Attacks and Malicious Code

- Chapter 3

Learning Objectives

- Explain denial-of-service (DoS) attacks
- Explain and discuss ping-of-death attacks
- Identify major components used in a DDoS attack and how they are installed
- Understand major types of spoofing attacks
- Discuss man-in-the-middle attacks, replay attacks, and TCP session hijacking

continued…

Learning Objectives

- Detail three types of social-engineering attacks and explain why they can be incredibly damaging
- List major types of attacks used against encrypted data
- List major types of malicious software and identify a countermeasure for each one

Denial-of-Service Attacks

- Any malicious act that causes a system to be unusable by its real user(s)
- Take numerous forms
- Are very common
- Can be very costly
- Major types
  - SYN flood
  - Smurf attack

SYN Flood

- Exploits the TCP three-way handshake
- Inhibits server's ability to accept new TCP connections

TCP Three-Way Handshake

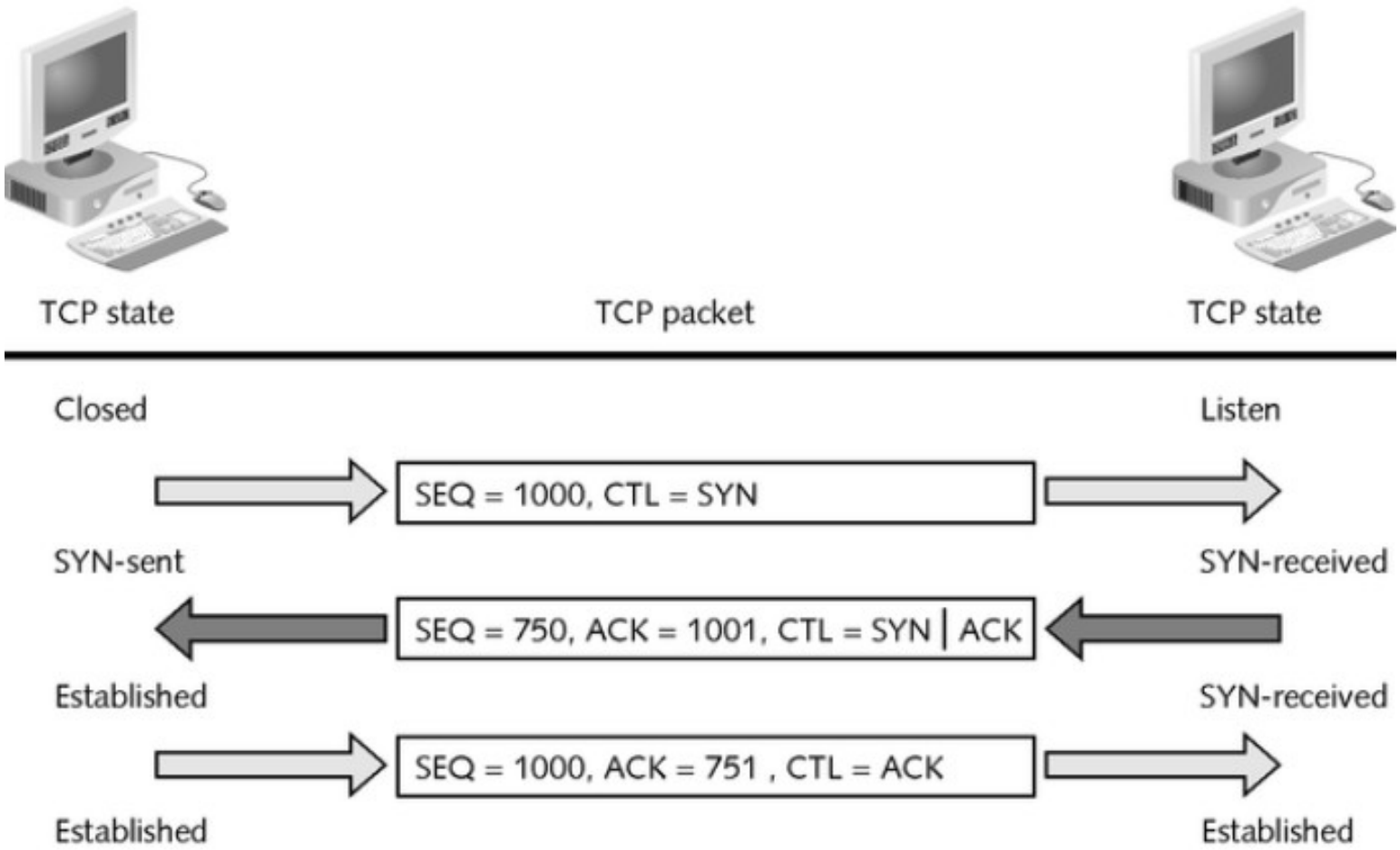


Figure 3-1 TCP three-way handshake

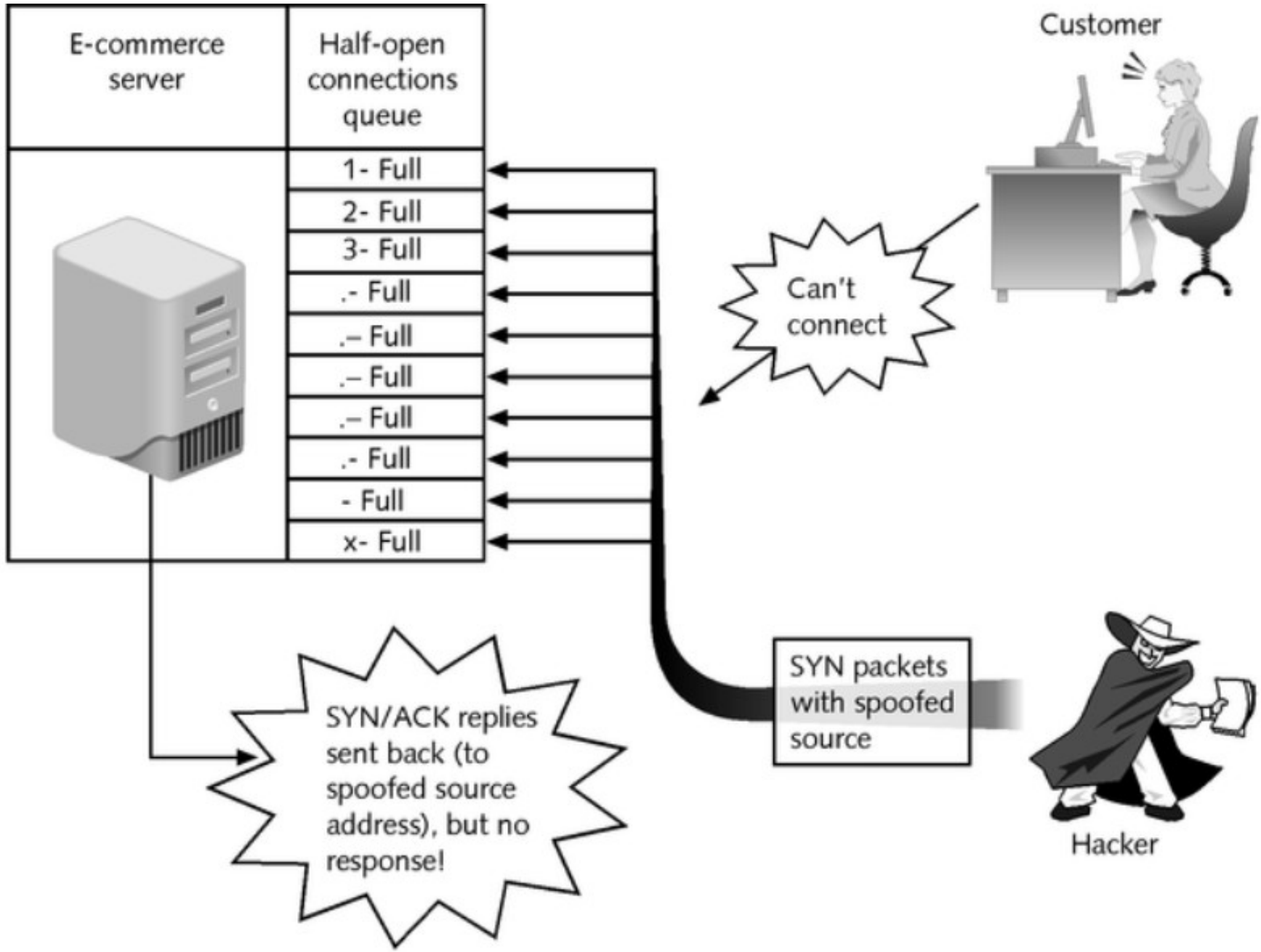


Figure 3-2 SYN flood attack

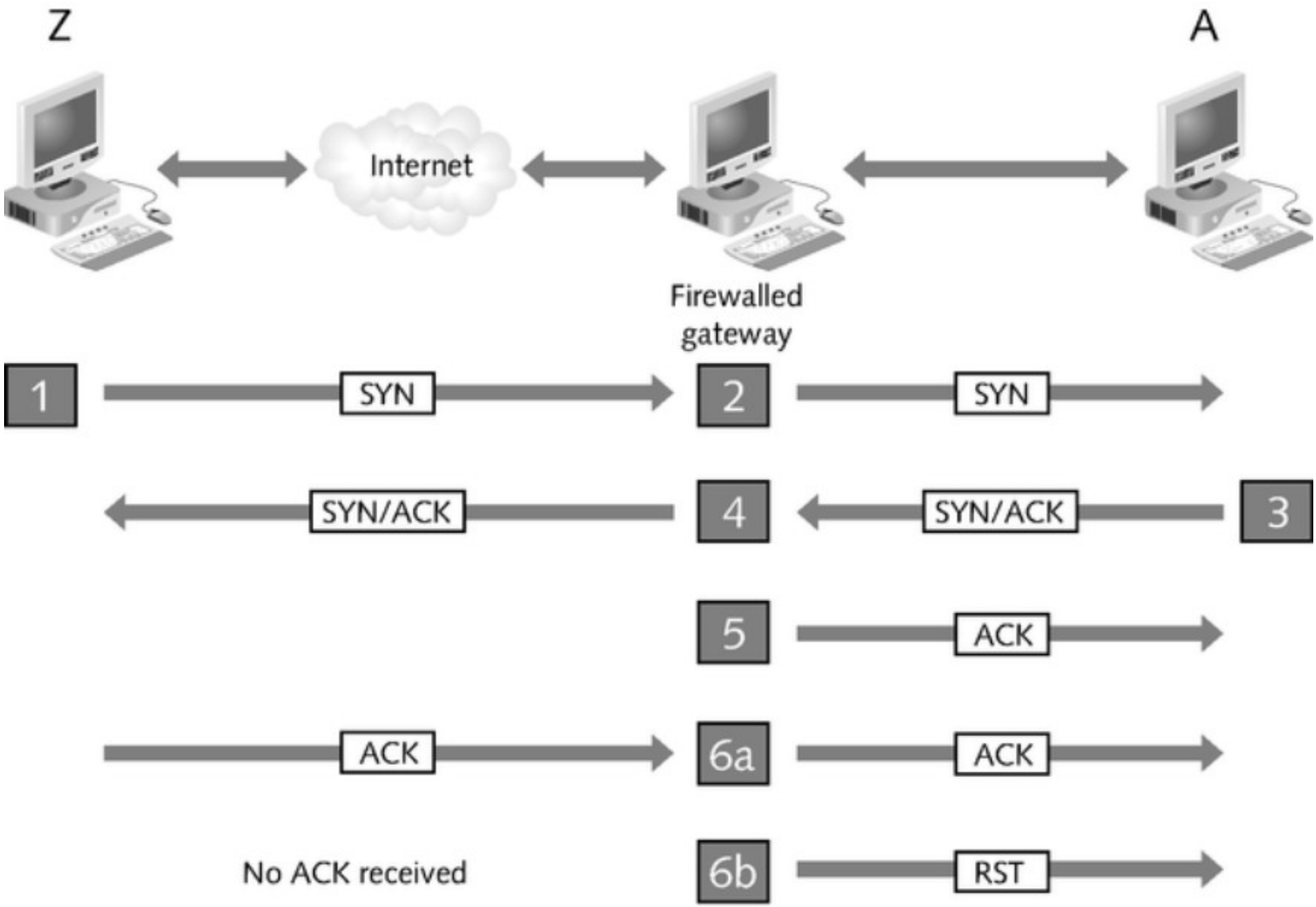


Figure 3-3 Defending against the SYN flood

Smurf

- Non-OS specific attack that uses the network to amplify its effect on the victim
- Floods a host with ICMP
- Saturates Internet connection with bogus traffic and delays/prevents legitimate traffic from reaching its destination

