

Reti di Calcolatori

Tipi di Attacchi Informatici

Giorgio Ventre

Gruppo di Ricerca sull'Informatica Distribuita
Dipartimento di Informatica e Sistemistica
Università di Napoli Federico II

Corso di Reti di Calcolatori II – Anno accademico 2004/2005

Dipartimento di Informatica e Sistemistica, Università di Napoli Federico II

Nota di Copyright

Quest'insieme di trasparenze è stato ideato e realizzato dai ricercatori del Gruppo di Ricerca sull'Informatica Distribuita del Dipartimento di Informatica e Sistemistica dell'Università di Napoli e del Laboratorio Nazionale per la Informatica e la Telematica Multimediali. Esse possono essere impiegate liberamente per fini didattici esclusivamente senza fini di lucro, a meno di un esplicito consenso scritto degli Autori. Nell'uso dovrà essere esplicitamente riportata la fonte e gli Autori. Gli Autori non sono responsabili per eventuali imprecisioni contenute in tali trasparenze né per eventuali problemi, danni o malfunzionamenti derivanti dal loro uso o applicazione.

Corso di Reti di Calcolatori II – Anno accademico 2004/2005

Dipartimento di Informatica e Sistemistica, Università di Napoli Federico II

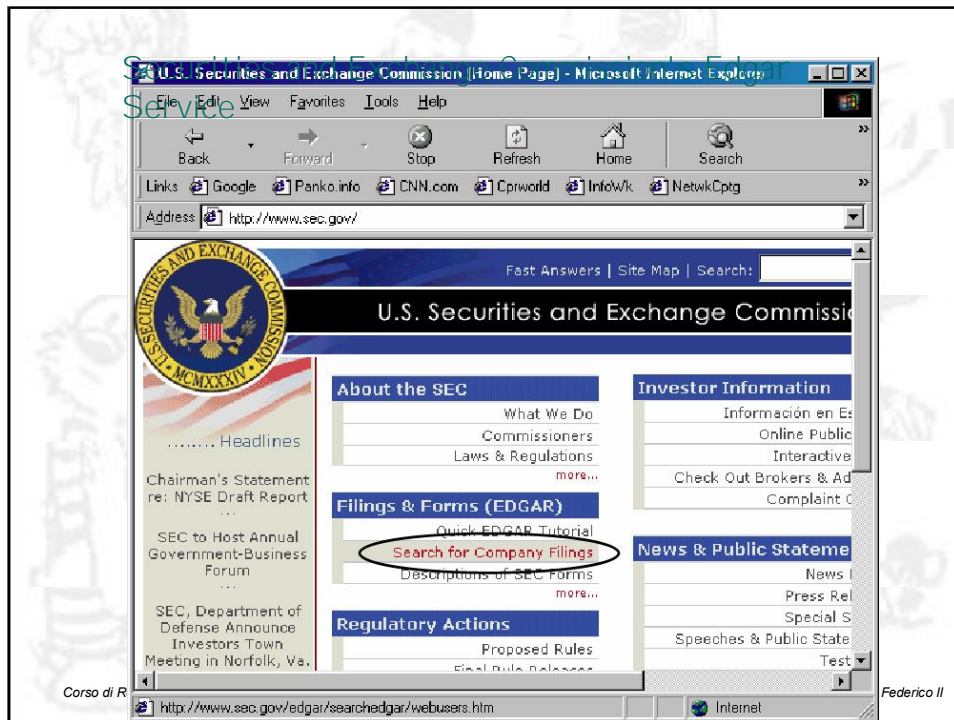
Targeted System Penetration (Break-In Attacks)

I Unobtrusive Information Collection

- » Do research before sending any packets into the network
 - Use in social engineering attacks
 - Use as background for packet attacks
- » Corporate website
- » Trade press (often online and searchable)
- » Securities and Exchange Commission (SEC) web-enabled Internet financial database

Corso di Reti di Calcolatori II – Anno accademico 2004/2005

Dipartimento di Informatica e Sistemistica, Università di Napoli Federico II



Targeted System Penetration (Break-In Attacks)

| Unobtrusive Information Collection

» Whois database

- Information about responsible person
- Information about IP addresses of DNS servers, to find firm's IP address block
- Easy if assigned a classful address block
- Difficult is CIDR address block or a block of ISP addresses

Corso di Reti di Calcolatori II – Anno accademico 2004/2005

Dipartimento di Informatica e Sistemistica, Università di Napoli Federico II

Whois Entry for Pukanui.Com (from www.netsol.com)

- | Registrant:
- | Panko, Ray ([PUKANUI-DOM](#))
- | 1000 Pukanui St.
- | Honolulu, HI 96821
- | US

- | Domain Name: PUKANUI.COM

- | Administrative Contact:
- | Panko, Ray ([RP17477](#))
- | Ray@Panko.com

- | 1000 Pukanui St.
- | Honolulu, HI 96821
- | US
- | (808) 956-8111

Corso di Reti di Calcolatori II – Anno accademico 2004/2005

Dipartimento di Informatica e Sistemistica, Università di Napoli Federico II

Whois Entry for Pukanui.Com (from www.netsol.com)

Registrant:
 Technical Contact:
 VeriSign, Inc. (HOST-ORG)
 namehost@WORLDNIC.NET
 VeriSign, Inc.
 21355 Ridgetop Circle
 Dulles, VA 20166
 US
 1-888-642-9675 fax: - namehost@worldnic.net

 Record expires on 07-Jul-2003
 Record created on 07-Jul-2001
 Database last updated on 7-Jun-2002 15:07:22 EDT.

Domain servers in listed order:

NS76.WORLDNIC.COM	216.168.225.216
NS75.WORLDNIC.COM	216.168.225.215

DNS Servers

Classful IP Address Allocations

Class	Initial IP Address in Class	Last IP Address in Class	Size or Network Part	Addresses in Block Allocated to Firm
A	0.0.0.1	127.255.255.254	8	16,777,214
B	128.0.0.1	191.255.255.254	16	65,534
C	192.0.0.1	223.255.255.254	24	254

Example

- » Suppose DNS server is 128.171.17.1
- » Must be a Class B address block (from table lookup)
- » Therefore, the network part is 16 bits: 128.171
- » Address block must be 128.171.0.1 to 128.171.255.254

Targeted System Penetration (Break-In Attacks)

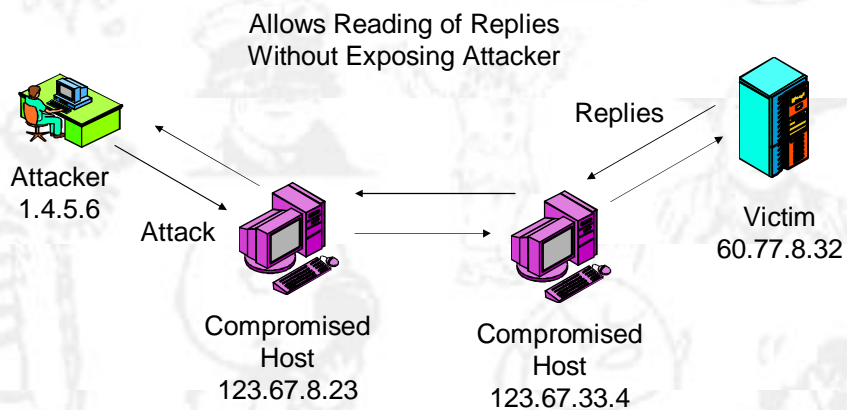
| IP Address Spoofing

- » Put false IP addresses in outgoing attack packets
 - Attacker is blind to replies
- » Use series of attack platforms

Corso di Reti di Calcolatori II – Anno accademico 2004/2005

Dipartimento di Informatica e Sistemistica, Università di Napoli Federico II

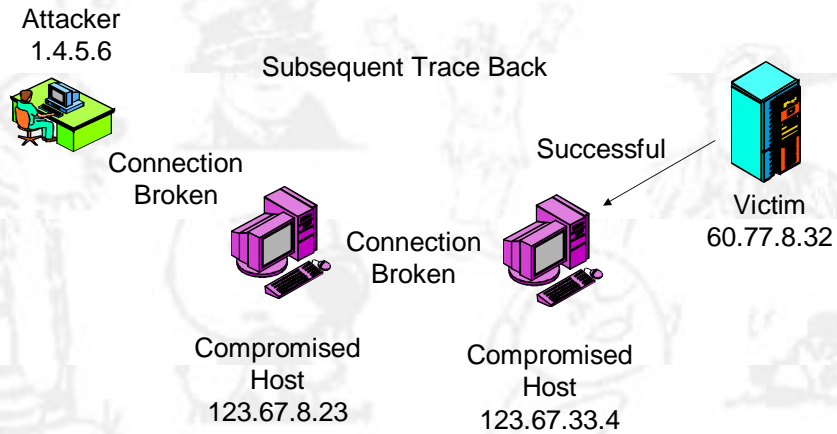
Using a Chain of Attack Hosts



Corso di Reti di Calcolatori II – Anno accademico 2004/2005

Dipartimento di Informatica e Sistemistica, Università di Napoli Federico II

Using a Chain of Attack Hosts



Corso di Reti di Calcolatori II – Anno accademico 2004/2005

Dipartimento di Informatica e Sistemistica, Università di Napoli Federico II

Targeted System Penetration (Break-In Attacks)

| Host Scanning

- » To identify IP addresses of potential victims
- » Ping individual hosts
- » Ping all IP addresses in block for live IP addresses

Corso di Reti di Calcolatori II – Anno accademico 2004/2005

Dipartimento di Informatica e Sistemistica, Università di Napoli Federico II

Ping at the Windows Command Prompt

```
Microsoft Windows [Version 5.00.5923.551]
(c) Copyright 1981-1999 Microsoft Corporation. All rights reserved.

C:\WINDOWS>ping 128.171.17.8

Pinging 128.171.17.8 with 32 bytes of data:

Reply from 128.171.17.8: bytes=32 time=22ms TTL=117
Reply from 128.171.17.8: bytes=32 time=26ms TTL=117
Reply from 128.171.17.8: bytes=32 time=28ms TTL=117
Reply from 128.171.17.8: bytes=32 time=34ms TTL=117

Ping statistics for 128.171.17.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 22ms, Maximum = 34ms, Average = 27ms

C:\WINDOWS>
```

Ping Scanning With Ping Sweep

PingSweep

File Options Help

Starting IP Address: 1
Ending IP Address: 1

1. Enter IP Address Range (Hidden) 2. Scan

IP Address	Response Time	DNS Lookup
1	57 ms	
1	26 ms	
1	31 ms	
1	24 ms	
1	18 ms	
1	20 ms	
1	22 ms	
1	19 ms	

3. Responding IP Addresses (Hidden) 4. Host Names of Responding Hosts If in DNS Server (Hidden)

Scan Completed Scan **100%** DNS **100%** 30

Targeted System Penetration (Break-In Attacks)

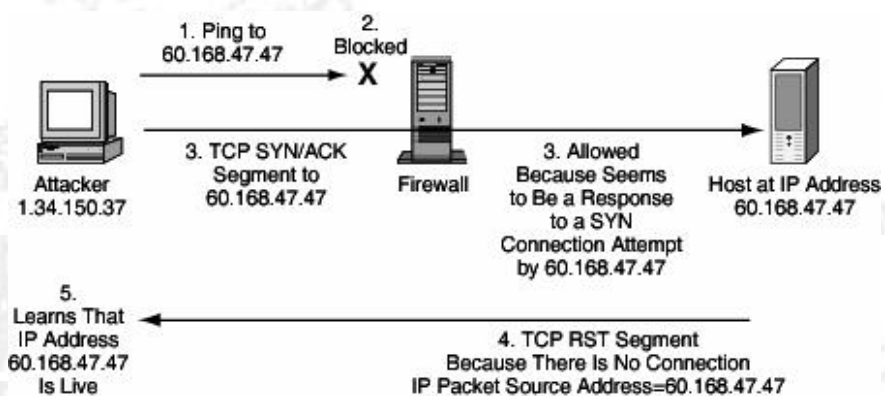
Host Scanning

- » Ping often is blocked by firewalls
- » Send TCP SYN/ACK to generate RST segments
 - These are carried in IP packets that reveal the potential victim's IP address
- » Other RST-generating attacks (SYN/FIN segments)

Corso di Reti di Calcolatori II – Anno accademico 2004/2005

Dipartimento di Informatica e Sistemistica, Università di Napoli Federico II

TCP SYN/ACK Host Scanning Attack



Corso di Reti di Calcolatori II – Anno accademico 2004/2005

Dipartimento di Informatica e Sistemistica, Università di Napoli Federico II

Targeted System Penetration (Break-In Attacks)

| Network Scanning

- » To learn about router organization in a network
- » Send Traceroute messages (Tracert in Windows systems)

Targeted System Penetration (Break-In Attacks)

| Port Scanning

- » Most break-ins exploit specific services
 - For instance, IIS webservers
 - Services listen for connections on specific TCP or UDP ports (HTTP=80)
- » Scan servers for open ports
 - Send SYN segments to a particular port number
 - Observe SYN/ACK or reset (RST) responses

Targeted System Penetration (Break-In Attacks)

| Port Scanning

- » May scan for all well-known TCP ports (1024) and all well-known UDP ports (1024)
- » Or may scan more selectively
- » Scan clients for Windows file sharing ports (135-139)

Targeted System Penetration (Break-In Attacks)

| Fingerprinting

- » Identify a particular operating system or application program and (if possible) version
 - For example, Microsoft Windows 2000 Server
 - For example, BSD LINUX 4.2
 - For example, Microsoft IIS 5.0
- » Useful because most exploits are specific to particular programs or versions

Targeted System Penetration (Break-In Attacks)

| Fingerprinting

» Active fingerprinting

- Send odd messages and observe replies
- Different operating systems and application programs respond differently
- Odd packets may set off alarms

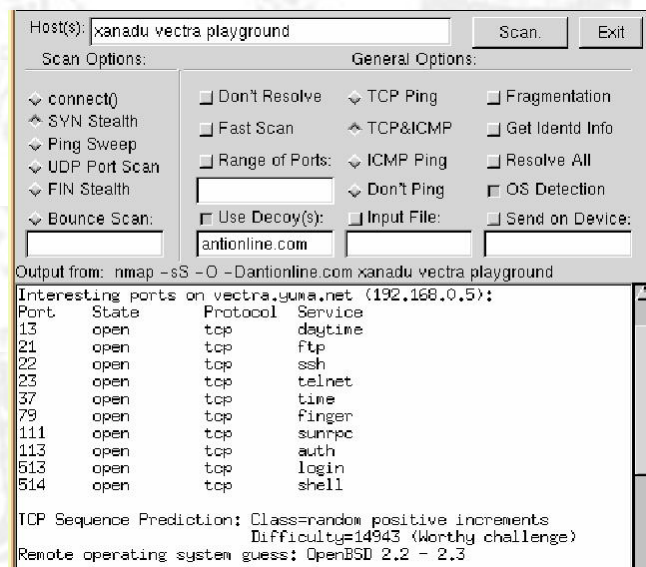
Targeted System Penetration (Break-In Attacks)

| Fingerprinting

» Passive fingerprinting

- Read packets and look at parameters (TTL, window size, etc.)
 - | If TTL is 113, probably originally 128. Windows 9X, NT 4.0, 2000, or Novell NetWare
 - | Window size field is 18,000. Must be Windows 2000 Server
- Less precise than active fingerprinting

NMAP Port Scanning and Operating Systems Fingerprinting



Host(s): xanadu vectra playground [Scan] [Exit]

Scan Options: General Options:

- connect() Don't Resolve TCP Ping Fragmentation
- SYN Stealth Fast Scan TCP&ICMP Get Identd Info
- Ping Sweep Range of Ports: ICMP Ping Resolve All
- UDP Port Scan Don't Ping OS Detection
- FIN Stealth Bounce Scan: Use Decoy(s): Input File: Send on Device:

Output from: nmap -sS -O -Dantionline.com xanadu vectra playground

Interesting ports on vectra.yuma.net (192.168.0.5):

Port	State	Protocol	Service
13	open	tcp	daytime
21	open	tcp	ftp
22	open	tcp	ssh
23	open	tcp	telnet
37	open	tcp	time
79	open	tcp	finger
111	open	tcp	sunrpc
113	open	tcp	auth
513	open	tcp	login
514	open	tcp	shell

TCP Sequence Prediction: Class=random positive increments
Difficulty=14943 (Worthy challenge)
Remote operating system guess: OpenBSD 2.2 - 2.3

Corso di Reti di Calcolatori II – Anno accademico 2004/2005

Dipartimento di Informatica e Sistemistica, Università di Napoli Federico II

Targeted System Penetration (Break-In Attacks)

- | **Stealth scanning**
 - » Scan fewer systems and ports and/or scan more slowly to avoid detection

Corso di Reti di Calcolatori II – Anno accademico 2004/2005

Dipartimento di Informatica e Sistemistica, Università di Napoli Federico II

Targeted System Penetration (Break-In Attacks)

| The Break-In

» Password Guessing

- Seldom works because attacker is locked out after a few guesses

» Exploits that take advantage of known vulnerabilities that have not been patched

- Exploits are easy to use
- Frequently effective
- The most common break-in approach today

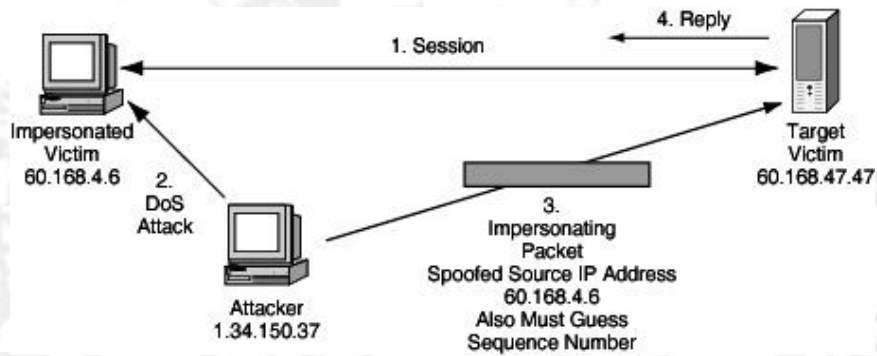
Targeted System Penetration (Break-In Attacks)

| The Break-In

» Session hijacking

- Take over an existing TCP communication session
- Difficult to do (must guess TCP sequence numbers), so not commonly done

Session Hijacking



Corso di Reti di Calcolatori II – Anno accademico 2004/2005

Dipartimento di Informatica e Sistemistica, Università di Napoli Federico II

Targeted System Penetration (Break-In Attacks)

| After the Break-In

- » Install rootkit
 - Usually downloaded through trivial file transfer protocol (TFTP)
- » Erase audit logs
- » Create backdoors for reentry if original hacking vulnerability is fixed
 - Backdoor accounts
 - Trojanized programs that permit reentry

Corso di Reti di Calcolatori II – Anno accademico 2004/2005

Dipartimento di Informatica e Sistemistica, Università di Napoli Federico II

Targeted System Penetration (Break-In Attacks)

| After the Break-In

- » Weaken security
- » Unfettered access to steal information
- » Install victimization software
 - Keystroke capture programs
 - Spyware
 - Remote Administration Trojans (RATs)
 - Attack software to use against other hosts

Corso di Reti di Calcolatori II – Anno accademico 2004/2005

Dipartimento di Informatica e Sistemistica, Università di Napoli Federico II

Denial-of-Service (DoS) Attacks

| Introduction

- » Attack on availability
- » Act of vandalism

| Single-Message DoS Attacks

- » Crash a host with a single attack packet
- » Examples: Ping-of-Death, Teardrop, and LAND
- » Send unusual combination for which developers did not test

Corso di Reti di Calcolatori II – Anno accademico 2004/2005

Dipartimento di Informatica e Sistemistica, Università di Napoli Federico II

Denial-of-Service (DoS) Attacks

| Flooding Denial-of-Service Attacks

» SYN flooding

- Try to open many connections with SYN segments
- Victim must prepare to work with many connections
- Victim crashes if runs out of resources; at least slows down
- More expensive for the victim than the attacker

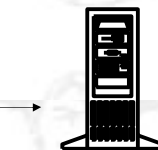
Corso di Reti di Calcolatori II – Anno accademico 2004/2005

Dipartimento di Informatica e Sistemistica, Università di Napoli Federico II

SYN Flooding DoS Attack


Attacker
1.34.150.37

SYN SYN SYN SYN SYN



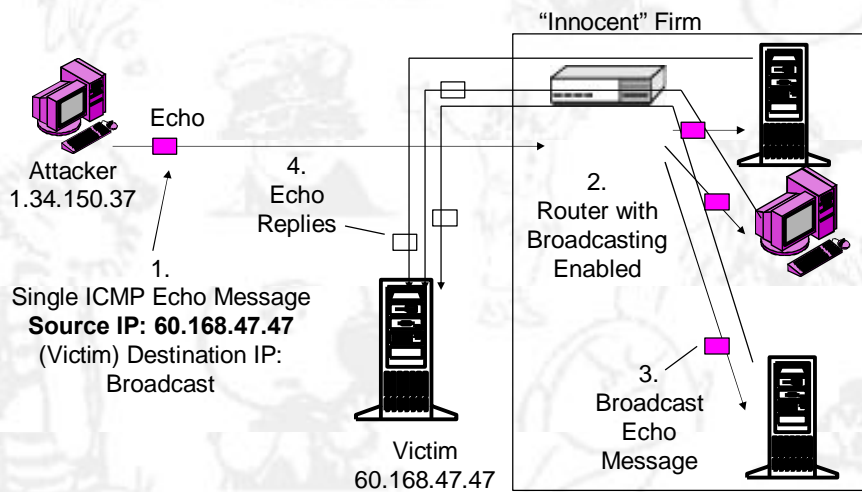
Victim
60.168.47.47

Attacker Sends Flood of SYN Segments
Victim Sets Aside Resources for Each
Victim Crashes or Victim Becomes Too
Overloaded to Respond to the SYNs
from Legitimate Uses

Corso di Reti di Calcolatori II – Anno accademico 2004/2005

Dipartimento di Informatica e Sistemistica, Università di Napoli Federico II

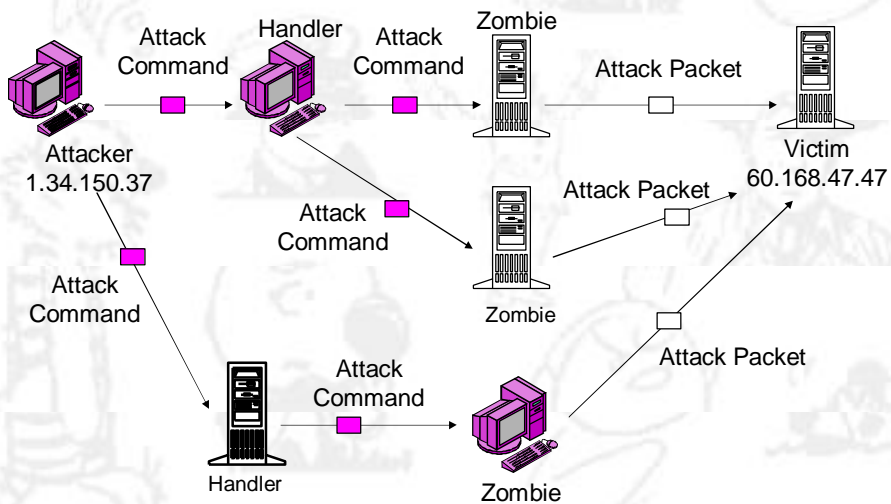
Smurf Flooding DoS Attack



Corso di Reti di Calcolatori II – Anno accademico 2004/2005

Dipartimento di Informatica e Sistemistica, Università di Napoli Federico II

Distributed Denial-of-Service (DDoS) Attack



Corso di Reti di Calcolatori II – Anno accademico 2004/2005

Dipartimento di Informatica e Sistemistica, Università di Napoli Federico II

Denial-of-Service (DoS) Attacks

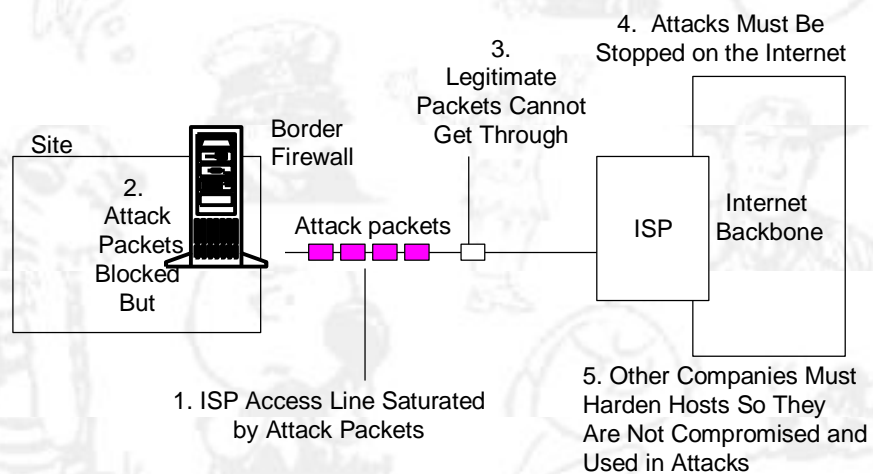
Stopping DoS Attacks

- » Ingress filtering to stop attack packets (Figure 4-14)
- » Limited ability of ingress filtering because link to ISP might become overloaded
- » Egress filtering by attacker's company or ISP
- » Requires cooperating from attacker's company or ISP
- » Requires a community response; victim cannot do it alone

Corso di Reti di Calcolatori II – Anno accademico 2004/2005

Dipartimento di Informatica e Sistemistica, Università di Napoli Federico II

The Difficulty of Stopping DoS Attacks



Corso di Reti di Calcolatori II – Anno accademico 2004/2005

Dipartimento di Informatica e Sistemistica, Università di Napoli Federico II

Malicious Software (Malware)

- | Malware: Malicious software
- | Essentially an automated attack robot capable of doing much damage
- | Usually target-of-opportunity attacks

Malicious Software (Malware)

- | Types of malware
 - » Viruses: infect files or system sectors on disk
 - Attach themselves to executable programs or to disk system sectors (mostly the former)
 - Infected file must be executed for virus to be able to work
 - » Worms: propagate by themselves between hosts

Malicious Software (Malware)

| Types of malware

» Payloads

- Malicious: designed to do damage
- “Benign” may do damage accidentally

Malicious Software (Malware)

| Types of malware

» Active Content in Webpages, HTML E-Mail Bodies

- HTML scripts or small programs (applets)
- Attack directly when clicked on or download a malicious program
- User can turn off active content execution, but webpage functionality will be reduced

» Non-mobile malware

- Trojan horses, etc.

Malicious Software (Malware)

| Types of malware

- » Blended threats combine attack vectors and after-attack damage tools
 - Propagate in multiple ways: as viruses, worms and active content
 - Afterward, do damage directly, and download non-mobile attack programs

Malicious Software (Malware)

| Viruses

- » Executable versus macro viruses
 - Executable viruses attach to executable programs (traditional)
 - Macro viruses attach as macros (series of commands) to data file; executed when file is opened

Malicious Software (Malware)

| Viruses

» Propagation vectors

- Exchange floppy disks (rare)
- E-mail attachments
 - | E-mail offers easy attachment delivery
 - | 90% of viruses spread via e-mail attachments today

Malicious Software (Malware)

| Viruses

» Propagation vectors

- E-mail attachments
 - | An epidemic: virus in every 200 to 400 e-mail messages
 - | Some users open attachments from people they trust

Malicious Software (Malware)

| Viruses

» Propagation vectors

– E-mail attachments

- | But good people get viruses
- | Viruses send e-mail pretending to be coming from victim
- | Should open e-mail attachments only if specifically expected and still scan with updated virus program
- | HTML bodies may execute malware automatically

Corso di Reti di Calcolatori II – Anno accademico 2004/2005

Dipartimento di Informatica e Sistemistica, Università di Napoli Federico II

Malicious Software (Malware)

| Viruses

» Propagation vectors

- IRC and instant messaging (IM)
- FTP and website downloads

Corso di Reti di Calcolatori II – Anno accademico 2004/2005

Dipartimento di Informatica e Sistemistica, Università di Napoli Federico II

Malicious Software (Malware)

| Antivirus Protection

» Location for Filtering

- On clients (often disabled by users)
- On mail servers (does not require user compliance)
- Outsourced e-mail scanning outside the firm (advantages of scale and experience)

Malicious Software (Malware)

| Antivirus Protection

» Scanning Method

- Signature scanning (characteristic sequence of commands for a particular virus)
 - | Dominant scanning method today
- Behavioral scanning (what the virus tries to do, for instance reformat the hard drive)
 - | Can stop new viruses and worms
 - | Many false alarms and misses

Malicious Software (Malware)

| Antivirus Protection

» Two nightmares for antivirus professionals

– Flash viruses that spread too rapidly for signatures to be developed

| Not a theoretical concern. In 2001, Nimda became the most widespread Internet virus/worm within 22 minutes!

| Behavioral scanning and outsourcing firms that see many instances quickly will become important

Corso di Reti di Calcolatori II – Anno accademico 2004/2005

Dipartimento di Informatica e Sistemistica, Università di Napoli Federico II

Malicious Software (Malware)

| Antivirus Protection

» Two nightmares for antivirus professionals

– Metamorphic viruses

| Instead of placing their code at the end of the infected file, they place it throughout the file

| Might make signature detection inaccurate

| Might make signature detection too slow to be workable

Corso di Reti di Calcolatori II – Anno accademico 2004/2005

Dipartimento di Informatica e Sistemistica, Università di Napoli Federico II

Malicious Software (Malware)

| Antivirus Protection

» Recovery

- Detection and Identification

- Repair

- | Go to the antivirus vendor's website

- | Malware-specific repair program or manual procedure

Malicious Software (Malware)

| Antivirus Protection

» Recovery

- Repair

- | Often, infected programs must be reinstalled-
sometimes the entire operating system

- | Some or all data since the last backup might be lost

- | If damage to data files took place over a period of time, a company might not know when its last clean backup was

- | Extremely time consuming

Malicious Software (Malware)

| Nimda Worm of 2001

- » Highly sophisticated blended threat
- » Spread by infected clients infecting other clients
 - Spread by sending e-mail in client's name (often accepted because receivers recognize and trust the name)
 - Spread by open file shares on client

Malicious Software (Malware)

| Nimda Worm of 2001

- » Spread by infected clients infecting webservers
 - Client scanning for IIS webservers almost constitutes a DoS attack
 - Client infects IIS webserver through backdoors left by previous viruses and worm
 - Client infects IIS webserver through unpatched directory traversal vulnerability

Malicious Software (Malware)

| Nimda Worm

- » Spread by IIS webserver infecting clients with malicious links, often executed automatically when the page is downloaded
- » Trojanizes various files so they are difficult to find and clean out
- » Multiple propagation vectors allowed Nimda to become the Internet's most widespread virus/worm within 22 minutes