

Network Security Tools and Defense – An Overview



Jeff Huberty
Business Information Technology Solutions (BITS)
www.bits-solutions.com

Has Your System Been Compromised?



OUTLINE

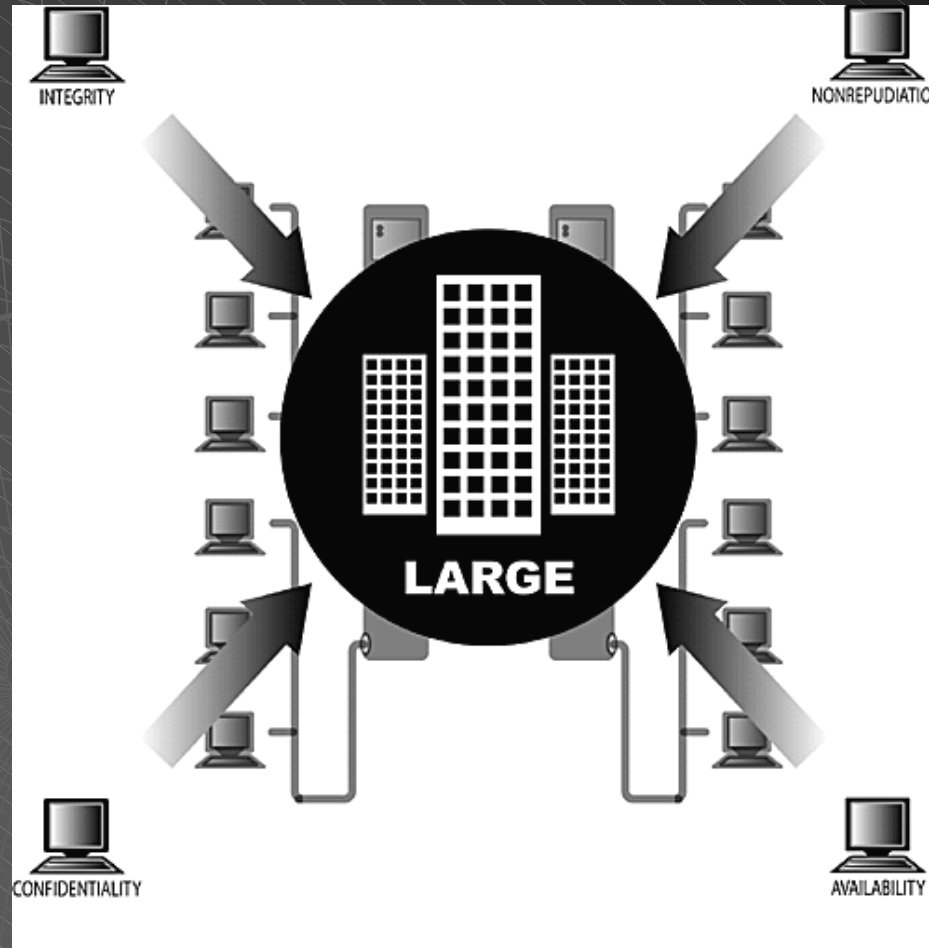
- ◆ CSI/FBI Survey Results
- ◆ Security Goals
- ◆ Security Threats
- ◆ Internet and Network Tools Used
- ◆ What Can We Do? (best practices)
- ◆ Access Control Overview
- ◆ Phases of Attacks and Defenses
- ◆ Small Business and Home Practices

CSI/FBI Survey Results (06/2004)

- ◆ **The Computer Security Institute (CSI) held its ninth annual Computer Crime and Security Survey with the following results:**
 - **Financial losses totaled \$141.5 million (494 respondents); significant decrease from 530 respondents reporting \$202 million last year.**
 - **The most expensive computer crime was denial of service (DoS). Theft of intellectual property, the prior leading category, was the second most expensive last year.**
 - **The vast majority of organizations in the survey do not outsource computer security activities.**
- ◆ **Survey suggests that organizations that raise their level of security awareness have reason to hope for measurable returns on their investments.**

