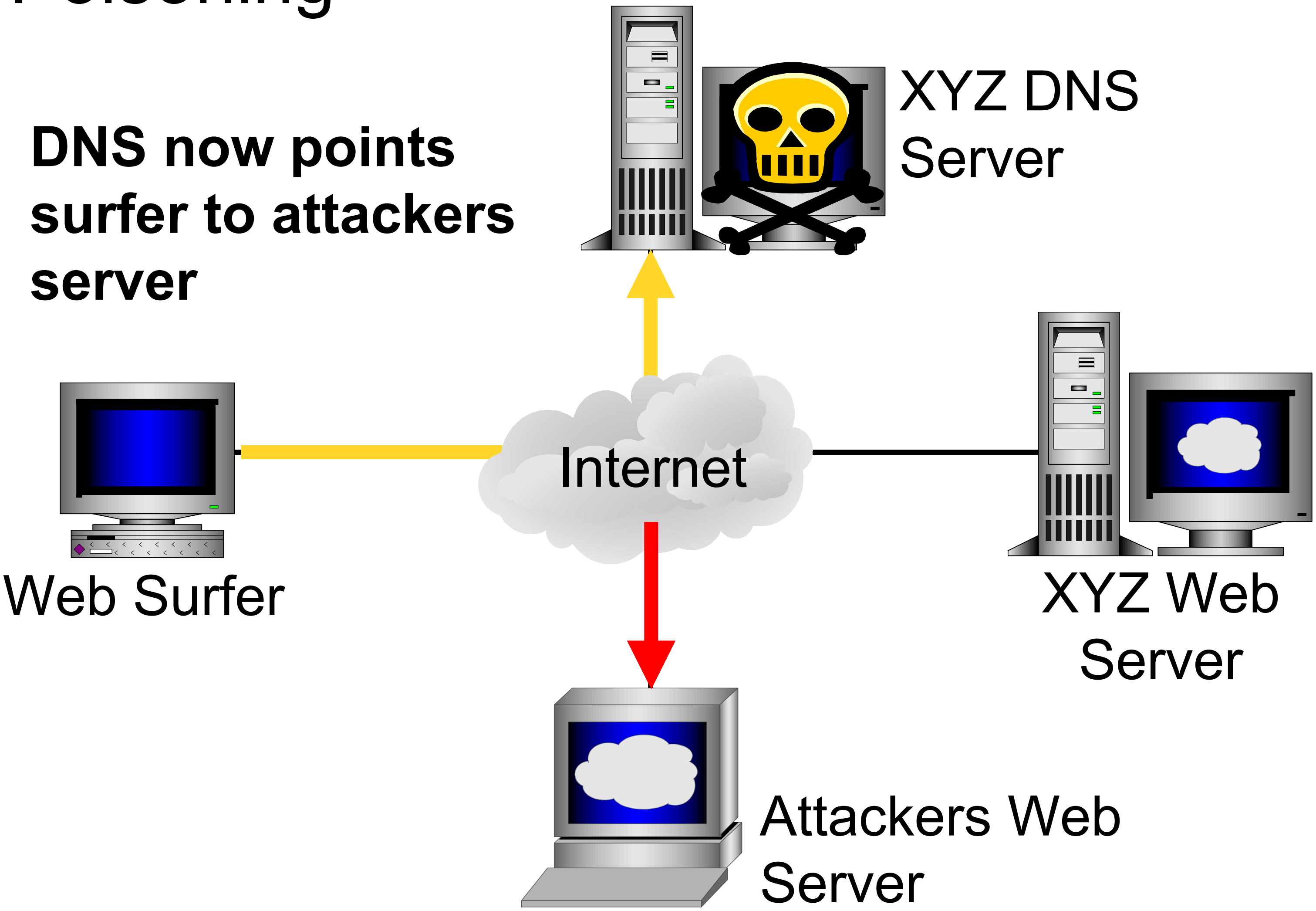
Web Surfer

XYZ Web Server

Attackers Web Server

DNS server is compromised and the cache poisoned

DNS Poisoning



DNS now points surfer to attackers server

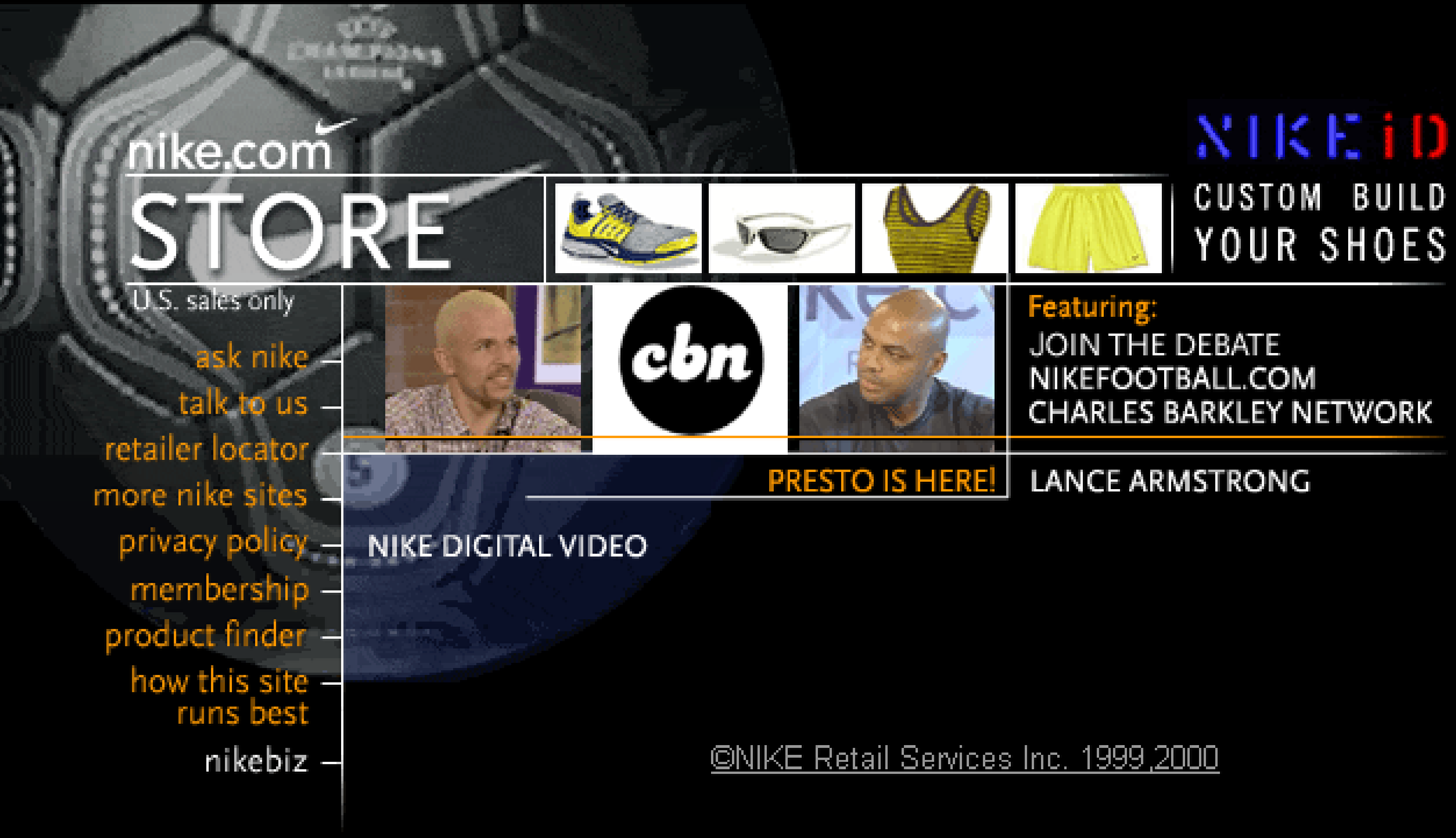
XYZ DNS Server

Internet

Web Surfer

XYZ Web Server

Attackers Web Server



nike.com

STORE

U.S. sales only

NIKE iD

CUSTOM BUILD YOUR SHOES

Featuring:

JOIN THE DEBATE

NIKEFOOTBALL.COM

CHARLES BARKLEY NETWORK

PRESTO IS HERE!

LANCE ARMSTRONG

NIKE DIGITAL VIDEO

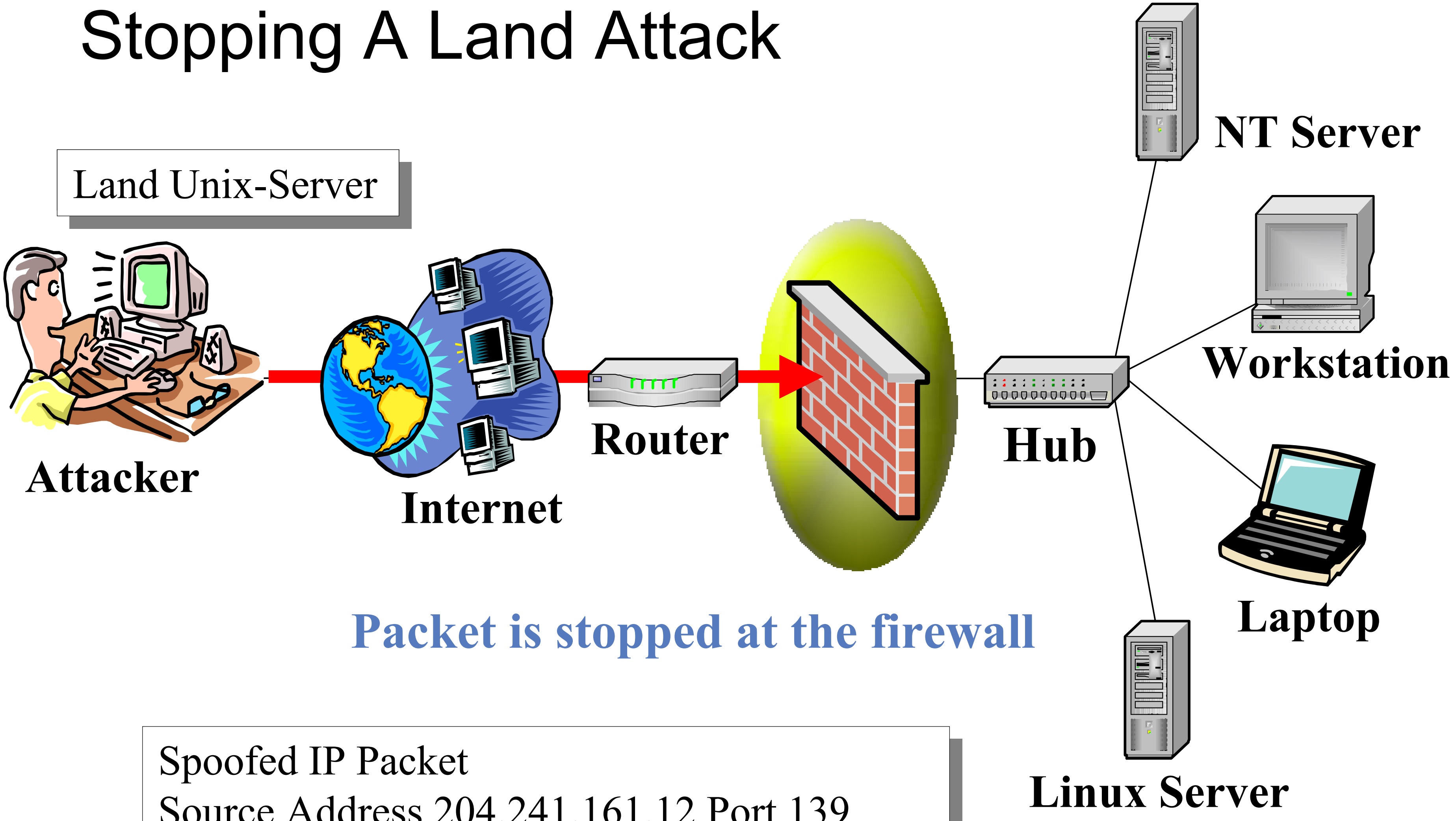
- ask nike
- talk to us
- retailer locator
- more nike sites
- privacy policy
- membership
- product finder
- how this site runs best
- nikebiz

featuring: unions greens ngos students you me workers artists
melbourne crown casino september 11-13
global justice
is coming - prepare now!
s-11
seattle + washington = melbourne
COUNTDOWN to the WEF shutdown : 9am september 11
enter site

