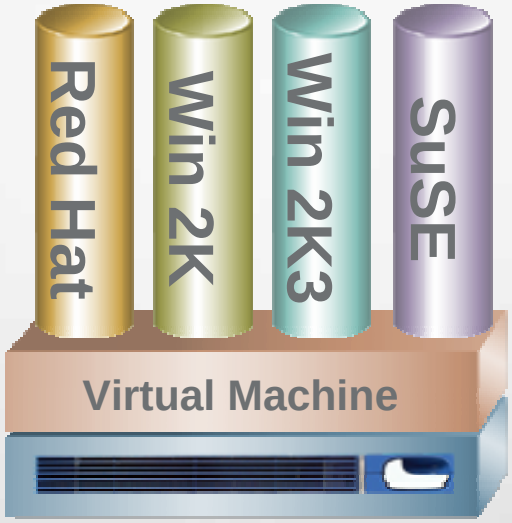
VMworld2005
virtualizenow

Concepts in Network Security

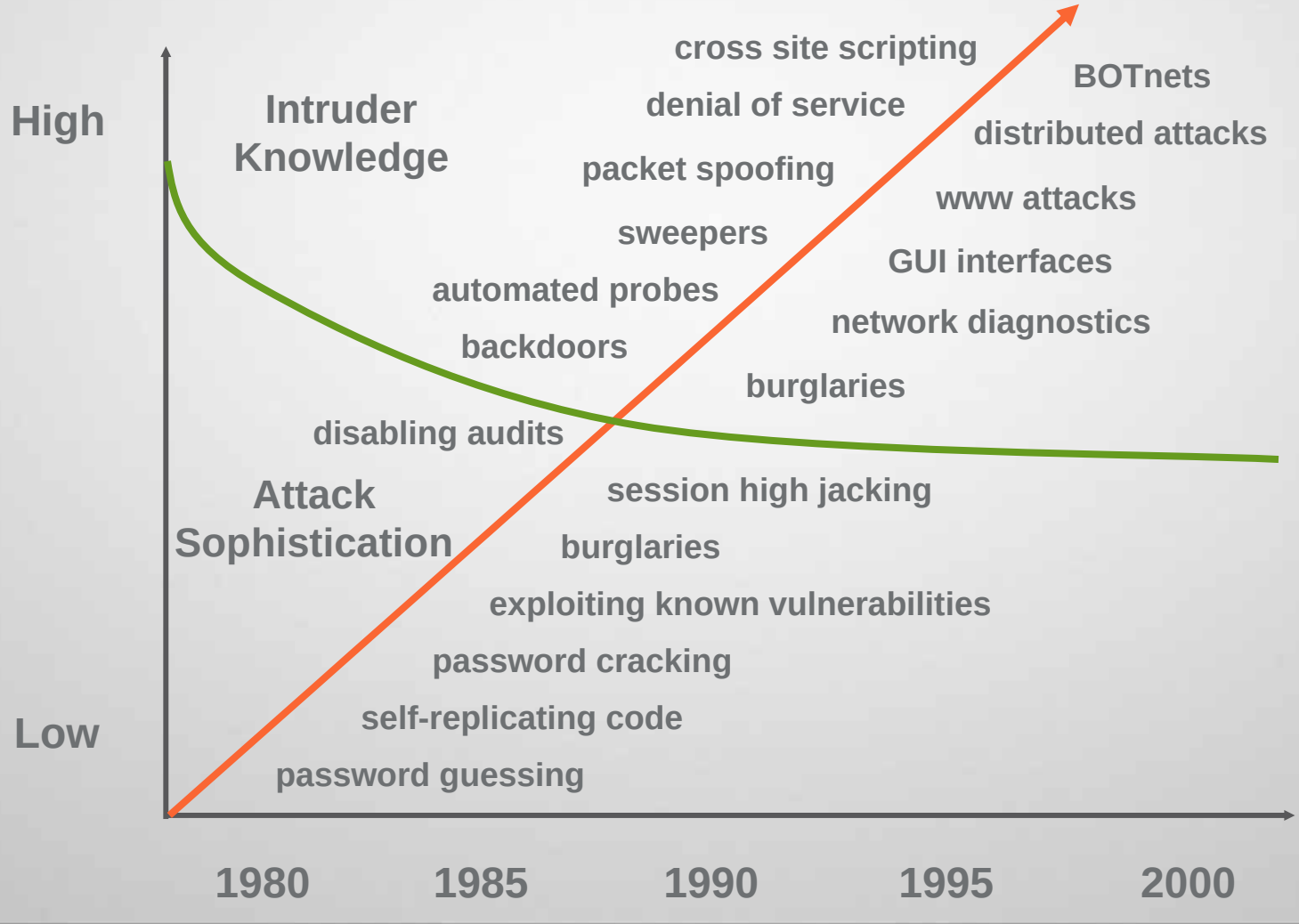


LTC Ronald Dodge, Ph.D.
United States Military Academy

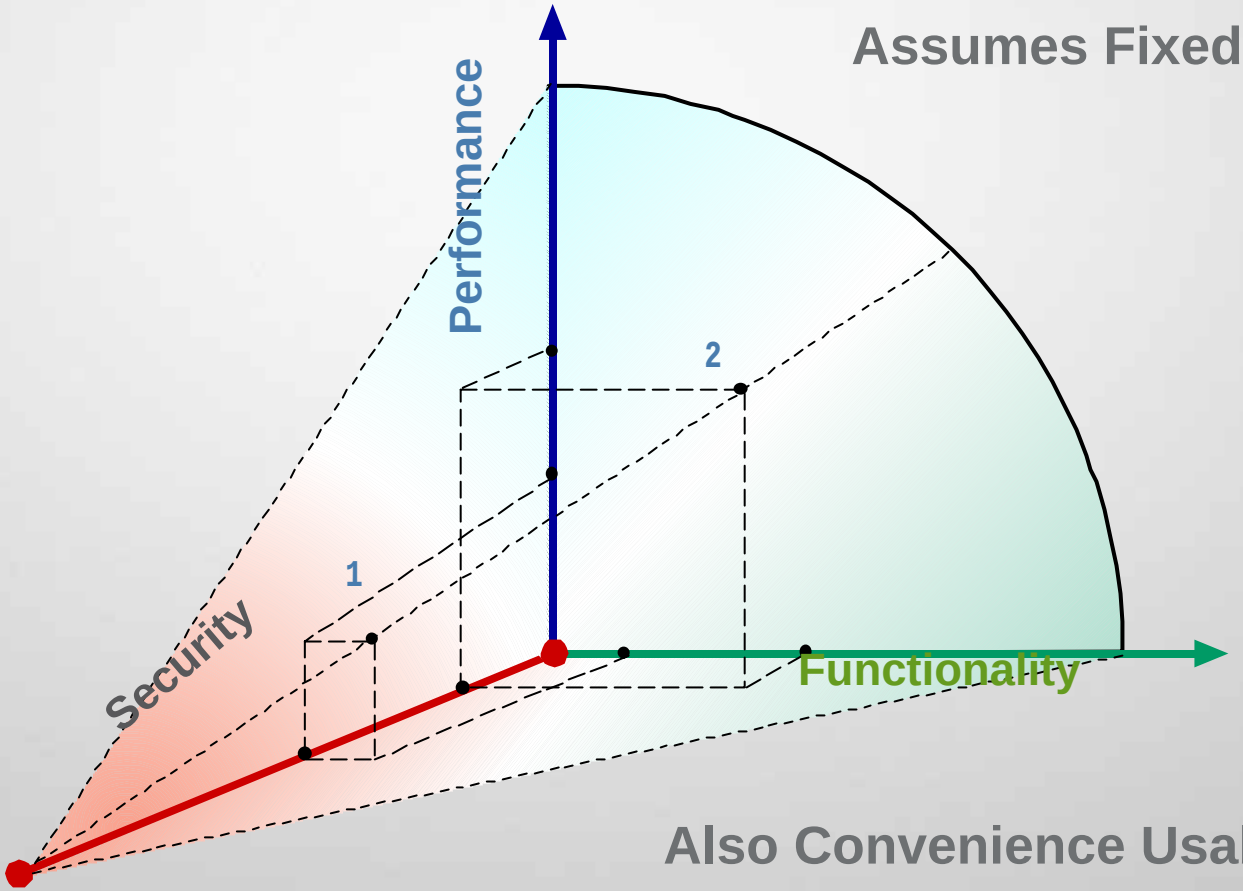
Trends in Network Security

- Attackers
  - Increasing sophistication
  - Increasing communication/ collaboration
- Defenders
  - Increasing complexity
  - Increasing dependency
  - Increasing attrition
  - Decreasing budgets
  - Persistent ignorance/ increasing awareness/ more knowledgeable sysadmin
- Network systems
  - Increasing connectivity
  - Increasing complexity
  - Increasing functionality
  - Increasing “computrons”
  - Increased application security
- Activity
  - Increased state and non-state sponsorship
  - Increased patching
  - Increasing probes and “Recon by Fire”