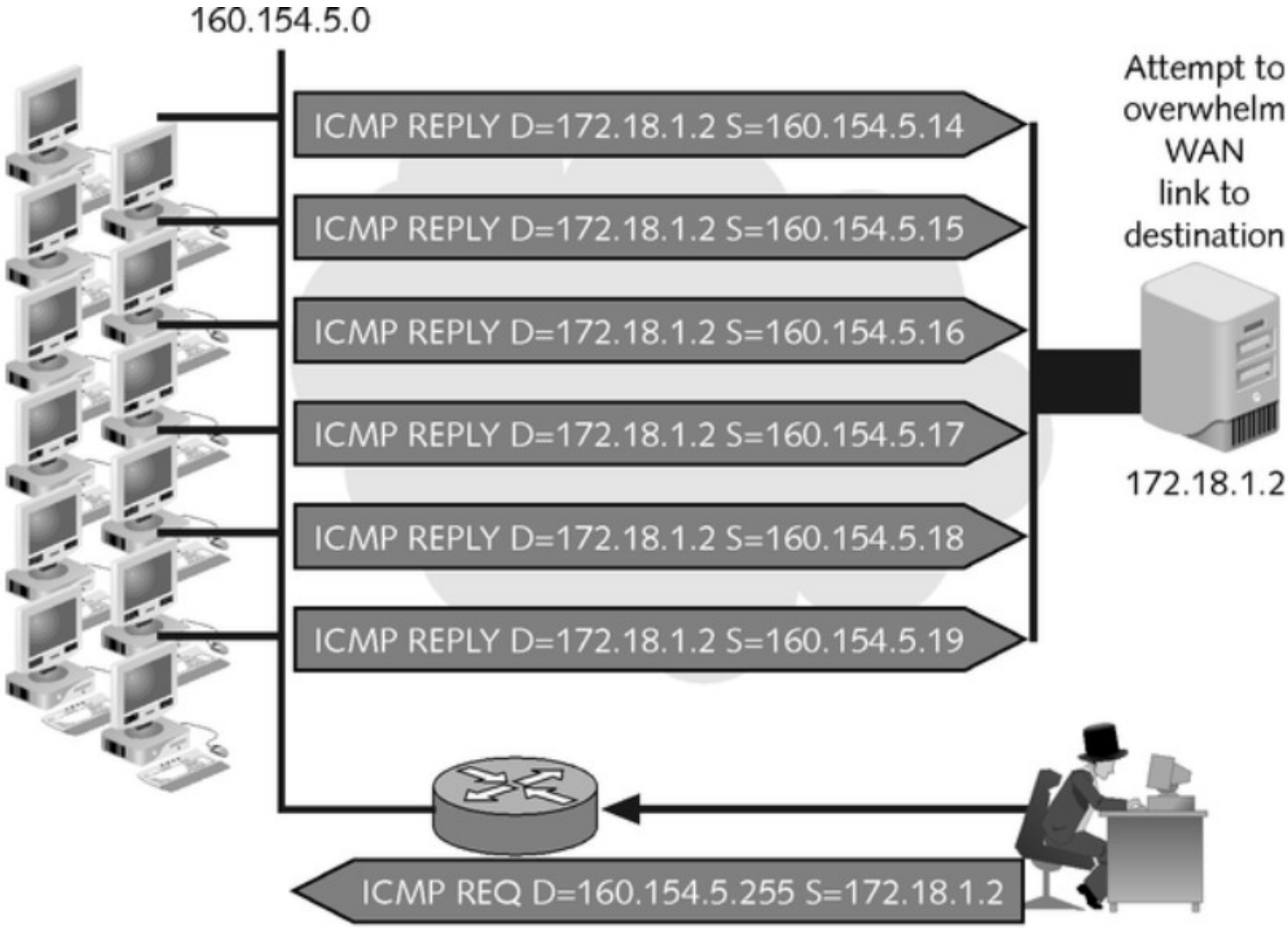


Figure 3-4 Smurf attack

IP Fragmentation Attacks: Ping of Death

- Uses IP packet fragmentation techniques to crash remote systems

Ping of Death

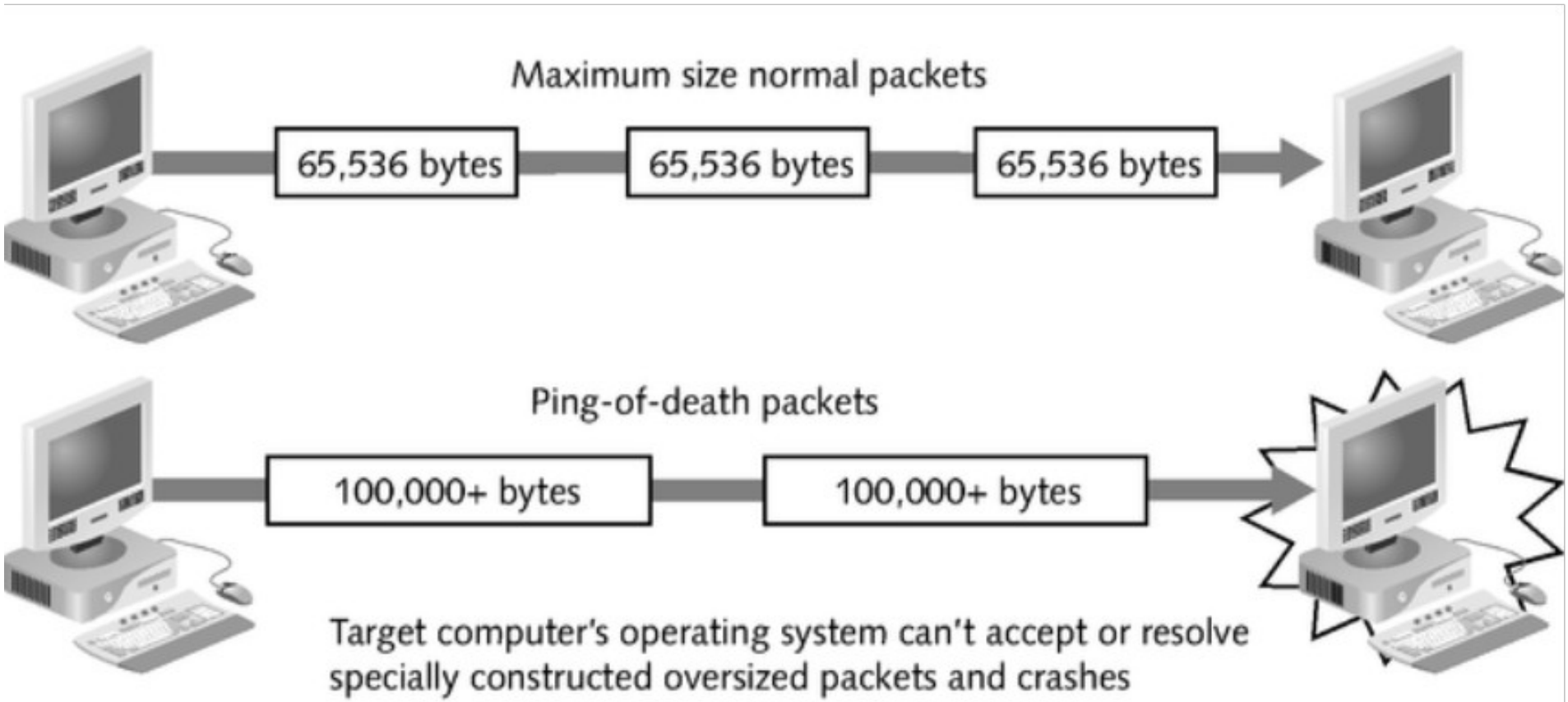


Figure 3-5 Ping of death

FORESEC

Distributed Denial-of-Service Attacks

- Use hundreds of hosts on the Internet to attack the victim by flooding its link to the Internet or depriving it of resources
- Used by hackers to target government and business Internet sites
- Automated tools; can be executed by script kiddies
- Result in temporary loss of access to a given site and associated loss in revenue and prestige

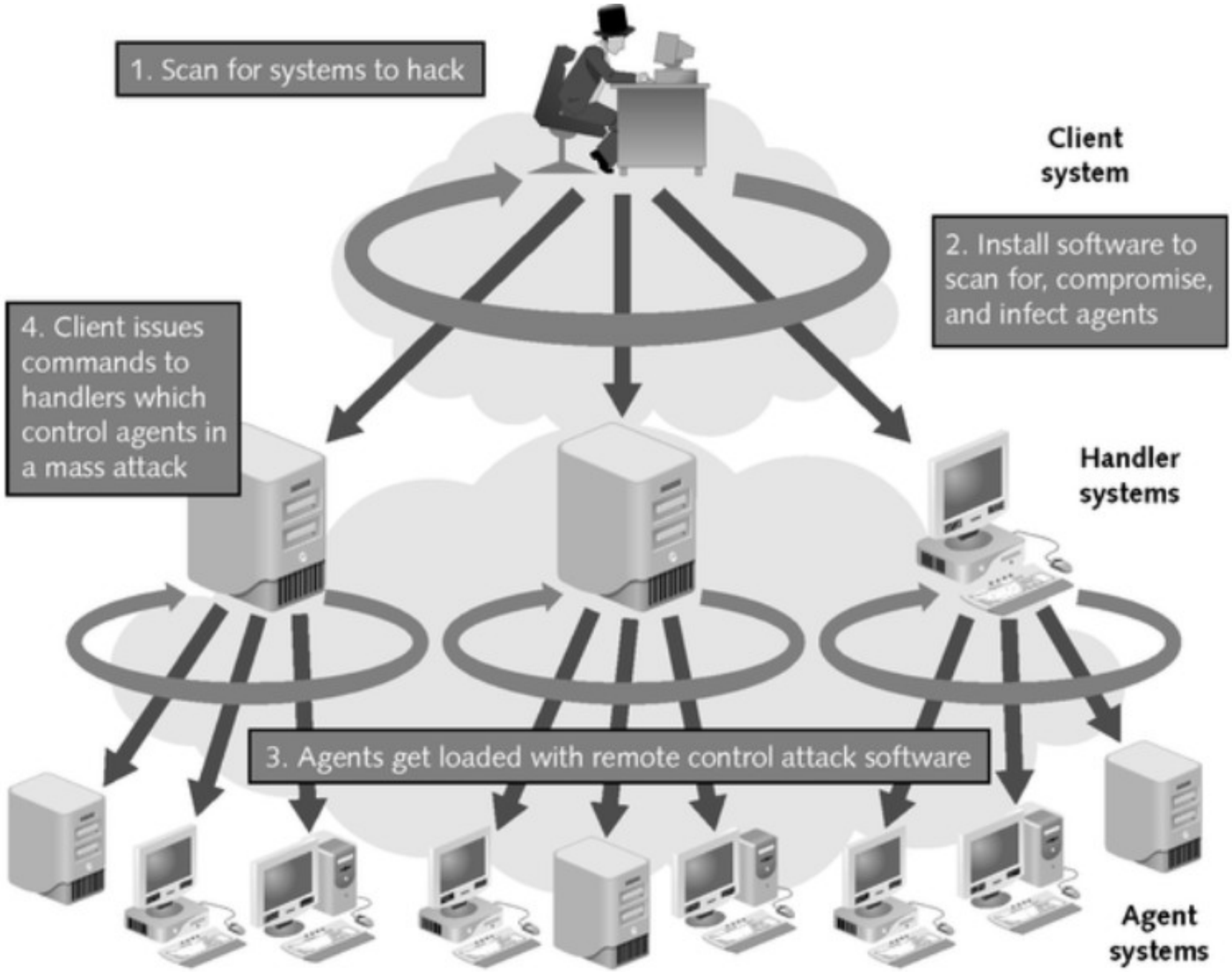


Figure 3-6 Distributed denial-of-service attack

Conducting DDoS Attacks

Table 3-1 DDoS tools and attack methods

Tools	Flooding or Attack Methods
Trin00	UDP
Tribe flood network	UDP, ICMP, SYN smurf
Stacheldracht and variants	UDP, ICMP, SYN smurf
TFN 2K	UDP, ICMP, SYN smurf
Shaft	UDP, ICMP, SYN combo
