Chapter 9
Phase 3: Denial-of-Service Attacks

ATTACK IS LAUNCHED...	STOPPING SERVICES	EXHAUSTING RESOURCES
LOCALLY	• Process killing • System reconfiguring • Process crashing	• Forking processes to fill the process table • Filling up the whole file system
REMOTELY (across the network)	• Malformed packet attacks (e.g., Land, Teardrop, etc.)	• Packet floods, (e.g., SYN Flood, Smurf, Distributed Denial of Service)

Fig 9.1 Denial-of-Service attack categories

Stopping Local Services

- Process killing (eg. inetd, httpd, named, sendmail)
- System reconfiguration (eg. Stop file sharing)
- Process crashing (eg. Stack-based buffer overflow)
- Logic bomb

Defenses against Locally Stopping Services

- Keep systems patched
- Principle of Least Privilege applied to user accounts
- Run integrity-checking programs (eg.Tripwire)

Locally Exhausting Resources

- Filling up the process table
  - Achieved by forking recursively
  - Prevents other users from running new processes
- Filling up the file system
  - By continuously writing lots of data to file system
  - Prevents other users from writing to files
  - May causing system to crash
- Sending outbound traffic that fills up the network link
  - By running a program that constantly sends bogus network traffic
  - Consumes cpu cycles and network bandwidth

Defenses against Locally Exhausting Resources

- Apply Principle of Least Privileges when creating and maintaining user accounts
- Run system monitoring tools
  - Eg. Big Brother

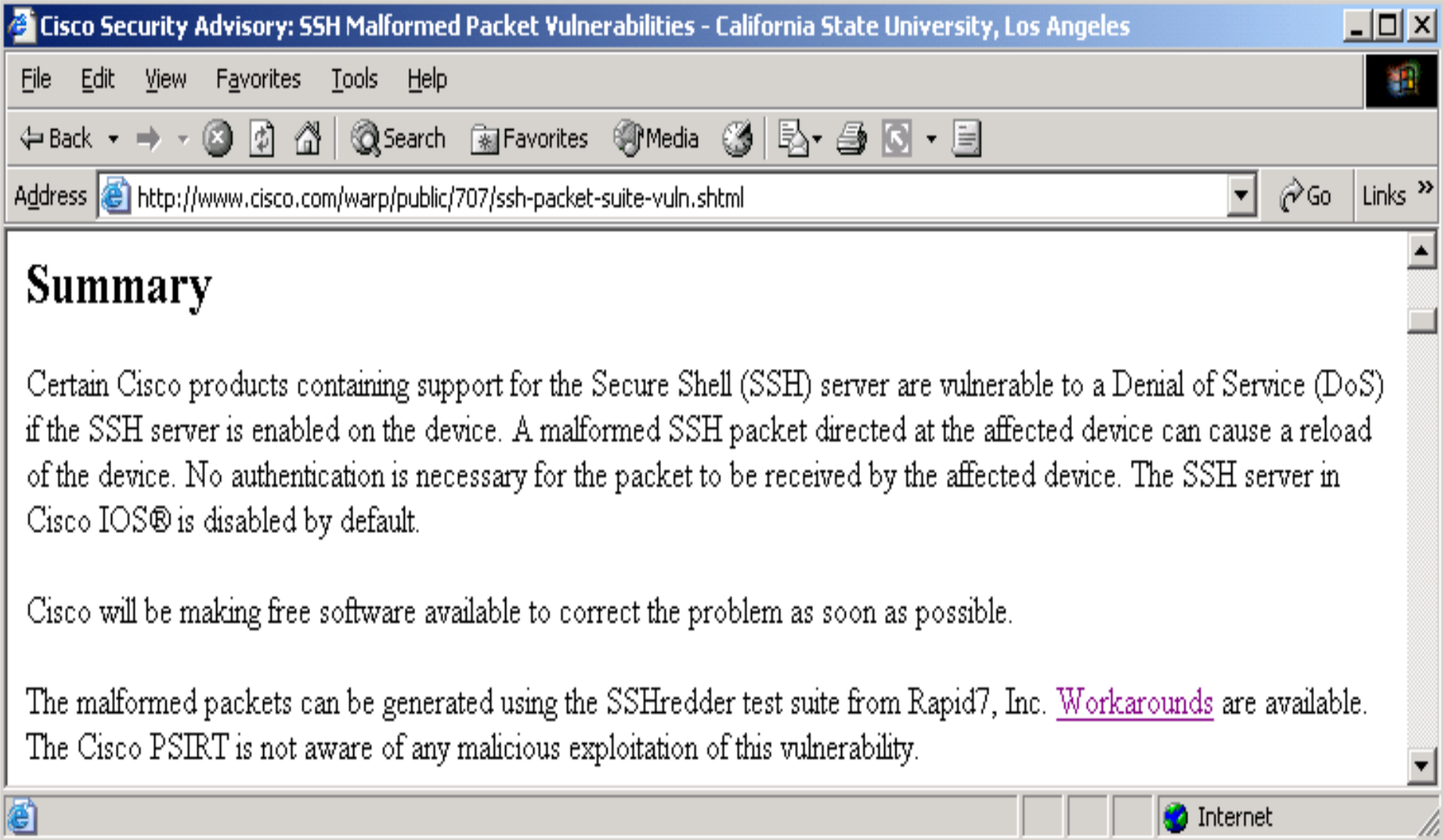
Remotely Stopping Services via Malformed Packet DOS Attacks