80days 22hours 41mins 51secs

quick re-entry

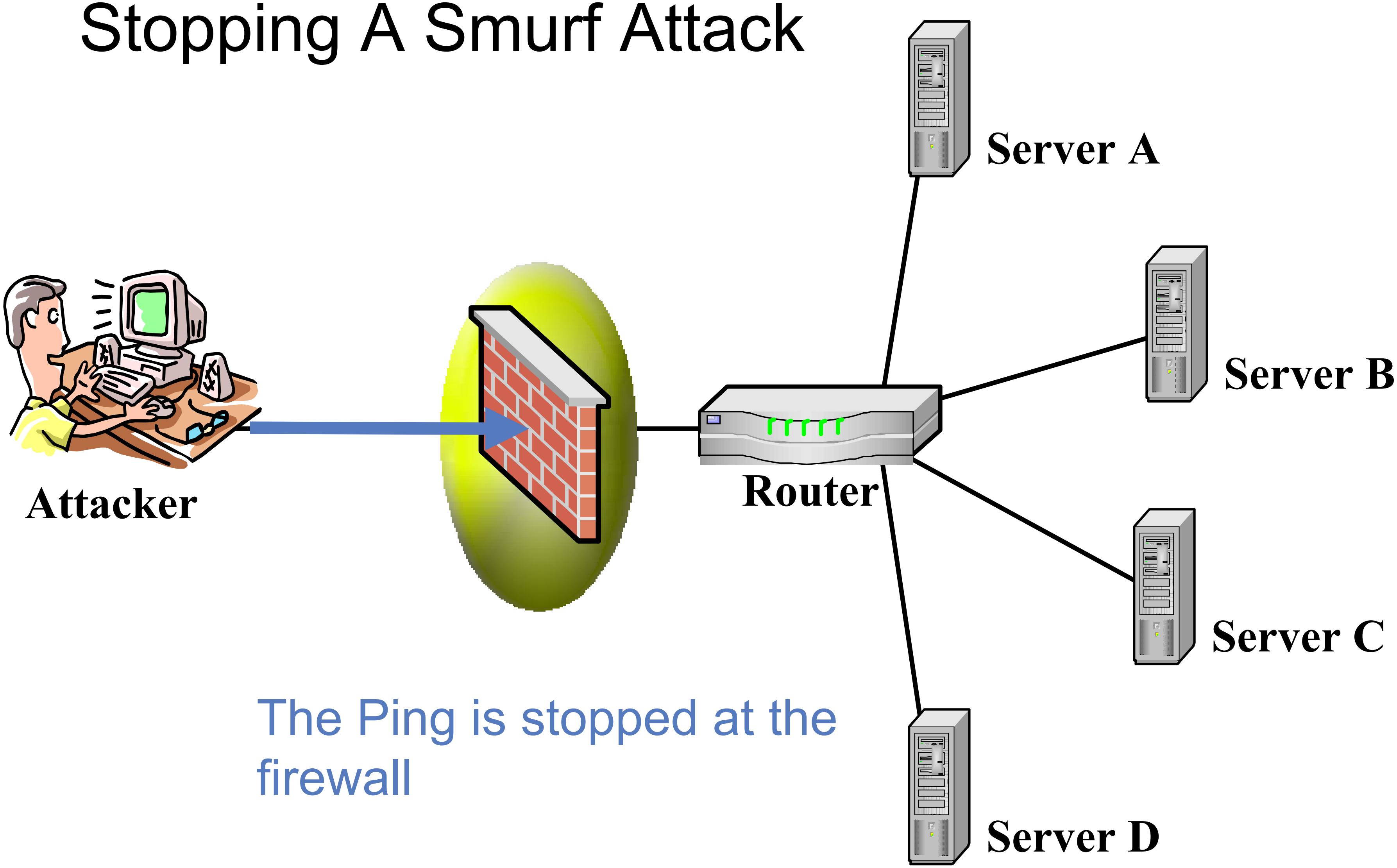
Stopping A Land Attack



Packet is stopped at the firewall

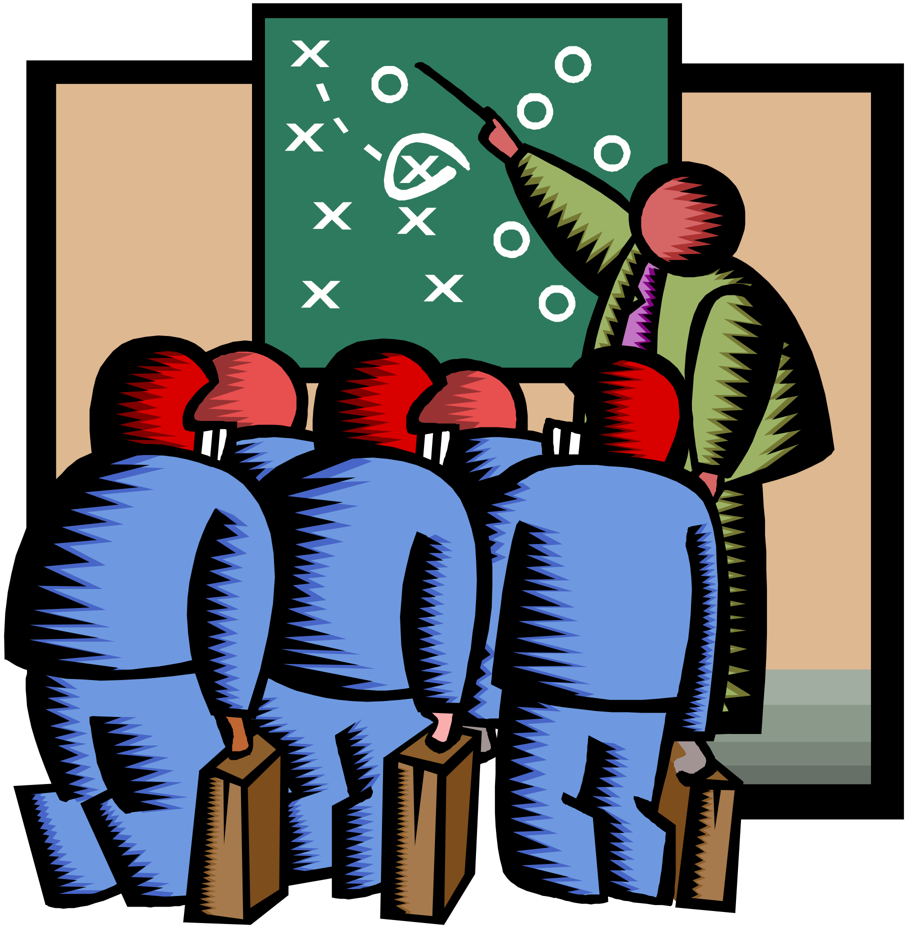
Spoofed IP Packet
Source Address 204.241.161.12 Port 139
Destination Address 204.241.161.12 Port 139
TCP Open

Stopping A Smurf Attack



The Ping is stopped at the firewall

II: Distributed Denial-of-Service



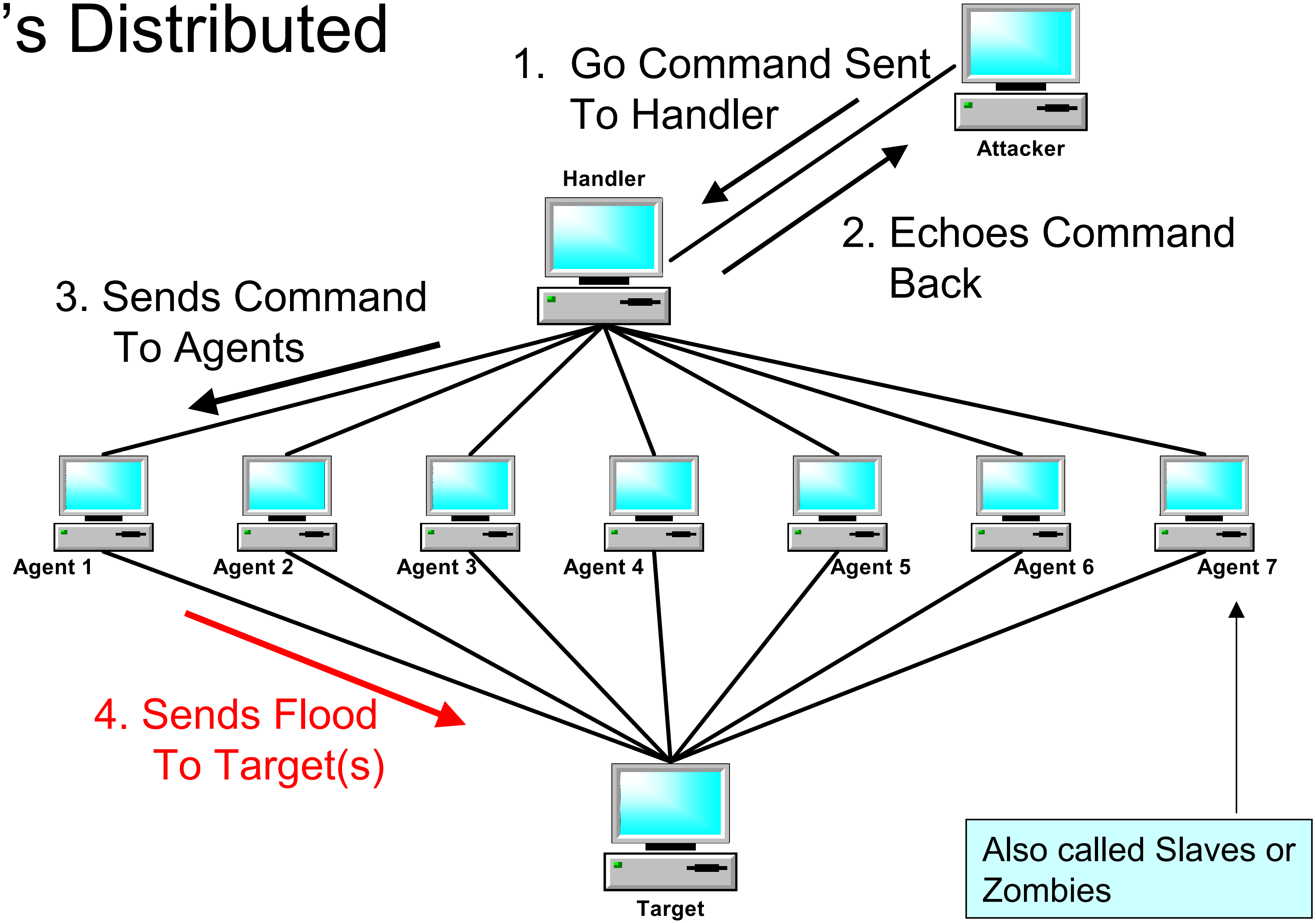
A Definition Found on the Internet

"A computer attack that hijacks dozens or sometimes hundreds of computers around the Internet and instructs each of them to inundate a target site with meaningless requests for data."

