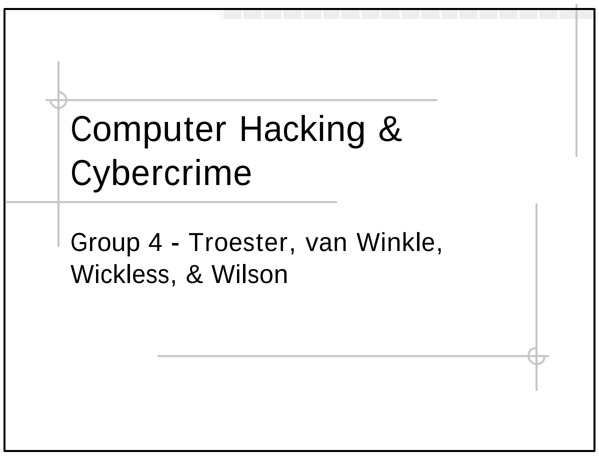
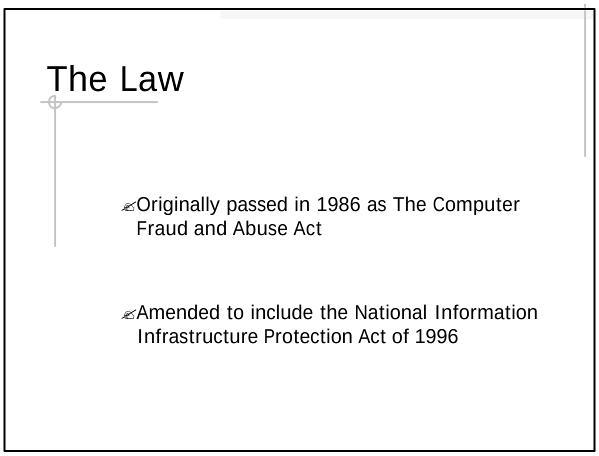


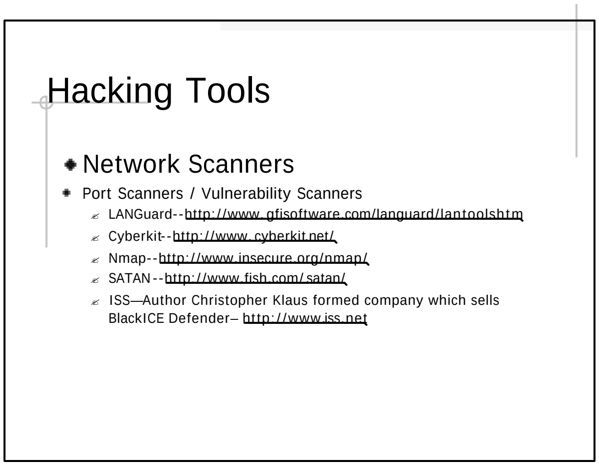
Computer Hacking & Cybercrime

Group 4 - Troester, van Winkle, Wickless, & Wilson



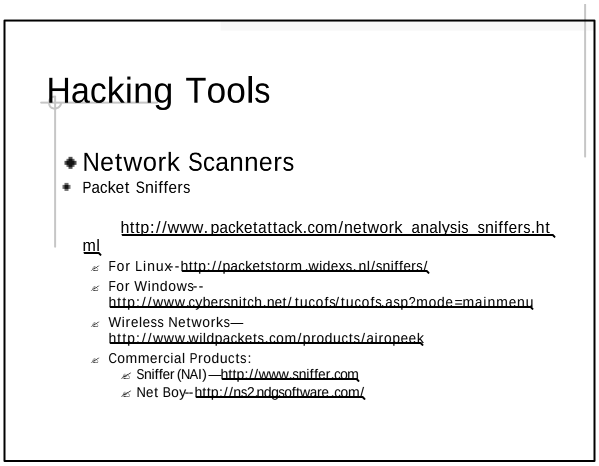
The Law

- Originally passed in 1986 as The Computer Fraud and Abuse Act
- Amended to include the National Information Infrastructure Protection Act of 1996



Hacking Tools

- Network Scanners
- Port Scanners / Vulnerability Scanners
  - LANGuard--http://www.gfisoftware.com/languard/lantoolshtm
  - Cyberkit--http://www.cyberkit.net/
  - Nmap--http://www.insecure.org/nmap/
  - SATAN--http://www.fish.com/satan/
  - ISS—Author Christopher Klaus formed company which sells BlackICE Defender– http://www.iss.net



Hacking Tools

- Network Scanners
- Packet Sniffers

  http://www.packetattack.com/network_analysis_sniffers.html
  - For Linux--http://packetstorm.widexs.nl/sniffers/
  - For Windows--http://www.cybersnitch.net/tucofs/tucofs.asp?mode=mainmenu
  - Wireless Networks—http://www.wildpackets.com/products/airopeek
  - Commercial Products:
    - Sniffer (NAI)—http://www.sniffer.com
    - Net Boy--http://ns2.ndgsoftware.com/

Hacking Tools

- Password Crackers
  - L0phtCrack
    - Company has now gone legit, sells security services--http://www.l0pht.com
  - Password Remover
    - Removes passwords from Excel Spreadsheets--http://www.straxx.com/excel/password.html
  - Brutus--http://www. hoobie.net/ brutus/
  - Others:
    - http://www.megasecurity.org/PwCrack.html
    - http://www.intertek.org.uk/downloads/
    - http://internettrash.com/users/hacknvp/pswcrackers1lllllllll.html
    - http://www.blackcode.com/archive/windows/
    - http://www.bokler.com/bsw_crak.html

Hacking Tools

- Buffer Overflows
  - Causes code to execute on remote machine
  - Sometimes causes system to drop down to command prompt

Hacking Tools

- Social Engineering
  - Unsuspecting employees are tricked into revealing logins, passwords, and network information.

Hackers

- Covering Their Tracks
  - Give the exploiting applications common names
  - Remove log entries
  - Looping—breaking into one system and using that system to break into third system

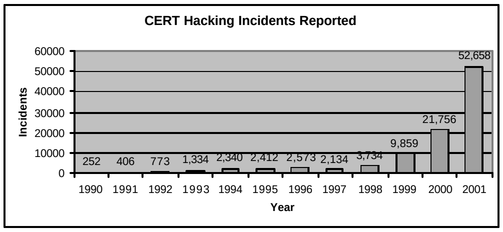
Information Theft/Tampering

- Objectives
  - Gathering Trophies
  - General Mischief
  - Financial Gain
  - Warfare/Revenge
  - Protest

Information Theft/Tampering

- Popular Attacks
  - Web Attacks
  - DNS Attacks
- Other Attacks
  - DoS
  - Ping Of Death
  - Smurf
  - SYN Flooding

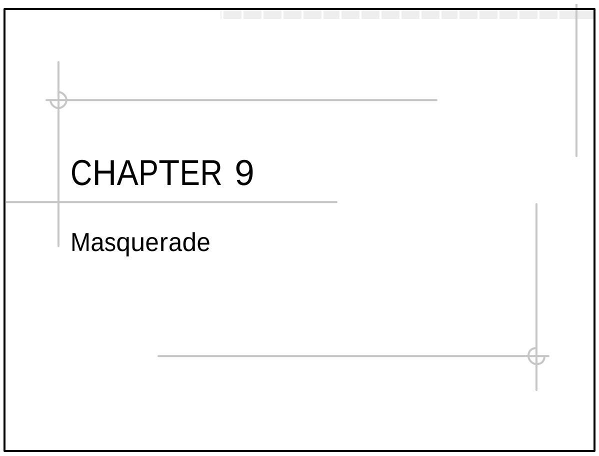
Hacking Extent



Source: http://www.cert.org/stats/cert_stats.html

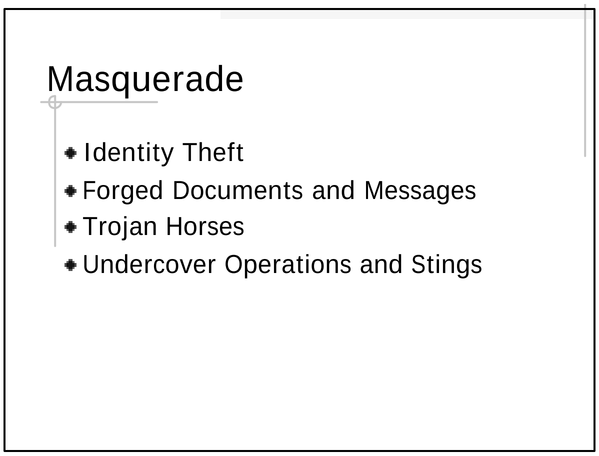
Hacker Tool Sites

- http://www.insecure.org/tools.html
- http://www.cleo-and-nacho.com/mainpages/hacking.htm
- http://www.hackerscenter.com/Hacking/default.asp
- http://netsecurity.about.com/cs/hackertools/
- http://packetstorm.decepticons.org/
- http://www.hackerwhacker.com/
- http://www.net-security.org/various/software/
- http://www.mycert.mimos.my/resource/scanner.htm
- http://www.cybersnitch.net/tucofs/tucofs.asp?mode=mainmenu
- http://www.thenewbiesarea.com
- http://www.users.freenetname.co.uk/~sandradelgado/hackertoolkit1.htm



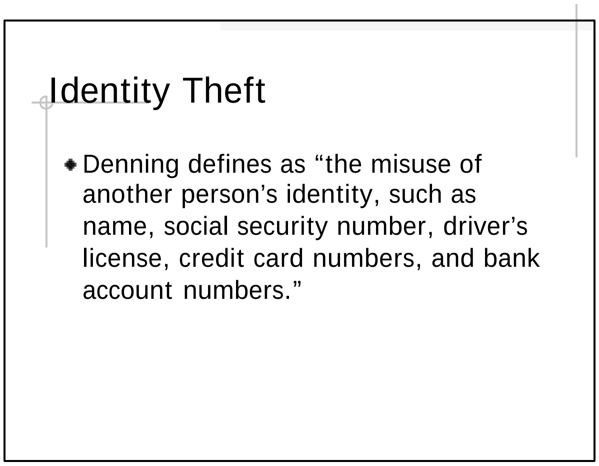
CHAPTER 9

Masquerade



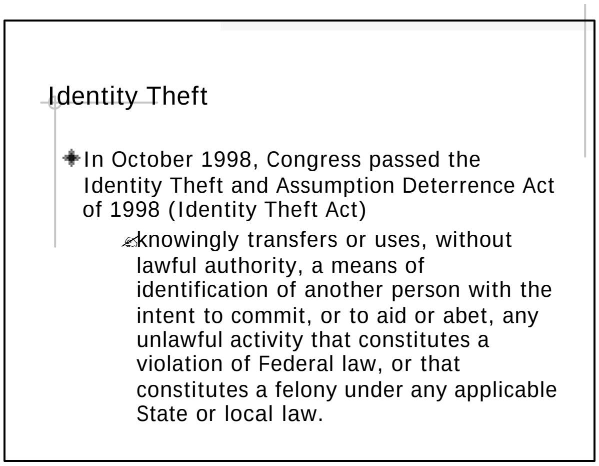
Masquerade

- Identity Theft
- Forged Documents and Messages
- Trojan Horses
- Undercover Operations and Stings



Identity Theft

- Denning defines as "the misuse of another person's identity, such as name, social security number, driver's license, credit card numbers, and bank account numbers."



Identity Theft

- In October 1998, Congress passed the Identity Theft and Assumption Deterrence Act of 1998 (Identity Theft Act)
  - ✍knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.

Identity Theft

- Some methods used:
  - Dumpster Diving
  - Employees of organizations who you provide the information to
  - Internet
  - ATM Machines

Forged Documents and Messages

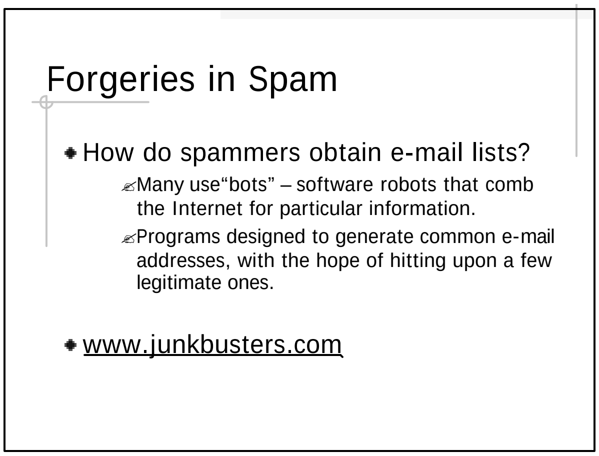
- Denning defines as “an act of information warfare that targets a set of documents allegedly originating from a particular person or entity.”

Forged Documents and Messages

- E-mail Forgeries
- Forgeries in Spam
- E-mail Floods
- IP Spoofing
- Counterfeiting

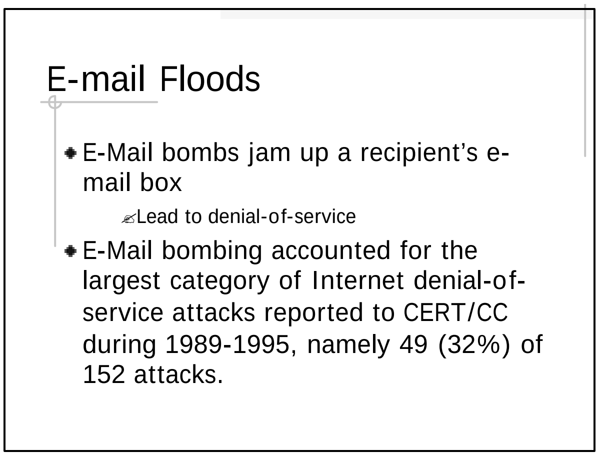
E-Mail Forgeries

- Recipients can be harmed by fraud
  - AOL
- Victims reputations may not fully recover
  - Can have a long life if archived
  - New readers may not be aware of the forgery



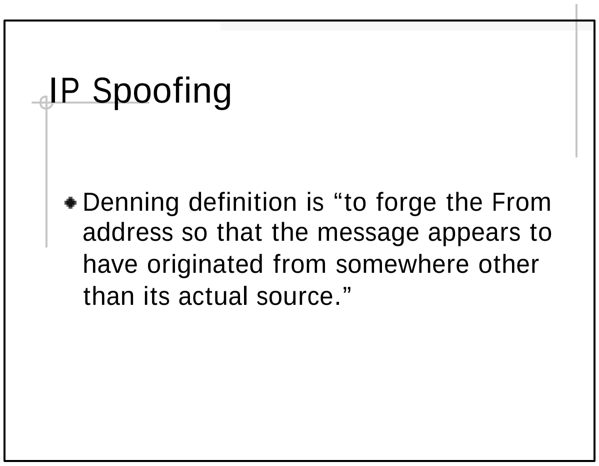
Forgeries in Spam

- How do spammers obtain e-mail lists?
  - Many use“bots” – software robots that comb the Internet for particular information.
  - Programs designed to generate common e-mail addresses, with the hope of hitting upon a few legitimate ones.
- www.junkbusters.com



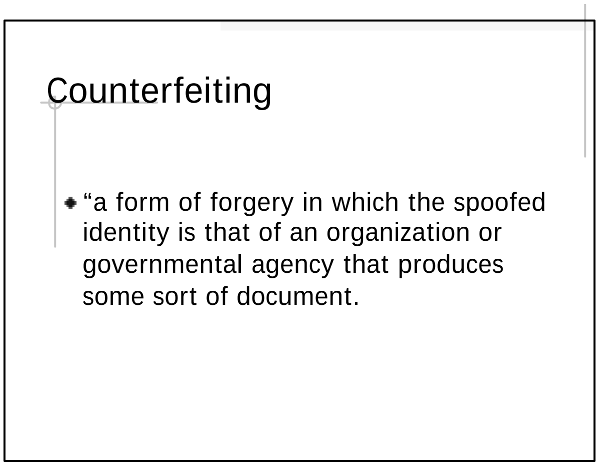
E-mail Floods

- E-Mail bombs jam up a recipient’s e-mail box
  - Lead to denial-of-service
- E-Mail bombing accounted for the largest category of Internet denial-of-service attacks reported to CERT/CC during 1989-1995, namely 49 (32%) of 152 attacks.



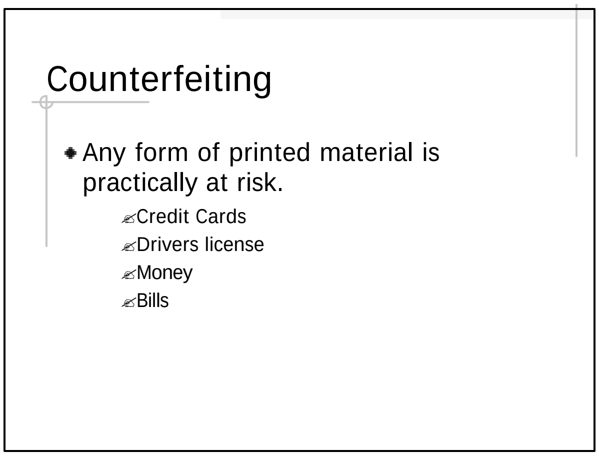
IP Spoofing

- Denning definition is “to forge the From address so that the message appears to have originated from somewhere other than its actual source.”



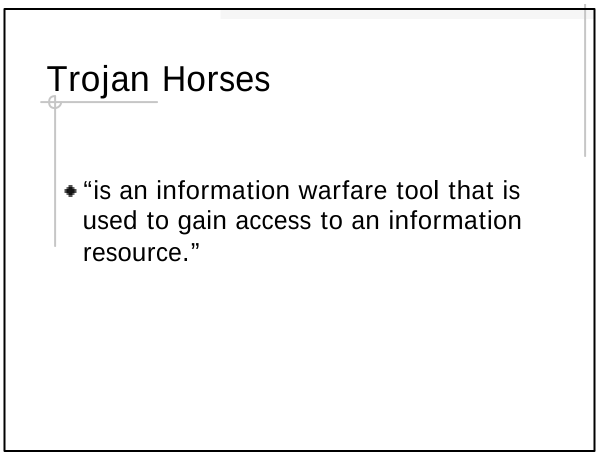
Counterfeiting

- “a form of forgery in which the spoofed identity is that of an organization or governmental agency that produces some sort of document.



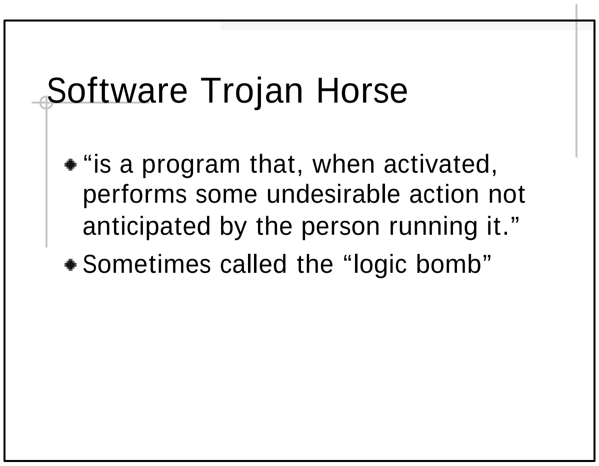
Counterfeiting

- Any form of printed material is practically at risk.
  - Credit Cards
  - Drivers license
  - Money
  - Bills



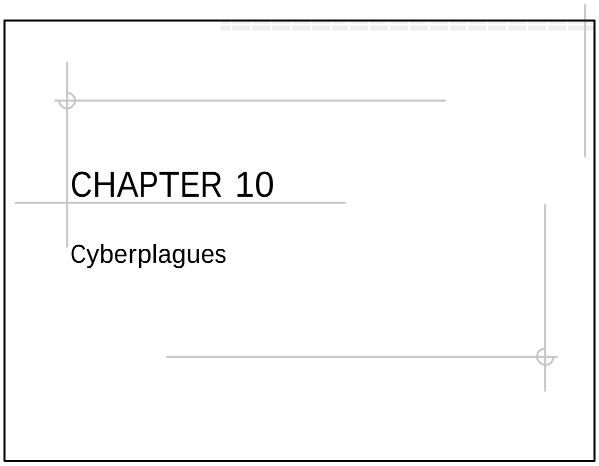
Trojan Horses

- “is an information warfare tool that is used to gain access to an information resource.”



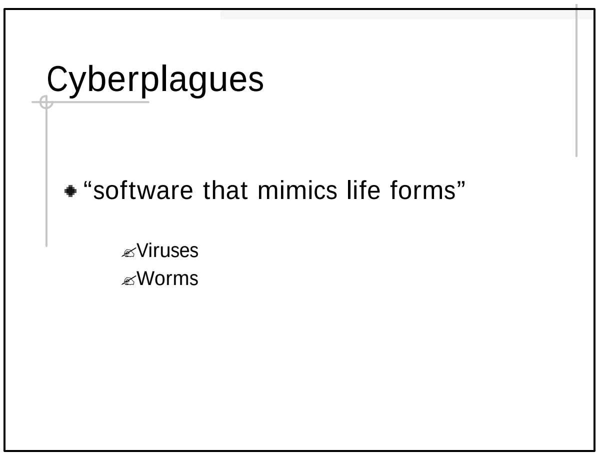
Software Trojan Horse

- “is a program that, when activated, performs some undesirable action not anticipated by the person running it.”
- Sometimes called the “logic bomb”



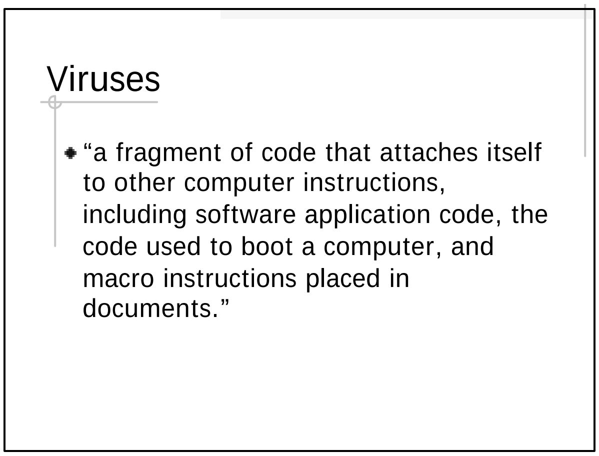
CHAPTER 10

Cyberplagues



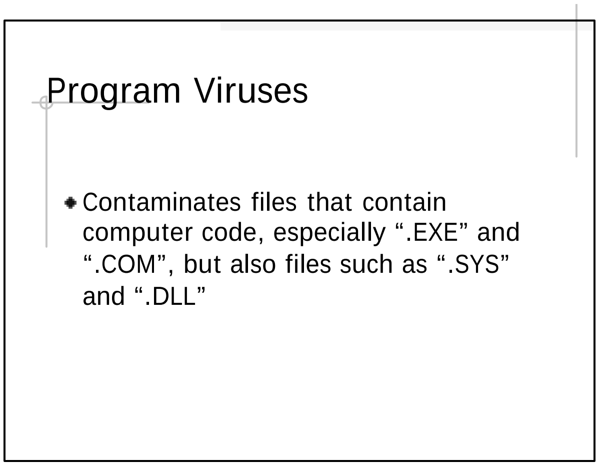
Cyberplagues

- “software that mimics life forms”
  - Viruses
  - Worms



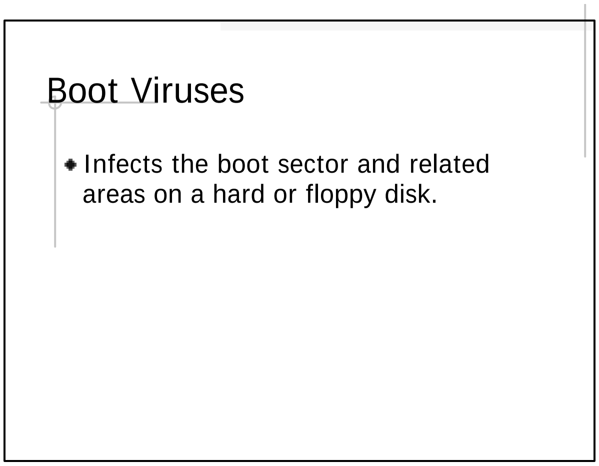
Viruses

- “a fragment of code that attaches itself to other computer instructions, including software application code, the code used to boot a computer, and macro instructions placed in documents.”



Program Viruses

- Contaminates files that contain computer code, especially “.EXE” and “.COM”, but also files such as “.SYS” and “.DLL”



Boot Viruses

- Infects the boot sector and related areas on a hard or floppy disk.

Concealment Techniques

- Stealth Viruses
  - Intercept certain systems calls and return false information.
- Encrypting Viruses
  - Hide their presence by storing the bulk of their code in encrypted form.
- Polymorphic Viruses
  - Mutate as they replicate, fooling scanners looking for fixed patterns.

Viruses

- Statistics
- Cert
- Hoax

Worms

- “is a program that propagates from one computer to another over a computer network by breaking into the computers in much the way that a hacker would break into them.

Offensive Information Warfare Operation

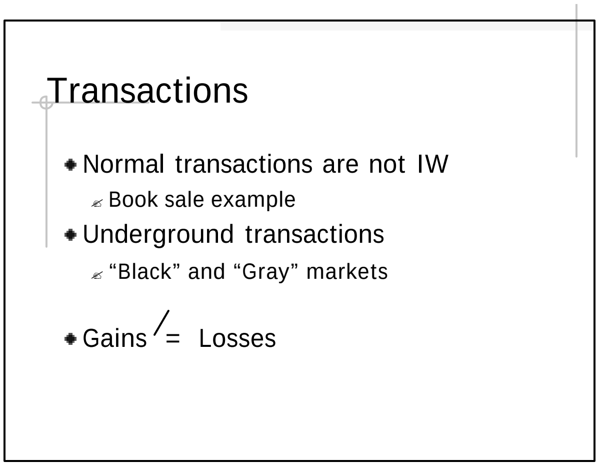
- Targets or exploits a particular information resource with the objective of increasing its value to the offensive player and decreasing its value to the defensive player
- Win-lose situation
- Hostile or nonconsensual act

Offensive Gains

- Financial
- Amusement or thrills
- Credentials to join
- Revenge
- Advantage

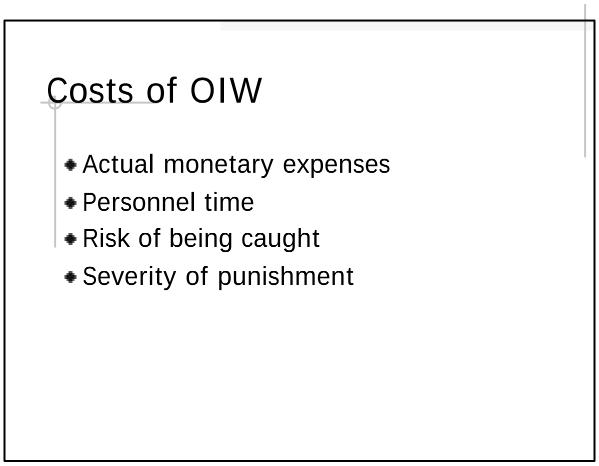
Defensive Losses

- Financial
- Public confidence
- Competitive position
- Productivity
- Fines/penalties
- Life
- Privacy



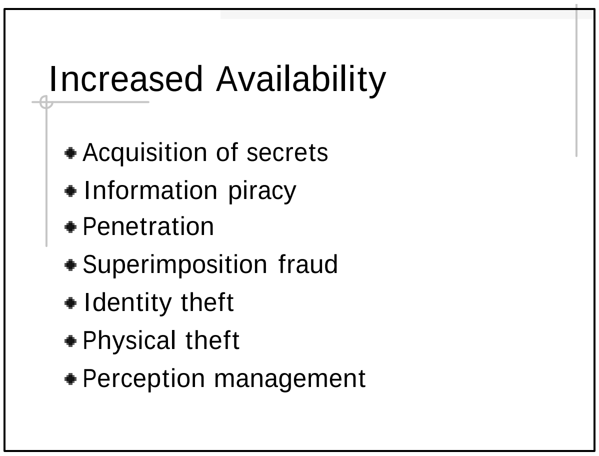
Transactions

- Normal transactions are not IW
  - Book sale example
- Underground transactions
  - “Black” and “Gray” markets
- Gains $\neq$ Losses



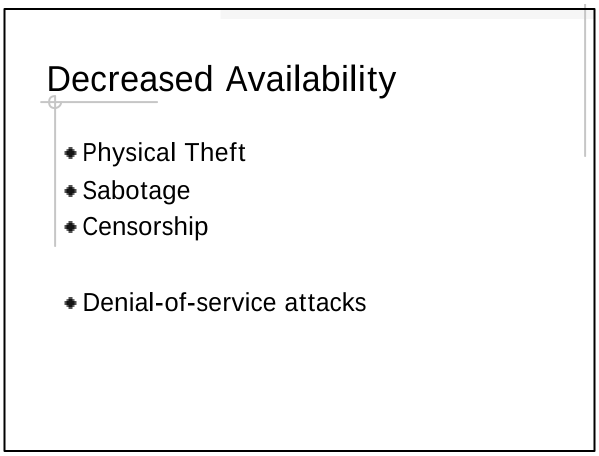
Costs of OIW

- Actual monetary expenses
- Personnel time
- Risk of being caught
- Severity of punishment



Increased Availability

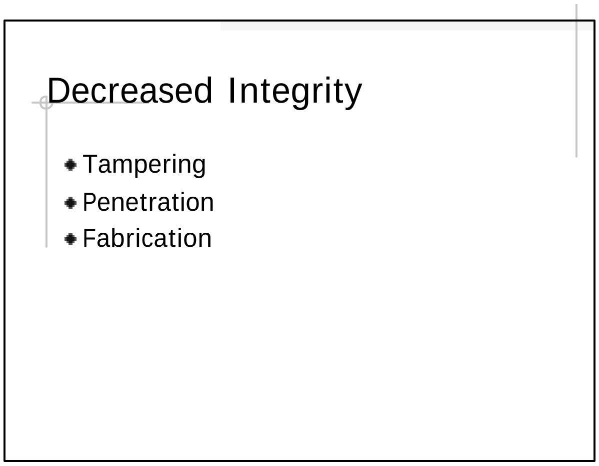
- Acquisition of secrets
- Information piracy
- Penetration
- Superimposition fraud
- Identity theft
- Physical theft
- Perception management



Decreased Availability

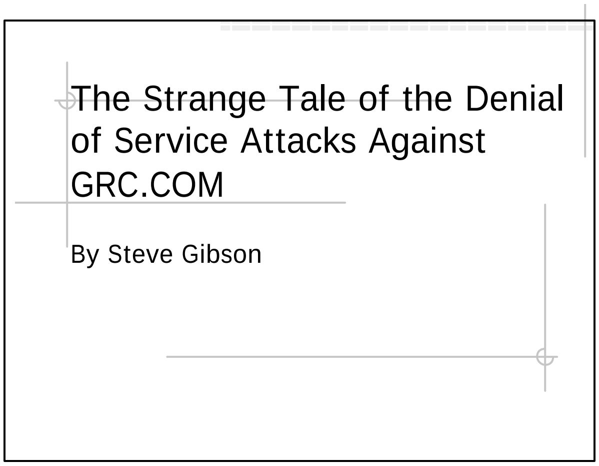
- Physical Theft
- Sabotage
- Censorship

- Denial-of-service attacks



Decreased Integrity

- Tampering
- Penetration
- Fabrication



The Strange Tale of the Denial of Service Attacks Against GRC.COM

By Steve Gibson

What Happened

- Denial of Service Attack
  - Caused by a “packet flooding attack”
  - Huge packets fragmented into minute packets
  - Consumed all bandwidth of Internet connection
  - Aimed at bogus port of GRC.COM

Profile of the Attack

- Attacked by 474 security-compromised Windows-based PCs
- “Distributed” Denial of Service
- 6 total attacks
- Top two U.S. residential cable-modem ISPs
  - @Home.com
  - RoadRunner

Attack Summary

- Attack #1
  - May 4th 17 hours
- Attack #2
  - May 13th 8 hours
- Attack #3a
  - May 14th
  - Targeted at the IP of firewall

- Attack #3b
  - May 14th
  - Targeted at one T1 interface of router
- Attack #4
  - May 15th 6 ½ hours
- Attack #5
  - May 16th

- Attack #6
  - May 17th, 18th, 19th, 20th
- On May 16th
  - 12,248,097 malicious packets stopped with 666 destination
  - 538,916,268 total malicious packets

- Monday May 21st
  - 2,399,237,016 total malicious packets blocked

Trojan attack Zombies

- Each security compromised machine receives a complimentary copy of Sub7Server Trojan
- Allows the “Zombie-master” absolute control over victims’ machines
- Keystroke monitoring to capture online passwords, credit card numbers, eBanking passwords

FBI and cybercrime

- No crime until $5,000 in damages
- FBI prosecution is $200,000 so case prioritization is necessary
- Youth is an impenetrable shield

Chapter 18 Attack Methodology Schneier

By: Chaz Van Winkle

Vulnerability

- Is simply a weakness
  - In order for the vulnerability to be exploited an attacker must:
    - Find the target
    - Plan the attack
    - Execute the attack
    - Get away
- Location and access are key to exploit a vulnerability

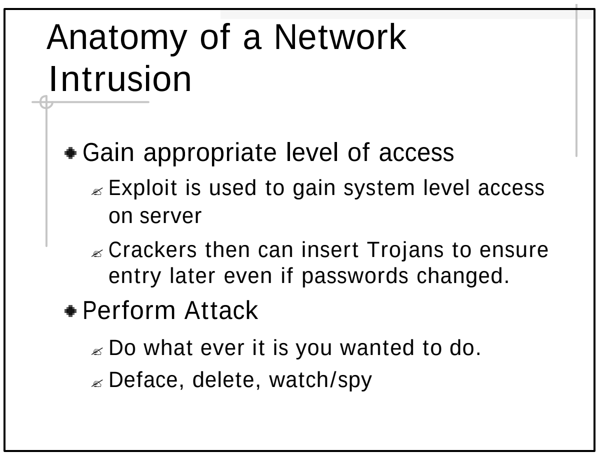
Attacking the vulnerability

Five Steps

- Identify target and gather information
- Analyze and identify vulnerability
- Gain the appropriate level of access to target
- Perform attack
- Erase evidence and avoid retaliation

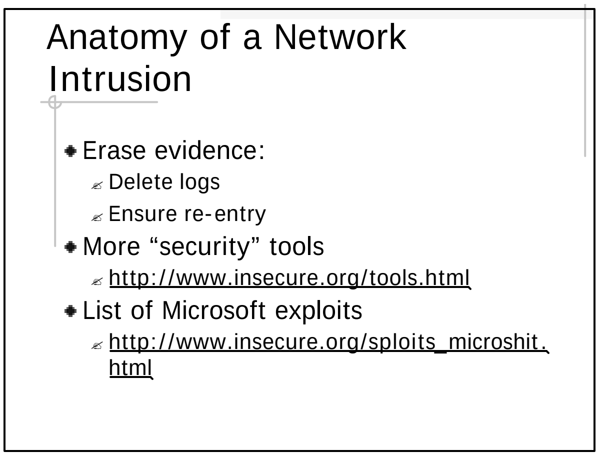
Anatomy of a Network Intrusion by Shipley

- Identify target and gather information: Somedomain.com, Identification of host and IP ranges DNS used.
  - Next the use of hacking tools to identify OS and services running http://www.insecure.org/ NMap
- Analyze and identify vulnerability: Hacking tools used to identify vulnerabilities
  - Two types of vulnerabilities,local and remote



Anatomy of a Network Intrusion

- Gain appropriate level of access
  - Exploit is used to gain system level access on server
  - Crackers then can insert Trojans to ensure entry later even if passwords changed.
- Perform Attack
  - Do what ever it is you wanted to do.
  - Deface, delete, watch/spy



Anatomy of a Network Intrusion

- Erase evidence:
  - Delete logs
  - Ensure re-entry
- More “security” tools
  - http://www.insecure.org/tools.html
- List of Microsoft exploits
  - http://www.insecure.org/sploits_microshit.html