Final Exam Review (Part 2)

(Thursday 12/6/2007)

LEARNING GOALS

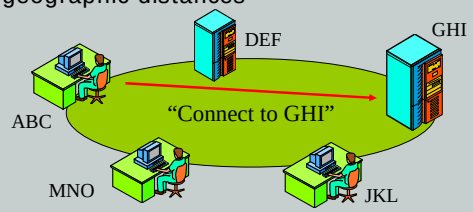
- Understand the advantages of a LAN vs. stand-alone computers.
- Identify hardware and software needed to implement a LAN.
- Choose between P2P and C/S
- Understand security attack strategy
- Recognize different malware threats based on their MO

NETWORKING TECHNOLOGIES

Computer Network

Once connected to the network, the computer (or another device) becomes a network ***node***

- An interconnection of computers and computing equipment using either wires or radio waves over small or large geographic distances



4

Why Networking ?

- Resource sharing
  - Sharing Hardware (printers, CPU, etc.)
  - Sharing Software (programs, data files)
- High reliability
  - Automatic backup of programs and data at different locations)
- Cost saving
  - Through programs sharing
  - Through hardware (e.g. printers) sharing
- Communication tool
  - Internal email service
  - Remote Access service

5

NewContoso Inc. Network

NewContoso Inc. has 25 desktop PCs. All of the PCs have Windows XP Professional installed. The PCs are used as stand-alone computers by the company's employees to perform regular office work like word processing, creating spreadsheet documents, and managing databases. Ten out of the 25 PCs have a 100 Mbps Ethernet NIC. The company is thinking about implementing a LAN to provide shared Internet access to all employees, as well as software sharing and database service through a new model of server computer that is scheduled to be on the market next month. The new server will also be used to provide print service with a non-existing network laser printer. A consultant hired by the company recommended installing a 100BaseTX local area network.

6

NewContoso Inc. Network (cont.)

1) What hardware and software items the company needs to get in order to implement the local area network?
2) Based on the information provided in the case, what network architecture will allow providing the services in a more effective way: P2P or Client/Server? Explain.
3) Assuming that a 100BaseTX switch is used as the central collection point of the network, how many seconds or minutes it will take to send twenty five documents, of 0.5 megabytes each, from one node to another? You should assume that only the two nodes involved are sending/receiving, and no other nodes are sending/receiving during the time the two nodes are involved in the transmission.

7

SECURITY & PRIVACY

8

Received: from hotmail.com (bay103-f21.bay103.hotmail.com [65.54.174.31])
by barracuda1.eiu.edu (Spam Firewall) with ESMTP id B10BA1F52DC
for <aillia@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: aillia@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

9

Attack strategy

- Scanning
  - Ping messages (To know if a potential victim exist, is connected to the network, and is responsive)
  - Supervisory messages (To know if victim available)
  - Tracert, Traceroute (to know about the route that lead to target)
  - Check the Internet (e.g. www.cert.org) for latest systems vulnerabilities
- Use Social engineering strategy to get other information
  - Tricking employees to provide passwords, keys and other info.
  - Misleading people to provide confidential info through email, fake websites, etc.

10

Attack strategy (cont.)

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

11

Major security threats

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

12

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 designed to **damage** or **take control** of the host computer)
  - Illicit content
    - Pornography
    - Sexually or racially harassing e-mails
    - Spams (unsolicited commercial e-mails)

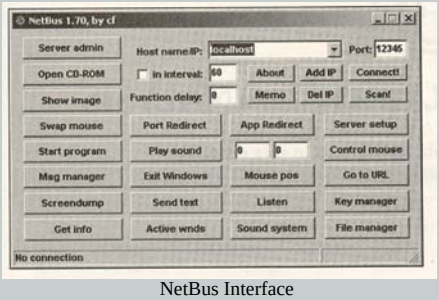
13

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 **damage** or **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
- NetBus and SubSeven used to be attackers' favorite programs for target remote control

14

Trojan horse



NetBus Interface

15

NewContoso Inc. network security

During the last few months, NewContoso Inc. has been the target of a series of computer and network security attacks. As a result, the IT personnel at NewContoso Inc. have been busy working on the computers in order to assess and fix the damage caused by the attacks with the goal of restoring network services. The IT personnel have reported the following incidents.

16

NewContoso Inc. network security (cont.)

Almost all of the company's computers have been infected by a malicious peace of software called Mytob. According to their report, Mytob was able to harvest IP addresses of the LAN nodes by reading the infected computer's ARP table content. It is also able to gather email addresses from the Windows address book. The malware primarily spread through mass-mailing using its own SMTP email engine. Mytob has the potential of deleting files on the infected computers and seriously slowing down communication on the network by consuming the victims' processing capacity.

- Based on the information provided in the case, what type of malware is Mytob? Explain.

_____
_____
_____
_____

17

NewContoso Inc. network security (cont.)

Another malicious peace of software mentioned in the report is called Redlof. It was found on computers running Windows operating systems. Once introduced in a computer system, Redlof attaches itself to the kermel32.dll system file. Then, proceeds by searching the entire system for files with the following extensions: .html, .htm, .asp, .php, .jsp, and .vbs. It then attaches itself to those files. Redlof has the potential of slowing down the processing speed of the infected targets. It can also make the infected computers reboot over an over again.

- Based on the information provided in the case, what type of malware is Redlof? Explain

_____
_____
_____
_____

18

NewContoso Inc. network security (cont.)

A third malware called SpySheriff disguises itself as an anti-spyware program, in order to trick the user of the infected computer to buy the program, by repeatedly informing them of false threats to their system. SpySheriff often goes unnoticed by actual anti-spyware programs. Once installed, SpySheriff can stop the infected computer from connecting to the Internet, and will display an error message reading "The system has been stopped to protect you from Spyware." It blocks several websites, including the ones that have downloadable anti-spyware software. It can also delete some system files.

- Based on the information provided in the case, what type of malware is SpySheriff? Explain

_____
_____
_____
_____

19

Summary Questions

	Book	Notes
1) What are the main advantages of implementing a LAN over using stand-alone computers?		
2) What hardware components are needed to implement a 100BaseTX?		
3) What is the difference between a P2P network and a C/S network?		
4) What are ping messages used for?		
5) What is the Tracert command used for?		
6) What is meant by social engineering?		
7) Distinguish between a virus, a worm, and a Trojan horse.		

20