- Land attack
  - Sends a spoofed packet to target where source IP and port numbers are same as target IP and port numbers, causing network services of vulnerable target to die
- Latierra attack
  - Sends multiple Land attack packets to multiple ports
- Ping of Death
  - Sends an oversized (> 65 kB) ping packet which causes network TCP/IP stack of vulnerable machines to stop working.
- Jolt2 attack
  - Sends continuous stream of packet fragments, none of which have a fragment offset of zero.
  - Target machine's CPU cycle spent on packet reassembly

Remotely Stopping Services via Malformed Packet DOS Attacks(cont.)

- Teardrop, Newtear, Bonk, Syndrop
  - Sends overlapping IP packet fragments, causing TCP/IP stacks of vulnerable machines to crash
- Winnuke
  - Sends garbage data to an open file sharing port (TCP port 139) on a Windows machine, causing the vulnerable machine to crash since data does not conform to SMB protocol
- Targa http://packetstorm/security.com/Dos/
  - Contains a suite of malformed packet DOS attacks
- ARP spoofing to poison router's ARP cache using DSniff

SSH Malformed Packet Vulnerability on Cisco IOS



Defenses against Remote Stopping Services

- Apply system patches to fix vulnerable TCP/IP stacks and services
- Install anti-spoof filters on routers to thwart Land attacks
- Use static ARP tables to thwart ARP spoofing

Denial-of-Service Attacks that Remotely Exhaust Resources

- SYN Flood
- Smurf Attacks
- Distributed Denial-of-Service Attacks

SYN Flood

- Attacker sends continuous stream of SYN packets to target
- Target allocates memory on its connection queue to keep track of half-open connections
- Attacker does not complete 3-way handshake, filling up all slots on connection queue of target machine
- If target machine has a very large connection queue, attacker can alternatively send sufficient amount of SYN packets to consume target machine’s entire network bandwidth

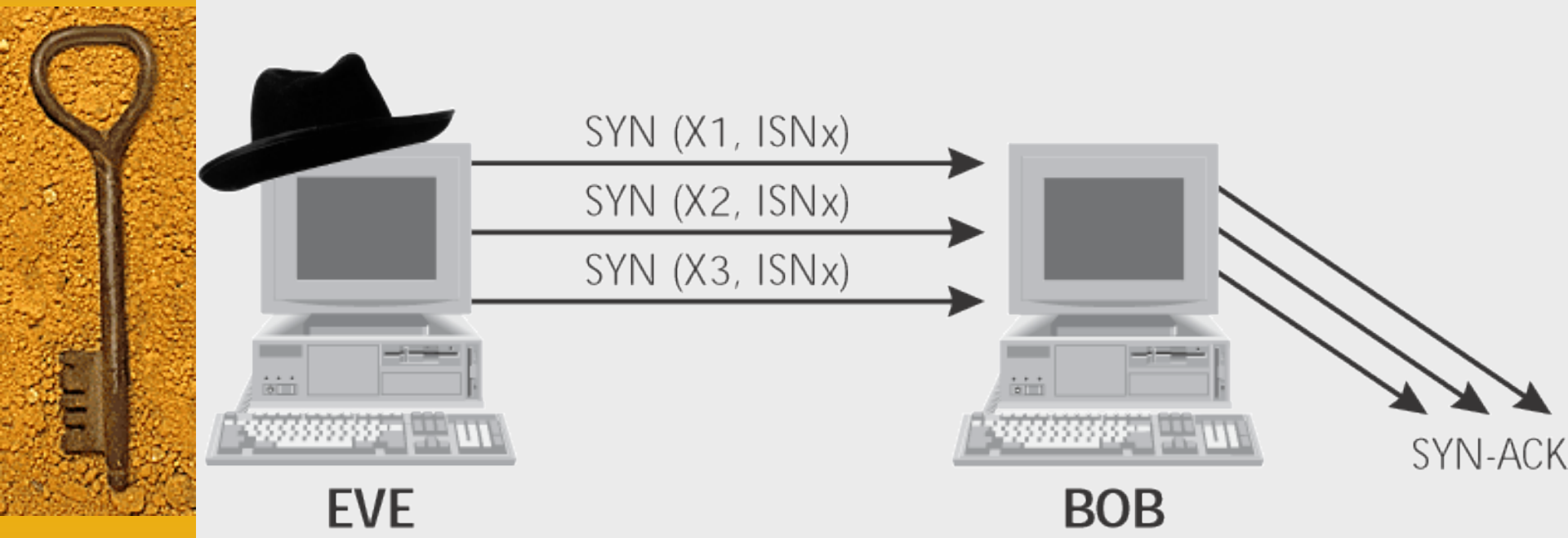


Fig 9.2 A SYN flood using spoofed source IP addresses that are not live

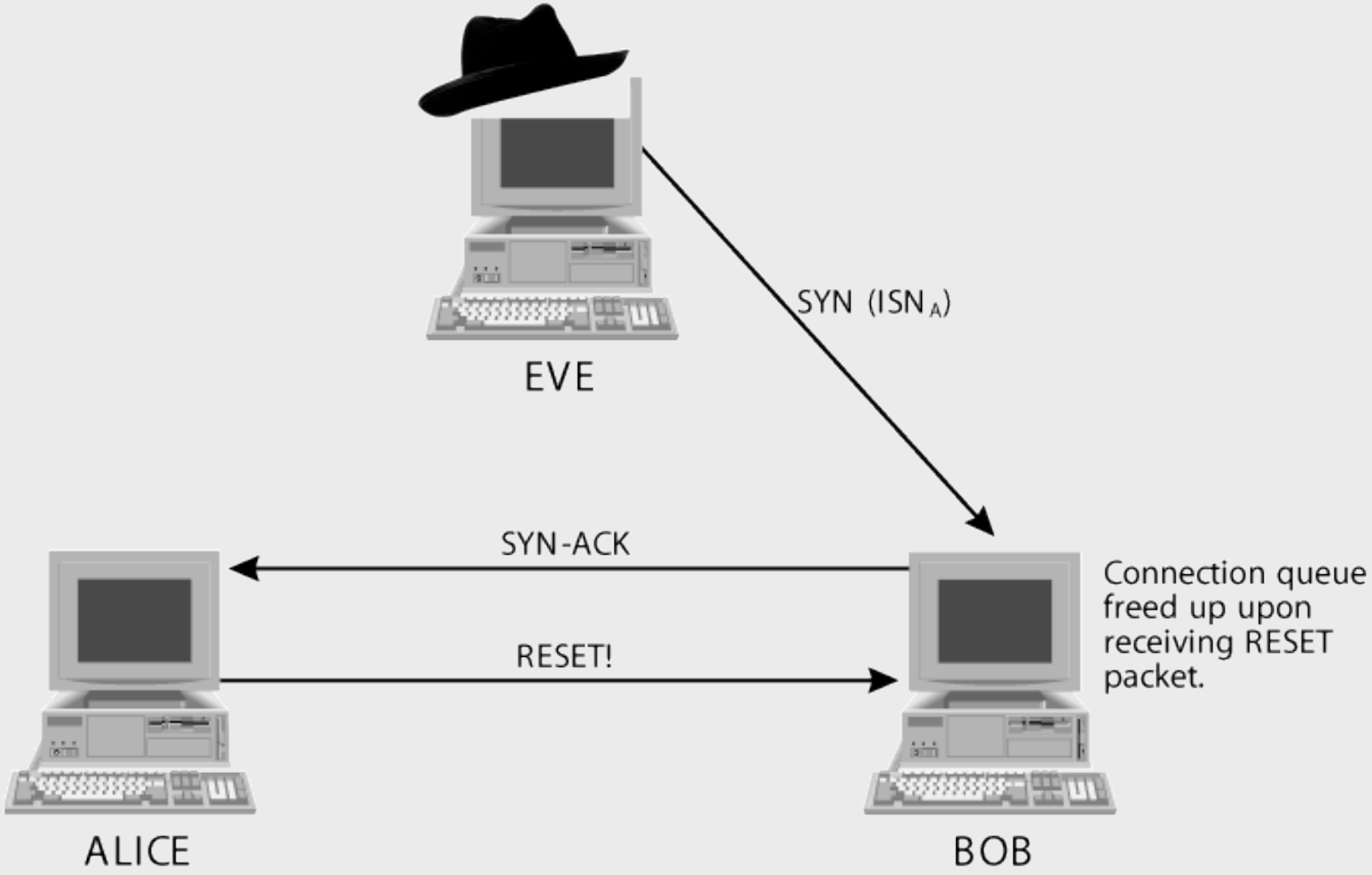


Fig 9.3 Attackers often spoof using unresponsive addresses to prevent RESET from freeing up the target's connection queue resources

SYN Flood Defenses

- Critical servers should have adequate network bandwidth and redundant paths
- Use two different ISPs for Internet connectivity
- Install traffic shaper to limit number of SYN packets
- Increase the size of connection queue or lower the timeout value to complete a half-open connection
  - http://www.nationwide.net/~aleph1/FAQ
- Use SYN cookies on Linux systems
  - A calculated value based on the source and destination IP address, port numbers, time, and a secret number
  - Calculated SYN cookie is loaded into the ISN of SYN-ACK response
  - no need to remember half-open connections on the connection queue
  - Activated via “echo 1 > /proc/sys/net/ipv4/tcp_syncookies”

