InfoSec Update

Overview of 2000

Technical Vulnerabilities
David Kennedy CISSP
Director of Research Services
<david.kennedy@acm.org>

icsa.net
WE SECURE THE WEB
Agenda

• Good News

• Bad News
  – DDoS--No excuses, we had plenty of warning
  – ILOVEYOU-- No excuses, we had plenty of warning
  – Pervasive Scanning
  – 2000--The Year of the Buffer Overflow ($n_{th}$ iteration)
Agenda (cont)

– It may work, but it doesn’t work
– Trojans and Back Doors
– Nightmares
– KISS
Sources

• Bugtraq
• NTBugtraq
• FIRST Member Advisories
• Vendor Advisories
• 104 Other Security and UG Mailing Lists
• USENET
• ~1400 ‘Net Sites and BBS

Wall Street Journal 9/30/99, page B21
Good News

• Vendors are getting proficient at making security notifications (Practice makes perfect?)
• Source auditing for security is paying off.
• Job security outlook continues to be rather bright
Bad News

- DDoS--We Had Plenty of Warning
- ILOVEYOU--We Had Plenty of Warning
- Scans
- Buffer overflows continue
ILOVEYOU--Talismans

• Happy99 a.k.a W32/SKA.exe (1/99)
• Melissa Macro.W97.Melissa (3/99)
• VBS.Freelink (7/99)
• Barok (same author(s)) (9/99)
• Bubbleboy I-Worm.BubbleBoy (11/99)
Scans

NMAP
DNS Queries
SNMP Walk
Whois and NSLookup
Rootshell & Packetstorm
SATAN
stobe
mscan
Nessus

SAINT
Asmodeus
Internet Probe Droid

Warez
ISS
CyberCop
HackerShield
Security Analyzer
2000A.D.--The Year of the Buffer Overflow (Again)

- Phrack 49 & Fall '96 2600 Article
- Stackguard
- Languages

*from Ghosh & O'Connor p 374 NISSC 21
Denial of Service

- DDoS
- Network
  - SYN
  - Ping of Death
  - SMURF
  - LAND/BOINK/Teardrop/Newtear/fraggle
  - nuke
- OS & Application
Operating System Vulnerabilities FY 00

Operating System

BSDI
Free BSD
Open BSD
Net BSD
Digital UNIX
HPUX
IBM AIX
IRIX
Caldera
Debian
Red Hat
Slackware
SuSE
SCO
SunOS/Solaris
NT
UNIX

• Migration among Distributions
• Reverse engineering
• ftp daemon
• rpc
• Desktops
  – CDE
  – KDE
  – X11
UNIX

- Migration among Distributions
- Reverse engineering
- ftp daemon
- rpc
- Desktops
  - CDE
  - KDE
  - X11
Microsoft Windows NT

• Maturity
• DoS
  – Out of Band
  – Fragments
• Applications
  – IIS
  – FrontPage
  – Cold Fusion
  – IE
Applications

- **BIND**
- **World Wide Web**
  - **Server**
    - CGI
    - Back end processes
    - Cold Fusion
    - Front Page
  - **Clients**
Trojans and Back Doors

- **Backdoor-G**
  - most common malcode on USENET
- **Back Orifice/BO2**
- **DIRT ?**
- **Netbus**
- **.shs scrap object attachments**
- **.vbs script objects**
- **Virus Infections**
  highlight the severity of the vulnerability

Sir Dystic
Uh?

hey its me jenny tell me what u has been transferred.

OK
Beware of Geeks...
Subject: hey its me jenny tell me what u think about my pic / i m

Date: 08/26/1999 4:27:43 AM Eastern Daylight Time
From: BDASSGM
BCC: ACDS

File: JENN.SHS (243856 bytes)
DL Time (45333 bps): < 1 minute

I have blond hair
I go to school at BVDA in FLORDIA
I model for aqua pools
I like sports and I like you
Tell me what u think about my pic : D
<3 jenny
REMINDER: AOL Staff will never ask for your password or billing information.

E-mail Attachment Warning from AOL Neighborhood Watch

Warning! If you don't know who sent you this e-mail, do not download the attached file. This file contains executable code.

There is a chance that the attached file could contain a computer virus that may compromise the security of your AOL account, contain objectionable graphics, or damage computer files. Be cautious in downloading it.

Note: Parents may restrict their children from receiving e-mail with file attachments. To find out more, go to Keyword: Parental Controls. For more information about AOL's online safety features, go to Keyword: Neighborhood Watch.

Do you wish to download this file?

[Yes] [No]

Don't show me this warning again.
Bering Gifts

hey its me jenny tell me what u has been transferred.

OK
Nightmares

- Sophisticated scans
- Evil genius
- Collaboration
- Mentor
- Oh Gooey-gooey!
Basics

- Passwords (The road to damnation is paved with good intentions)
- Gratuitous functions
- Hardware has never been cheaper
- Currency (it’s more than money)
- Better is the Enemy of Good
- Salaries count
- Risk Management **not** Risk Avoidance!
Suggested Reading

At Large

Maximum Security

$10.40

$39.99
Contact

dkennedy@icsa.net

PGP Key ID: \textcolor{red}{0x2C 72226D}

PGP Fingerprint:

\textcolor{red}{45FB C B2C 37C9 D2AF 1FE6 C089 A490 2F82}