Mstream	Stream (ACK)
Trinity, Trinity v3	UDP, SYN, RST, Random Flag, ACK, Fragment

DDoS Countermeasures

- Security patches from software vendors
- Antivirus software
- Firewalls
- Ingress (inbound) and egress (outbound) filtering

Ingress and Egress Filtering

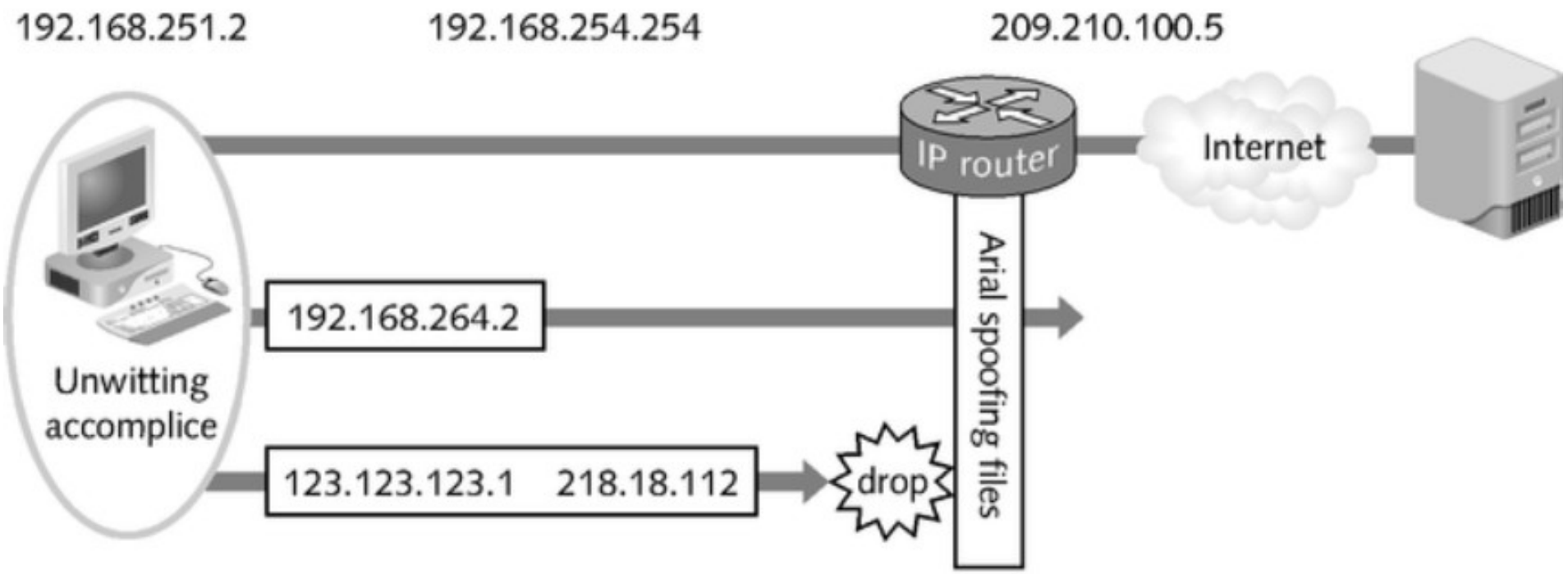


Figure 3-7 Ingress and egress filtering

FORESEC

Preventing the Network from Inadvertently Attacking Others

- Filter packets coming into the network destined for a broadcast address
- Turn off directed broadcasts on internal routers
- Block any packet from entering the network that has a source address that is not permissible on the Internet (see Figures 3-8 and 3-9)

continued…

Preventing the Network from Inadvertently Attacking Others

- Block at the firewall any packet that uses a protocol or port that is not used for Internet communications on the network
- Block packets with a source address originating inside your network from entering your network

