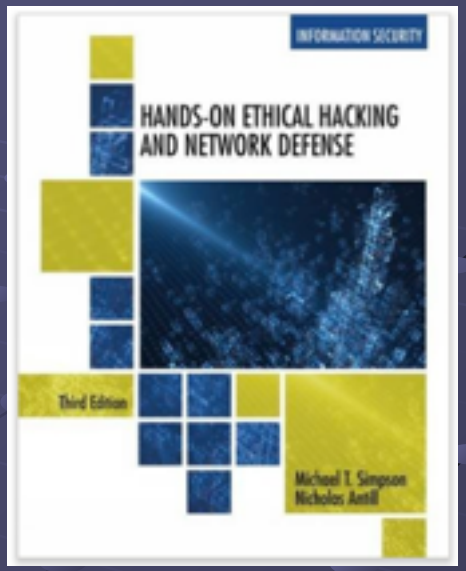
THOMSON
COURSE TECHNOLOGY

Hands-On Ethical Hacking and Network Defense



Chapter 3
Network and Computer Attacks

Last modified 1-11-17

Objectives

- Describe the different types of malicious software
- Describe methods of protecting against malware attacks
- Describe the types of network attacks
- Identify physical security attacks and vulnerabilities

Malicious Software (Malware)

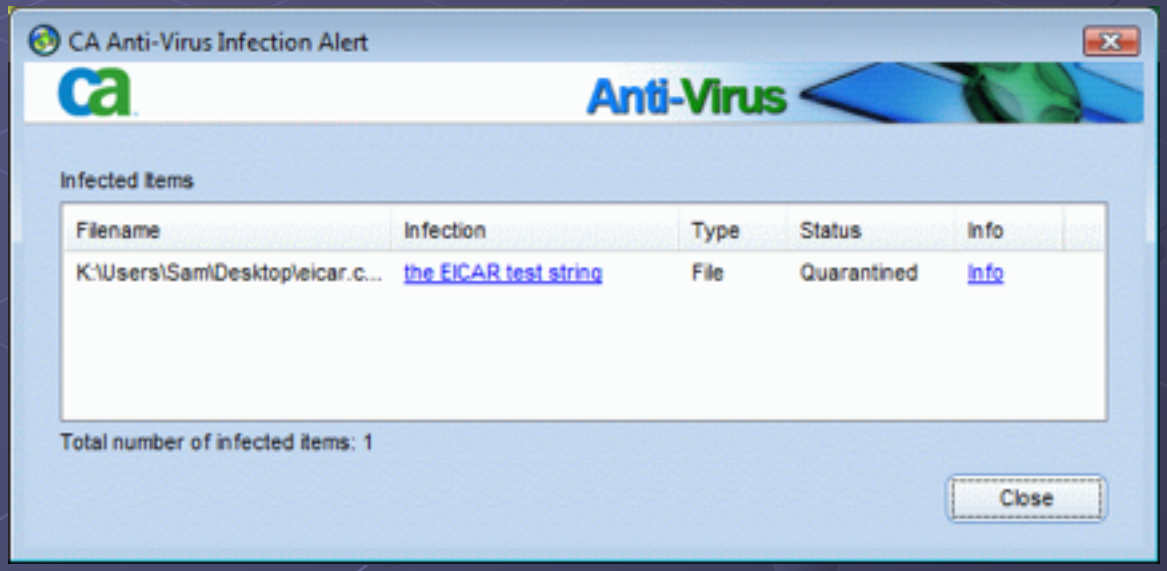
- Network attacks prevent a business from operating
- Malicious software (Malware) includes
  - Virus
  - Worms
  - Trojan horses
- Goals
  - Destroy data
  - Corrupt data
  - Shutdown a network or system

Viruses

- Virus attaches itself to an executable file
- Can replicate itself through an executable program
  - Needs a host program to replicate
- No foolproof method of preventing them

Antivirus Software

- Detects and removes viruses
- Detection based on virus signatures
- Must update signature database periodically
- Use automatic update feature



Common Viruses

Virus	Description
Gumblar	First detected in March 2009, it spread by mass hacking of hundreds of thousands of Web sites, which then exploited visiting browsers via Adobe PDF and Flash vulnerabilities. The malware steals FTP credentials that are used to further compromise Web sites the victim maintains. It also hijacks Google searches and blocks access to antivirus update sites to prevent removal. Recent variations install a backdoor that attempts to connect to a botnet.
Luckysploit	It's actually the attack side of a sophisticated cybercrime toolkit that spreads when Web surfers visit a hacked Web site hosting the malware. It uses obfuscated JavaScript code and asymmetric key encryption to prevent detection. The JavaScript code also targets victims based on recent vulnerabilities in OSs, applications, browser plug-ins, and so on.
Zlob	Purported to be the work of the Russian Business Network, Zlob has dozens of variants, some of which spread by masquerading as a codec needed to view an enticing video. Several variants are associated with "scareware," fake antivirus downloads that change home router settings to redirect victims to more malicious sites.
Gpcode	This "ransomware" virus detected in 2008 isn't widespread but is unique because it uses practically unbreakable 1024-bit asymmetric key encryption to hide a user's documents on the computer and hold them for ransom until the victim pays to get the encryption key.

Los Angeles college pays $28,000 in ransomware

JANUARY 10, 2017, 9:35 AM

A community college in the San Fernando Valley has become one of the latest institutions to pay ransom to hackers who took control of its computer system.

Los Angeles Valley College in Valley Glen said it paid $28,000 in bitcoins to the hackers, who had used malicious software to commandeer a variety of systems, including key computers and emails.

Ransomware
Encrypts files, demands ransom for the key
Doesn't need to be reported as a breach, because no data was stolen

Base 64 Encoding

- Used to evade anti-spam tools, and to obscure passwords
- Encodes six bits at a time (0 – 63) with a single ASCII character
  - A - Z: 0 – 25
  - a – z: 26 – 51
  - 1 – 9: 52 – 61
  - + and - 62 and 63
    - See links Ch 3a, 3b

Base64 Example

Input String	O	R	A	C	L	E	.	.
Binary Representation	01001111_2	01010010_2	01000001_2	01000011_2	01001100_2	01000101_2	.	.
After regrouping into 6-bit groups. *[Binary and decimal equivalents are shown.]*	010011_2 [19_{10}]	110101_2 [53_{10}]	001001_2 [9_{10}]	000001_2 [1_{10}]	010000_2 [16_{10}]	110100_2 [52_{10}]	110001_2 [49_{10}]	$000101\backslash_2$ [5_{10}]
After mapping the above eight 8-bit bytes using Table 1	T	1	J	B	Q	0	x	F

Base64 encoded string : **T1JBQ0xF**

- ORACLE -> T1JBQ0xF
  - Link Ch 3r

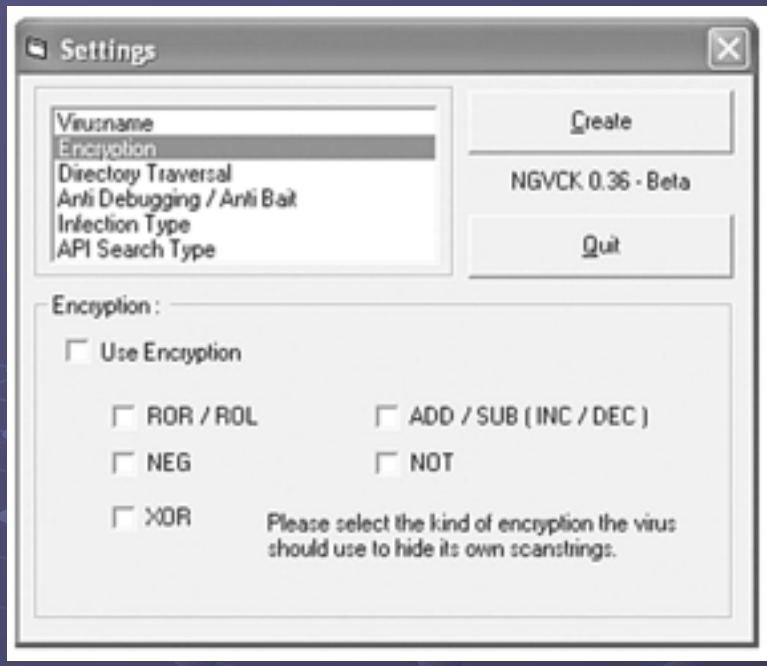
Viruses (continued)

- Commercial base 64 decoders
- Shell
  - Executable piece of programming code
  - Should not appear in an e-mail attachment

Macro Viruses

- Virus encoded as a macro
- Macro
  - Lists of commands
  - Can be used in destructive ways
- Example: Melissa
  - Appeared in 1999
  - It is very simple – see link Ch 3c for source code

Writing Viruses

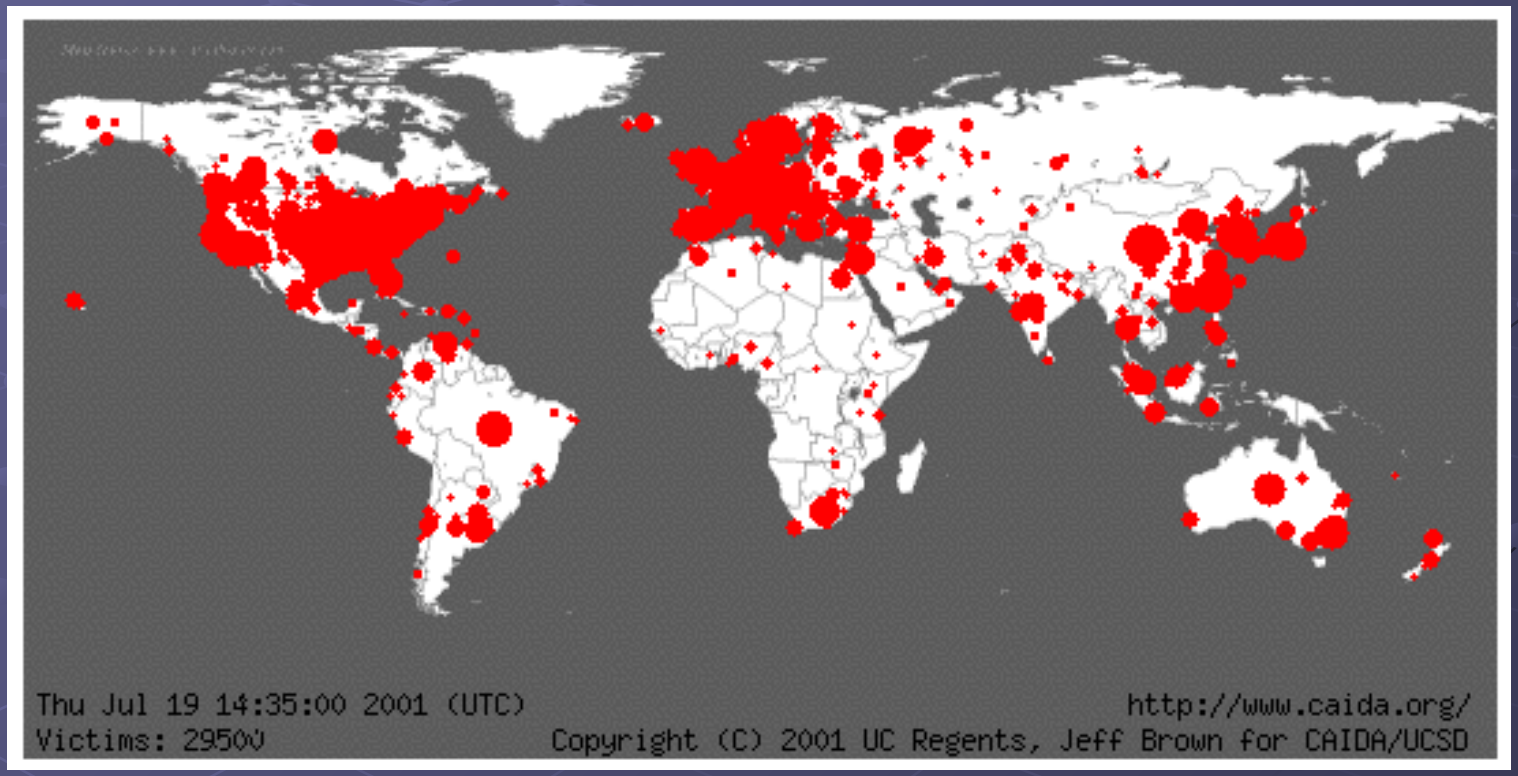


- Even nonprogrammers can create macro viruses
  - Instructions posted on Web sites
  - Virus creation kits available for download (see link Ch 3d)
- Security professionals can learn from thinking like attackers
  - But don’t create and release a virus! People get long prison terms for that.

Worms

- Worm
  - Replicates and propagates without a host, often through email
- Infamous examples
  - Code Red
  - Nimda
- Can infect every computer in the world in a short time
  - At least in theory

Spread of Code Red Worm



- See link Ch 3u

ATM Machine Worms

- Cyberattacks against ATM machines
- Slammer and Nachi worms
- Trend produces antivirus for ATM machines
  - See links Ch 3g, 3h, 3i
- Nachi was written to clean up damage caused by the Blaster worm, but it got out of control
  - See link Ch 3j
- Diebold was criticized for using Windows for ATM machines, which they also use on voting machines

Important Worms

Worm	Description
Storm	Detected in January 2007, it's spread by automatically generated e-mail messages. It's estimated that this botnet Trojan program and its variants infected millions of systems.
Mytob	Detected in 2005, it's a hybrid worm with backdoor capabilities spread by mass e-mailing and exploiting Windows vulnerabilities.
Waledac	This e-mail worm harvests and forwards passwords and spreads itself in an e-mail with an attachment called eCard.exe. It has many variants that can be controlled remotely. A recent variant uses a geographic IP address lookup to customize the e-mail message so that it looks like a Reuters news story about a dirty bomb that exploded in a city near the victim.
Conficker	Detected in late 2008, this botnet worm and its variants propagated through the Internet by using a Microsoft network service vulnerability. It updates itself dynamically but can be detected remotely with a standard port scanner, such as Nmap, and a special Conficker signature plug-in.
Mod_ssl	Detected in 2002, this worm affects Linux systems running Apache OpenSSL. It scans for vulnerable systems on TCP port 80 and attempts to deliver the exploit code through TCP port 443. A system infected with this worm begins spreading it to other systems on a network. See VU#102795 and CA-2002-23 at *www.kb.cert.org/vuls* for more information; this site cross-references vulnerabilities listed at *www.cve.mitre.org*.
Slammer	Detected in 2003, this worm was purported to have shut down more than 13,000 ATMs of one of the largest banks in America by infecting database servers located on the same network.

Trojan Programs

- Insidious attack against networks
- Disguise themselves as useful programs
  - Hide malicious content in program
    - Backdoors
    - Rootkits
  - Allow attackers remote access

Firewalls

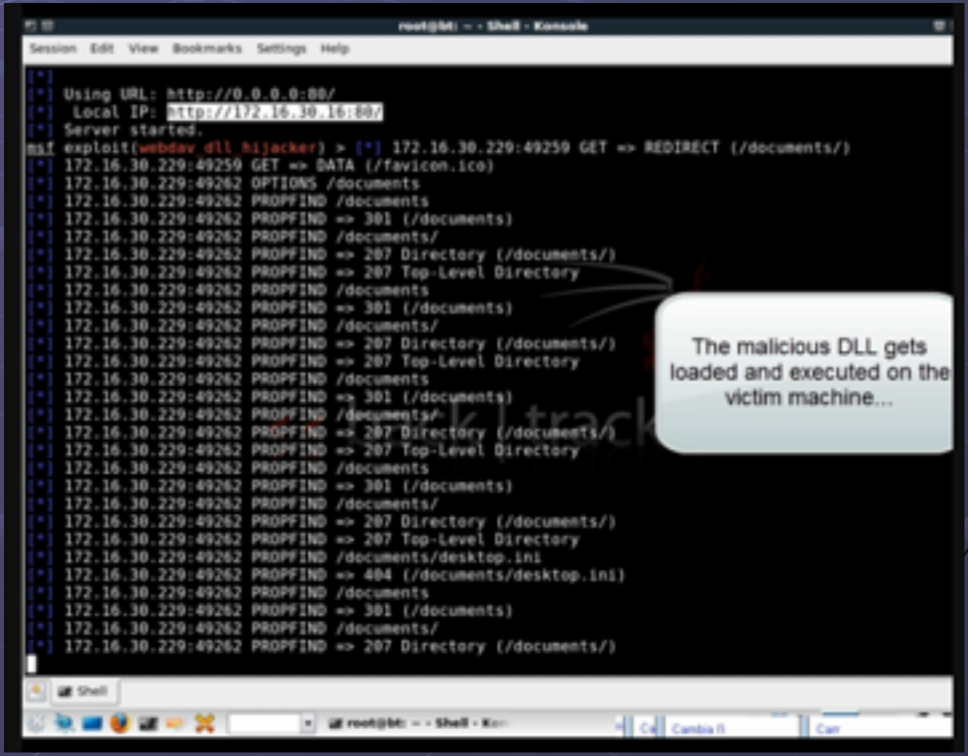
- Identify traffic on uncommon ports
- Can block this type of attack, if your firewall filters outgoing traffic
  - Windows Firewall in XP SP2, Vista, and Win 7 does not filter outgoing traffic by default
- Trojan programs can use known ports to get through firewalls
  - HTTP (TCP 80) or DNS (UDP 53)

Table 3-3 Trojan programs and ports

Trojan Program	TCP Ports Used
W32.Korgo.A	13, 2041, and 3067
Backdoor.Rtkit.B	445
Backdoor.Systsec, Backdoor.Zincite.A	1034
W32.Beagle.Y@mm	1234
Trojan.Tilser	6187
Backdoor.Hacarmy.C, Backdoor.Kaitex, Backdoor.Clt, Backdoor.IRC.Flood.E, Backdoor.Spigot.C, Backdoor.IrcContact, Backdoor.DarkFtp, Backdoor.Slackbot.B	6667
Backdoor.Danton	6969
Backdoor.Nemog.C	4661, 4242, 8080, 4646, 6565, and 3306

Windows DLL Hijacking Vulnerability

- DLL files are loaded from the incorrect directory
- Affects over 200 applications on every version of Windows
- No good patch yet (8-31-2010)
  - Link Ch 3s, 3t, 3w



Spyware

- Sends information from the infected computer to the attacker
  - Confidential financial data
  - Passwords
  - PINs
  - Any other stored data
- Can register each keystroke entered (keylogger)
- Prevalent technology
- Educate users about spyware

Deceptive Dialog Box

Figure 3-2 A spyware initiation program

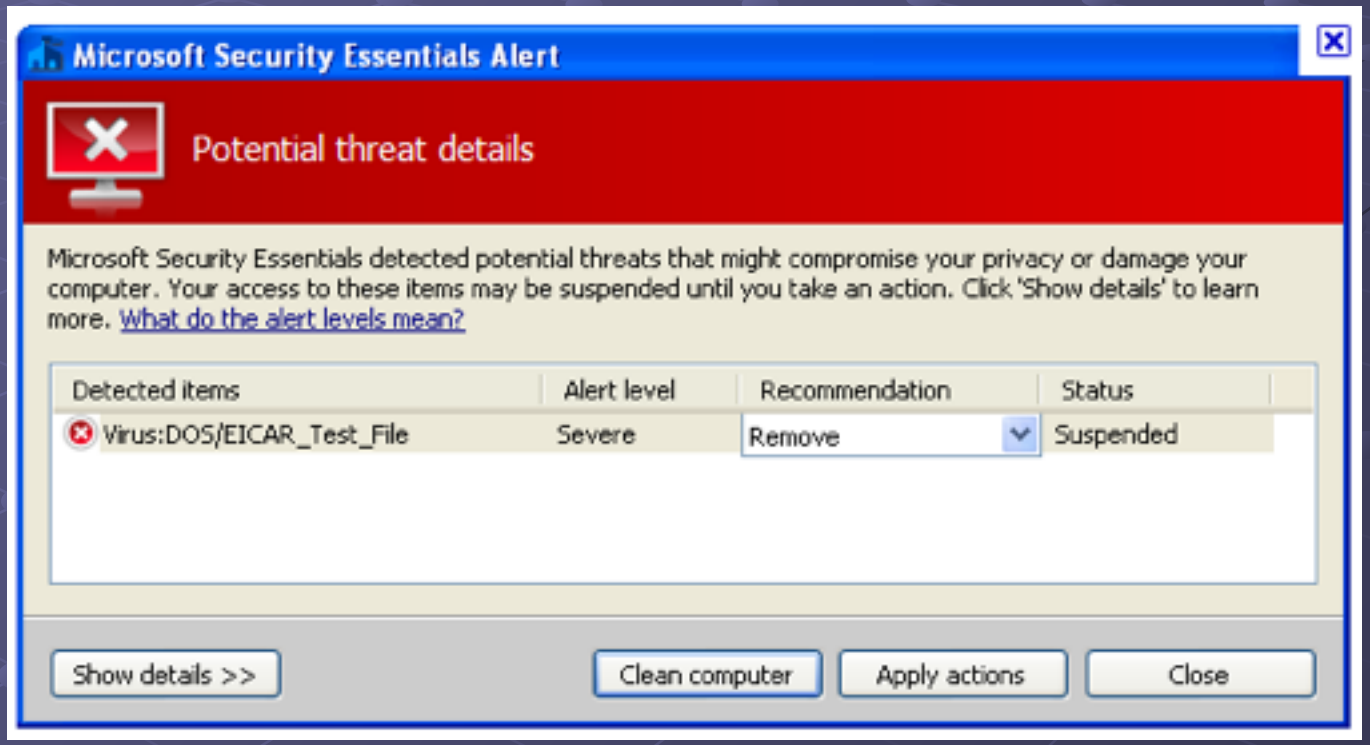
Adware

- Similar to spyware
  - Can be installed without the user being aware
- Sometimes displays a banner
- Main goal
  - Determine user's online purchasing habits
  - Tailored advertisement
- Main problem
  - Slows down computers

Protecting Against Malware Attacks

- Difficult task
- New viruses, worms, Trojan programs appear daily
- Antivirus programs offer a lot of protection
- Educate your users about these types of attacks

Virus Alert


Microsoft Security Essentials Alert
Potential threat details
Microsoft Security Essentials detected potential threats that might compromise your privacy or damage your computer. Your access to these items may be suspended until you take an action. Click 'Show details' to learn more. What do the alert levels mean?
Detected items
Alert level
Recommendation
Status
Virus:DOS/EICAR_Test_File
Severe
Remove
Suspended
Show details >>
Clean computer
Apply actions
Close

Educating Your Users

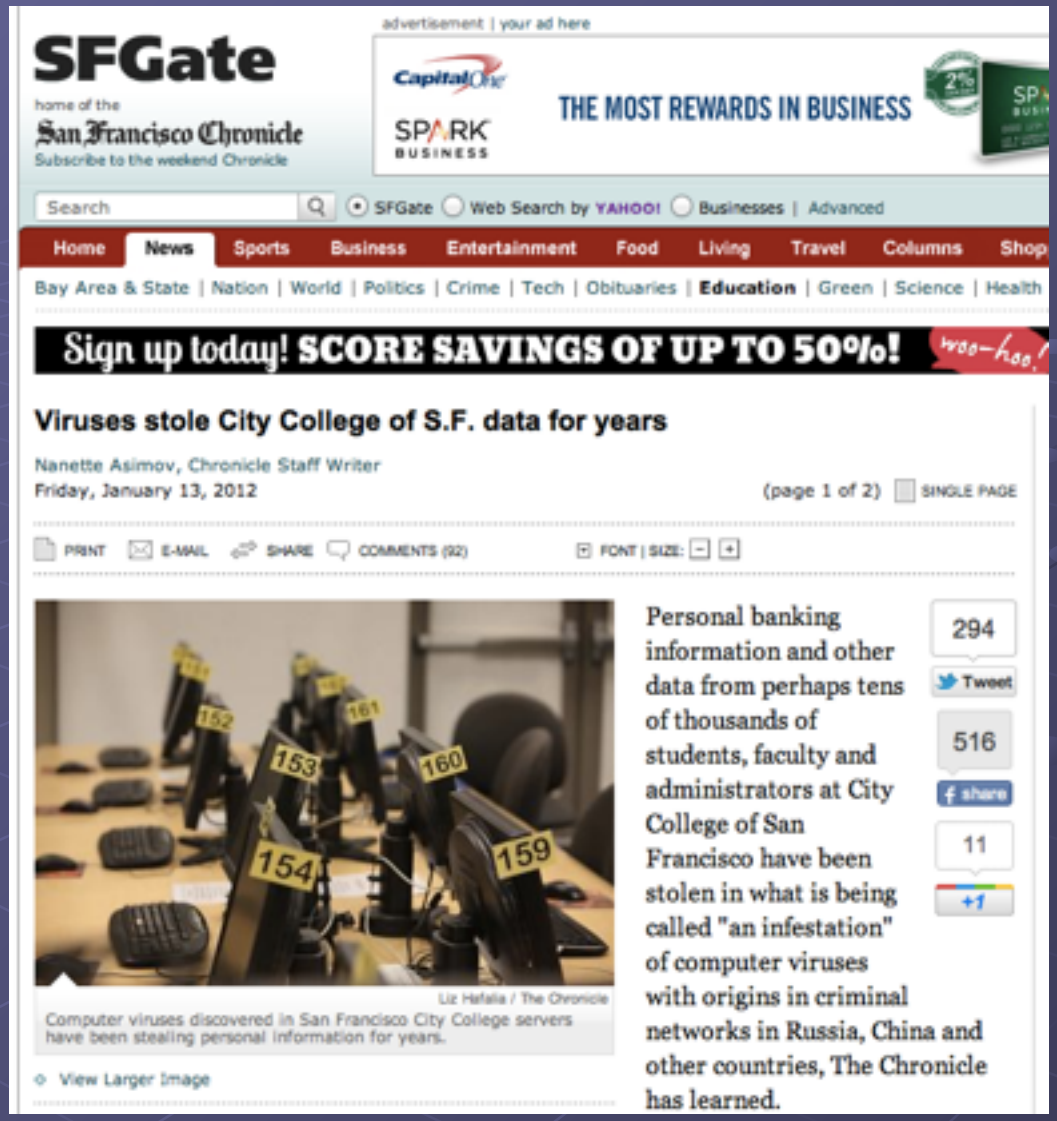
- Structural training
  - Includes all employees and management
  - E-mail monthly security updates
- Update virus signature database automatically

Educating Your Users

- SpyBot and Ad-Aware
  - Help protect against spyware and adware
  - Windows Defender is excellent too
- Firewalls
  - Hardware (enterprise solution)
  - Software (personal solution)
  - Can be combined
- Intrusion Detection System (IDS)
  - Monitors your network 24/7

FUD

- Fear, Uncertainty and Doubt
  - Avoid scaring users into complying with security measures
  - Sometimes used by unethical security testers
  - Against the OSSTMM's Rules of Engagement
- Promote awareness rather than instilling fear
  - Users should be aware of potential threats
  - Build on users' knowledge


SFGate
home of the
San Francisco Chronicle
Subscribe to the weekend Chronicle
advertisement | your ad here
Capital One
SPARK BUSINESS
THE MOST REWARDS IN BUSINESS
Search
SFGate
Web Search by YAHOO!
Businesses
Advanced
Home
News
Sports
Business
Entertainment
Food
Living
Travel
Columns
Shop
Bay Area & State | Nation | World | Politics | Crime | Tech | Obituaries | Education | Green | Science | Health
Sign up today! SCORE SAVINGS OF UP TO 50%!
Viruses stole City College of S.F. data for years
Nanette Asimov, Chronicle Staff Writer
Friday, January 13, 2012
(page 1 of 2)
SINGLE PAGE
PRINT
E-MAIL
SHARE
COMMENTS (92)
FONT | SIZE:
152
161
153
160
154
159
Liz Hafalia / The Chronicle
Computer viruses discovered in San Francisco City College servers have been stealing personal information for years.
View Larger Image
Personal banking information and other data from perhaps tens of thousands of students, faculty and administrators at City College of San Francisco have been stolen in what is being called "an infestation" of computer viruses with origins in criminal networks in Russia, China and other countries, The Chronicle has learned.
294
Tweet
516
share
11
+1

- Link Ch 3v

Intruder Attacks on Networks and Computers

- Attack
  - Any attempt by an unauthorized person to access or use network resources
- Network security
  - Security of computers and other devices in a network
- Computer security
  - Securing a standalone computer--not part of a network infrastructure
- Computer crime
  - Fastest growing type of crime worldwide

Denial-of-Service Attacks

- Denial-of-Service (DoS) attack
  - Prevents legitimate users from accessing network resources
  - Some forms do not involve computers, like feeding a paper loop through a fax machine
- DoS attacks do not attempt to access information
  - Cripple the network
  - Make it vulnerable to other type of attacks

Testing for DoS Vulnerabilities

- Performing an attack yourself is not wise
  - You only need to prove that an attack could be carried out

Distributed Denial-of-Service Attacks

- Attack on a host from multiple servers or workstations
- Network could be flooded with billions of requests
  - Loss of bandwidth
  - Degradation or loss of speed
- Often participants are not aware they are part of the attack
  - They are remote-controlled "zombies"

Buffer Overflow Attacks

- Vulnerability in poorly written code
  - Code does not check predefined size of input field
- Goal
  - Fill overflow buffer with executable code
  - OS executes this code
  - Can elevate attacker's permission to Administrator or even Kernel
- Programmers need special training to write secure code

Buffer overflow	Description
Solaris X Window Font Service	This buffer overflow affects Sun Microsystems Solaris 2.5.1, 2.6, 7, 8, and 9 and Solaris X Window Font Service systems. It allows attackers to run arbitrary code in memory. See VU#312313 (*www.kb.cert.org/vuls*) for more information.
Windows Server	Microsoft Security Bulletin MS08-067 (*www.microsoft.com/technet/security/Bulletin/MS08-067.mspx*) discusses this buffer overflow vulnerability, which makes it possible for attackers to run arbitrary code placed in memory. This vulnerability allowed the Conficker worm to spread.
Remote Sendmail	This buffer overflow vulnerability affects all versions of Sendmail Pro and some versions of Sendmail Switch. The vulnerability allows attackers to gain root privileges on the attacked system. See VU#398025 for more details.
Windows Messenger Service	The Windows Messenger Service has a buffer overflow vulnerability that enables the attacker to run arbitrary code and gain privileges to the attacked system.
Windows Help and Support Center	Contains buffer overflow in code used to handle Human Communications Protocol (HCP). A buffer overflow vulnerability in the Help and Support Center function affects Windows XP and Windows Server 2003. The vulnerability allows attackers to create a URL that could run arbitrary code at the local computer security level when users enter that URL.
Sendmail	All systems running Sendmail versions before 8.12.10, including UNIX and Linux systems, are vulnerable to a buffer overflow attack that enables attackers to possibly elevate privileges to that of the root user.
Microsoft RPCSS Service	There are two buffer overflow vulnerabilities in the RPCSS Service, which handles DCOM messages. This service is enabled by default on many versions of Windows, but the vulnerability affects only Windows 2000 systems. For more information, see VU#483492 and VU#254236.
Internet Explorer	A total of five vulnerabilities affect Microsoft systems running Internet Explorer 5.01, 5.50, and 6.01. For more information, see Microsoft Security Bulletin MS03-032.

Ping of Death Attacks

- Type of DoS attack
- Not as common as during the late 1990s
- How it works
  - Attacker creates a large ICMP packet
    - **More than 65,535 bytes**
  - Large packet is fragmented at source network
  - Destination network reassembles large packet
  - Destination point cannot handle oversize packet and crashes
  - Modern systems are protected from this (Link Ch 3n)

AUGUST 13, 2013

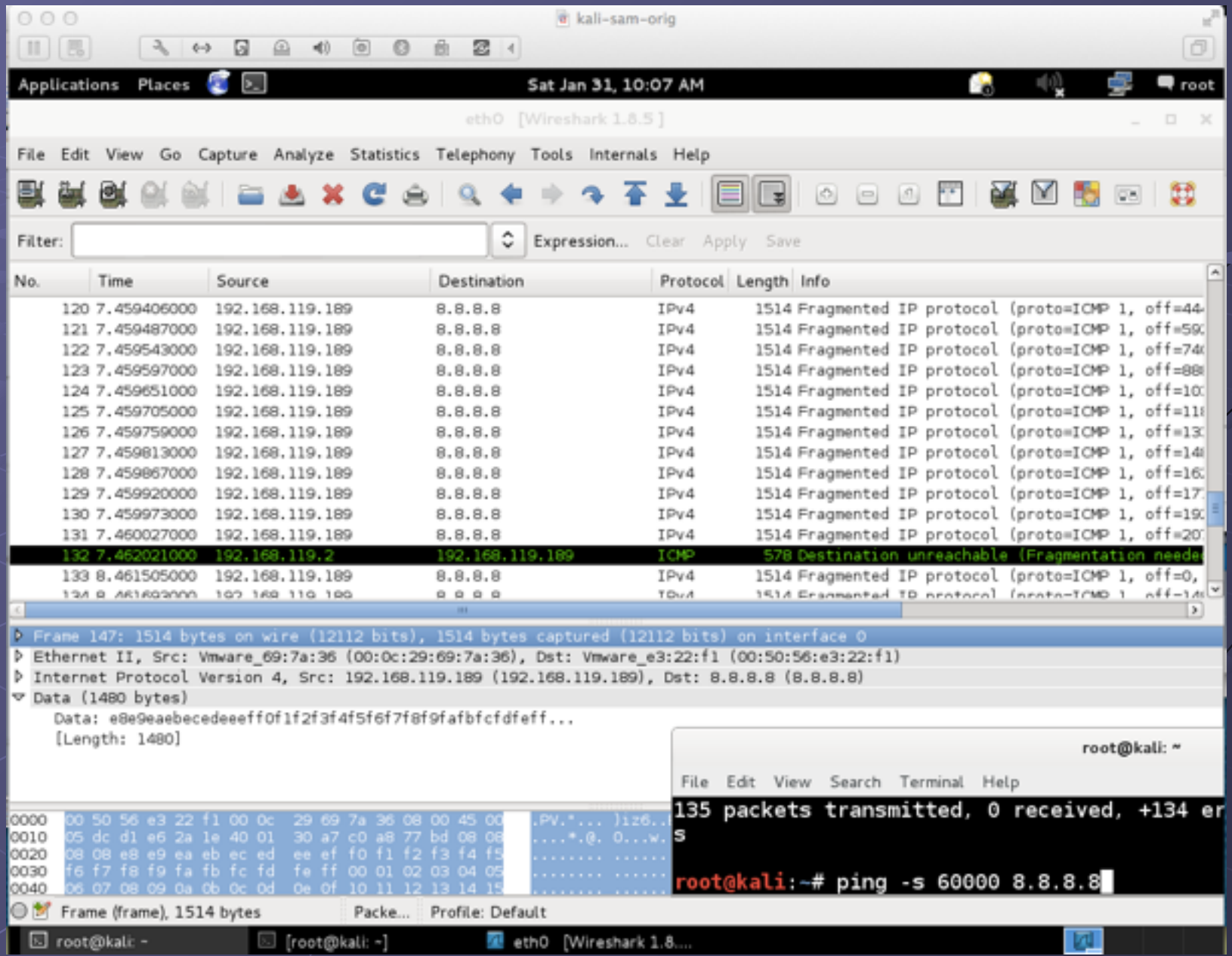
Microsoft Patch Tuesday: The Ping of Death returns, IPv6-style

This month's round of Microsoft patches address must-fix vulnerabilities in Internet Explorer and Microsoft Mail

By Joab Jackson | IDG News Service

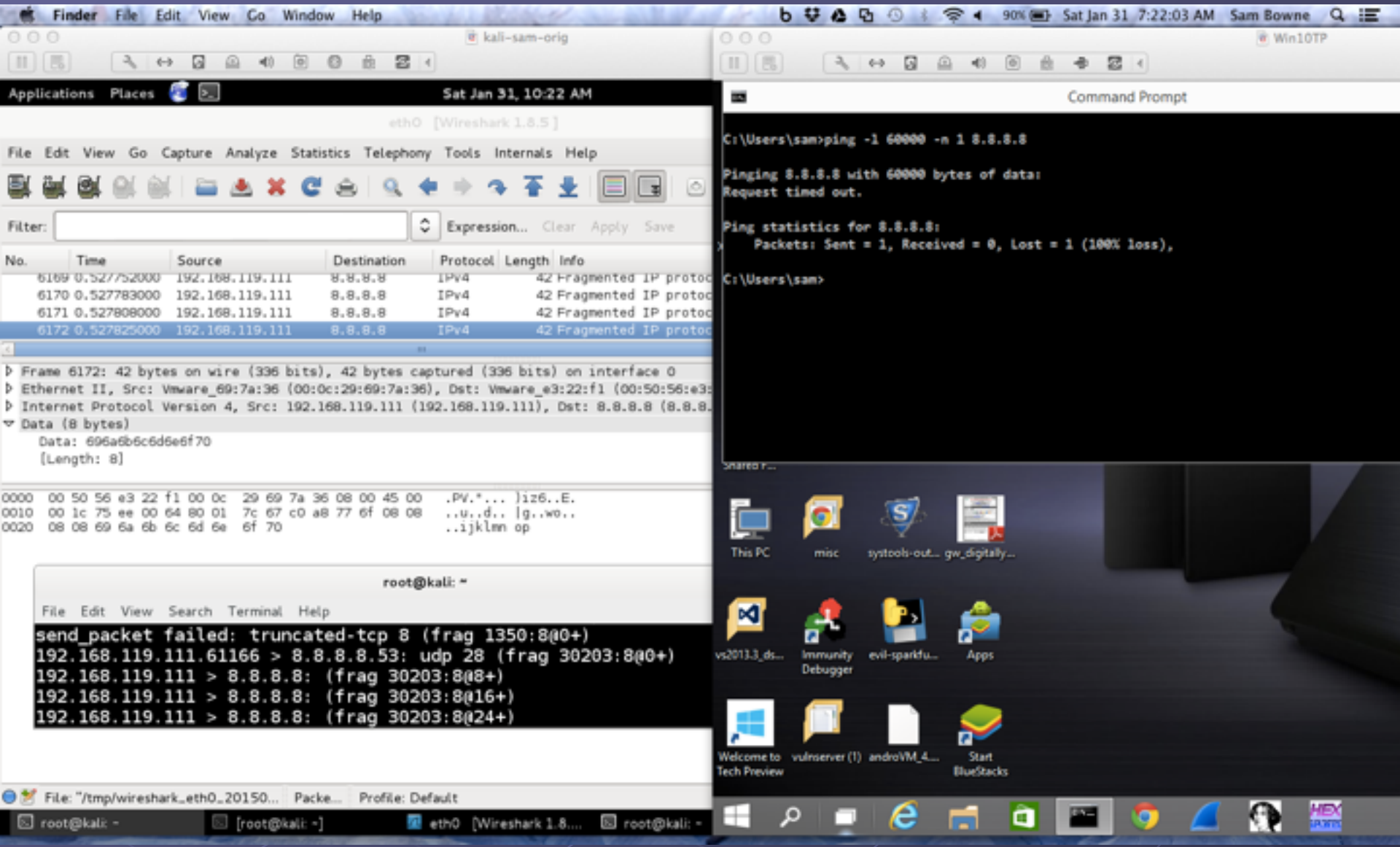
- Link Ch3x

Ping Fragmentation Example



Fragrouter Demo

- Kali Linux
  - fragrouter –F 1
- Another VM on same network, set default route to Kali's IP address
- All network traffic will be fragmented at layer 3 into 8-byte packets
- Often bypasses IDS


Finder File Edit View Go Window Help
Sat Jan 31 7:22:03 AM Sam Bowne
kali-sam-orig
Win10TP
Applications Places
Sat Jan 31, 10:22 AM
eth0 [Wireshark 1.8.5]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
6169 0.527752000 192.168.119.111 8.8.8.8 IPv4 42 Fragmented IP protoc
6170 0.527783000 192.168.119.111 8.8.8.8 IPv4 42 Fragmented IP protoc
6171 0.527808000 192.168.119.111 8.8.8.8 IPv4 42 Fragmented IP protoc
6172 0.527825000 192.168.119.111 8.8.8.8 IPv4 42 Fragmented IP protoc
Frame 6172: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
Ethernet II, Src: Vmware_69:7a:36 (00:0c:29:69:7a:36), Dst: Vmware_e3:22:f1 (00:50:56:e3:
Internet Protocol Version 4, Src: 192.168.119.111 (192.168.119.111), Dst: 8.8.8.8 (8.8.8.
Data (8 bytes)
Data: 696a6b6c6d6e6f70
[Length: 8]
0000 00 50 56 e3 22 f1 00 0c 29 69 7a 36 08 00 45 00 .PV."...)iz6..E.
0010 00 1c 75 ee 00 64 80 01 7c 67 c0 a8 77 6f 08 08 ..u..d.. |g..wo..
0020 08 08 69 6a 6b 6c 6d 6e 6f 70 ..ijklmn op
root@kali: ~
File Edit View Search Terminal Help
send_packet failed: truncated-tcp 8 (frag 1350:8@0+)
192.168.119.111.61166 > 8.8.8.8.53: udp 28 (frag 30203:8@0+)
192.168.119.111 > 8.8.8.8: (frag 30203:8@8+)
192.168.119.111 > 8.8.8.8: (frag 30203:8@16+)
192.168.119.111 > 8.8.8.8: (frag 30203:8@24+)
File: "/tmp/wireshark_eth0_20150... Packe... Profile: Default
root@kali: ~
[root@kali: ~]
eth0 [Wireshark 1.8....
root@kali: ~
Command Prompt
C:\Users\sam>ping -l 60000 -n 1 8.8.8.8
Pinging 8.8.8.8 with 60000 bytes of data:
Request timed out.
Ping statistics for 8.8.8.8:
Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
C:\Users\sam>
This PC
misc
systools-out...
gw_digitally...
vs2013.3_ds...
Immunity Debugger
evil-sparkfu...
Apps
Welcome to Tech Preview
vulnserver (1)
androVM_4...
Start BlueStacks

Session Hijacking

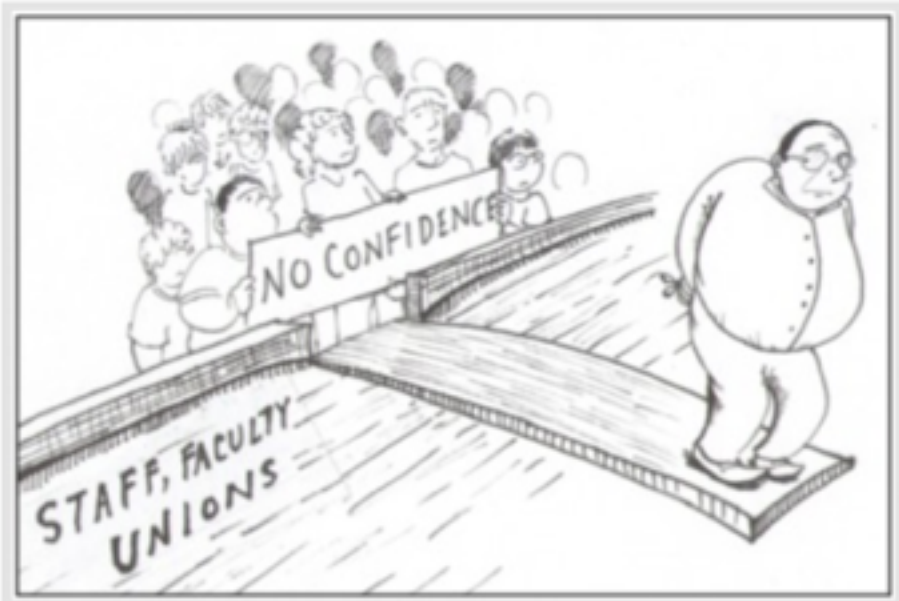
- Enables attacker to interrupt a TCP session
- Taking over another user's session

Addressing Physical Security

- Protecting a network also requires physical security
- Inside attacks are more likely than attacks from outside the company

Insider Threats

CCSF's CTO



An interpretive image of the "no confidence" petition. Art by Jessica Kwan/The Guardsman

San Francisco's NetAdmin

Mon 3-2
SCIE 200, 6 PM

Conrad del Rosario
Assistant District Attorney
San Francisco District Attorney's Office
White Collar Crimes Division

Case study on the Terry Childs case & more

image from BoingBoing

Cyber-Bullying Accusation

Company Goes After One Of The World's Biggest Cyber Bully's Sam Bowne

Company goes after one of the world's biggest cyber bully's sam bowne professor at the city college of san francisco city college employee uses school networks to commit cyber bullying

FOR IMMEDIATE RELEASE

PRLog (Press Release) - *Jan 07, 2011* -
COMPANY GOES AFTER ONE OF THE WORLD'S BIGGEST CYBER BULLY'S SAM BOWNE PROFESSOR AT THE CITY COLLEGE OF SAN FRANCISCO

Keyloggers

- Used to capture keystrokes on a computer
  - Hardware
  - Software
- Software
  - Behaves like Trojan programs
- Hardware
  - Easy to install
  - Goes between the keyboard and the CPU
  - KeyKatcher and KeyGhost

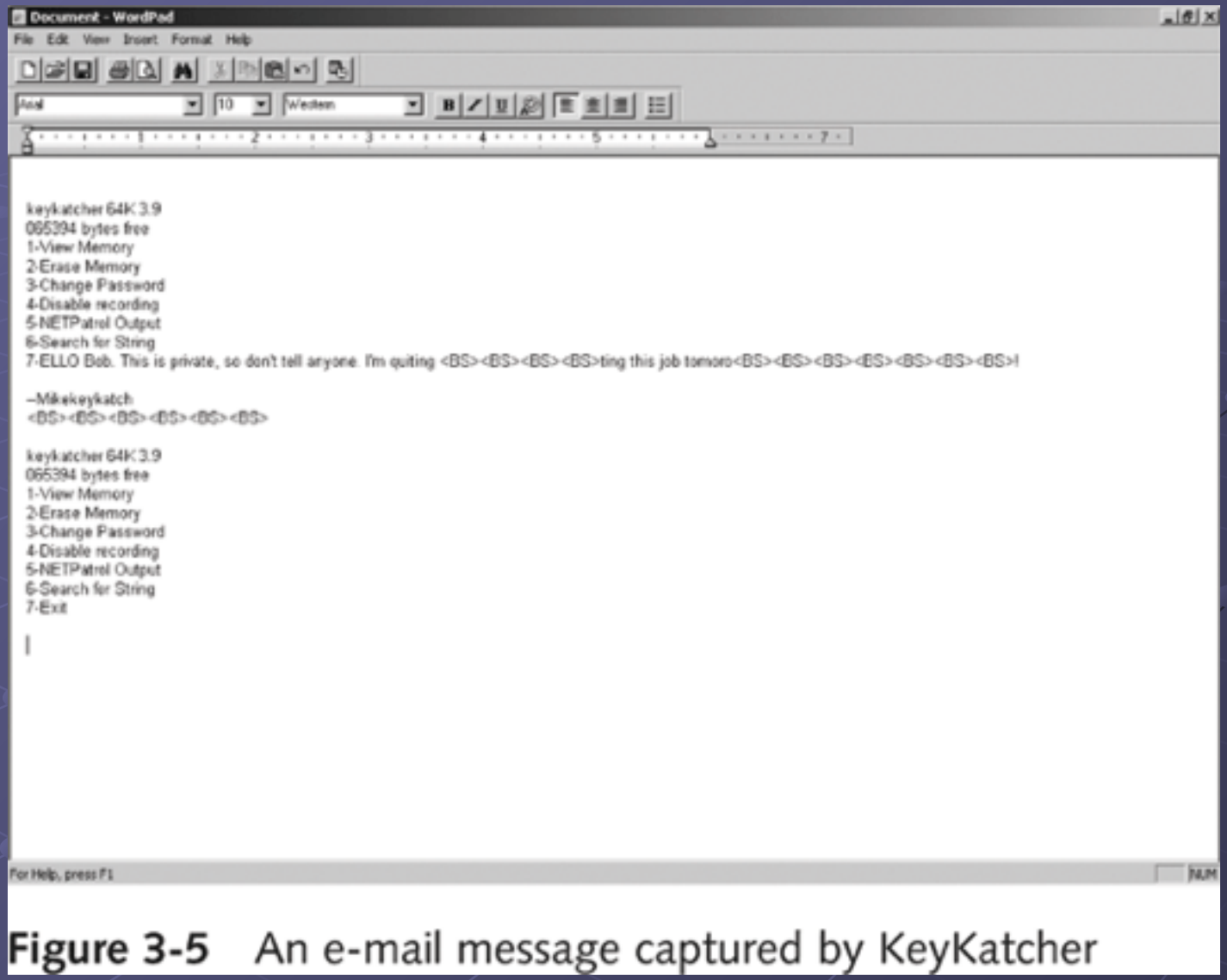


Figure 3-5 An e-mail message captured by KeyKatcher

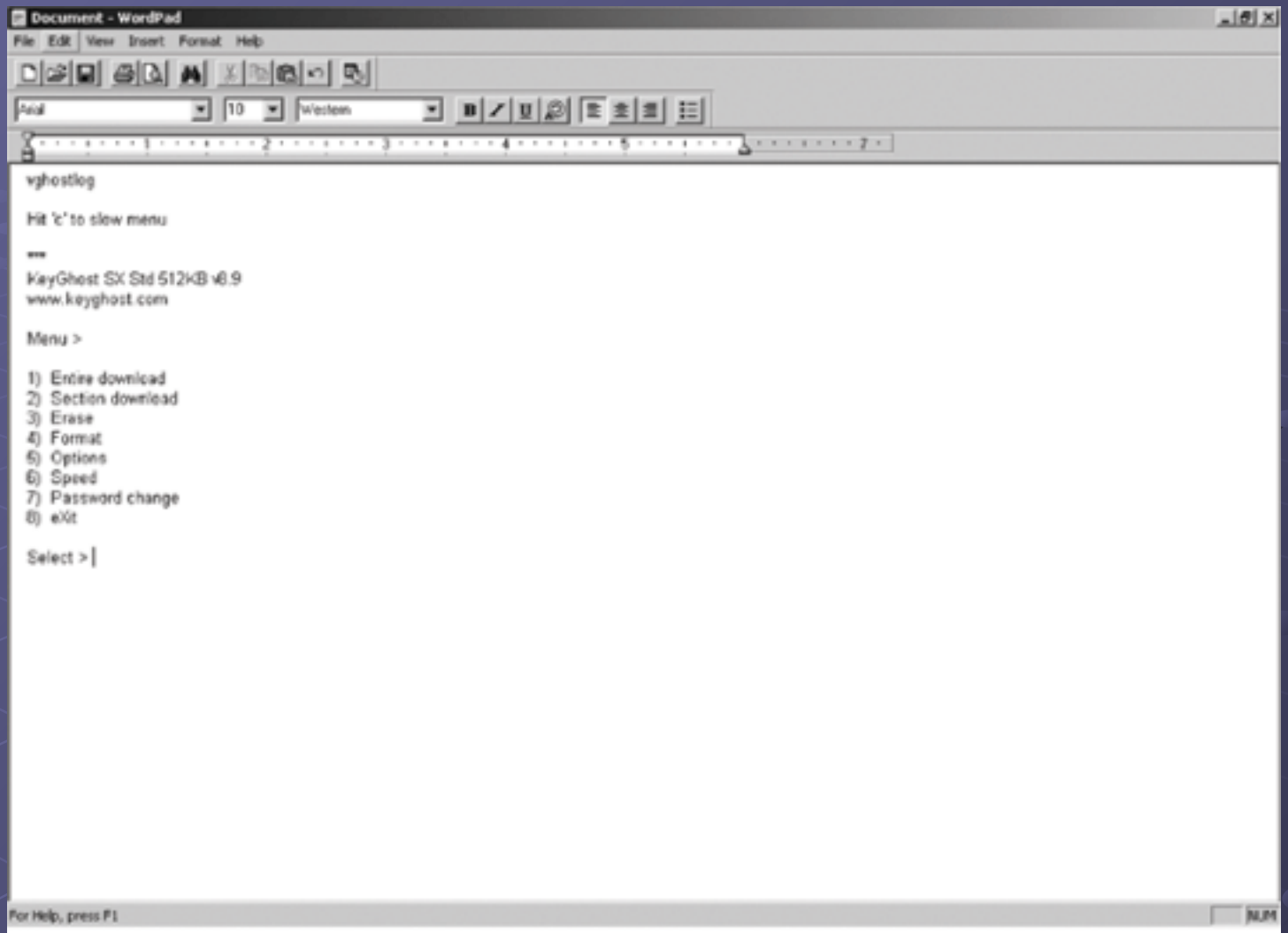


Figure 3-6 The KeyGhost menu

Keyloggers (continued)

- Protection
  - Software-based
    - Antivirus
  - Hardware-based
    - Random visual tests
    - Look for added hardware
    - Superglue keyboard connectors in

Behind Locked Doors

- Lock up your servers
  - Physical access means they can hack in
  - Consider Ophcrack – booting to a CD-based OS will bypass almost any security

Lockpicking

- