SECURING INFORMATION SYSTEMS

(November 7, 2016)

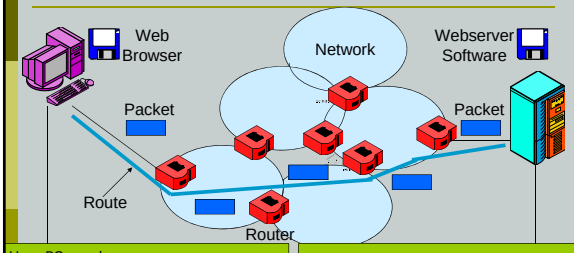
LEARNING GOALS

- Understand security attacks' preps
- Discuss the major threats to information systems.
- Discuss protection systems

The Security Problem

- 2014 Computer Crime and Security Survey
  - 90% of large companies and government agencies reported computer security breach
  - 80% reported sizeable financial loss
  - Only 40% indicated security attacks came from outside the company
  - 85% reported as victim of computer virus

Internet (www) operation - Review



User PC needs:
- Workstation Operating System
- TCP/IP
- Web browser (e.g. Internet Explorer)
- Internet access (e.g. thru an ISP)
- IP Address (e.g. 128.150.50.9)

Webserver needs:
- Network (or Server) Operating System
- TCP/IP
- Domain name (e.g. eiu.edu)
- Internet access
- IP Address (e.g. 139.67.8.3)

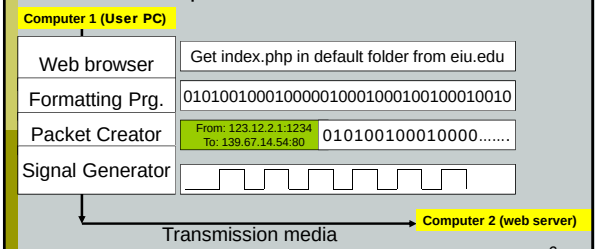
Test Your Internet knowledge

- Your business has 10 employees. You just bought 10 desktop computers and subscribed to Internet DSL service. Which of the following will be needed to connect the computers to the Internet and navigate the World Wide Web?
  a) A server operating system
  b) Workstations operating systems
  c) TCP/IP protocol
  d) Web browsers
  e) Domain names

5

TCP/IP-based Communications

- Requesting a web page from eiu.edu: http://www.eiu.edu



6

TCP/IP Packet

- TCP/IP Packets or computer messages have two parts:
  - Communications protocols
  - Actual message to be delivered

Source IP Address: 123.12.2.1 Source Program: Web Browser 1234 Destination IP Address: 139.67.14.54 Destination Program: Server Program 80 Formatting scheme: ASCII	Get index.php From: server eiu.edu Location: Home directory

Protocols tell the receiving computer:
- Sender's ID
- How to read the message

Message to be delivered

7

Received: from hotmail.com (bay103-f21.bay103.hotmail.com [65.54.174.31])
by barracuda1.eiu.edu (Spam Firewall) with ESMTP id B10BA1F52DC
for <ailia@eiu.edu>; Wed, 8 Feb 2006 18:14:59 -0600 (CST)
Received: from mail pickup service by hotmail.com with Microsoft SMTPSVC;
Wed, 8 Feb 2006 16:14:58 -0800
Message-ID: <BAY103-F2195A2F82610991D56FEC0B1030@phx.gbl>
Received: from 65.54.174.200 by by103fd.bay103.hotmail.msn.com with HTTP;
Thu, 09 Feb 2006 00:14:58 GMT
X-Originating-IP: [192.30.202.14]
X-Originating-Email: [macolas@hotmail.com]
X-Sender: macolas@hotmail.com
In-Reply-To: <10E30E5174081747AF9452F4411465410C5BB560@excma01.cmamdm.enterprise.corp>
X-PH: V4.4@ux1
From: <macolas@hotmail.com>
To: ailia@eiu.edu
X-ASG-Orig-Subj: RE: FW: Same cell#
Subject: RE: FW: Same cell#
Date: Thu, 09 Feb 2006 00:14:58 +0000
Mime-Version: 1.0
Content-Type: text/plain; format=flowed
X-OriginalArrivalTime: 09 Feb 2006 00:14:58.0614 (UTC) FILETIME=[DCA31D60:01C62D0D]
X-Virus-Scanned: by Barracuda Spam Firewall at eiu.edu
X-Barracuda-Spam-Score: 0.00

Hi,

I just wanted to let you know that I have received the packet you sent.