What Is It?

- **Represents a new level of attack**
- **Use of multiple, sometimes compromised systems, to launch attacks**
- **Type of attacks include:**
  - Denial-of-service (Trinoo, tribal flood network, …)
  - Password cracking (saltine cracker, Slurpie)
  - Information gathering (none available yet)

It’s Distributed



1. Go Command Sent To Handler

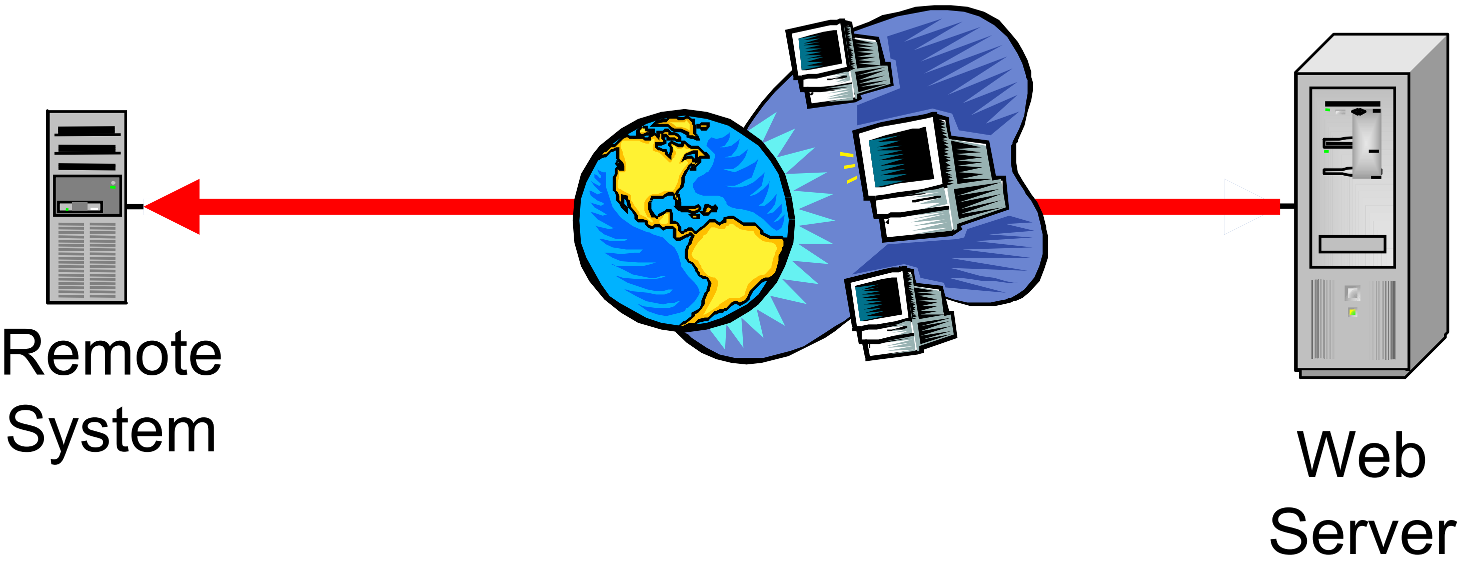
2. Echoes Command Back

3. Sends Command To Agents

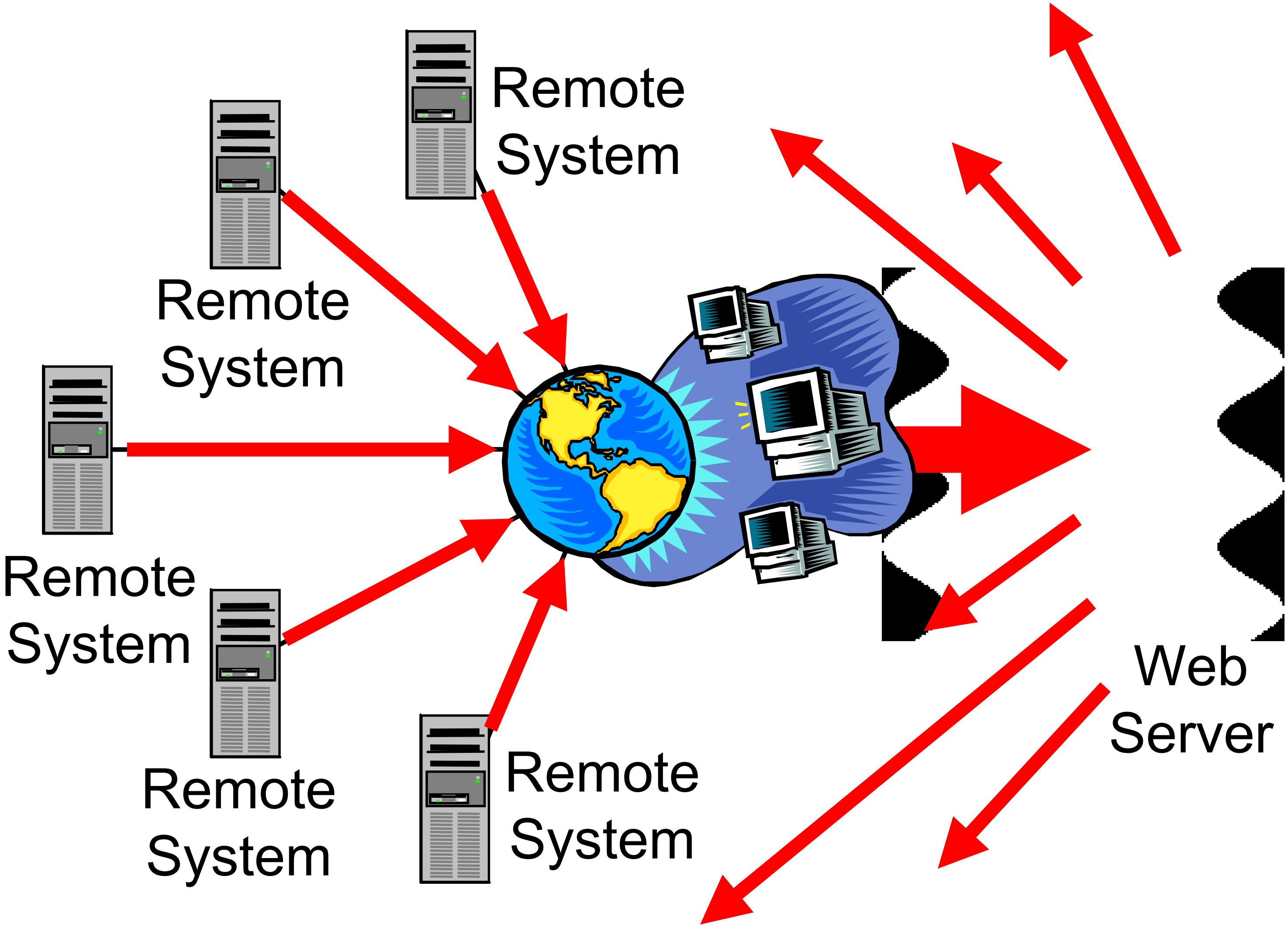
4. Sends Flood To Target(s)

Also called Slaves or Zombies

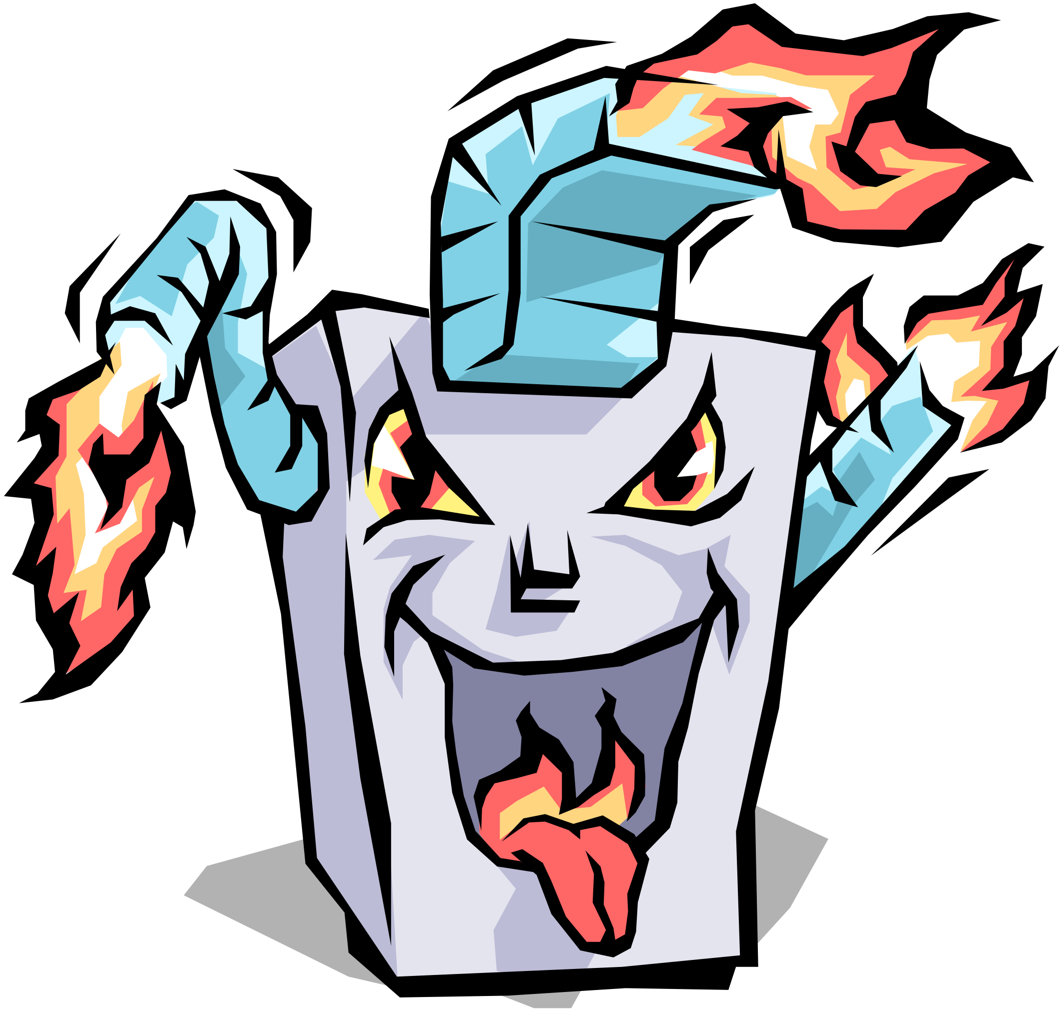
Simple ICMP (Ping)



ICMP (Ping) Flood



III: Trends and Factors



Development

- **Attack technologies are being developed in a open source environment and are evolving quickly**
  - Underground community providing quick feed back
  - New ideas and features discussed in group forums
  - Global development teams via the internet
  - The time between idea and deployment can outpace the system and security administrators (opening a window of opportunity for abuse)
  - As long as defensive strategies are defensive, this situation will continue
  - Solutions must be international in scope