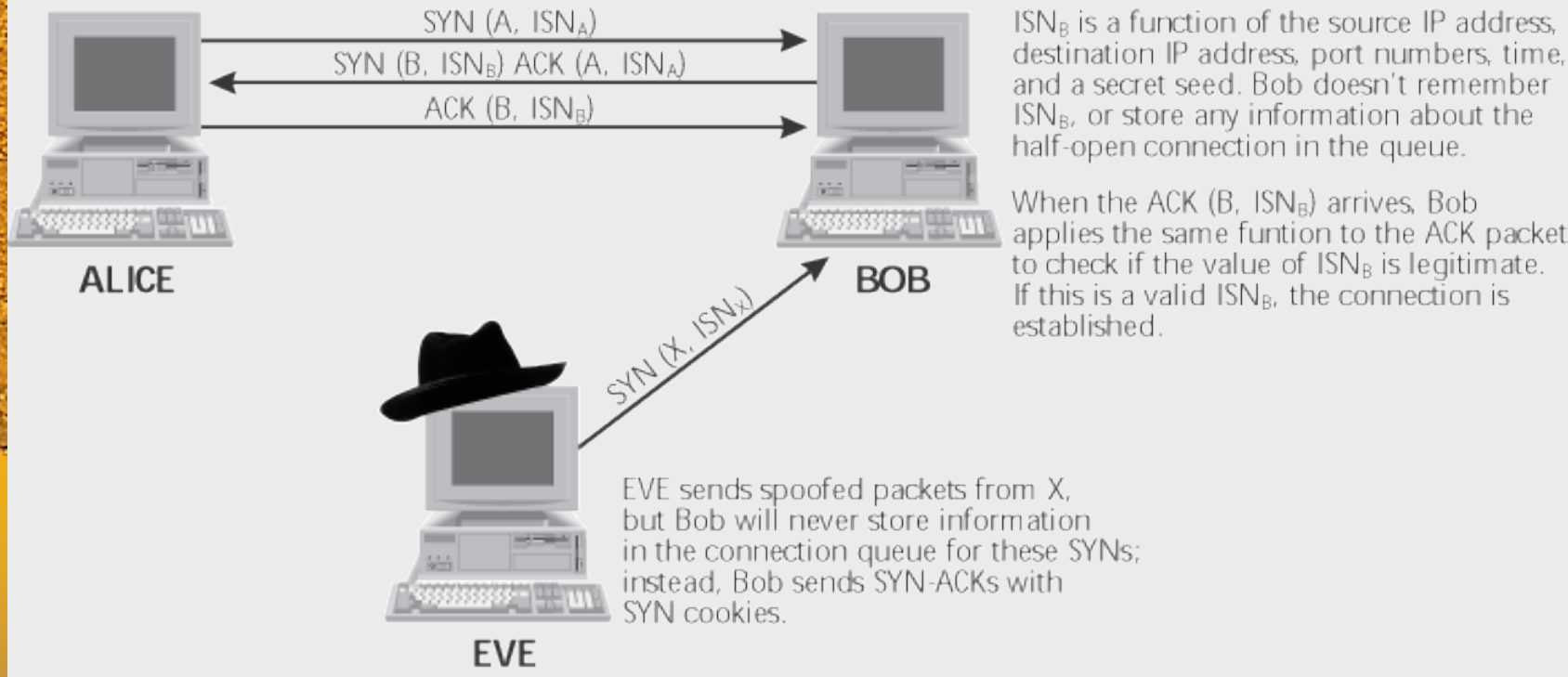


Fig 9.4 SYN cookies

Smurf Attacks

- Aka directed broadcast attacks
- Smurf attacks rely on an ICMP directed broadcast to create a flood of traffic on a victim
- Attacker uses a spoofed source address of victim
- Smurf attack is a DOS that consumes network bandwidth of victim
- Smurf amplifier is a network that responds to directed broadcast messages