Ingress Filtering of Packets with RFC 1918 Addresses

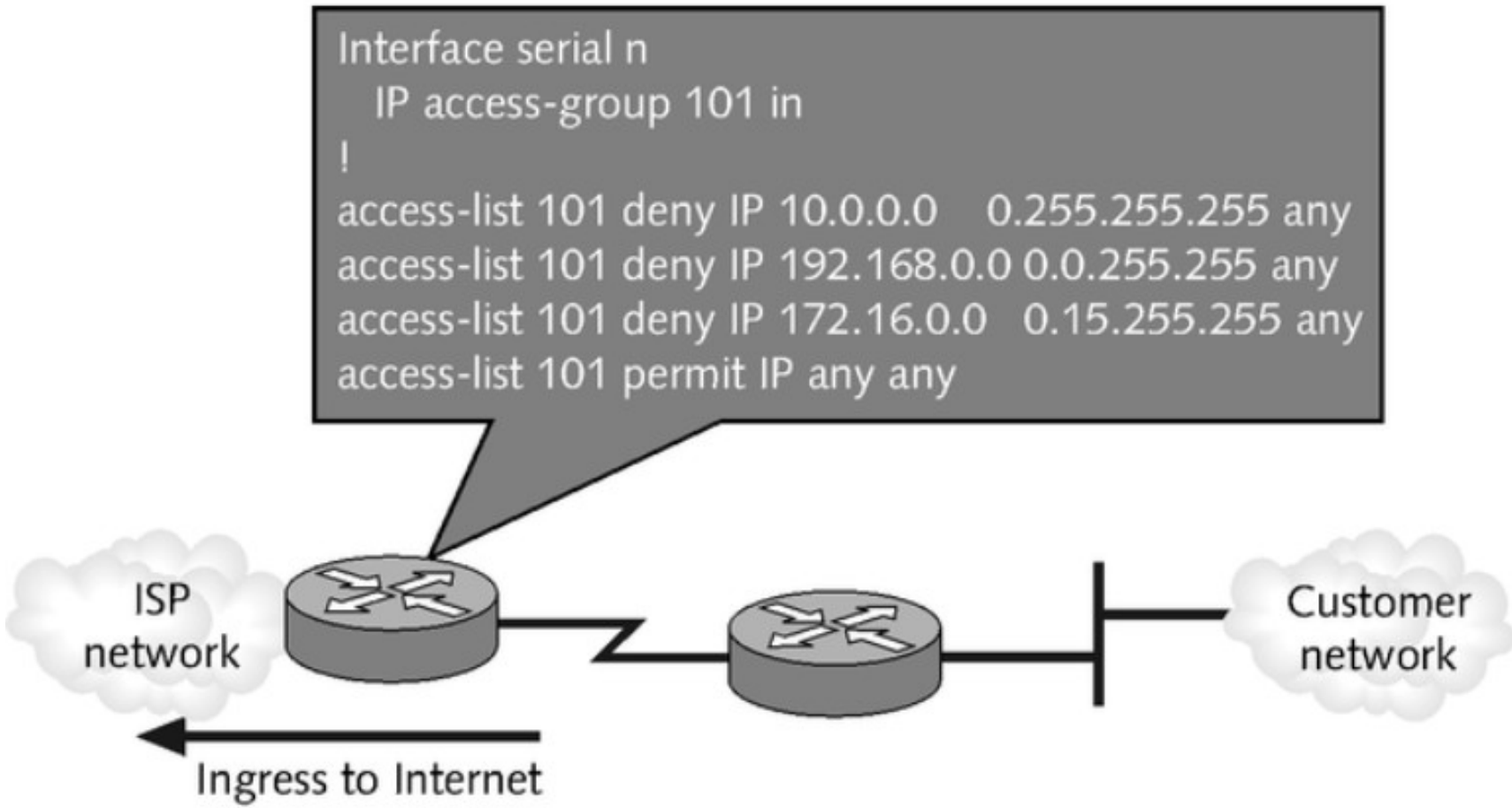


Figure 3-8 Ingress filtering of packets with RFC 1918 addresses

Filtering of Packets with RFC 2827 Addresses

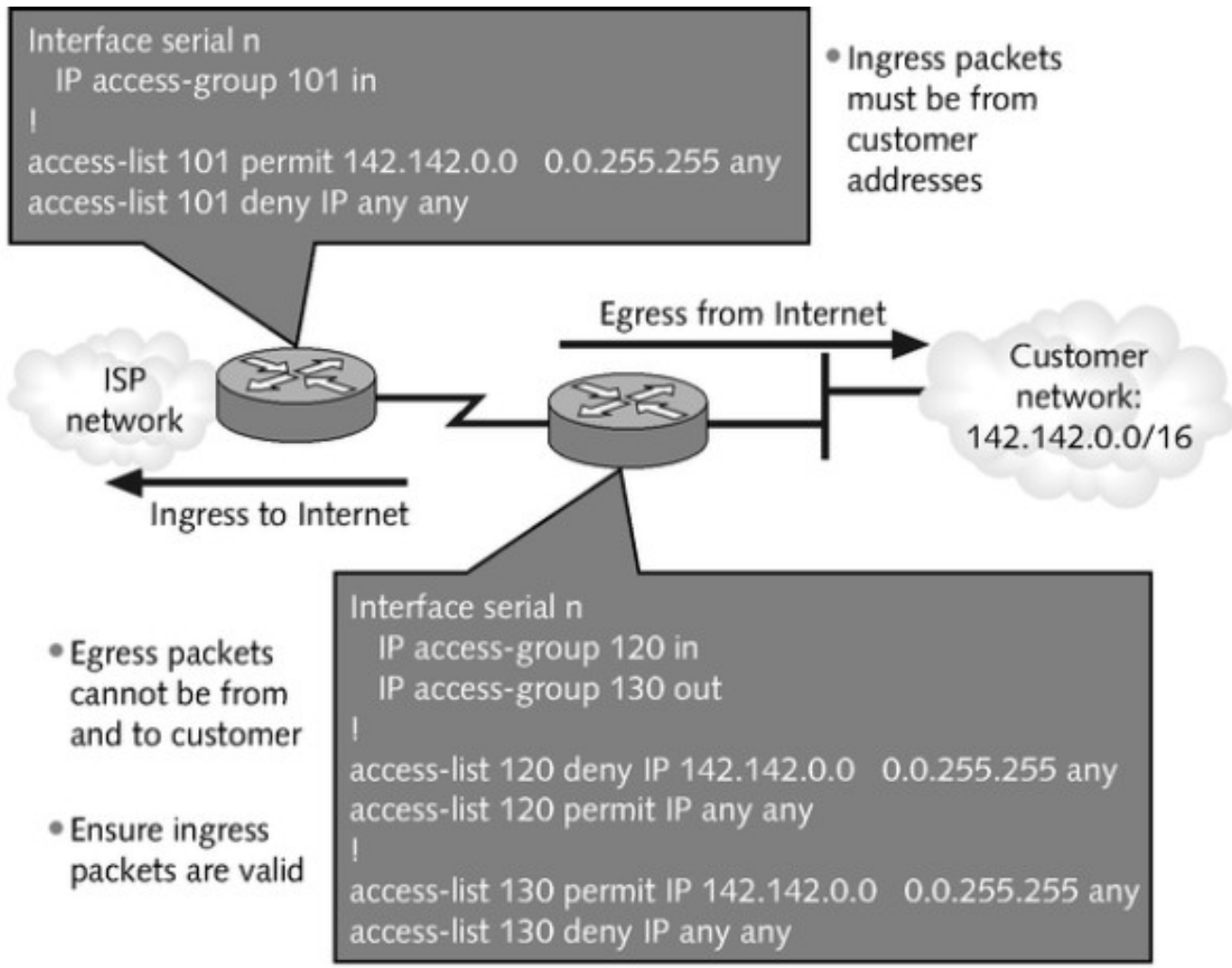


Figure 3-9 Filtering of packets with RFC 2827 addresses

FORBSEC

Spoofing

- Act of falsely identifying a packet's IP address, MAC address, etc
- Four primary types
  - IP address spoofing
  - ARP poisoning
  - Web spoofing
  - DNS spoofing

IP Address Spoofing

- Used to exploit trust relationships between two hosts
- Involves creating an IP address with a forged source address