Easy Deployment

- **There are tens of thousands (perhaps even millions) of computers with week security connected to the internet**
  - They make easy targets for attack
  - Attackers will compromise many of these systems
  - Backdoors, Trojan horses and/or Distributed Denial-of-Service clients (zombies) will be installed
  - These systems systems can then be combined to form attack networks
  - Availability of broadband internet connections in the home, schools, libraries, and other locations (likely without any implemented security measures) increases the problem

Vulnerabilities

- **Increasing complex software is being written**
  - New developers with little or no training in writing secure code
  - Many working in environments where time-to-market is more important that security
  - Testing time and QA has not always increased to match the code complexity
  - Complex software is being deployed in security-critical environments
  - The end user is at risk

Demand for Features

- **User demand for new features**
  - Industry response is often to put security last or even as an afterthought
  - Results in software that is increasingly subject to:
    - **Subversion**
    - **Computer viruses**
    - **Data theft**
    - **Other forms of abuse**

Internet Complexity

- **It is unlikely that changes to specific technologies will eliminate newly emerging problems due to the scope and variety of the internet**
  - Broad community action required
  - Point solutions only help dampen effects of attacks
  - Need robust solutions that may require concentrated effort and several years
  - Many issues are due to inadequacies and shortcomings in a design that is over 30 years old

Technical Talent

- **Technical talent is growing scarce**
  - The growth of the internet has out paced availability
  - The average level technical ability and knowledge has decreased of the past few years
  - People with little or no technical experience are being placed in system and network administrative positions (often right out of school)
  - Graduates have little real experience and there is little effort to improve this in the educational system

Finding the Attacker

- **International law and the complexity of attacks makes apprehension and prosecution of computer crime difficult or unlikely**
  - Attack systems me be located across the globe
  - Incriminating evidence may be unattainable
  - True identify of perpetrator may never be determined
  - The attack may not even be illegal in the country where the attacker lives
  - Some governments unwilling to aid other (enemy) in an investigation

IV: A History in the Making

The Internet Meltdown – February 7, 2000

- **Yahoo hit by first recorded denial-of-service attack.**
- **Many other high profile commercial sites where hit next over a three day period of time.**
- **During proceeding months many sites with high speed connections were broken into and infested with "zombies".**
- **Zombie systems waited until they received attack command.**
- **System owners were unaware of their participation.**
- **Broadcast amplification using "ICMP echo reply" intensified attack.**
- **Flood estimated at over 1 gigabit per second.**

The Internet Meltdown – February 7, 2000

- **The following Sites where attacked:**

Yahoo	10:20 a.m.	2/7/00 PST	3 hours
Buy.com	10:50 a.m.	2/8/00 PST	3 hours
eBay	3:20 p.m.	2/8/00 PST	90 minutes
CNN.com	4:00 p.m.	2/8/00 PST	110 minutes
Amazon.com	5:00 p.m.	2/8/00 PST	1 hour
ZDNet	6:45 a.m.	2/9/00 PST	3 hours
E*Trade	5:00 a.m.	2/9/00 PST	90 minutes

- **Many others sites rumored to have been attacked**

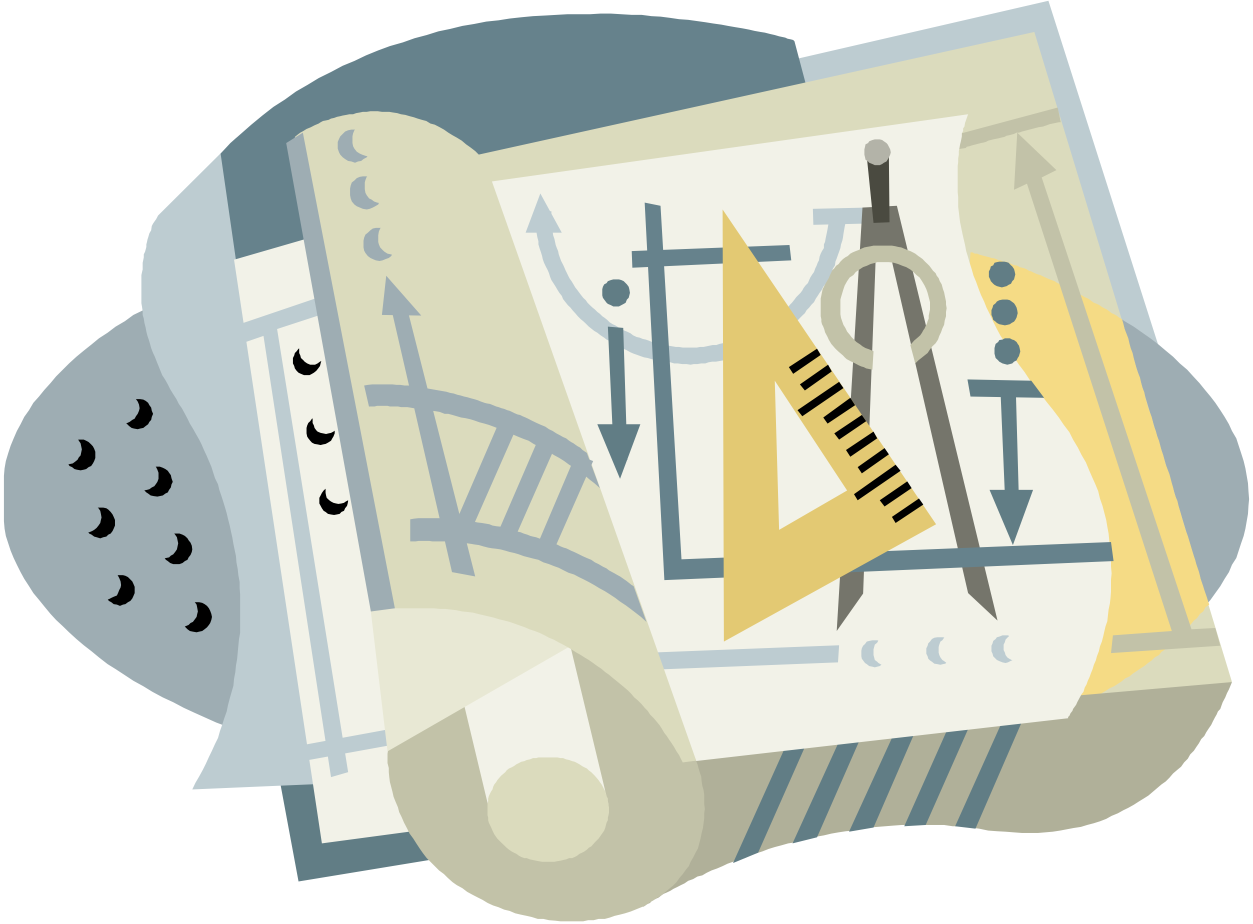
Why Should I Be Worried – February 2001

- **Microsoft (router glitch)**
- **IRC servers**
- **It has been estimated by at least one internet service provider that up to 10 percent of internet traffic on it's networks are from attackers attempting a denial of service attack (source ZDNet)**

Why Should I Be Worried – To The Present

- **Massive DDoS attack against all 13 root DNS servers – October 21, 2002**
    - 13 servers are distributed across the globe
    - Zombies traced to computers in United States and South Korea
    - Seven of the 13 servers failed to accept legitimate requests and 2 others failed intermittently during the attack
    - Largest attack to date
    - Work done to increase protection and robustness of servers
- **Latest threat from fast spreading worms that deliver and install zombie code**
    - Could possibly build DDoS network of gigantic size in under an hour
    - Zombie code may join IRC Channel and wait for instructions
    - Worm could contain target information – difficult to trace back to attacker
- **New attacks and methods are being created even as we speak**

V: Distributed Denial-of-Service Tools



Distributed Denial-of-Service Tools

- **These are some of the automated tools that attackers might use to simplify the task**
  - Mstream
  - Trin00
  - TFN/TFN2K– Tribe Flood Network
  - Trinity
  - Stacheldraht
  - Shaft
  - omegav3
- **Primary purpose is to inundate a web site or server with data, stopping the servers ability to respond to other request**

Distributed Denial-of-Service Tools

- **mstream**
  - TCP ACK Flood
- **Trin00**
  - No source IP spoofing
  - UDP Flood Attack
- **TFN/TFN2K– Tribe Flood Network**
  - Source IP randomization
  - UDP Flood Attack
  - TCP SYN Flood
  - ICMP Echo Request Flood
  - ICMP Directed Broadcast (smurf)

Distributed Denial-of-Service Tools

- **Stacheldraht**
  - Encrypted communications
  - Source IP randomization
  - UDP Flood Attack
  - TCP SYN Flood
  - ICMP Echo Request Flood
  - ICMP Directed Broadcast (smurf)
  - TCP ACK flood
  - TCP NULL (no flag) flood

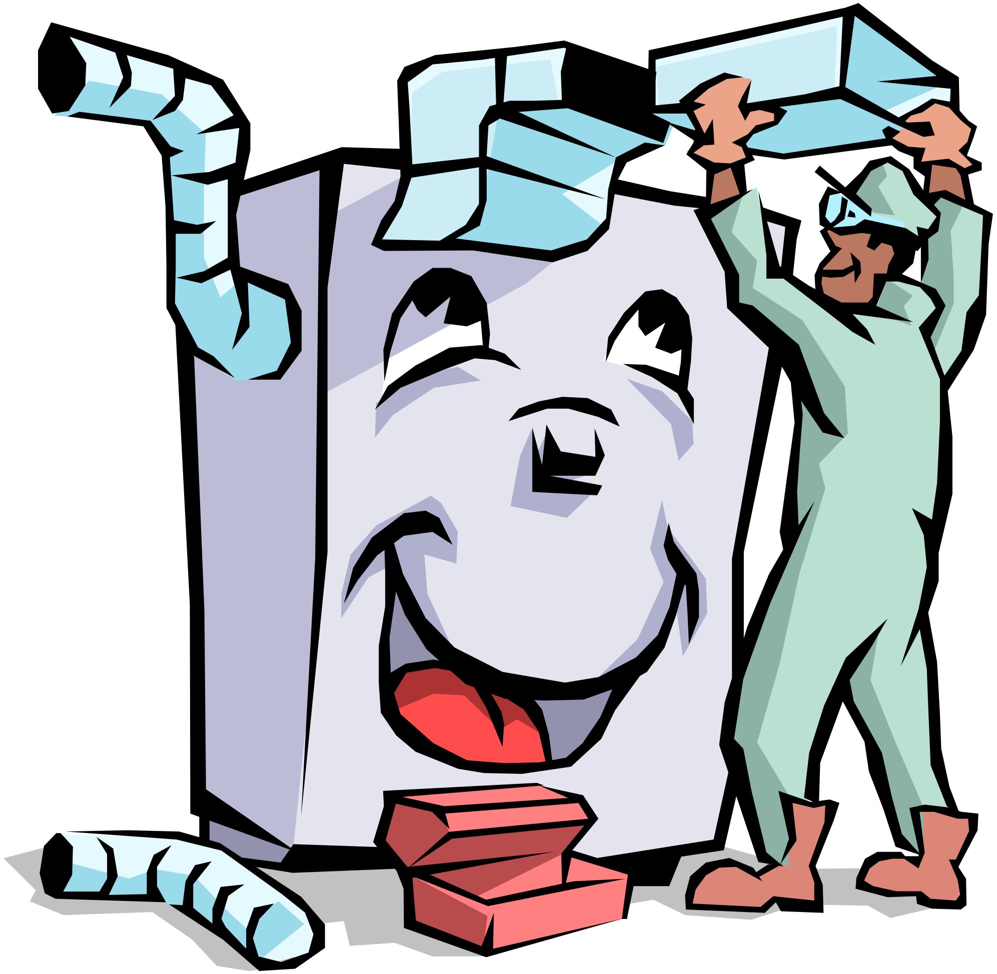
Distributed Denial-of-Service Tools

- **Shaft**
  - UDP flood
  - TCP SYN flood
  - ICMP Echo Flood
  - Can randomize all Three floods
- **Omegtav3**
  - TCP ACK flood
  - ICMP flood
  - IGMP flood
  - UDP flood