Trends: Another Picture



Security Trade-offs

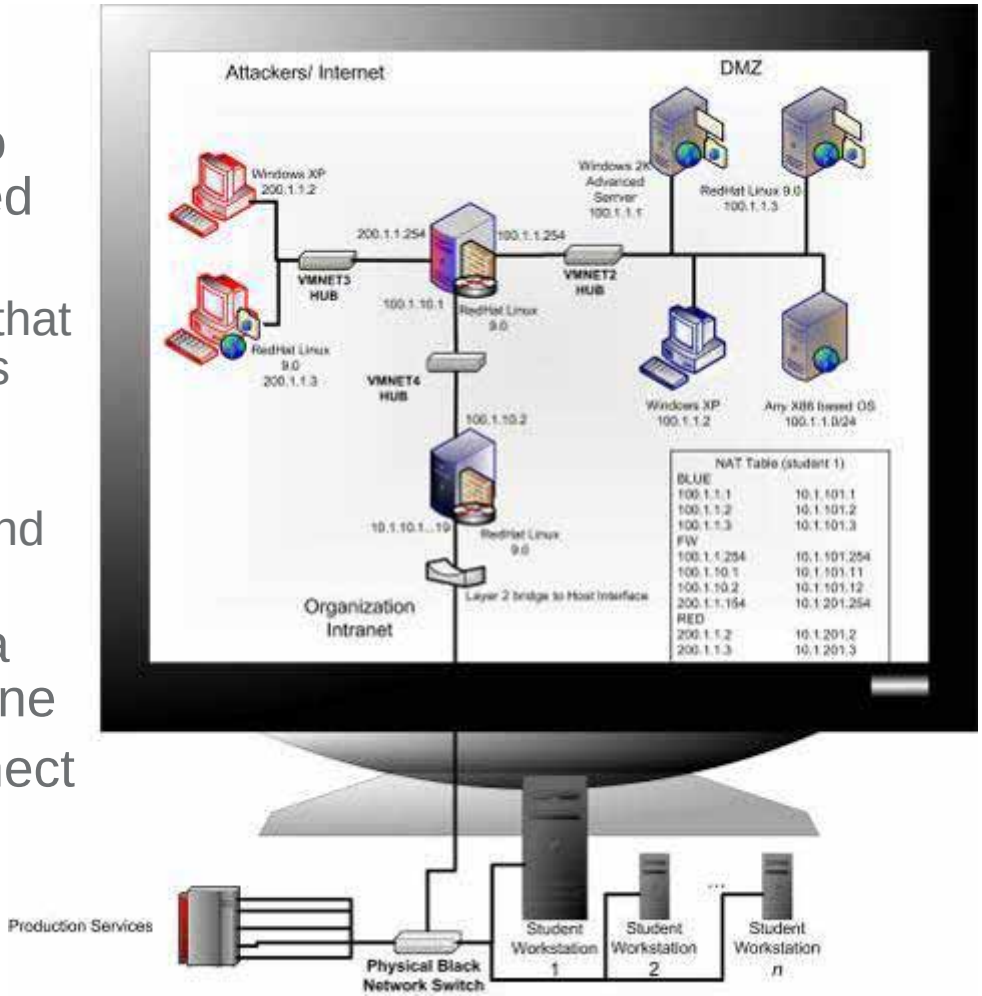


Overview

- Motivation
- Virtual Information Assurance Network (VIAN) introduction
- Viruses, Worms and Trojans – Oh My!
  - (And don't forget about SPAM)

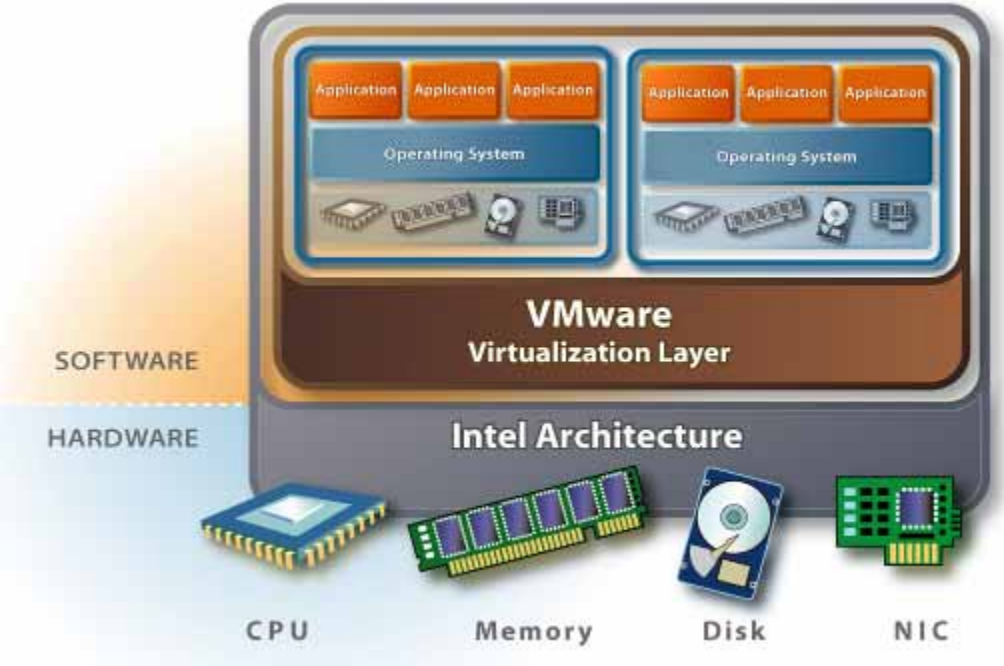
USMA VIAN

- Virtual network design presents students with two internal networks separated by a firewall
  - Red – contains machines that are used to launch exploits
  - Blue – contains target machines (running installations of Windows and Linux systems)
- A second firewall acts as a gateway to the host machine
- Virtual Machines can connect to “physical network” by bridging through the host interface



How Does VMware Workstation Work?