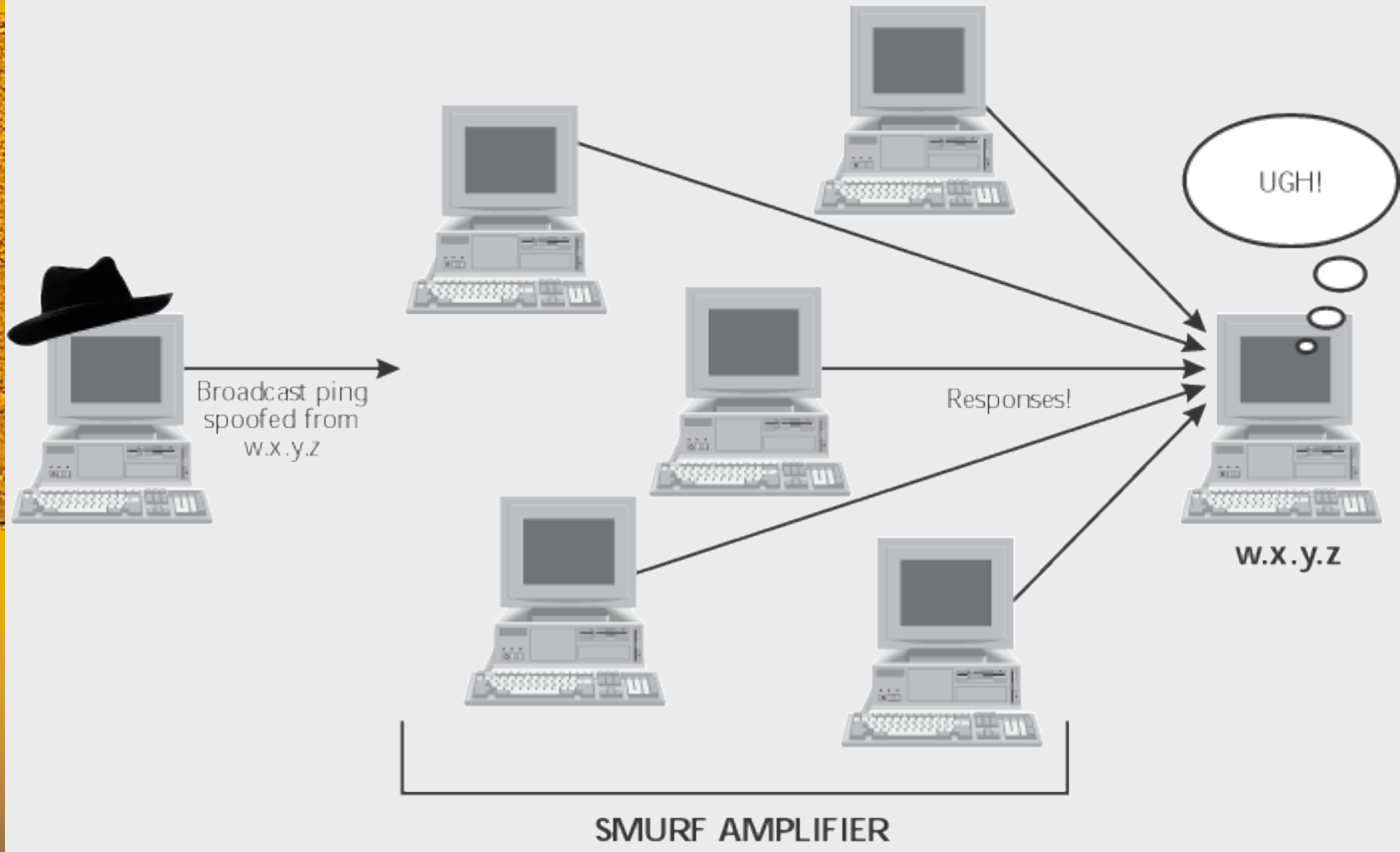


Fig 9.5 A Smurf attack results in a flood of the victim

Directed Broadcast Attack Tools

- Smurf
  - Creates ICMP floods
- Fraggle
  - Uses UDP instead of ICMP
  - Sends spoofed IP broadcast packets to a UDP port that will respond such as UDP port 7 (echo)
- Papasmurf
  - Uses both Smurf and Fraggle attacks
- List of broadcast amplifiers
  - http://www.netscan.org
  - http://www.pulltheplug.com/broadcasts2.html
- Use of Nmap to find broadcast amplifiers
  - Perform ping sweep of broadcast addresses
  - http://packetstorm.securify.com/9901-exploits/smurf.BIP-hunting-namp.txt

Smurf-Attack Defenses

- http://www.pentic.net/denial-of-service/white-papers/smurf.cgi
- Install adequate bandwidth and redundant paths
- Filter ICMP messages at your border router
- Make sure that your network cannot be used as a Smurf amplifier
  - Test via http://www.powertech.no/smurf
  - Insert “no ip directed-broadcast” on Cisco border routers

Distributed Denial-of-Service Attacks (DDoS)

- More powerful than Smurf attacks
- No limitation on number of machines used to launch attack
- No limitation on bandwidth that can be consumed
- Used against Amazon, eBay, Etrade, and Zdnet in Feb 2000
- Before performing a DDOS flood, attack must take over a large number of victim machines (zombies) and install zombie software
- Attacker communicates with client machines which in turn send commands to zombies