Distributed Denial-of-Service Tools

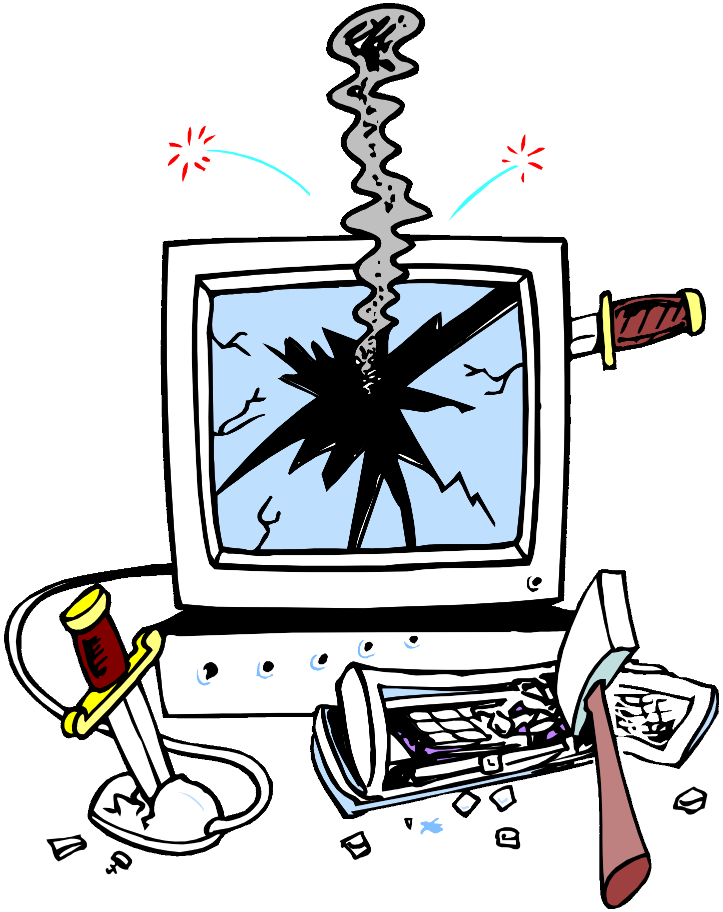
- **Trinity**
  - Can be controlled through IRC (Trinity connects to IRC and chooses a nickname)
  - UDP flood
  - Fragmented flood
  - TCP SYN flood
  - TCP RST flood
  - TCP Random Flag flood
  - TCP ACK flood
  - Establish flood

VI: Is There a Solution?



Indicators And Safeguards

- **Indications your system may have been compromised for the purpose of being used as a Distributed Denial-of-Service agent or handler**
    - Unknown open ports (the tools can change port numbers at compile time)
    - Startup scripts may have changed
    - Run “strings” on unknown binaries (see CERT advisories)
    - May have rootkit or back orifice install

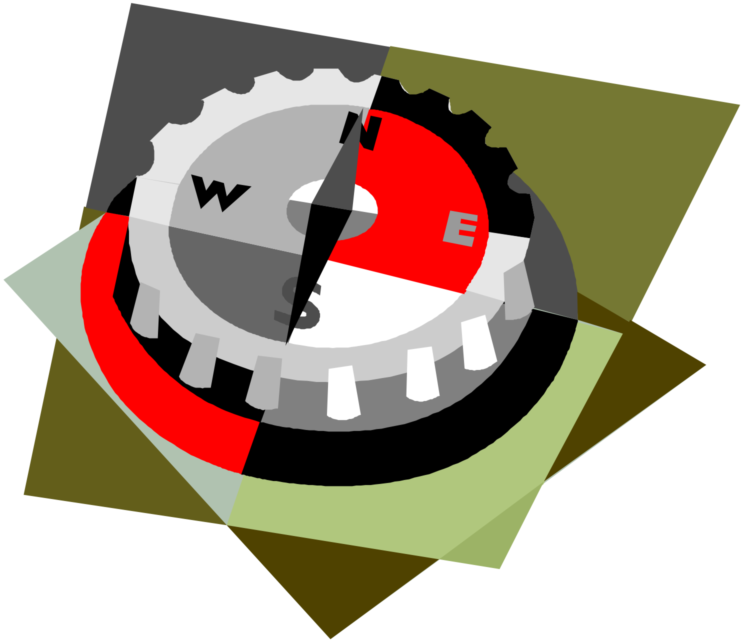


Offensive Problems

- **Source IP spoofing makes it very difficult to identify the attack system**
- **Broadcast amplification can increase attack intensity by magnitude greater**
- **Lack of appropriate response to attacks – many organizations will not respond to complaints of misuse**
- **Hundreds (possibly thousands) of attack systems intensify the issue – many with little or no security that where enlisted as zombies by the attacker**
- **Distributed Denial-of-Service attacks appear as normal network connection/control traffic – no way to identify it as an attack until its to late)**

IP Spoofing

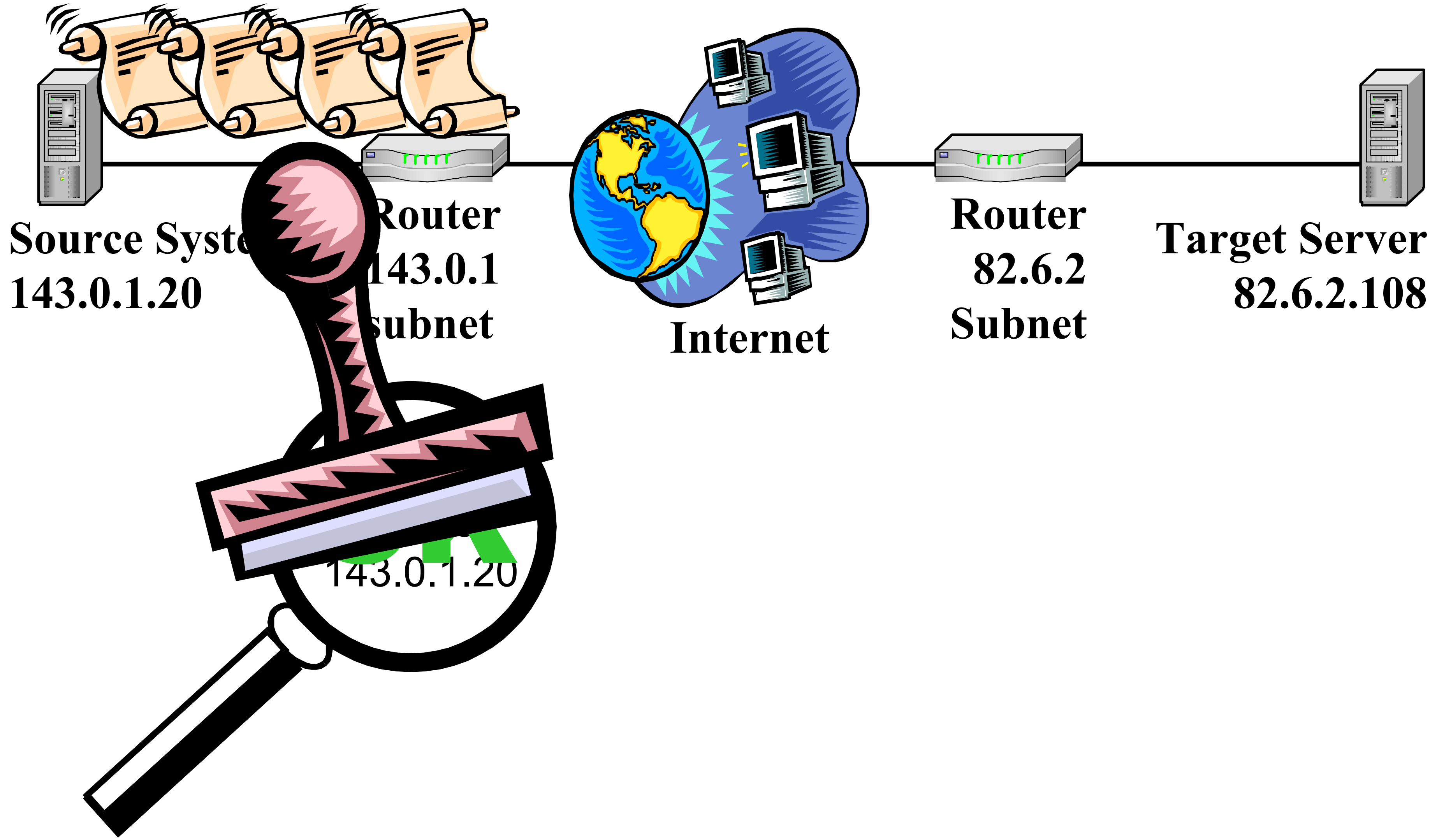
- **Egress filtering**
  - Insure that packets leaving a site contain a source IP address consistent with that site
  - Insure that no packets with unroutable packets are sent from the site
  - Limits IP spoofing to addresses within the site
  - Attack could be traced back to site (helps identify attack traffic source)
- **Ingress filtering**
  - ISPs only accept traffic from authorized sources



IP Spoofing

- **Dialup users**
  - Ensure that proper filters are in place to prevent dial-up connections from using spoofed addresses
  - Network equipment vendors should ensure that no-IP-spoofing is a user setting, and the default setting, on their dial-up equipment
- **itrace (an ICMP Traceback message) has bee proposed by the engineering task force to help solve problem of spoofed IP addresses**
  - Routers would generate a Traceback message that is sent along to the destination
  - With enough Traceback messages from enough routers along the path, the traffic source and path can be determined

Egress / Ingress Filtering



Source Syste
143.0.1.20

Router
143.0.1
subnet

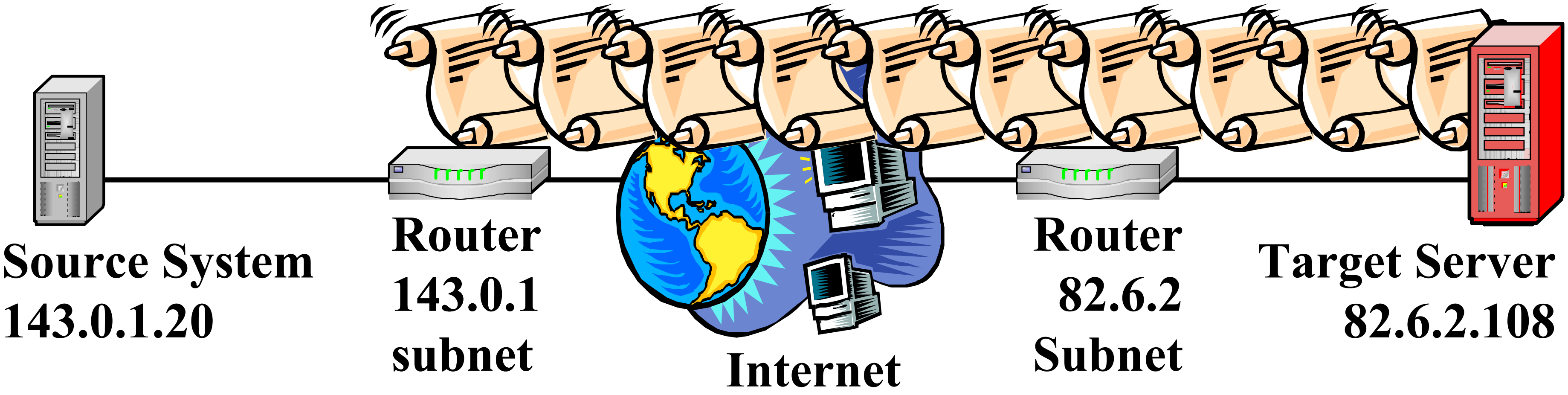
Internet

Router
82.6.2
Subnet

Target Server
82.6.2.108

143.0.1.20

Egress / Ingress Filtering



Source System
143.0.1.20

Router
143.0.1
subnet

Internet

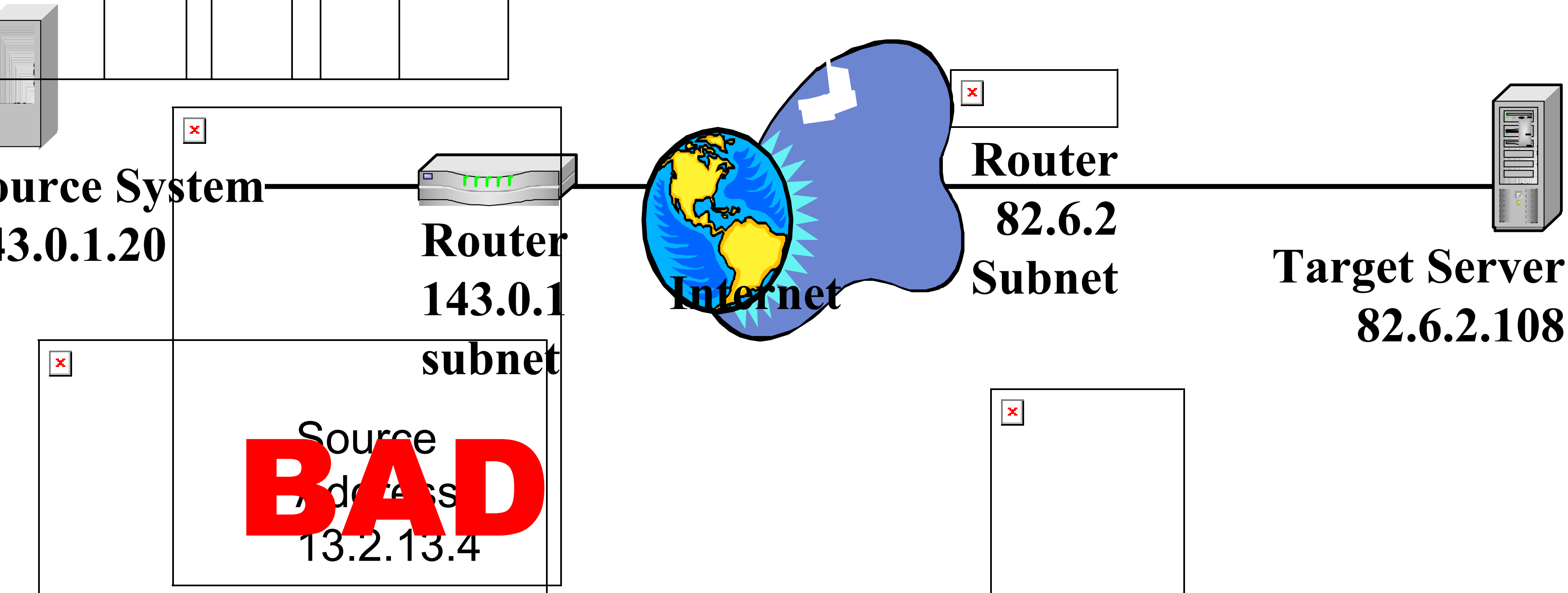
Router
82.6.2
Subnet

Target Server
82.6.2.108

Source Address
143.0.1.20

OK

Egress / Ingress Filtering



ource System
l3.0.1.20

Router
143.0.1
subnet

Internet

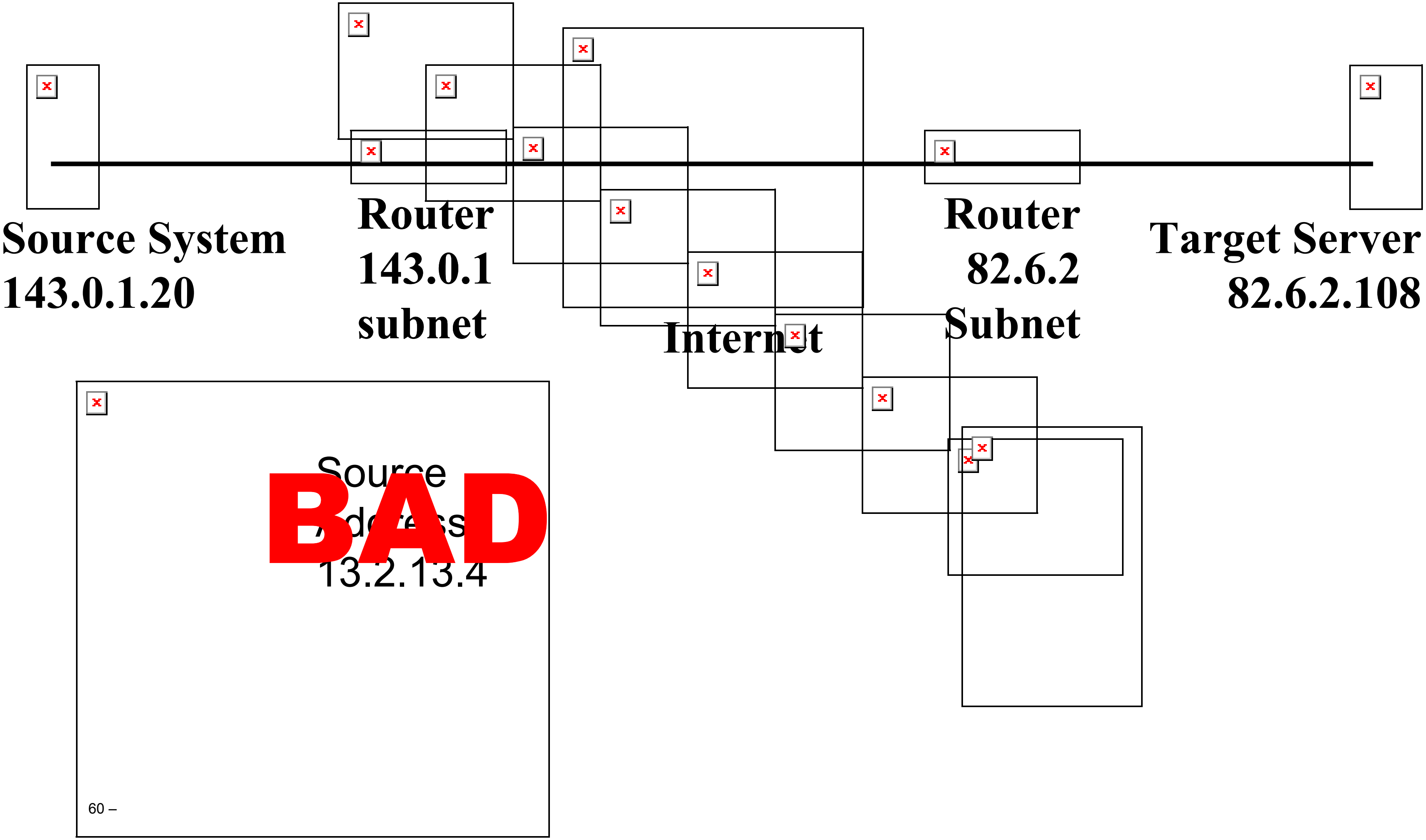
Router
82.6.2
Subnet

Target Server
82.6.2.108

Source
Address
13.2.13.4

BAD

Egress / Ingress Filtering



Source System
143.0.1.20

Router
143.0.1
subnet

Internet

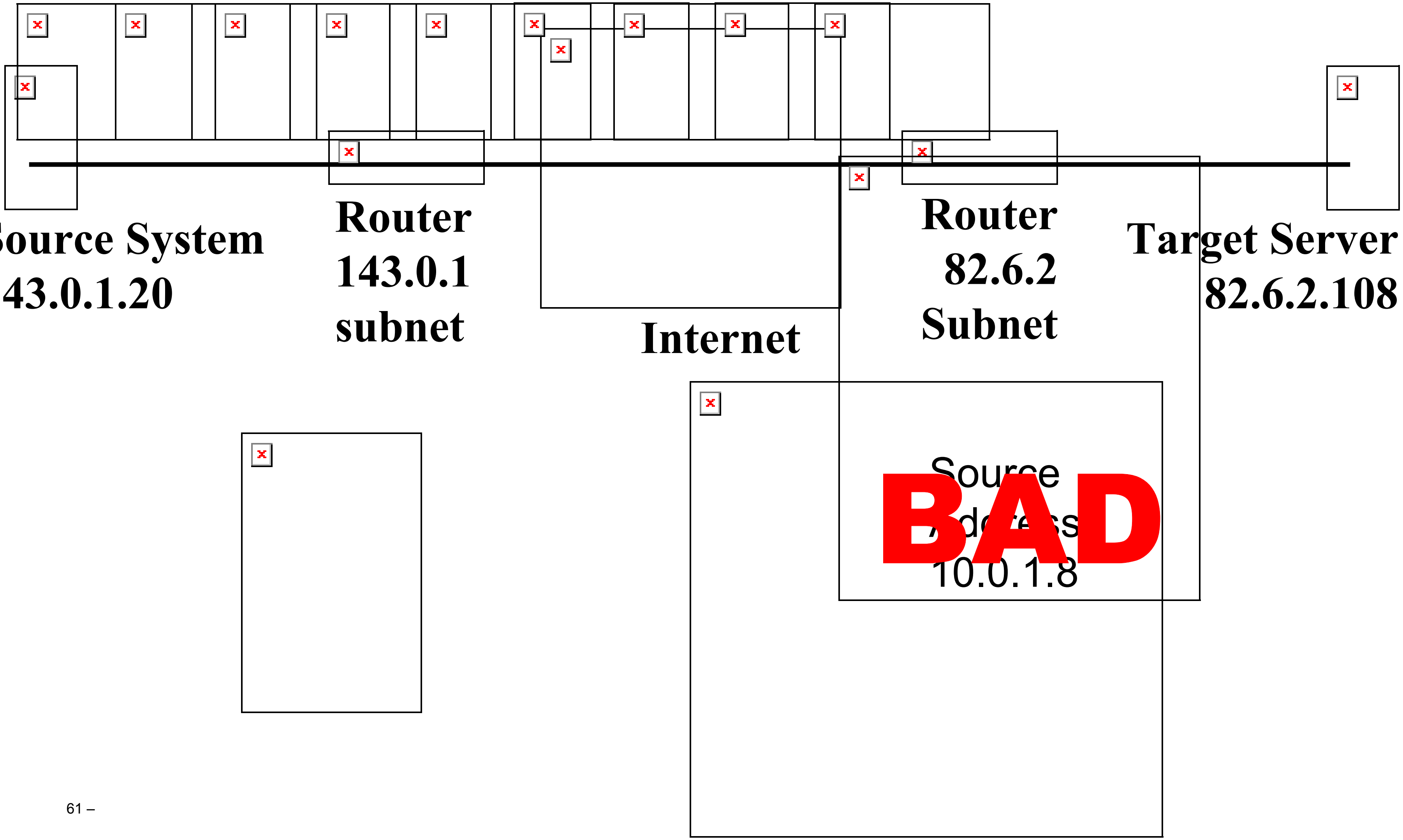
Router
82.6.2
Subnet

Target Server
82.6.2.108

Source
Address
13.2.13.4

BAD

Egress / Ingress Filtering



Source System
143.0.1.20

Router
143.0.1
subnet

Internet

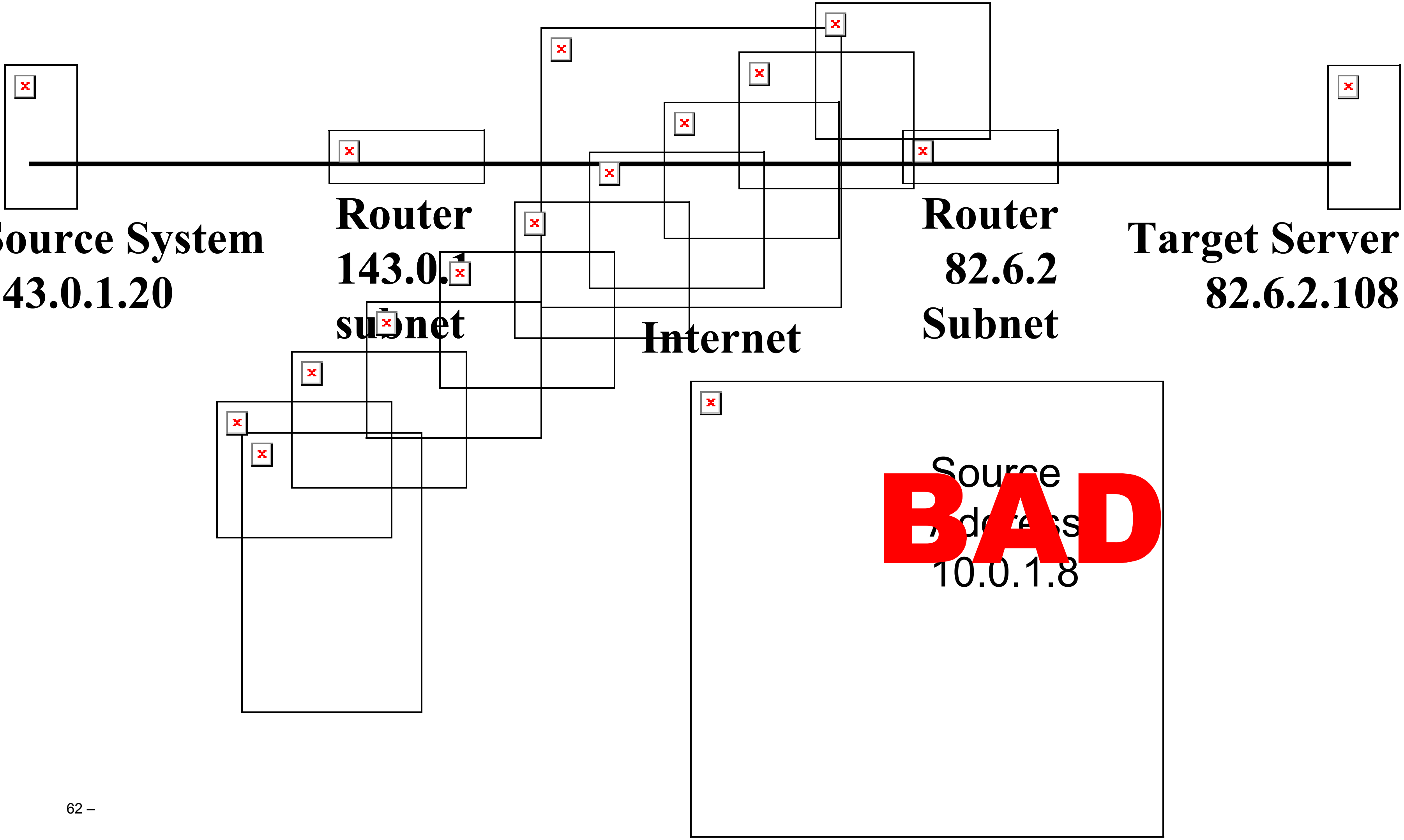
Router
82.6.2
Subnet

Target Server
82.6.2.108

Source
Address
10.0.1.8

BAD

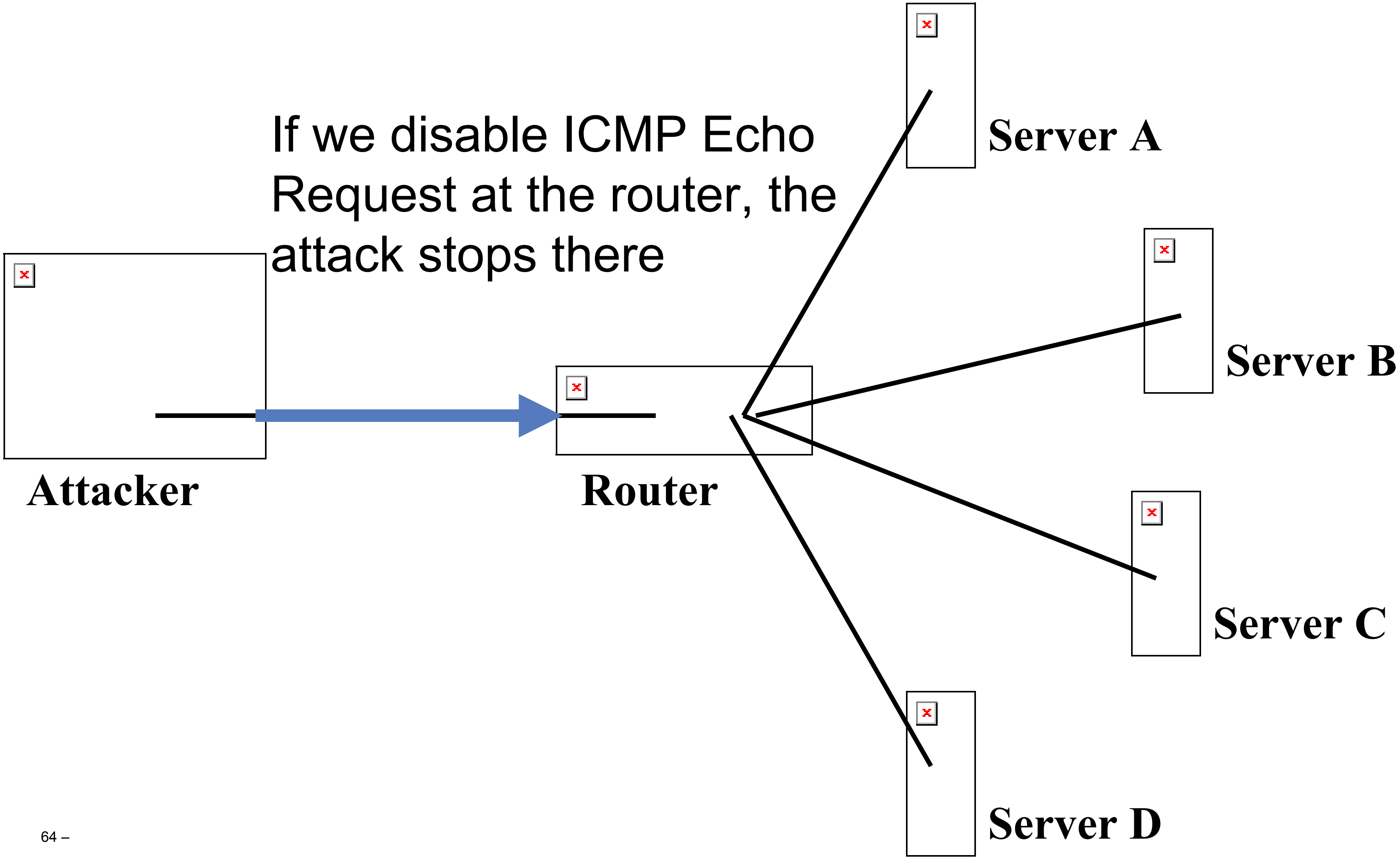
Egress / Ingress Filtering



Broadcast Amplification

- **Forwarding of directed broadcast traffic should be turned of unless there is a legitimate use**
  - If there is a legitimate use, disable all traffic to the broadcast address except those types that may be needed (e.g., ICMP Echo Reply) to protect against smurf attacks
- **Network hardware vendors should turn off IP directed broadcast packet (RFC 2644) and this should be the default.**
- **Chargen and echo services should be disabled**

Stopping Broadcast Amplification



If we disable ICMP Echo Request at the router, the attack stops there

Lack of Response to Attack

- A incident response policy should be written that clearly defines responsibilities and procedures
- ISPs should define methods of quick response and should be followed by staff
- Encourage participation in industry-wide early warning systems (ARIS at securifyfocus.com)
- Report attacks and system flaws to appropriate authorities

Unprotected Computers - Gateway

- Vulnerability and risk assessment
- Multiple ISP's (I.e. different providers using different pipes)
- Load balancing
- Redundancy or fail over in network devices and servers
- Install firewalls and harden with rule sets that tightly to limit traffic (incoming and outgoing) to required needs
- Use Network based Intrusion Detection

Unprotected Computers - Host

- **Vulnerability and risk assessment**
- **Use Host based Intrusion Detection**
- **Run minimum systems (no applications or services that are not needed)**
- **Keep your systems, applications and network devices updated to latest patch levels**
- **Check for Trojan horse and zombie code – don't allow your system(s) to be used as zombies in an attack against another site**
    - Network vulnerability scans
    - Tripwire/Anti Virus/Network and host based Intrusion Detection
- **Good password discipline**

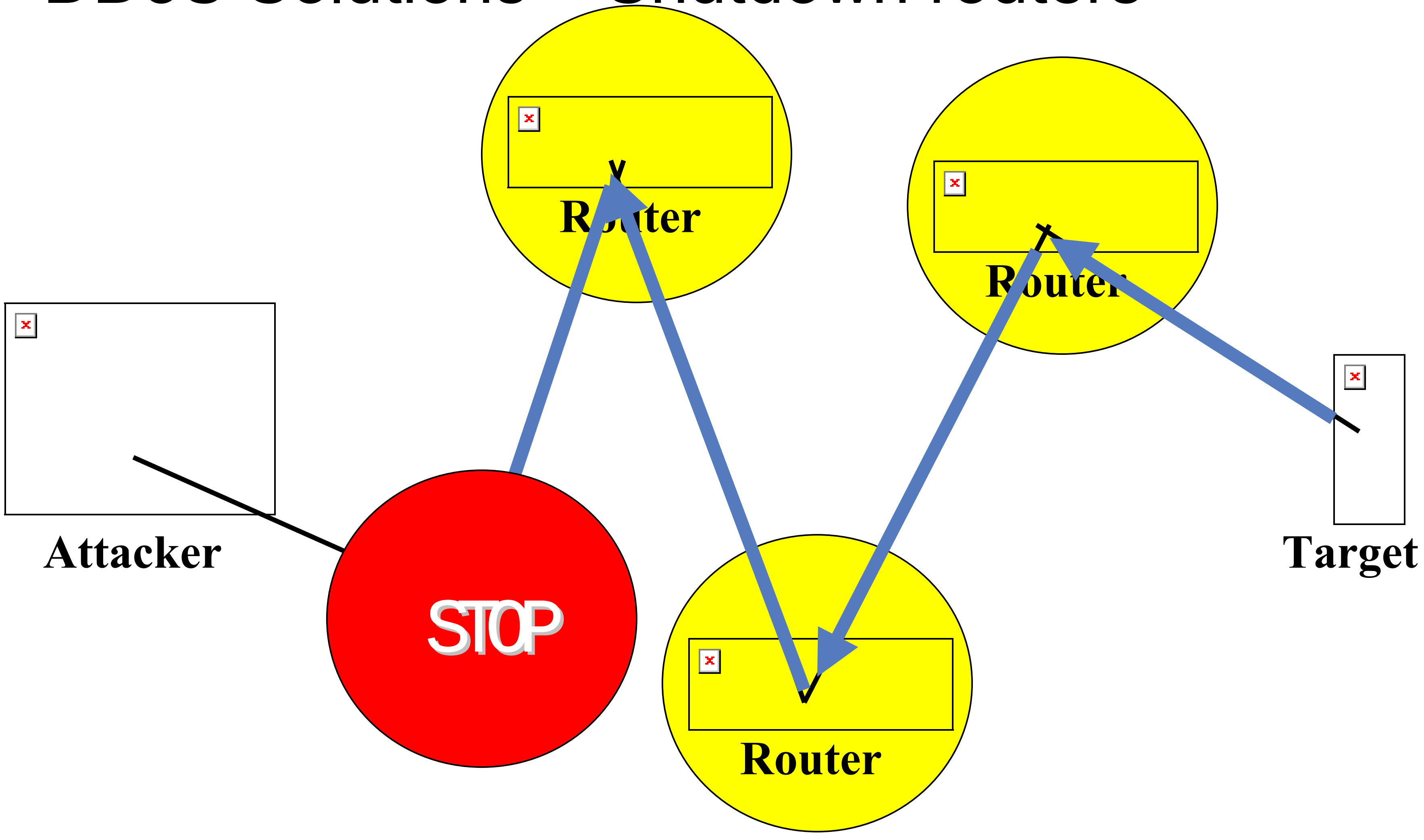
Unprotected Computers - Personnel

- Adopt a security policy
- Train IT staff on security issues
- Educate end users on system uses and security issues
- Participate in security community bug tracking discussions (BUGTRAQ, NTBUGTRAQ, …)
- Vendors need to incorporate system hardening controls to allow novice system administrators to obtain a reasonable level of security – security defaults should be set to highest levels by default

DDoS Solutions – Shutdown routers

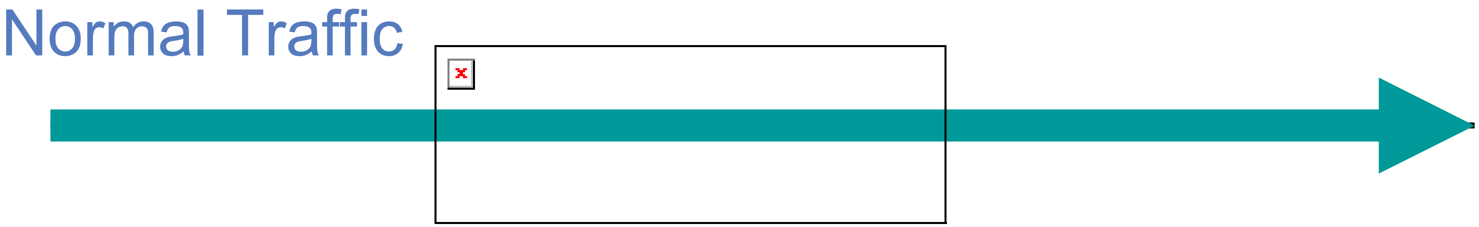
- **Identify Core router that attack is passing through to you boarder router**
- **Contact owner of Core router and provide them with the details of your attack**
- **They should then attempt to identify the router that is feeding that the attack is passing through to them**
- **They should then contact the owner of that router**
- **This process should continue down the line as far as possible**
- **The closer to the source of the attack the better**
- **The closes router to the source of the attack should be shutdown or configured to block traffic to your site**
- **Not all router owners will be cooperative or available (path may lead across multiple countries and continents**

DDoS Solutions – Shutdown routers



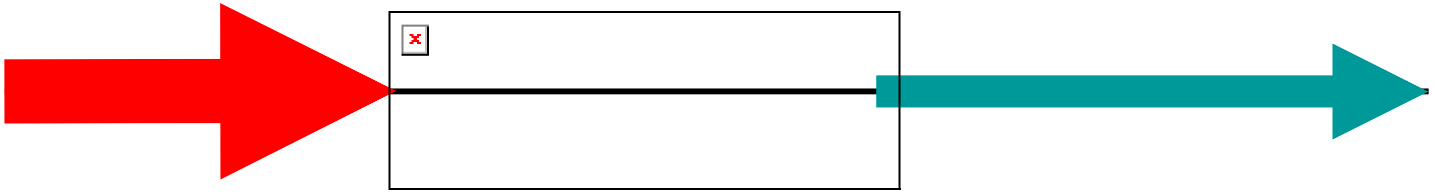
DDoS Solutions - Router Traffic Limits

- **Identify normal traffic for specific packet types (I.E. RST packets)**
- **Set traffic limit that limits traffic of that specific network packet type to a reasonable threshold**
- **This allows normal traffic to be routed without being impeded**
- **Prevents excessive amounts of specific network traffic from clogging your network**



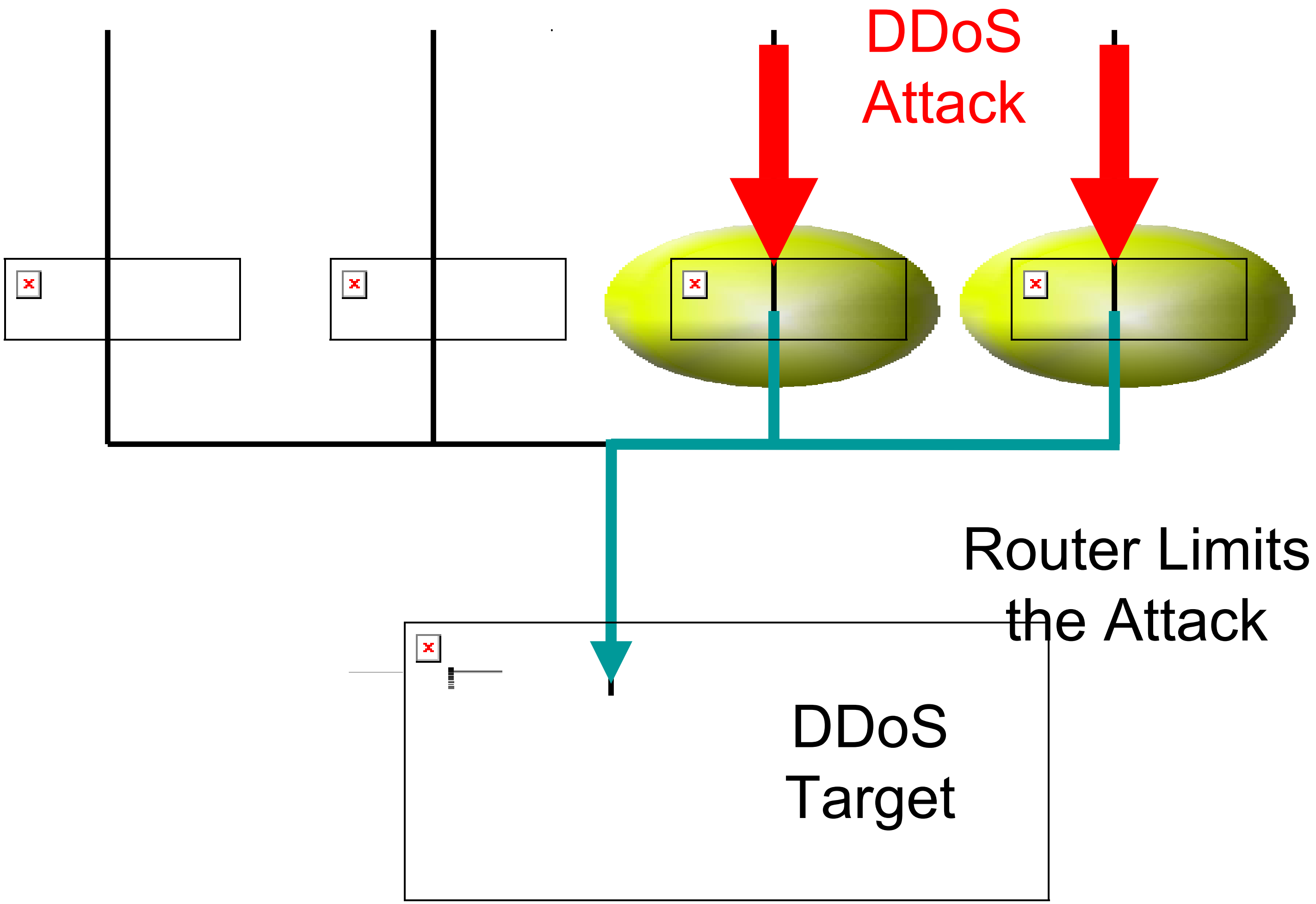
DDoS Solutions - Router Traffic Limits

- In the event of a DDoS flood (I.e. RST packets) the router threshold eliminates much of the attack traffic that would have chocked the target.
- Router thresholds are best placed as close as possible to the attack
- They should however be far enough back to catch a reasonable portion of the attack.
- You may need to use multiple router traffic limits to deal with a large scale DDoS attack



Flood Traffic is limited by router

DDoS Solutions - Router Traffic Limits



DDoS Attack

Router Limits the Attack

DDoS Target

DDoS Solutions – Add Resources

- **Add additional systems to server clusters**
- **Utilize second channel ISP**
- **Limited solution**
- **Requires before hand preparation**

VII: Where Can I Find More Information?

Where You Can Find More Information

- **Symantec Corporation**
  - http://www.symantec.com
- **Security Focus (Home of BUGTRAQ)**
  - http://www.securityfocus.com
- **Packet Storm**
  - http://www.packetstormsecurity.com
- **CVE (Common Vulnerability and Exposures)**
  - http://cve.mitre.org

Where You Can Find More Information

- **SANS Institute**
  - http://www.sans.org
- **The Center for Internet Security**
  - http://www.cisecurity.org
- **Linux Security**
  - http://www.linuxsecurity.com
- **Network Security Library**
  - http://secinf.net

VIII: Conclusion

Conclusion

- **Distributed Denial-of-Service attacks like these are publicly available**
- **They can simply be downloaded and installed**
- **They are very difficult to deal with when under attack**
  - They exploit unforeseen design flaws in the way the Internet works
- **We have to understand the technical aspects to combat the threat**
- **We need our own tools to fight back**

IX: Questions?