Network Security

Outlines:

- Who's vulnerable
- Who's attacking
- What are the kinds of attacks
- How do we protect ourselves
- What do you do when you've been attacked
- LAB: Famous Attacks and Bots

By: Arash Habibi Lashkari
July - 2010

What is Network Security?

Network security addresses the vulnerabilities to which your organization is uncover as a consequence of being connected to a network.

Who's vulnerable?

- Everyone in your organization who uses computers or networks in the process of doing their job
- Everyone in your organization who is affected by the information stored in computers
- Everyone in your organization
- Outsiders who rely on your organization – your customers

Who's vulnerable?

- Both Servers and End-Users are subject to attack.
  - Web servers, E-mail servers, File servers, Communications servers, Network devices
  - End-users receiving e-mail, visiting web sites, downloading files, participating in online services

Who's vulnerable?

- You are exposed to network security threats by:
  - using e-mail (e.g. viruses, worms)
  - using web-browsers (e.g. malicious applets and scripts)
  - simply being connected to the network (protocol hacks, breaking and entering)

Who's vulnerable?

- 20-year-old man arrested for breaking into two computers of NASA's Jet Propulsion Laboratory.
- Hacking started in 1998
- One computer was used to host chat room devoted to hacking
- Thousands of usernames and passwords were stolen

Reuters News, July 12, 2000

Who's vulnerable?

- ILOVEYOU Virus
- MELISSA Virus
- Anna Kournikova Virus ("Here you have, ;o)") of last week
- Denial of Service attack against Microsoft two weeks ago
- Home users with network connections – dialup or dedicated

Who's attacking?

- Attacks from within
  - "Within" means originating from inside the LAN/intranet, a "trusted source"

Who's attacking?

– "Case studies have shown that a vast majority of attacks originate from within an organization. In fact, some studies state that as much as 70% of all attacks from someone within an organization or from someone with inside information (such as an ex-employee)"

Chris Brenton, Mastering Network Security, c. 1999, SYBEX Network Press, p.6.

Who's attacking?

- Sometimes the damage is done without intent
  - People making mistakes
    - Only give root privileges to people who know what they are doing
  - People experimenting with things they've heard about
    - "I was just testing this downloaded script...."

Who's attacking?

- Sometimes the damage is done on purpose
  - Malicious attacks from disgruntled people (e.g. ex-employees)
  - Snoop attacks from nosey co-workers
  - Acts of vandalism
  - Espionage

Who's attacking?

- Attacks from the Outside
  - "Outside" means originating from anyone/anyplace outside of your LAN/intranet, an unknown source.
  - Sometimes the damage is done without intent....
  - Sometimes the damage is done on purpose.

Who's attacking?

- What do they hope to gain?
  - bragging rights, simply to say "I did it!"
  - theft of information
  - theft of service
  - theft of real assets/money
  - defacement/vandalism
  - destruction of data
  - corruption of data

Who's attacking?

- What do they hope to gain, *continued*
  - corruption of operational systems controlled by computers (phone system, TV systems, etc.)
  - denial of service
  - plant 'bots which can be remotely activated and controlled to accomplish any of the attacks listed above using your machine as the host

What are the kinds of attacks?

- Denial of Service (DoS) attacks
  - DoS attacks have one goal – to knock your service off the net.
    - Crash your host
    - Flood your host
    - Flood the network connecting to your host

What are the kinds of attacks?

- Viruses
  - A computer virus attaches itself to files on the target machine
  - Master Boot Sector/Boot Sector viruses
  - File viruses, Macro viruses
  - Stealth viruses, Polymorphic viruses
  - Hoax Viruses

    http://www.mcafee.com/anti-virus

    http://www.symantec.com/avcenter

What are the kinds of attacks?

- Trojans, Worms and Backdoors
  - Trojans are programs that appear to perform a desirable and necessary function that perform functions unknown to (and probably unwanted by) the user.
  - Worms are memory resident viruses. Unlike a virus, which seeds itself in the computer's hard disk or file system, a worm will only maintain a functional copy of itself in active memory.

What are the kinds of attacks?

- Worms frequently “sleep” until some event triggers their activity - send password file to hacker, send copy of registry to hacker.
- Worms and Trojans are frequently methods by which Backdoors are enabled on a system.
- Backdoors allow hidden access and control of a system (e.g. Back Orifice, BO2K, SubSeven).