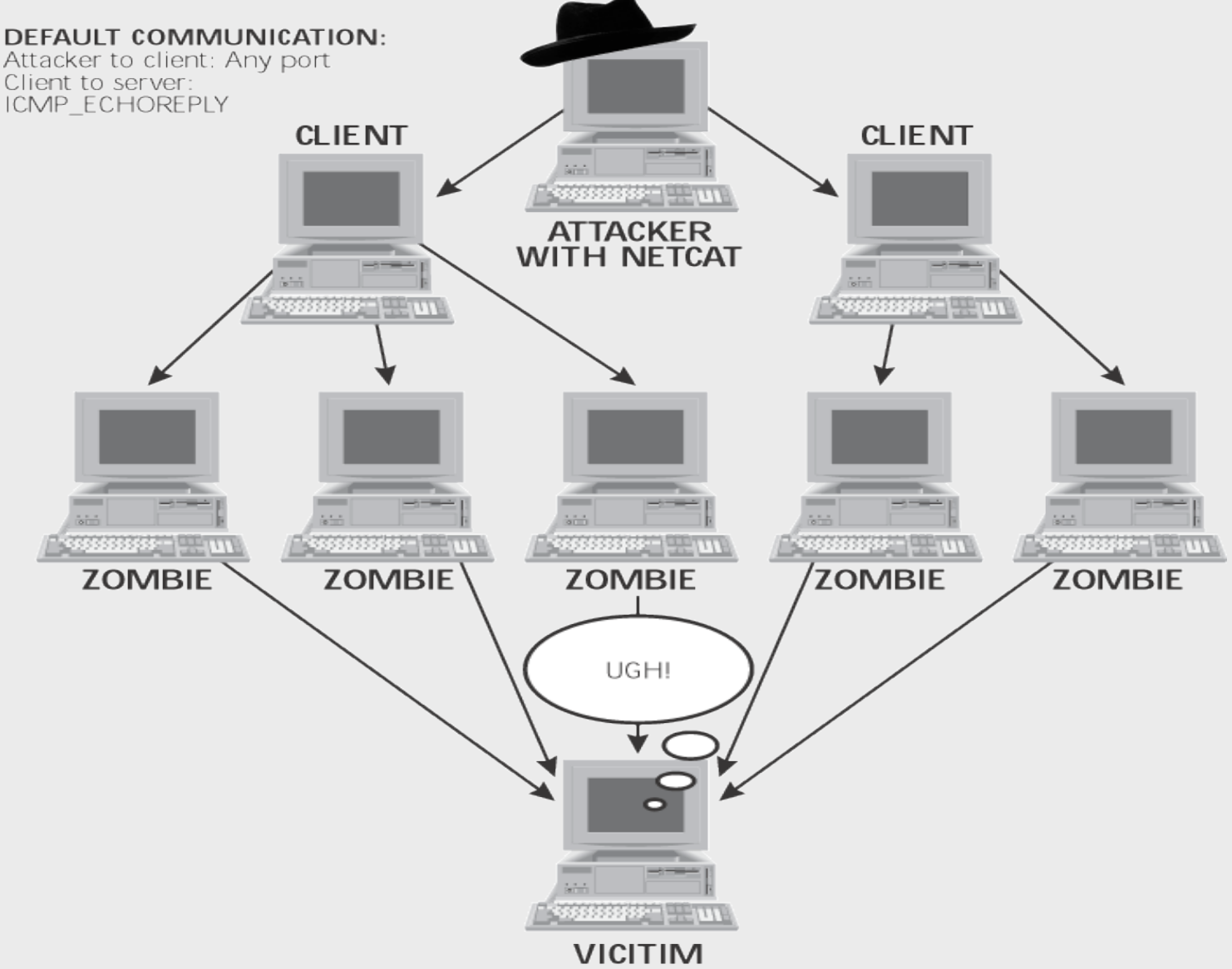


Fig 9.6 A DDoS attack using Tribe Flood Network 2000

DDoS Tools

- Tribe Flood Network
- TFN2K
- Blitznet
- MStream
- Trin00
- Trinity
- Shaft
- Stacheldraht (“barbed wire”)
  - Combines features of TFN and Trin00
- http://packetstorm/securify.com/distributed
- http://mixter.warrior2k.com
- Description of DDOS tools
  - http://www.washington.edu/People/dad/

TFN2K

- Successor to Tribe Flood Network
- Allows attacker to command zombies to launch various attacks
  - Targa (malformed packet DoS attack
  - UDP flood
  - SYN flood
  - ICMP flood
  - Smurf attack
  - “Mix” attack using UDP, SYN, and ICMP floods
- Communication from client to zombies uses ICMP Echo Reply packets
- Zombies not detectable via Nmap
- Clients and zombies can spoof source IP address
- Very difficult to find attacker

DDoS Defenses

- Keep systems patched up-to-date
- Install adequate bandwidth, redundant paths using different ISPs, and traffic shaper
- Install IDS tools that can alert you when a DDoS attack start
- Install egress anti-spoof filters on external router to thwart DDoS zombie on your network from spoofing source IP address

DDoS Defenses (cont.)

- Check for zombies via "Find DDoS" http://www.nipc.gov/warning/advisories/2000/00-44-htm
  - Scans Linux and Solaris systems locally looking for Tin00, TFN, TFN2K, Mstream, Stacheldraht, and Trinity
- Use Zombie Zapper to deactivate active zombies configured with default ports and passwords
  - http://razor.bindview.com/tools/ZombieZapper_form.shtml