Test Your TCP/IP knowledge

- You have received an email from a potential business partner who pretends to be overseas. Which of the following could help determine the location of the computer he/she used to send the message?
  a) Check the domain name that appears after the @ in the sender's email address
  b) The destination IP address
  c) The Source IP address that appears in the communication protocols' part of the email

From: rlking@gmail.com
To: tewilliams@eiu.edu
Subject: meeting

Hi,

I couldn't make it to the meeting because I am overseas in business.

9

Attack strategy

- Scanning
  - Ping messages (To know if a potential target exist, is connected to the network, and is responsive)
  - Supervisory messages (To know if victim available)
  - Tracert, Traceroute (to know about the route that leads to target)
  - Check the Internet (e.g. www.cert.org) for latest systems vulnerabilities
- Use Brute Force attack or Dictionary attack
  - Trying different usernames and passwords in an attempt to "break" a password and gain an unauthorized access.
- Use Social engineering strategy to get other information
  - By tricking employees to provide passwords, keys and other info. over the telephone
  - By phishing i.e. misleading people to provide confidential info through emails, fake websites, etc.

10

Recent Social engineering targeting EIU

11

Attack strategy (cont.)

- Examining Collected data
  - Users login names and password
  - IP addresses of potential victims
  - What programs are running on target computers
    - Different programs have different weaknesses
  - Potential victim's operating systems, version number, etc.
- Deciding types of attacks
  - Examples:
    - DoS attacks targeting computers with older operating systems
    - Content attacks using identified Open Mail servers & collected emails
    - System intrusion on improperly configured servers
- Launch the attacks

12

Test Your Attacks Strategy Knowledge

- An attacker is preparing an attack. He got the IP address of a potential target. Which of the following could he use in order to determine whether or not the potential target exist, is connected to the network, and is maybe responsive?
  a) Do some scanning using the ***connected*** command
  b) Use the ***tracert*** command
  c) Do some scanning by sending *ping messages* to the target computer
  d) None of the above
- Which of the following has more chance of succeeding?
  a) An attack launched by a hacker using a computer that is not part of the target corporate network.
  b) An attack launched by a hacker using a computer that is part of the target corporate network.
  c) a and b have the same chance of succeeding

13

Major security threats

- Denial of Service (DoS) attacks
  - The attacker makes a target (usually a server) crash in order to deny service to legitimate users
- Content attack
  - Sending messages with illicit or malicious content
- System intrusion
  - Getting unauthorized access to a network

14

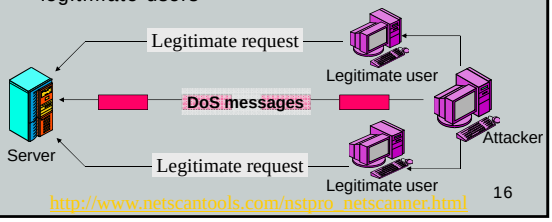
Denial of Service (DoS) attacks

- There are two major types of DoS attacks
  - Single-message DoS attacks
  - Tear-Drop DoS attacks
- In Single-message DoS
  - Target crashes upon receiving a single “deadly” attack message
- In Tear-Drop DoS
  - The target slows down or crashes as a result of receiving more request messages than it can handle.

15

Tear Drop DoS

- Intentionally sending a stream of request messages to a target server in order to
  - Make the target run very slowly or crash
- Objective is to have the target deny service to legitimate users



http://www.netscantools.com/nstpro_netscanner.html

16

Single message attacks: Ping of Death

- Ping of Death attacks take advantage of
  - Some operating systems' inability to handle packets larger than 65 536 bytes
- Attacker sends request messages that are larger than 65,536 bytes (i.e. oversized packets)
- Most operating systems have been fixed to prevent this type of attack from occurring.
  - But attacks occurred recently on Win Server 2003 systems

17

Defense against DoS attacks

- Most DoS attack messages
  - Include protocol settings with fake IP addresses or program numbers that do not match the type of message

Spoofing: using fake source IP address

Program number not consistent with the message supposed to be delivered.

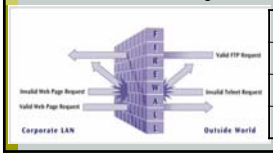
Source IP Address: 10.1.2.1 Source Program: Web Browser 1234 Destination IP Address: 139.67.14.54 Destination Program: Server Program 80 Formatting scheme: ASCII	Get index.php From: server eiu.edu Location: Home directory

Defense systems for protecting against DoS attacks are designed to check messages' protocols part for fake or inconsistent settings. Could be **Packet Firewalls**

18

What is a Packet Firewall?

- A security system that "seats" between a corporate network and an external network.
- A firewall examines each message that is to enter or to leave the corporate network.
- A firewall decides:
  - What messages can enter a network
  - What messages can leave the network



1	If incoming message has fake source IP address, Deny access
2	If incoming message's protocol values indicate a telnet request, Deny access
3	If incoming message's protocol values indicate a file transfer (FTP) request, Allow access
4	If outgoing message's protocol values indicate a request to a prohibited web site, Deny access

19

Test Your Attacks Knowledge

- An attacker has used a single computer to send a stream of attack messages to a server to the point that the server began to operate very slowly. Which of the following does the attacker attempt?
  a) An oversize attack
  b) A Worm attack
  c) A Denial-of-service attack
  d) A Ping-of-Death attack
- An attacker has sent a single oversized attack message to a server loaded with an old operating system. Upon receiving the oversized message, the server crashes. Which of the following happened?
  a) An oversize attack
  b) A Worm attack
  c) A Denial-of-service attack
  d) A Ping-of-Death attack

20

Content attacks

- Incoming messages with:
  - Malicious content (or malware)
    - Viruses (infect files on a single computer)
    - Worms (Propagate across system by themselves)
    - Trojan horses (programs that appear to be benign, but **do damage** or **take control** of a target computer)
  - Illicit content
    - Pornography
    - Sexually or racially harassing e-mails
    - Spams (unsolicited commercial e-mails)

Q: Besides through emails, how can a computer system be a victim of a virus, worm, or Trojan horse attack.

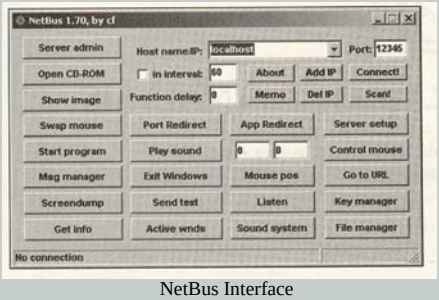
21

Trojan horse

- A computer program
  - That appears as a useful program like a game, a screen saver, etc.
  - But, is really a program designed to **do damage** or to open the door for a hacker to **take control** of the host computer
- When executed, a Trojan horse could
  - Format disks
  - Delete files
  - Allow a remote computer to take control of the host computer. This kind of Trojan is called Back Door.
- NetBus and SubSeven used to be attackers' favorite programs for target remote control

22

Trojan horse



NetBus Interface

23

Review Questions

- What is a type of malware that spreads itself, not just from file to file, but also from computer to computer?
  a) Computer virus
  b) Worm
  c) Trojan horse
  d) None of the above
- What is a malware that opens a way into the network for future attacks?
  a) Open Door
  b) Worm
  c) Back Door
  d) Trojan horse

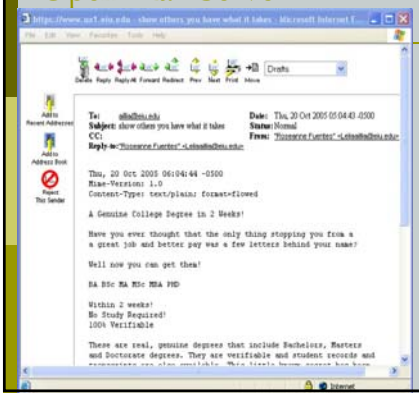
24

Open Mail Server

- Most content attack messages are sent through Open Mail Servers
  - Improperly configured Mail Servers that accept fake outgoing email addresses)

25

Open Mail Server



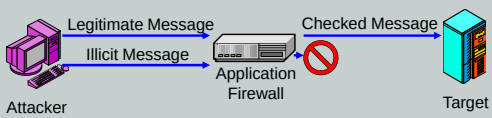
Question: How can you protect a stand-alone computer or a network against malicious content attacks?

26

Protocol Part	Message

Protection against content attacks

- Antivirus controls
  - PC-based antivirus control
  - Network antivirus control
- Application Firewalls
  - Catch every incoming message to check for illicit content in the *Message* part
  - If illicit content detected, message is blocked



27

System Intrusion

- System intrusion: Gaining unauthorized access to a computer system by an intruder
- A hacker is an intruder who breaks into a computer system without authorization.
  - [supposedly] Not causing damage
  - [supposedly] Not stealing information
- A cracker is an intruder who breaks into a computer system to cause damage and/or to steal information
- Script kiddies are young people with little programming skills who use publicly available software to breach into systems

28

Summary Questions

	Book	Notes
1) Distinguish between Tear-drop and ping-of-death attacks.		15
2) What is an illicit content attack? What is the difference between a virus, a worm, and a Trojan horse? How could a stand-alone computer or a network be a victim of an illicit content attack?		21-23
3) What is an Open Mail server? How could you protect a stand-alone computer or a network against illicit content attacks?		25, 26
4) What is a packet firewall? An application firewall?		19, 27
5) What is meant by social engineering? Ping messages?		10

29