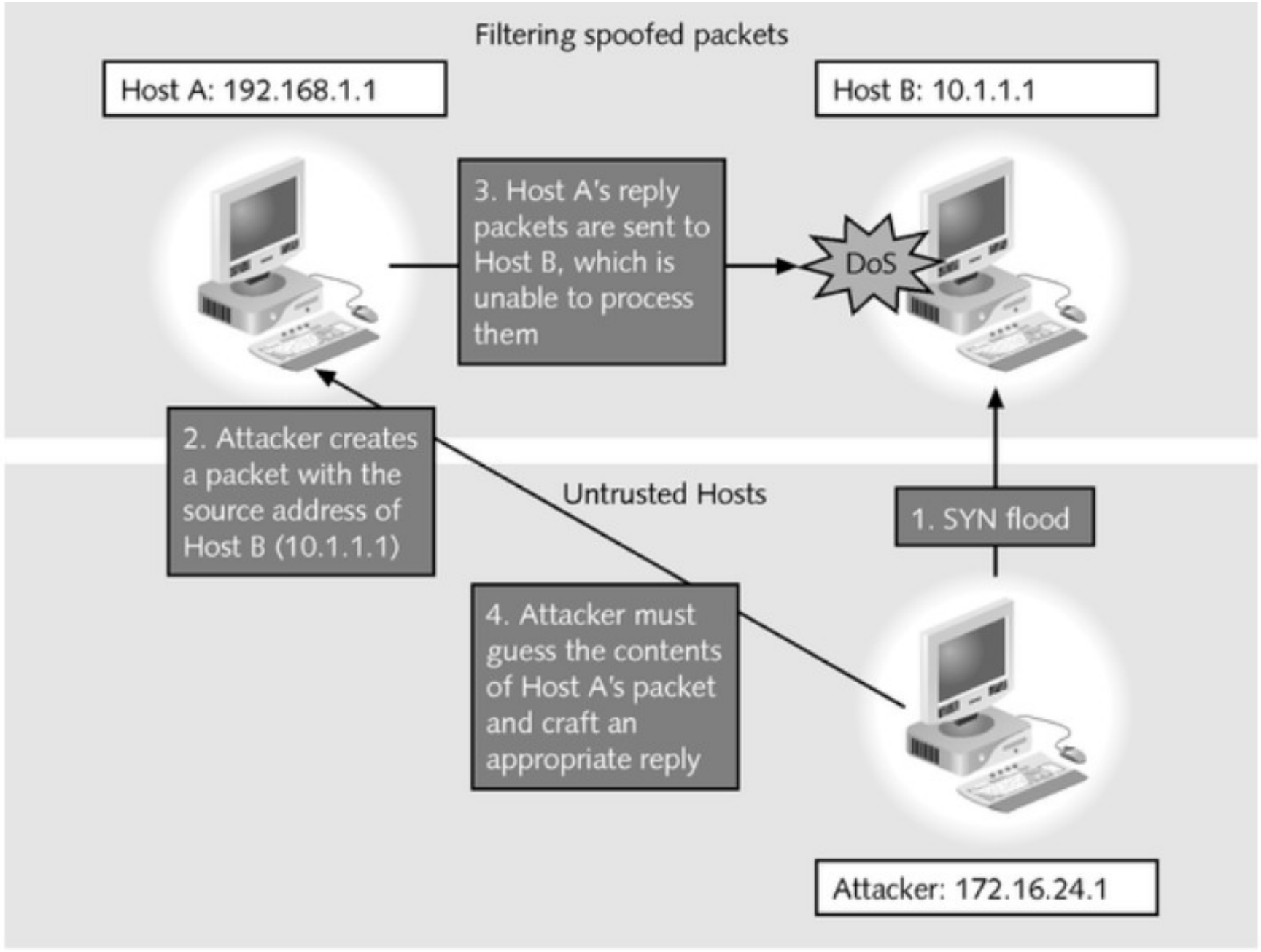


Figure 3-10 Filtering spoofed packets

ARP Poisoning

- Used in man-in-the-middle and session hijacking attacks; attacker takes over victim's IP address by corrupting ARP caches of directly connected machines
- Attack tools
  - ARPoison
  - Ettercap
  - Parasite

Web Spoofing

- Convinces victim that he or she is visiting a real and legitimate site
- Considered both a man-in-the-middle attack and a denial-of-service attack

Web Spoofing

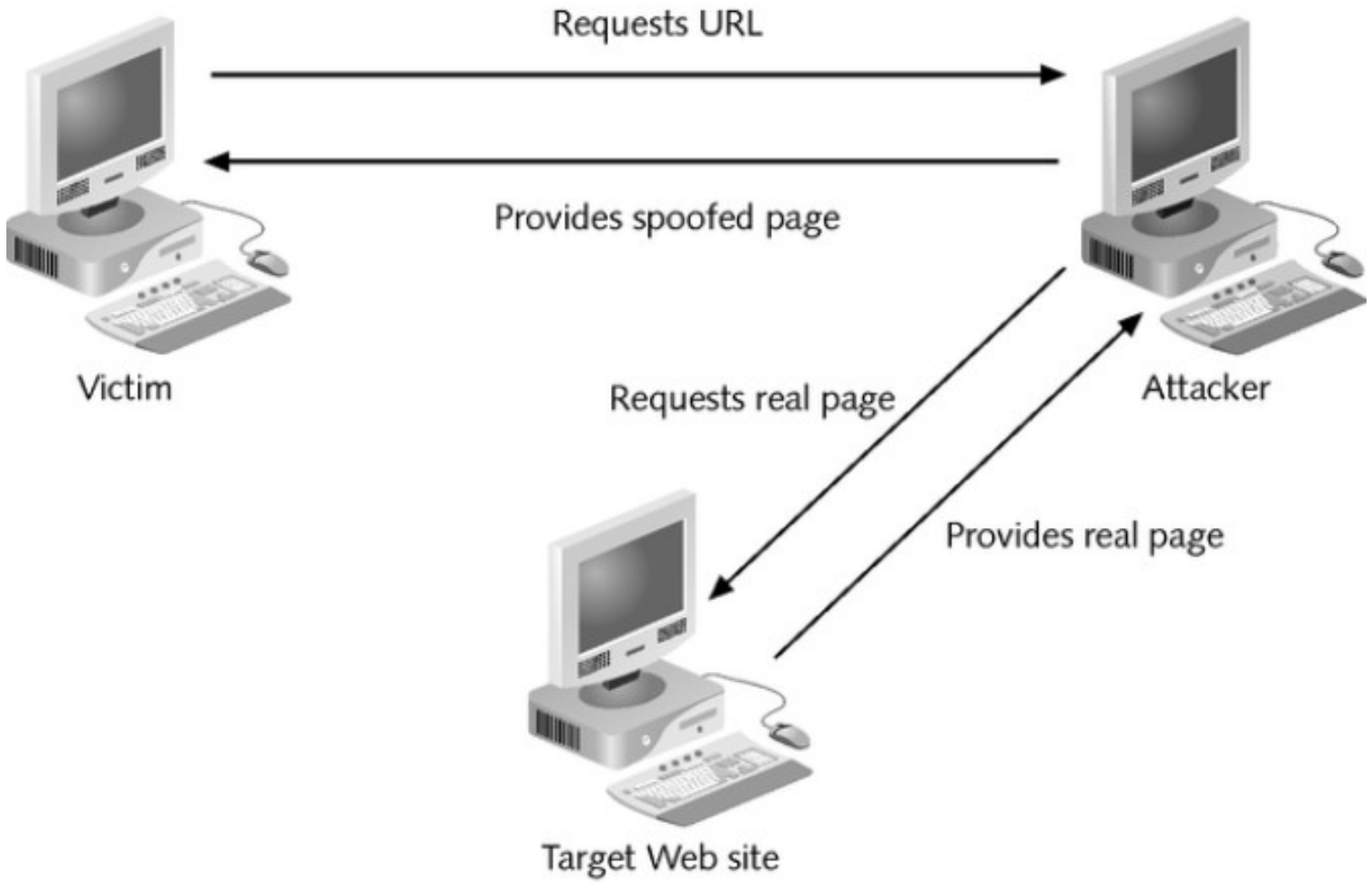


Figure 3-11 Web spoofing

DNS Spoofing

- Aggressor poses as the victim's legitimate DNS server
- Can direct users to a compromised server
- Can redirect corporate e-mail through a hacker's server where it can be copied or modified before sending mail to final destination