What are the kinds of attacks?

- Scanners
  - Programs that automatically detect security weaknesses in remote or local hosts.
  - Tells the hacker:
    - What services are currently running
    - What users own those services
    - Whether anonymous logins are supported
    - Whether certain network services require authentification

What are the kinds of attacks?

- Password Crackers
  - Some actually try to decrypt....
  - Most simply try “brute force” or intelligent “brute force”
    - Dictionary words, days of year, initials
- Social Engineering
  - “This is MIS, I need to fix your e-mail box, what’s your password?”

What are the kinds of attacks?

- Sniffers
  - Devices that capture network packets
  - Extremely difficult to detect because they are passive

What are the kinds of attacks?

- Botnets

  A botnet or robot network is a group of computers running a computer application controlled and manipulated only by the owner or the software source. The botnet may refer to a legitimate network of several computers that share program processing amongst them.

  IRC-Bot, P2p-Bot and HTTP-Bot

How do we protect ourselves?

- One product cannot provide full protection
- The computer networking environment consists of too many different subsystems for one product to provide full protection

How do we protect ourselves?

- Ethernet protocol
- IP protocol
- TCP protocol
- Routing protocols
- Operating Systems
- Presentation protocols - HTML, DHTML, XHTML, XML
- Remote Program execution protocols - VBS, ASP, DCOM, CORBA, JavaScript, Java Applets, Jini
- Applications - MS Outlook, Netscape Communicator, servers (MS IIS, etc.)

How do we protect ourselves?

- Anti-virus software
  - Personal Anti-virus SW on your machine
  - Make sure it is set to scan all executables, compressed files, e-mail, e-mail attachments, web pages
  - Keep your virus information files up to date!!!

How do we protect ourselves?

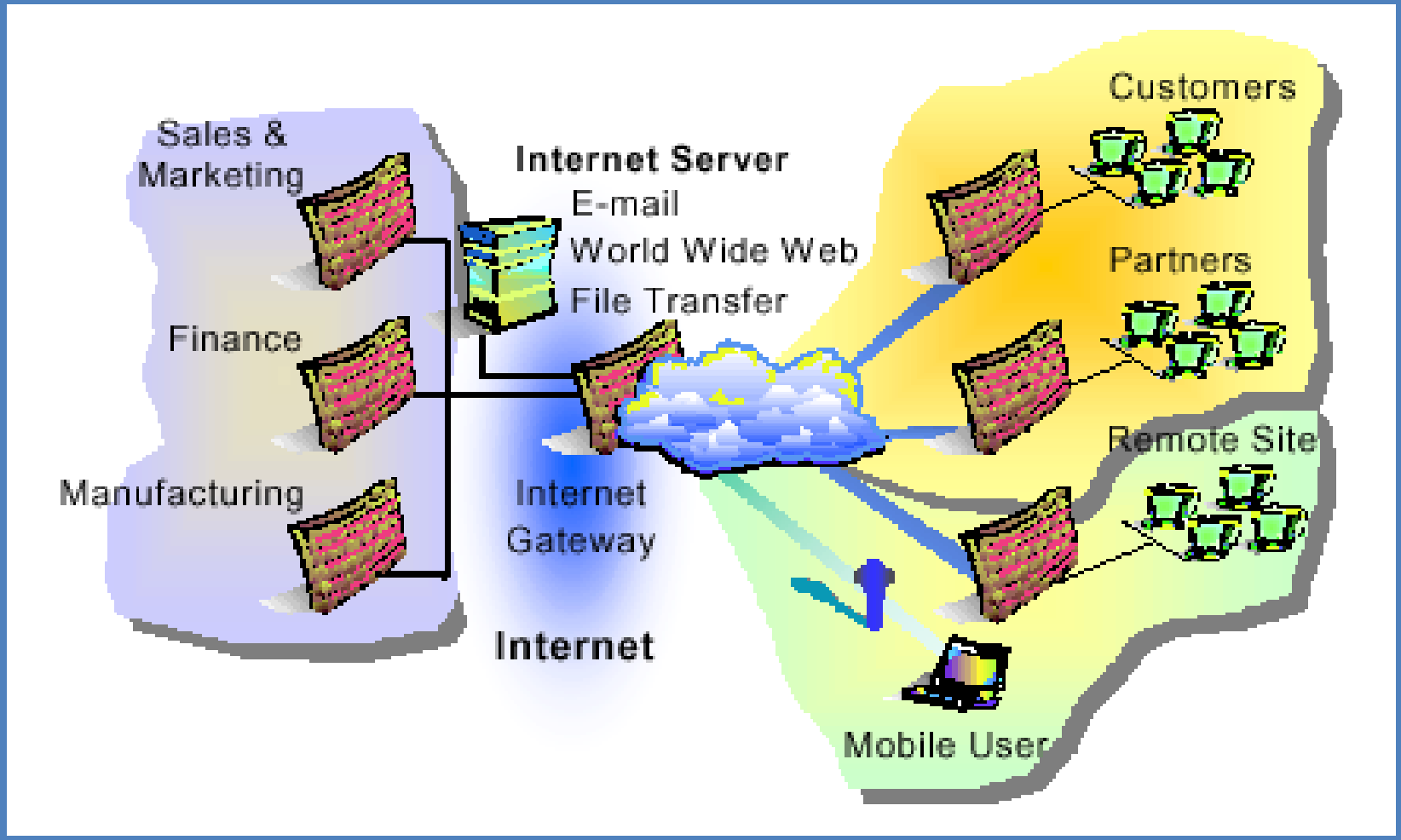
- Firewalls
  - “A combination of hardware and software resources positioned between the local (trusted) network and [an untrusted network]. The firewall ensures that all communication between an organization's network and the Internet connection conforms to the organization's security policy. Firewalls track and control communications, deciding whether to pass, reject, encrypt, or log communications.”

Checkpoint Firewall-1 Administration Guide

How do we protect ourselves?

- Types of Firewalls
  - Static Packet Filtering - a.k.a. Access Control Lists
  - Dynamic Packet Filtering - a.k.a. “Stateful Inspection”
  - Proxy - a.k.a. Application Gateway
    - Non-Transparent
    - Transparent

How do we protect



How do we protect ourselves?

- Today's firewalls are multi-purpose network security platforms:
  - CVP (Content Vector Protocol)
  - UFP (URL Filter Protocol)
  - Bandwidth Management
  - VPN (Virtual Private Networking)
  - Intrusion Detection (MAD)

How do we protect ourselves?

- E-mail Server filters
  - Provide anti-virus protection for e-mail passing through the server
  - Integrate directly with the E-mail Server software - MS Exchange, Lotus Notes, Netscape, cc:Mail, etc.
  - Example products: McAfee GroupShield, Trend Micro ScanMail

How do we protect ourselves?

- Web based protection filters
  - Web Server protection
    - Protects web server from hacking (e.g. AppShield (Sanctum Inc.))
  - Web Access Control
    - Restricts web sites to which you can connect. Can protect you by not allowing you to go to malicious web sites (e.g. WebSENSE)

How do we protect ourselves?

- Hidden Manipulation
- Parameter Tampering
- Cookie Poisoning
- Stealth Commanding
- Forceful Browsing
- BackDoors and Debug Options
- Configuration Subversion
- Buffer Overflow
- Vendor assisted hacking through 3rd-party software vulnerabilities

How do we protect ourselves?

- VPN technologies
  - Access Control
    - Who can talk to us through the network?
  - Authentication
    - How do we know you're who you say you are?
  - Integrity
    - How can we guarantee that what we receive is what you sent?
  - Confidentiality
    - How can we guarantee that no one else can read this information?

How do we protect ourselves?

- Intrusion Detection Systems
  - Suspicious Pattern Detection
    - Looks for known patterns of types of traffic that are common to electronically "casing the joint"
  - Bit Pattern Signature Detection
    - Looks for known signatures of attacks
  - Anomaly Detection - the AI approach
    - Monitors network for a period of time to establish a statistical norm for traffic on the network. Generates alarms when abnormal traffic occurs

What do you do when you've been hacked?

- Too big of a topic to go into here.... but it's a vital part of network security.
  - What can you do to ensure the compromise has been abated?
  - How do you identify what's been changed?
  - What did you lose?
  - What can you recover?

Questions

- Five famous attacks
- Five famous Bots