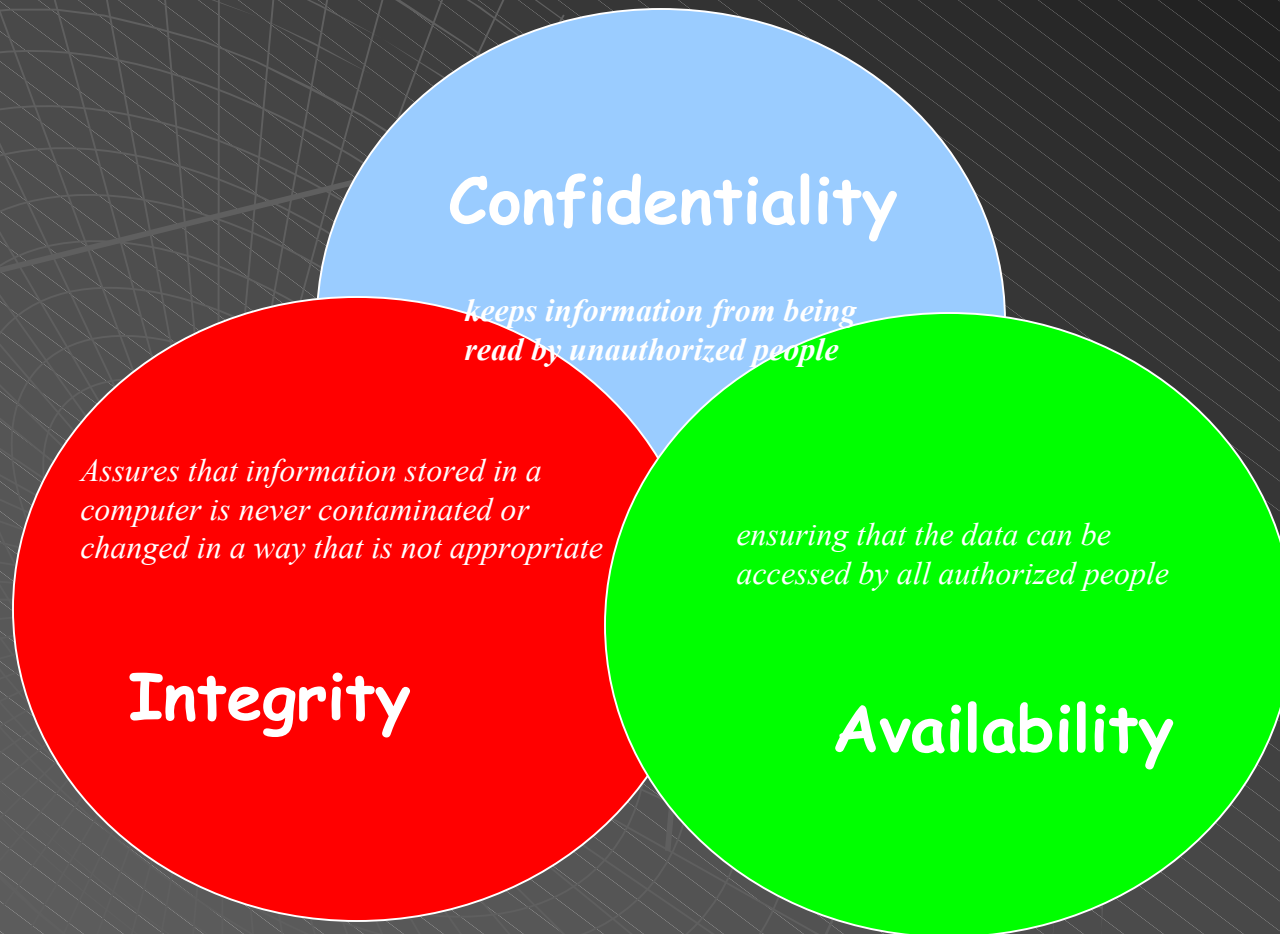
“Men are from Mars, Women are from Venus. Computers are from Hell!”

Four Objectives of Computer Security



*"A bus station is where a bus stops. A train station is where a train stops.
On my desk I have a workstation..."*

Security Goals



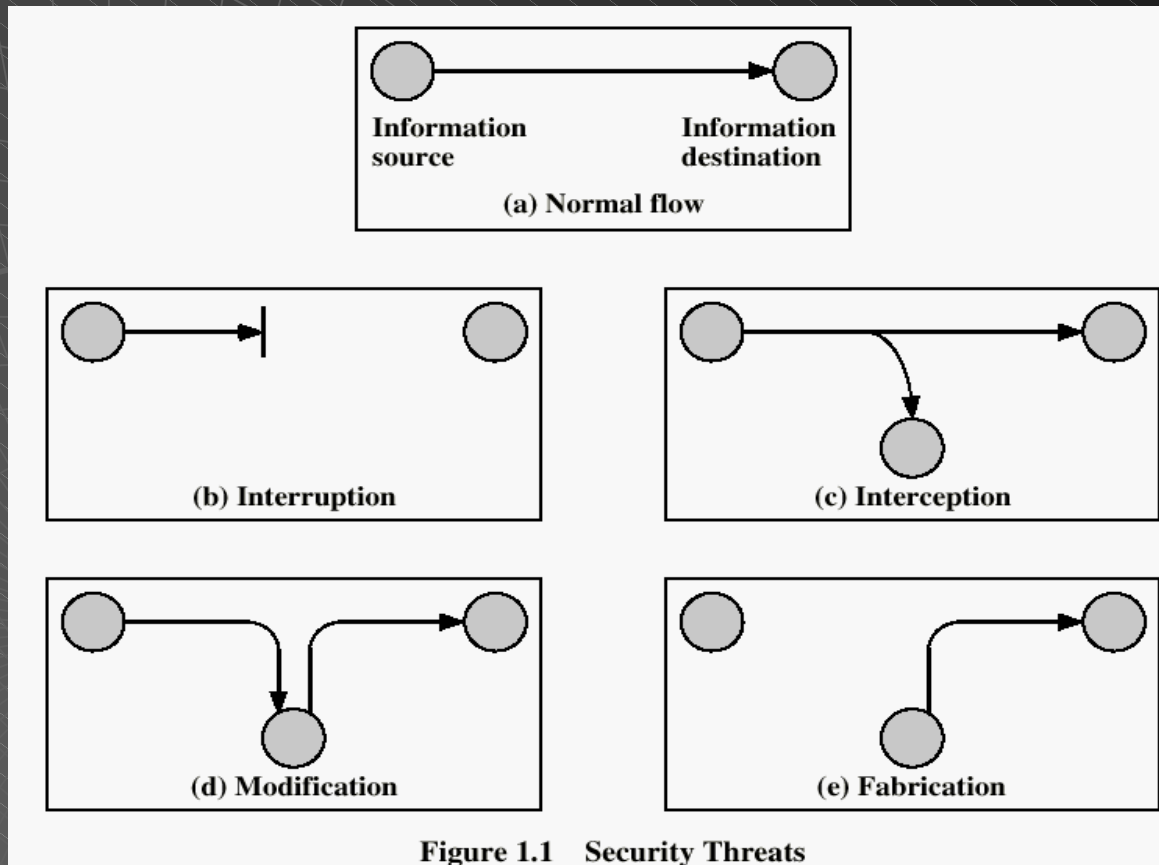
"The nice thing about standards is that there are so many to choose from."

Security Goals

- ◆ **Availability:** addresses issues from fault tolerance to protect against denial of service and access control to ensure that data is available to those authorized to access it.
- ◆ **Confidentiality:** provide protection mechanisms for the data while it is stored and transferred over networks between computers.
- ◆ **Integrity:** keeping data away from those who should not have it and making sure that those who should have it can get it are fairly basic ways to maintain the integrity of the data
- ◆ **NEW! Nonrepudiation:** Allows the formation of binding contracts w/o any paper being printed for written signatures (digital signatures)

“If it wasn't backed-up, then it wasn't important.” — *The sysadmin's moto.*

Security Threats



"The problem with computers is they do what you tell them."

Security Threats – SANS Top 20

(www.sans.org)

◆ Top Vulnerabilities to Windows

- ◆ Web Servers & Services
- ◆ Workstation Service
- ◆ Windows Remote Access Services
- ◆ Microsoft SQL Server (MSSQL)
- ◆ Windows Authentication
- ◆ Web Browsers
- ◆ File-Sharing Applications
- ◆ LSAS Exposures (OSPF)
- ◆ Mail Client
- ◆ Instant Messaging

◆ Top Vulnerabilities to UNIX

- ◆ BIND Domain Name System
- ◆ Web Server
- ◆ Authentication
- ◆ Version Control Systems
- ◆ Mail Transport Service
- ◆ Simple Network Management Protocol (SNMP)
- ◆ Open Secure Sockets Layer (SSL)
- ◆ Misconfiguration of Enterprise Services NIS/NFS
- ◆ Databases
- ◆ Kernel

"A computer's attention span is only as long as its power cord."

Tools Used for Attacking and Auditing Systems on the Net

- ◆ Port Scanners
- ◆ Windows Enumeration
- ◆ Web Hacking
- ◆ Password Cracking/Brute Force
- ◆ Backdoors and Remote Access
- ◆ Simple Source Auditing
- ◆ Combination Systems
- ◆ Auditing
- ◆ Port Redirection
- ◆ Sniffers
- ◆ Wireless Tools
- ◆ War Dialers
- ◆ TCP/IP Stack

"ASCII stupid question, get a stupid ANSI !"

Internet Tools

- Port Scanners (Nmap, SuperScan, IpEye, Fscan, WUPS, Udp_scan)
- Windows Enumeration (Winfingerprint, GetUserInfo, Enum, PsTools)
- Web Hacking
 - Vulnerability Scanners (Whisker, Nikto, Stealth, Twwwscan/Arirang)
 - All-Purpose (Curl, OpenSSL, Stunnel)
 - Application Inspection (Achilles, WebSleuth, Wget)
- Password Cracking/Brute-Force
 - PassFilt.dll and Windows Password Policies
 - PAM and UNIX Password Policies
 - OpenBSD login.conf

"ERROR: Computer possessed; Load EXOR.SYS ? [Y/N]"

Portscan Threat Example

- ◆ Below is a capture of a malicious port scan:

TCPDUMP Capture:

```
535> (DF) [tos 0x10]
20:38:27.470402 66.90.95.X.22 >
66.252.X.2.61627: P 271600:271792(192)
ack 289 win 65535 <nop,nop,timestamp
880842161 1498707535> (DF) [tos 0x10]
20:38:27.470426 66.90.95.X.22 >
66.252.X.2.61627: P 271792:271984(192)
ack 289 win 65535 <nop,nop,timestamp
880842161 1498707535> (DF) [tos 0x10]
20:38:27.470437 66.252.X.2.61627 >
66.90.95.X.22: . ack 260016 win 50180
<nop,nop,timestamp 1498707535
880842155> (DF)
```

This is seen from the Administrators side of the field.

- ◆ ***Here is the view from the attacks side using NMAP:***

Starting nmap 3.75 (<http://www.insecure.org/nmap/>) at 2004-11-30 21:57 EST

Interesting ports on (66.252.X.2):

(The 1655 ports scanned but not shown below are in state: filtered)

| PORT | STATE | SERVICE |
|---------|-------|---------|
| 21/tcp | open | ftp |
| 22/tcp | open | ssh |
| 25/tcp | open | smtp |
| 80/tcp | open | http |
| 113/tcp | open | auth |
| 443/tcp | open | https |

SHOWS us what services are running on this network. An attack could be staged on each or any of the services. A Denial of Service (DoS) attack would target open ports in an attempt to slow/halt the systems connections. An exploit attack would be directed to the service flaws running on that port. I.E. HTTP (Web Browsers) can be buffer overrun with the right knowledge and software.

"The definition of a hacker ? Someone who, after installing a new program, goes immediately into the [Tools][Options] menu."

What If MS Created NMap?

It looks like you are running a port scan.

Would you like help launching a:

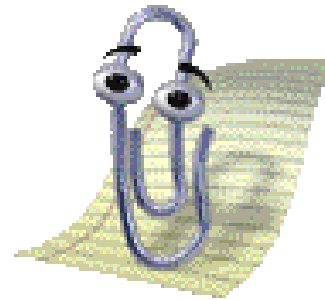
- Connect Scan
- Half-Open Scan (SYN)
- ACK Scan
- FIN Scan

▼ See more...



Options

Search



The target(s) you have selected include addresses registered to Microsoft corporation. This tool is built so that it cannot be used to scan Microsoft's own systems.

However, Microsoft Nmap will automatically redirect your scan to one of Microsoft's adversaries.

Which Microsoft enemy would you like to scan?

- AOL
- Assorted Open Source Site (Slashdot, linux.org, etc.)
- US Department of Justice
- State Attorney General Offices

Options

Search



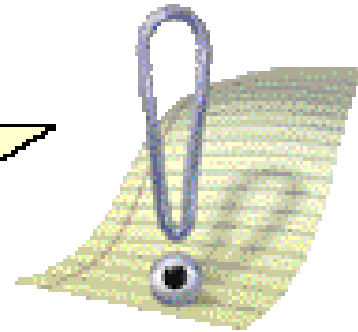
You have discovered a security vulnerability in a Microsoft product.

You can report this issue to Microsoft's product security team. Would you like to report this vulnerability and...

- Be completely ignored (default)
- Receive a friendly form letter from a fictional Microsoft employee full of platitudes about how much we care
- Spend numerous unbillable hours helping Microsoft fix the flaw and never, ever receive public acknowledgement for all your help?
- Get a quick, solid fix from Microsoft and full recognition for your effort

Options

Search



The scan configuration options you have selected violate local laws.

Do you want Microsoft Nmap to:

- Automatically contact your own personal attorney
- Recommend a lawyer to defend you using Microsoft's Lawyer Selection Wizard...

Options

Search



Internet Tools, cont'd

- Password Cracking/Brute Force Tools
 - John the Ripper
 - L0phtCrack
 - Grabbing Windows Password Hashes (PwDump, Lsadbump2, Winhash, Ddumper, XSCAN)
 - Active Brute-Force (SMBGrind, Nbaudit, John the ripper2x)
- Backdoors and Remote Access (VNC, Netbus, Back Orifice, SubSeven, Loki, stcpshell, Knark, AGOBOT, Phatbot, SDBOT)
- Simple Source Auditing (Flawfinder, RATS)
- Combination System Auditing (Nessus, STAT, Retina, Internet Scanner, Tripwire)

"Before software can be reusable it first has to be usable." — Ralph Johnson.

Network Tools

- Port Redirection (datapipe, Fpipe)
- Sniffers (BUTTSniffer, Tcpdump, Windump, Ethereal, Dsniff, Snort)
- Wireless (Netstumbler, AiroPeek)
- War Dialers (ToneLoc, THC-Scan)
- TCP/IP Stack (ISIC, Iptest, Nemesis)

"It's 5.50 a.m.... Do you know where your stack pointer is ?"

What Can We Do?

- ◆ Take steps to increase security awareness
 - Education, training, periodic bulletins, etc., cultivate user acceptance of security technologies that need to be deployed.
- ◆ Policies need to be established and enforced
 - Describe the responsibilities of individuals and groups in safeguarding organizational assets from loss or misuse.
- ◆ IT infrastructure needs to be security-enabled
 - IT and network administrators need to keep themselves informed about security vulnerabilities and fixes, to include best-of-breed technologies and methodologies for coping with security threats.
- ◆ On-going vigilance, in the form of vulnerability assessments must be part of the operational routine
 - Security should be seen as a work in progress and never a finished project. Hackers adapt; so should the organization.

Policies and Settings

Policy

No outside Web access.

Outside connections to Public Web Server Only.

Prevent Web-Radios from eating up the available bandwidth.

Prevent your network from being used for a Smuft DoS attack.

Prevent your network from being tracerouted or scanned.

Firewall Setting

Drop all outgoing packets to any IP, Port 80

Drop all incoming TCP SYN packets to any IP except 150.160.170.180, port 80

Drop all incoming UDP packets - except DNS and Router Broadcasts.

Drop all ICMP packets going to a "broadcast" address (150.160.255.255 or 150.160.0.0).

Drop all incoming ICMP, UDP, or TCP echo-request packets, drop all packets with TTL < 5

"Unix is user-friendly. It's just very selective about who its friends are."

Access Control

- Today almost all systems are protected only by a simple password that is typed in, or sent over a network in the clear. Techniques for guessing passwords:
 - Try default passwords.
 - Try all short words, 1 to 3 characters long.
 - Try all the words in an electronic dictionary(60,000).
 - Collect information about the user's hobbies, family names, birthday, etc.
 - Try user's phone number, social security number, street address, etc.
 - Try all license plate numbers (123XYZ).
- Prevention: Enforce good password selection (j@1H7%!2u4rZ) with more than 10 characters

"The number of the beast — vi vi vi."

Password Gathering

- Look under keyboard, telephone, monitors, etc
- Look in the Rolodex under “X” and “Z”
- Call up pretending to be from “micro-support,” and ask for it.
- “Snoop” a network and watch the plaintext passwords go by.
- Tap a phone line - but this requires a very special modem, UI, VAMP.
- Use a “Trojan Horse” program to record key strokes.

"If debugging is the process of removing software bugs, then programming must be the process of putting them in."

Stages of a Network Intrusion

1. Scan the network to:
 - locate which IP addresses are in use,
 - what operating system is in use,
 - what TCP or UDP ports are “open” (being listened to by Servers).
2. Run “Exploit” scripts against open ports
3. Get access to Shell program which is “suid” (has “root” privileges).
4. Download from Hacker Web site special versions of systems files that will let Cracker have free access in the future without his cpu time or disk storage space being noticed by auditing programs.
5. Use IRC (Internet Relay Chat) to invite friends to the feast, control multiple machines, or just to host warez/P2P files.

"Computers make very fast, very accurate mistakes."

Phase 1: Reconnaissance

◆ ATTACK

- Social Engineering
- Physical Break-In

- Dumpster Diving
- Search the Web
 - ◆ Own Website
 - ◆ Usenet (newsgroups)
- Whois
- DNS

◆ DEFENSE

- User Awareness
- Security Badges, Card Readers, etc.
- Shredder, Move Bins
- Establish policies of what info is allowed on Web Servers
- Update registration data
- Keep additional info to a minimum, restrict zone transfers, use “split DNS”

"To err is human, but for a real disaster you need a computer."

Phase 2: Scanning

◆ ATTACK

- War Dialing
- Network Mapping
- Vulnerability
- Intrusion

◆ DEFENSE

- Modem Policies
- Hardening (close unused ports)
- Patch, Run Tools Against Own Net
- Intrusion Detection System

"hAS aNYONE sEEN MY cAPSLOCK KEY ?"

Phase 3: Gaining Access

◆ ATTACK

- Script Kiddie
- Sophisticated
 - ◆ Stack/Buffer Overflow
 - ◆ Password
 - ◆ Web Apps

◆ DEFENSE

- Patch, Event Logs
- IDS, mailing lists
- Tips discussed later
- DigiSign, Encrypt, dyna session IDs, timestamps

"If brute force doesn't solve your problems, then you aren't using enough."

Phase 3: Access via Network

◆ ATTACK

- Sniffing
- IP Address Spoof
- Session Hijacking

◆ DEFENSE

- Secure protocols, DMZ
- Test via NMap, SSH for UNIX
- Combine everything above

"Artificial Intelligence usually beats natural stupidity."

Phase 3: DDoS

◆ ATTACK

- Stopping Local Svc
- Locally Exhausting Resources
- Remotely Stopping Svcs
- Remotely Exhausting Resources

◆ DEFENSE

- Patches, Proper Privileges (no Adm)
- Principle of Least Privilege
- Patches, static ARP
- TFN2K (DDoS Tool)

"Smith & Wesson — the original point and click interface."

Phase 4: Maintaining Access

◆ ATTACK

- Trojan Horses
- Backdoors (BD)
- BDs in Trojans
- App-Level BD (BO2K)

- Traditional Rootkits

◆ DEFENSE

- ◆ AV Tools and Education are the best form of combat to these elements

- ◆ Hard to guess passwords, security patches, closing unused ports, and defined security programs in place

"Foolproof systems don't take into account the ingenuity of fools." — Gene Brown.

Phase 5: Duck and Cover

◆ ATTACK

- Altering Log Files
- (Unix/Windows)
- Altering Accounting Files in UNIX
- Altering UNIX Shell History

◆ DEFENSE

- ◆ Activate Logging
- ◆ Set Proper Permissions
- ◆ Use Separate Logging Server
- ◆ Encrypt Log Files
- ◆ Making Log Files Append Only
- ◆ Protecting Log Files with Write-Once Media
- ◆ Create Hidden Files and Directories

"Dude, I hate to be the bearer of bad news, but I'm afraid you've been hacked — the FTP server at 127.0.0.1 has all your personal files. See for yourself; just log in with your

Spyware, Viruses, Trojans (Oh, My!)

- Spyware - software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes; latest purposes are more sinister
- Virus - code that copies itself into other programs
- Payload - harmful things it does, after it has had time to spread.
- Worm - a program that replicates itself across the network (usually riding on email messages or attached documents (e.g., macro viruses).
- Trojan Horse - instructions in an otherwise good program that cause bad things to happen (sending your data or password to an attacker over the net).
- Logic Bomb - malicious code that activates on an event (e.g., date).
- Trap Door (or Back Door) - undocumented entry point written into code for debugging that can allow unwanted users.

"Enter any 11-digit prime number to continue..."

What Can I Do?

- Have a well-known virus protection program, configured to scan disks and downloads automatically for known viruses.
- Use a well-known firewall program (preferably hardware and software solution)
- Do not execute programs (or "macro's") from unknown sources (e.g., PS files, HyperCard files, MS Office documents, Java, ...), if you can help it.
- Avoid the most common operating systems and email programs, if possible.
- Run *legitimate* anti-spyware programs (Ad-aware SE Personal and Spybot Search and Destroy 1.3 are both free and highly recommended by professionals)
- Conduct monthly/quarterly audits on home/business PCs incorporating:
 - Deletion of temp files (sans .log files) contained in temporary internet folders and temp folders
 - Set security level for macros to *high* (requesting your permission)
 - Resetting IE security to Medium to Medium-High; shorten history settings and temporary internet files
 - Check local installed programs in Add/Remove programs for validity
 - Check Services for bogus service applications
 - Check Event Viewer (security, application, system)

Great Websites

- ◆ Packet Storm Security (packetstorm.security.com)
- ◆ SANS (sans.org)
- ◆ Security Focus Bugtraq Archives (securityfocus.com)
- ◆ @stake Security News (atstake.com/security_news)
- ◆ Security Portal (securityportal.com)
- ◆ 2600 (2600.com)
- ◆ White Hats (whitehats.com)
- ◆ Attrition (attrition.org)
- ◆ Information Security Magazine (infosecuritymagazine.com)
- ◆ CERT (cert.org)

Credits

- ◆ Secured Enterprise: Protecting Your Information Assets; F. Byrnes/P. Proctor, Prentice-Hall PTR (5/2002)
- ◆ Counter Hack; E. Skoudis, Prentice-Hall PTR (2002)
- ◆ Information Week (various articles)
- ◆ Network Security: A Hacker's Perspective; Fadia, Prentice Press (2003)
- ◆ Know Your Enemy: Revealing the Security Tools, Tactics, and Motives of the BlackHat Community; HoneyNet Project; Addison-Wesley (2002)

Login: yes

Password: i dont have one
password is incorrect

Login: yes

Password: incorrect

Any Questions?