To Thwart Spoofing Attacks

- IP spoofing
  - Disable source routing on all internal routers
  - Filter out packets entering local network from the Internet that have a source address of the local network
- ARP poisoning
  - Use network switches that have MAC binding features

continued…

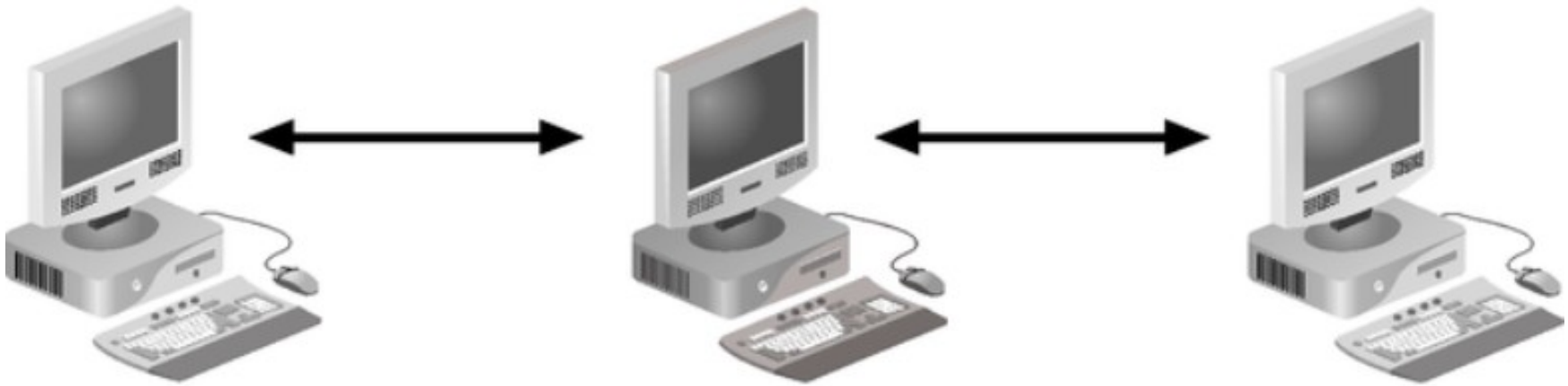
To Thwart Spoofing Attacks

- Web spoofing
  - Educate users
- DNS spoofing
  - Thoroughly secure DNS servers
  - Deploy anti-IP address spoofing measures

Man in the Middle

- Class of attacks in which the attacker places himself between two communicating hosts and listens in on their session
- To protect against
  - Configure routers to ignore ICMP redirect packets

Man-in-the-Middle Attacks



Host A

Thinks it's communicating with Host B

Attacker

Sits between the two hosts and is able to monitor and modify their transmissions

Host B

Thinks it's communicating with Host A

Figure 3-12 Man-in-the-middle attacks

Man-in-the-Middle Applications

- Web spoofing
- TCP session hijacking
- Information theft
- Other attacks (denial-of-service attacks, corruption of transmitted data, traffic analysis to gain information about victim's network)

Man-in-the-Middle Methods

- ARP poisoning
- ICMP redirects
- DNS poisoning

Replay Attacks

- Attempts to circumvent authentication mechanisms by:
  - Recording authentication messages from a legitimate user
  - Reissuing those messages in order to impersonate the user and gain access to systems

Replay Attack

Username: fred

Password: lisa

Figure 3-13 Replay attack

TCP Session Hijacking

- Attacker uses techniques to make the victim believe he or she is connected to a trusted host, when in fact the victim is communicating with the attacker
- Well-known tool
  - Hunt (Linux)

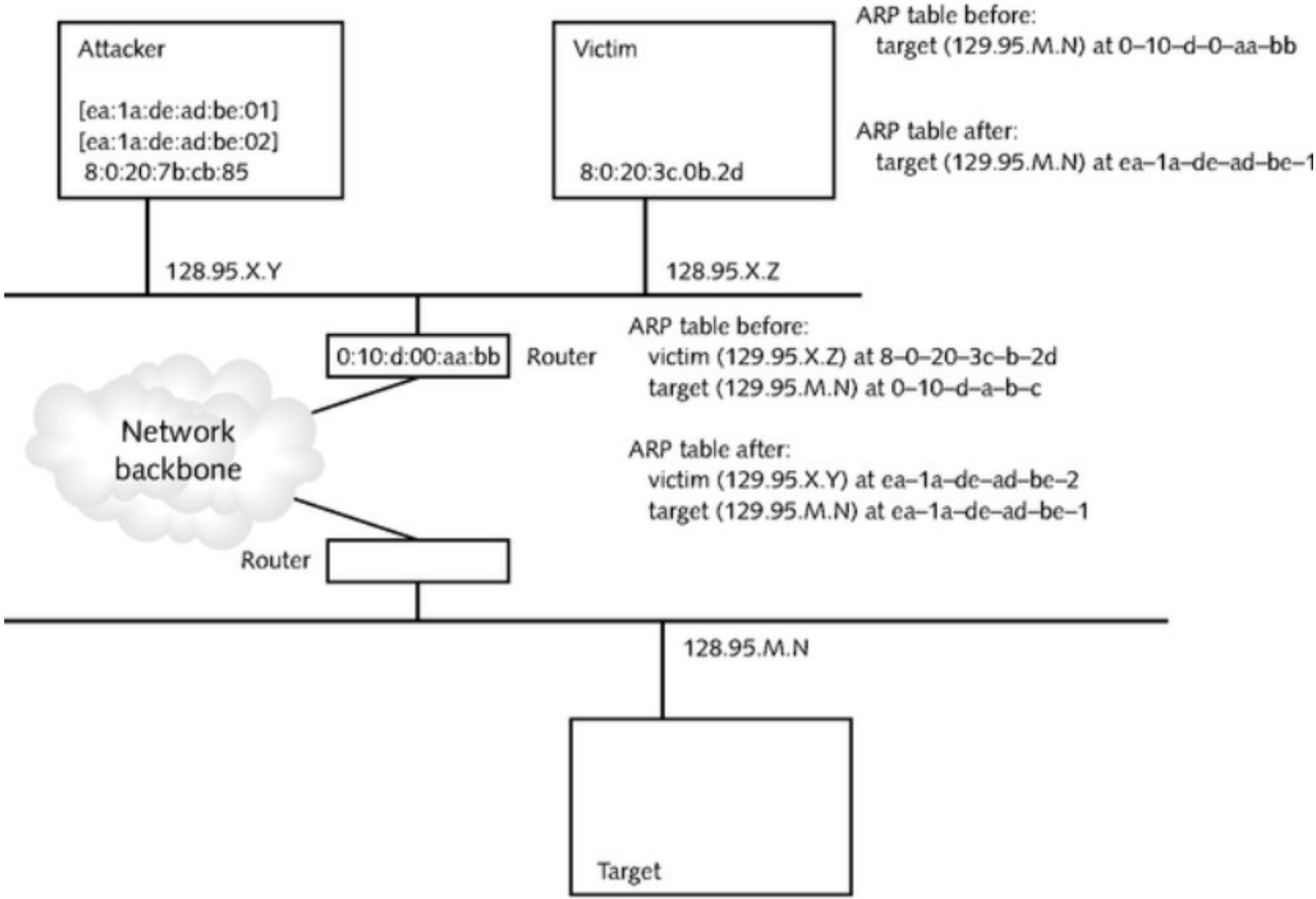
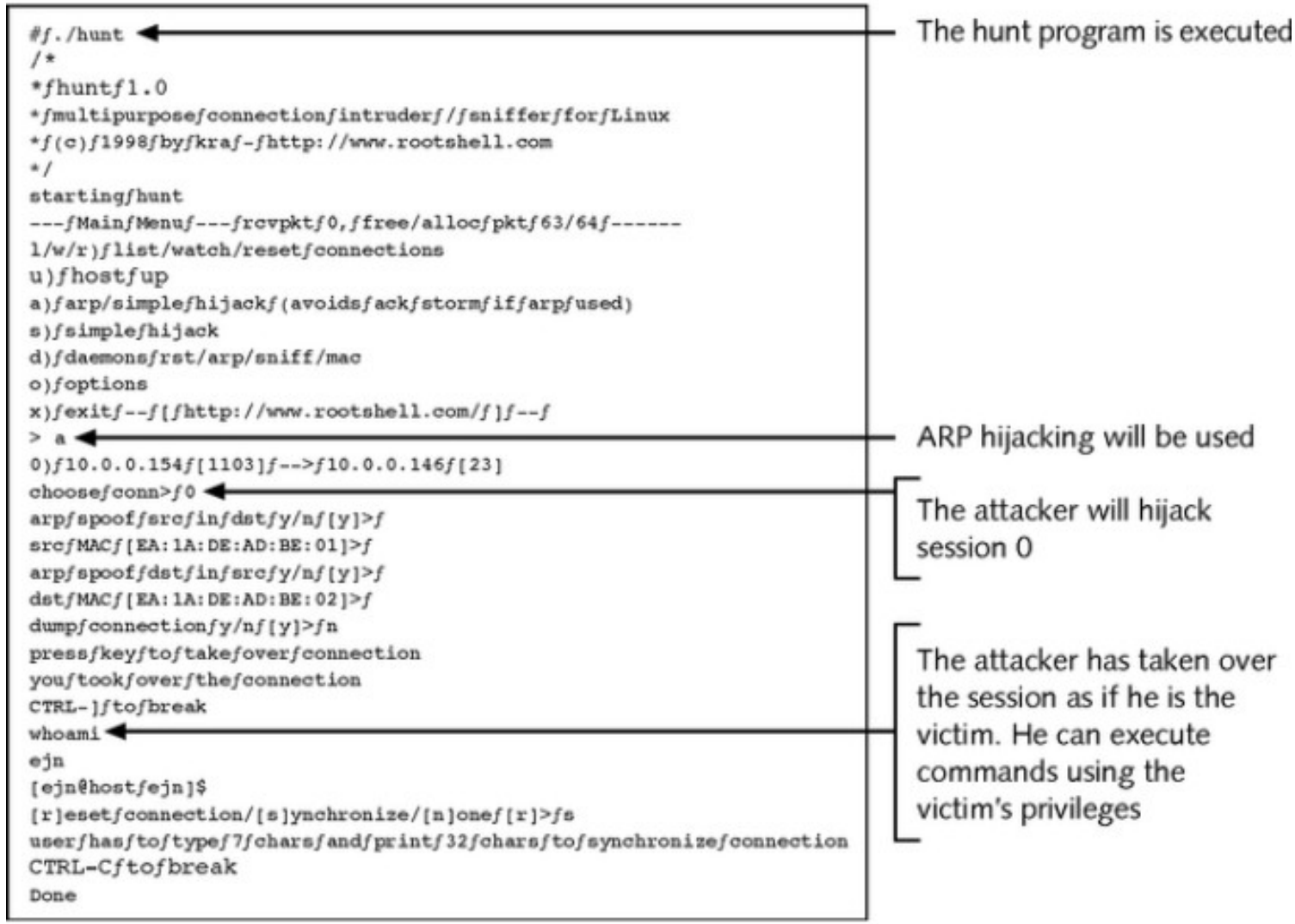