Intel Architecture with VMware



The VMware virtualization layer sites between the hardware and software and allows users to create virtual machines that are the full equivalent of a standard x86 machine

USMA VIAN Configuration

- VMware license: Academic $130 each
- OS licenses
  - Solaris: $20
  - MSDNAA: Deeply discounted
- Applications: Most all open source
- Hardware
  - P4 1.8GhZ, 1 GB RAM (512), 60 GB HD

USMA VIAN Operating Systems

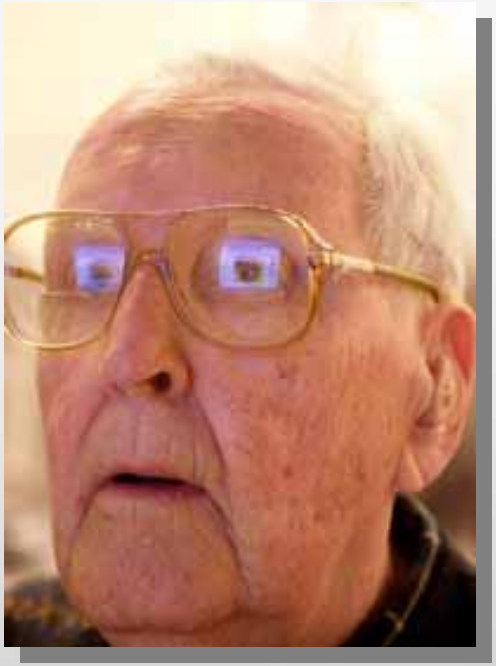
- Windows 2003 (all versions)
- Windows XP Pro
- Windows XP home
- Windows 2000 Server
- Windows 2000 Pro
- Windows NT
- Windows 98

- Debian 3
- Engarde
- Fedora
- Gentoo
- IPcop
- Netwosix
- Sentinix
- Slackware
- Smoothwall
- Trustix
- vexlinux
- Mandrake
- Red Hat Linux
- Free BSD
- OpenBSD
- Solaris 9

USMA VIAN Modules

- Attacking the Connection with Man in the Middle
- Defending with Firewalls: Basic
- Defending with Firewalls: In-depth
- Defending: Network intrusion detection using SNORT
- Defending: Host based intrusion detection with monitors
- Forensics: Intro
- Forensics: Advanced 1
- Forensics: Advanced 2
- Cryptography: Intro
- Cryptography: Advanced 1
- Cryptography: Advanced 2
- Sys Admin: Routing with Zebra
- Sys Admin: AD
- Sys Admin: Exchange
- Introduction to the VIAN environment and using virtual machines
- Introduction to the VIAN environment and network fundamentals
- Reconnaissance: Spyware
- Reconnaissance: SPAM/phishing
- Reconnaissance: Social engineering
- Reconnaissance: Port scanning
- Reconnaissance: OS finger printing
- Reconnaissance: Network enumeration
- Reconnaissance: Vulnerability scanning
- Attacking with Trojan horses using e-mail
- Attacking with buffer overflows
- Attacking with Virii
- Attacking passwords

Viruses, Worms and Trojans – Oh My!



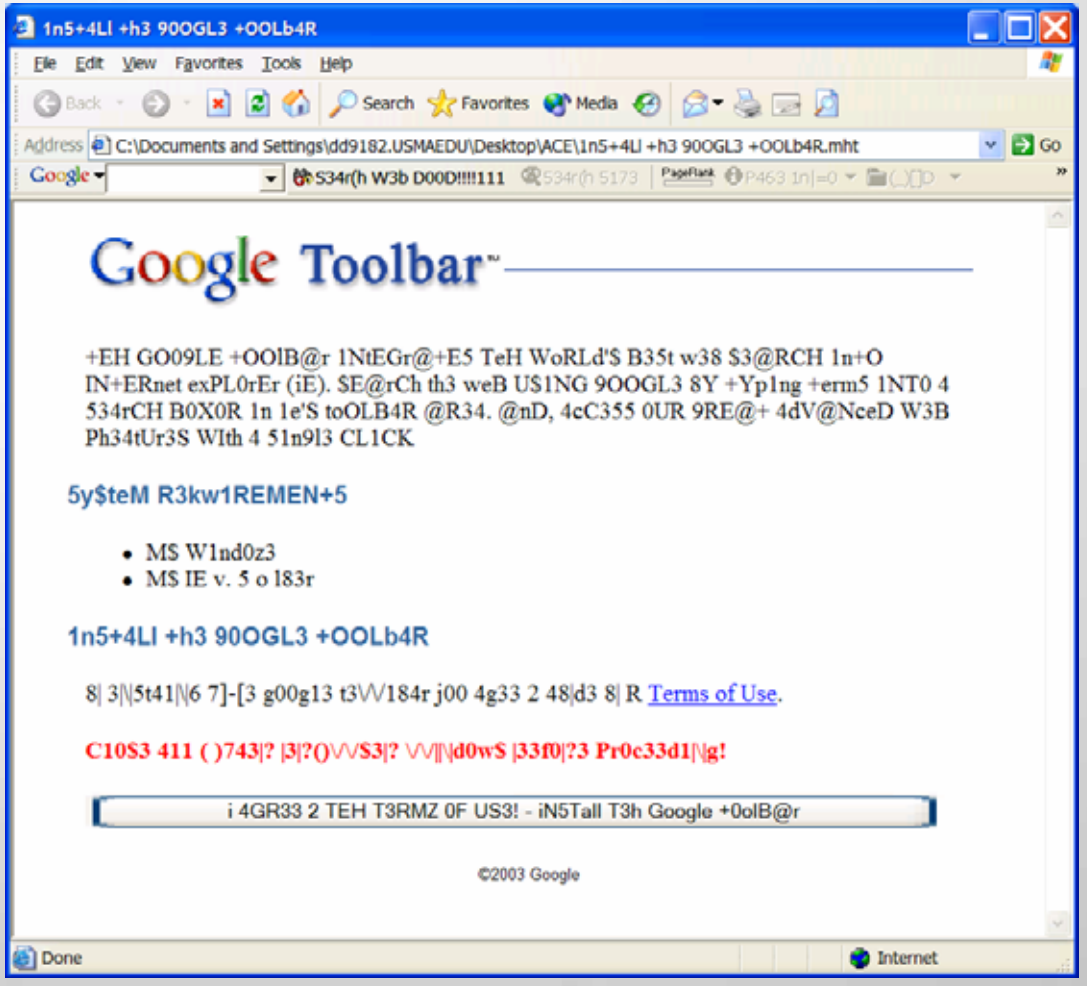
HACKER Pre-test

- Can you read this?
- T1hs iz da h0m3p4g3 0f d4 m0St l33T w4r3z gR0uP th3r3 iz, LWE! W3 f0cUs oN bRiNgIng j0 dA l4t3eSt 0-dAy 313373 w4r3z év3rydAy. J0 c4n f1nd aLl 0ur r3l3ases 0n ThIs l33t p4ge!! Ph34r 0ur sKiLlz!!

H4x0r Language Homework

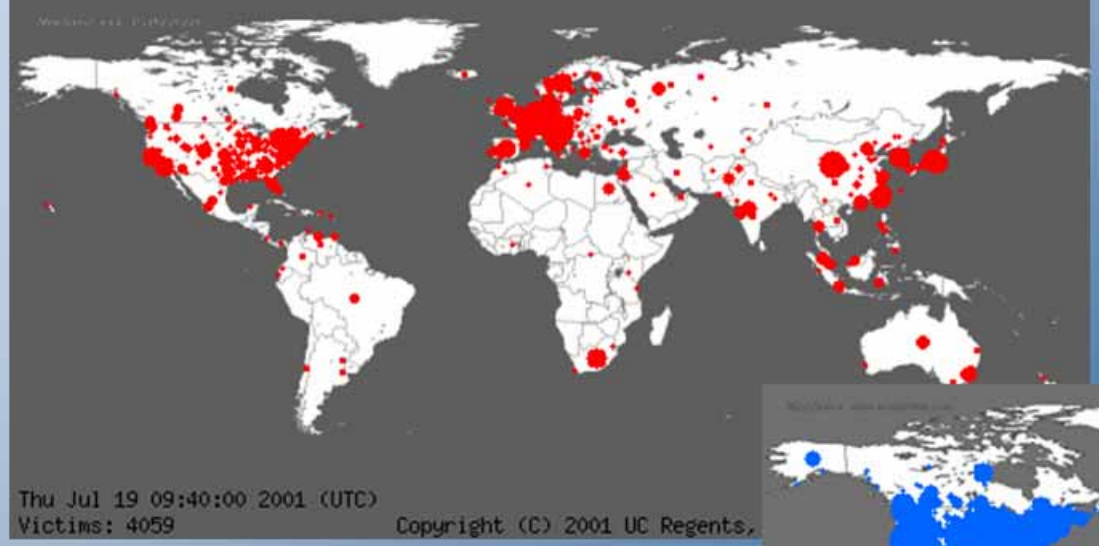
www.google.com

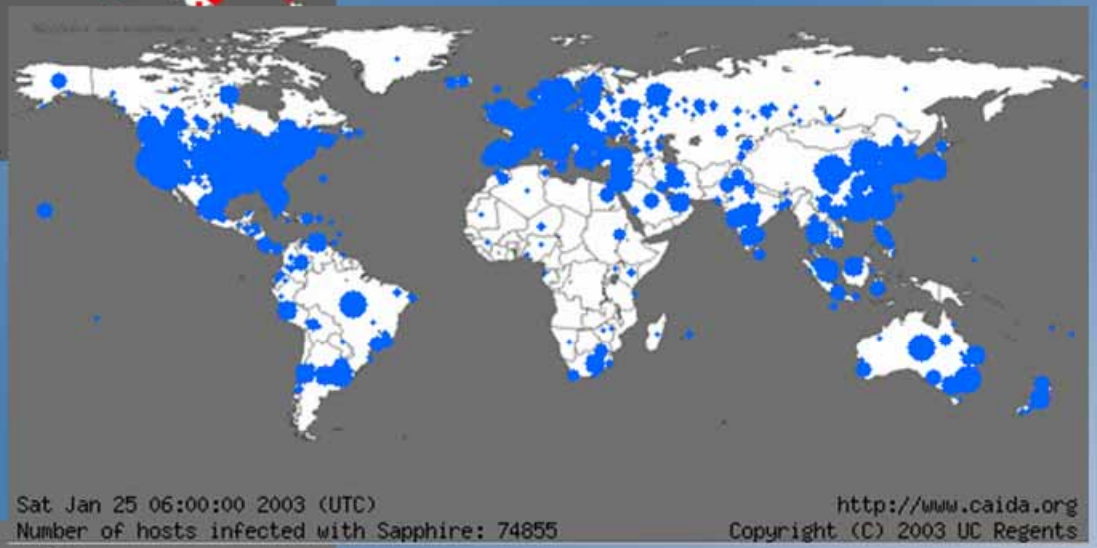
->preferences

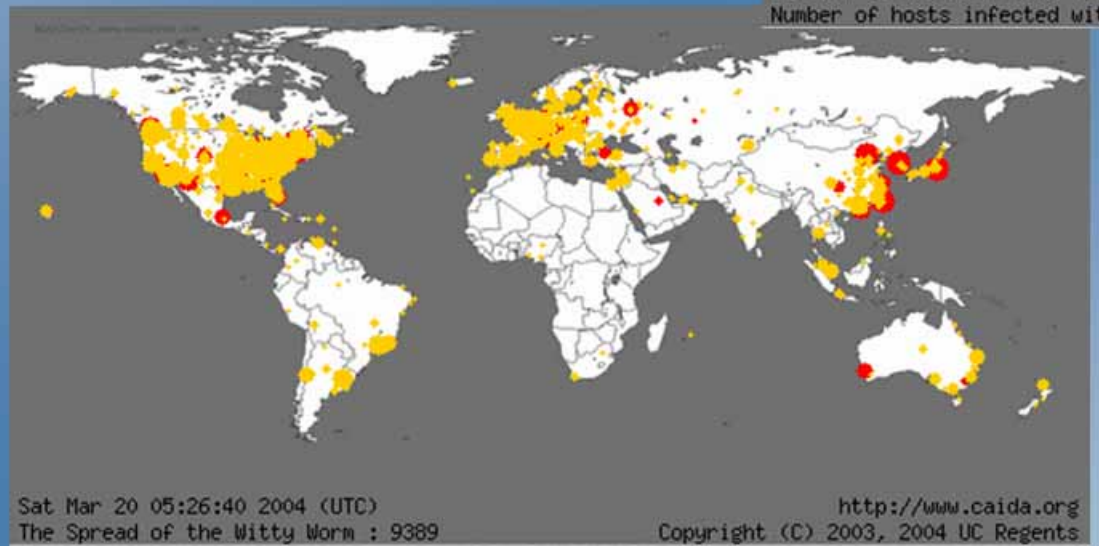


Example Malicious Program Types

- Viruses
- Worms
- Trojan horses
- Backdoors
- Buffer overflows
- Application misuse


Thu Jul 19 09:40:00 2001 (UTC)
Victims: 4059
Copyright (C) 2001 UC Regents,


Sat Jan 25 06:00:00 2003 (UTC)
Number of hosts infected with Sapphire: 74855
http://www.caida.org
Copyright (C) 2003 UC Regents


Sat Mar 20 05:26:40 2004 (UTC)
The Spread of the Witty Worm : 9389
http://www.caida.org
Copyright (C) 2003, 2004 UC Regents

Hacking, Step-by-Step

- Well, this ain't exactly for beginners, but it'll have to do. What all hackers have to know is that there are 4 steps in hacking...
  - Step 1: Getting access to site
  - Step 2: Hacking r00t
  - Step 3: Covering your traces
  - Step 4: Keeping that account

http://forbidden.net-security.org/txt/beginner.txt

Hacking, Step-by-Step

- More formally:
  - Reconnaissance
  - Exploitation
  - Consolidate
  - Reorganize

Reconnaissance

- Passive recon
  - Web-based recon
  - DNS recon
- Active recon
  - Social engineering
    - Via e-mail
    - Via telephone
    - Via casual conversation
    - Dumpster diving
  - Scanning
  - Finger printing operating systems

Scanning

- Scanning
  - A method for discovering exploitable communication channels. The idea is to probe as many listeners as possible, and keep track of the ones that are receptive or useful to your particular need
- SuperScan – NMAP – Nessus
- CORE Impact – Metasploit – WHAX 3.0 (a.k.a. WHOPPIX)

Sniffing

- Sniffing
  - A **packet sniffer** is a wire-tap devices that plugs into computer networks and eavesdrops on the network traffic. A “sniffing” program lets someone listen in on computer conversations
- Ethereal FTP/SFTP Demo

Exploitation

- Gain User Access to System
- Elevate Privileges
- Network Based
  - Passive Sniffing
  - Active Sniffing
  - Worms
  - Denial Of Service
- Operating System and Application Based
  - Buffer overflows
  - Passwords attacks
  - Virus
  - Denial of service

Exploits

- IIS buffer overflow
- DCOM

Consolidation

- Cover tracks
  - Delete/modify log files
  - Hide files
  - Tunnel communications
  - Use covert channels
- Demo:
  - PWdump
  - IISlogclean
  - VNC

Reorganization

- Maintain access
  - Patch
  - Install backdoor

User Security

- E-mail security
  - E-mail worm / Trojan horse / back door
    - Flip screen
    - Sub7
    - Netbus
  - Phishing
- Password security

Links

- USMA IWAR and VIAN
  - Web: http://www.itoc.usma.edu
  - E-mail: itoc@usma.edu

7th Annual IEEE Information Assurance Workshop
June 21-23, 2006
West Point, New York

Sponsored by IEEE SMC and NSA

http://www.itoc.usma.edu/workshop/2006/

VMworld 2005

virtualize now

las vegas • october 18-20, 2005