Figure 3-14 Attacker using source Ethernet segment as user

Attacker Using Victim's TCP Connection



FORESEC

Social Engineering

- Class of attacks that uses trickery on people instead of computers
- Goals
  - Fraud
  - Network intrusion
  - Industrial espionage
  - Identity theft
  - Desire to disrupt the system or network

Dumpster Diving

Table 3-2 Useful information gathered from trash bins

Internal phone directories	Names and numbers of people to target and impersonate—many usernames are based on legal names
Organizational charts	Information about people who are in positions of authority within the organization
Policy manuals	How secure (or insecure) the company really is
Calendars	Which employees are out of town at a particular time
Outdated hardware	Hard drives may be restored to provide all sorts of useful information
System manuals, network diagrams, and other sources of technical information	The exact information that attackers may seek, including the IP addresses of key assets, network topologies, locations of firewalls and intrusion detection systems, operating systems, applications in use, and more

FORESEC

Online Attacks

- Use chat and e-mails venues to exploit trust relationships

Social Engineering Countermeasures

- Take proper care of trash and discarded items
- Ensure that all system users have periodic training about network security

FORESEC

Attacks Against Encrypted Data

- Weak keys
- Mathematical attacks
- Birthday attack
- Password guessing
- Brute force
- Dictionary

Weak Keys

- Secret keys used in encryption that exhibit regularities in encryption, or even a poor level of encryption

Mathematical Attack

- Attempts to decrypt encrypted data using mathematics to find weaknesses in the encryption algorithm
- Categories of cryptanalysis
  - Cyphertext-only analysis
  - Known plaintext attack
  - Chosen plaintext attack

Birthday Attack

- Class of brute-force mathematical attacks that exploits mathematical weaknesses of hash algorithms and one-way hash functions

Password Guessing

- Tricks authentication mechanisms by determining a user's password using techniques such as brute force or dictionary attacks

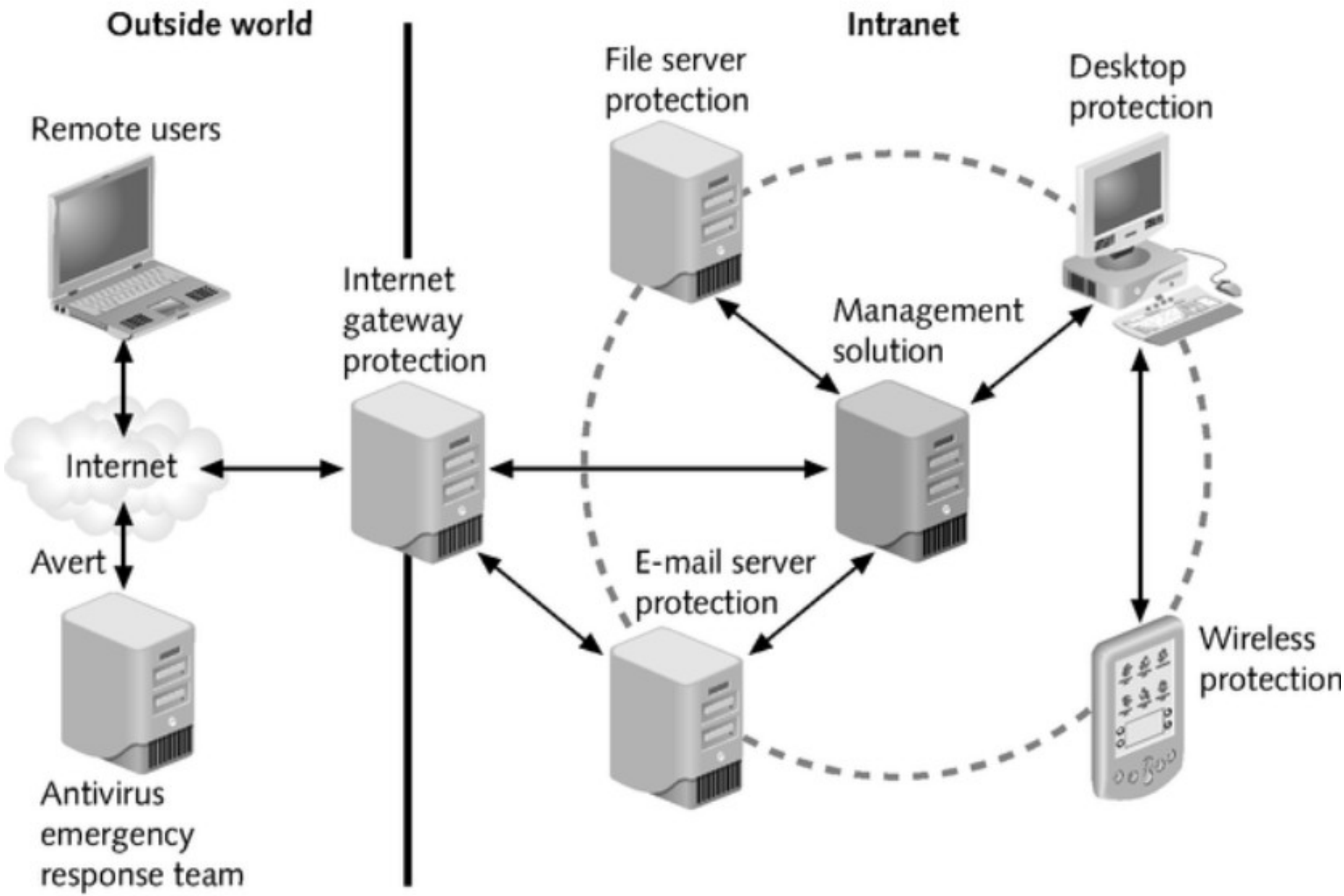


Figure 3-15 Multilayered approach to virus scanning

Brute Force

- Method of breaking passwords that involves computation of every possible combination of characters for a password of a given character length

Dictionary

- Method of breaking passwords by using a predetermined list of words as input to the password hash
- Only works against poorly chosen passwords

Software Exploitation

- Utilizes software vulnerabilities to gain access and compromise systems
- Example
  - Buffer overflow attach
- To stop software exploits
  - Stay appraised of latest security patches provided by software vendors

Malicious Software

Table 3-3 Malware differences

Type	Propagation	Examples
Virus	Copies itself into other executable programs and scripts	Melissa
Worm	Exploits vulnerabilities with the intent of propagating itself across the network	Code Red Code Red II Nimda
Trojan horse	Uses social engineering techniques to trick users into running the malware's executable	ILOVEYOU Naked Wife Anna Kournikova

Viruses

- Self-replicating programs that spread by “infecting” other programs
- Damaging and costly

Table 3-4 Virus types

Type	Primary Period	Description
Boot sector	1980s to mid-90s	Spread by infecting floppy or hard disk boot sectors; when an infected disk is booted, the virus is loaded into memory and attempts to infect any and all floppy disks inserted into the computer
File infector	mid-90s	A class called "parasitic viruses" because they must infect other programs, file infectors copy themselves into other programs. When an infected file is executed, the virus is loaded into memory and tries to infect other executables. File types commonly infected include: *.exe, *.drv, *.dll, *.bin, *.ovl, *.sys, *.com
Multipartite	mid-90s	Propagated using both boot sector and file infector methods
Macro viruses	Current	Currently accounting for the vast majority of viruses, macro viruses are application specific as opposed to OS specific and propagate very rapidly via e-mail. Many macro viruses are Visual Basic scripts that exploit commonly used Microsoft applications such as Word, Excel, and Outlook.

Virus Databases

Table 3-5: Virus Databases

Network Associates (McAfee)	http://vil.nai.com/VIL/default.asp
Symantec	http://securityresponse.symantec.com/avcenter/vinfodb.html
Computer Associates	www3.ca.com/virus/encyclopedia.asp
Trend Micro	www.antivirus.com/vinfo/virusencyclo/

Evolution of Virus Propagation Techniques

Table 3-6 Evolution of virus propagation techniques

SKA	January 1999	Single mailer
Melissa	March 1999	Mass mailer targeting 50 recipients in a single activation
Babylonia	December 1999	Mass mailer using plug-in techniques
LoveLetter	May 2000	Mass mailer targeting all recipients in the victim's address book, in multiple activations
MTX	August 2000	Mass mailer incorporating file infector, sharing network, and backdoor features
Nimda	September 2001	Mass mailer, also incorporating file infector, sharing network, backdoor process, and IIS infector methods

Protecting Against Viruses

- Enterprise virus protection solutions
  - Desktop antivirus programs
  - Virus filters for e-mail servers
  - Network appliances that detect and remove viruses
- Instill good behaviors in users and system administrators
  - Keep security patches and virus signature databases up to date

Backdoor

- Remote access program surreptitiously installed on user computers that allows attacker to control behavior of victim's computer
- Also known as remote access Trojans
- Examples
  - Back Orifice 2000 (BO2K)
  - NetBus
- Detection and elimination
  - Up-to-date antivirus software
  - Intrusion detection systems (IDS)

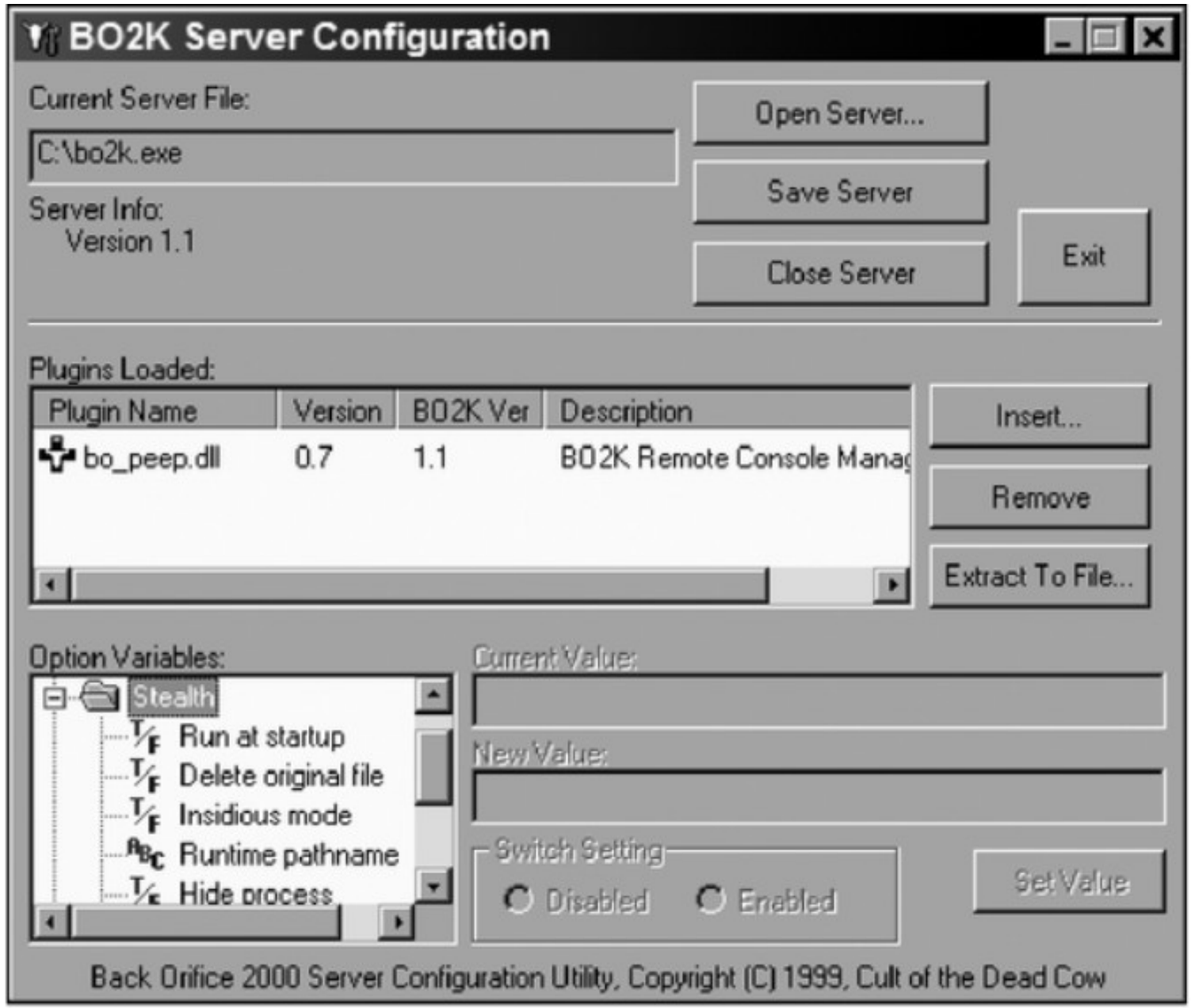


Figure 3-16 BO2K configuration screen

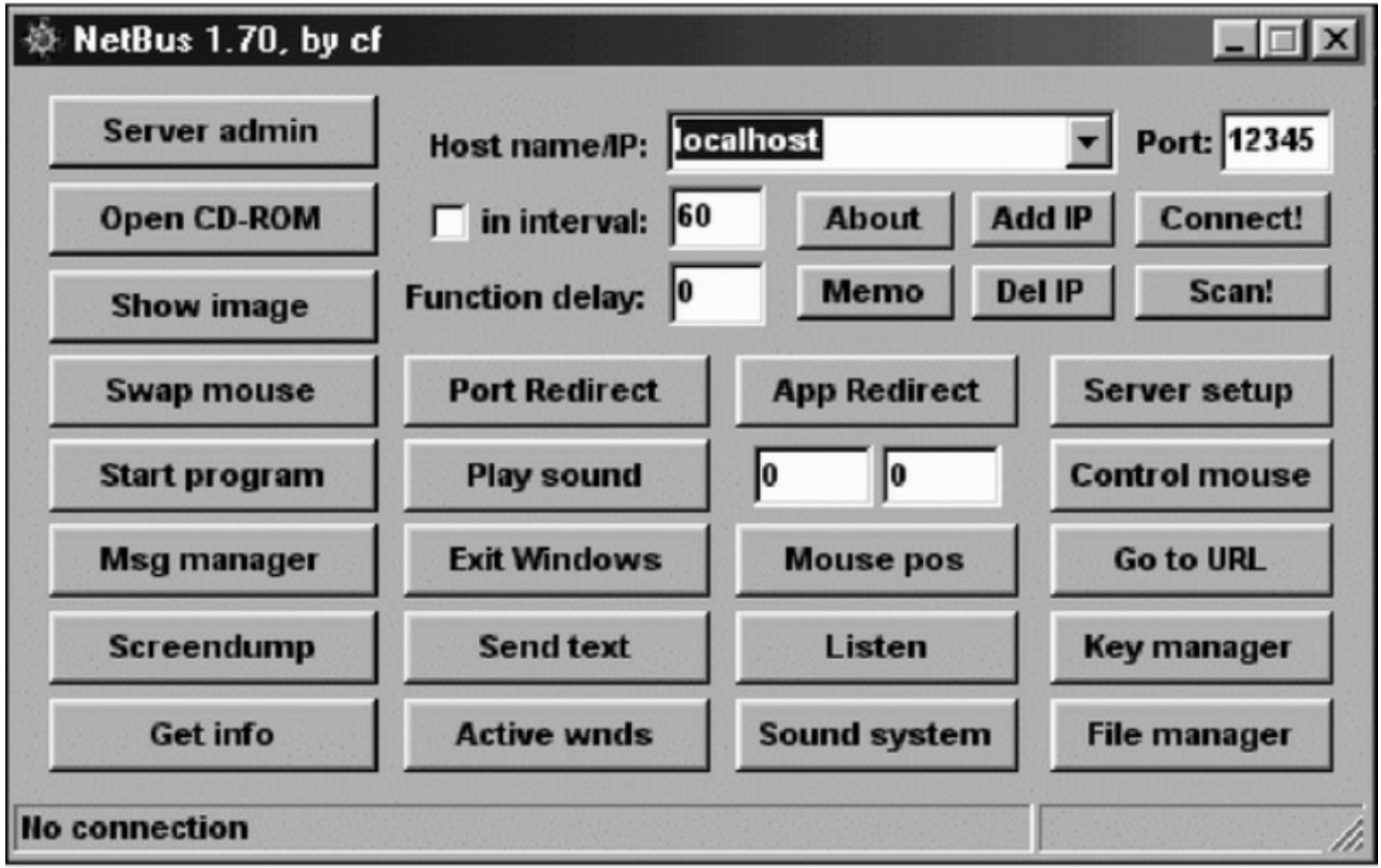


Figure 3-17 NetBus commands

Trojan Horses

- Class of malware that uses social engineering to spread
- Types of methods
  - Sending copies of itself to all recipients in user's address book
  - Deleting or modifying files
  - Installing backdoor/remote control programs

Logic Bombs

- Set of computer instructions that lie dormant until triggered by a specific event
- Once triggered, the logic bomb performs a malicious task
- Almost impossible to detect until after triggered
- Often the work of former employees
- For example: macro virus
  - Uses auto-execution feature of specific applications

Worms

- Self-contained program that uses security flaws such as buffer overflows to remotely compromise a victim and replicate itself to that system
- Do not infect other executable programs
- Account for 80% of all malicious activity on Internet
- Examples: Code Red, Code Red II, Nimda

Defense Against Worms

- Latest security updates for all servers
- Network and host-based IDS
- Antivirus programs

Chapter Summary

- Mechanisms, countermeasures, and best practices for:
  - Malicious software
  - Denial-of-service attacks
  - Software exploits
  - Social engineering
  - Attacks on encrypted data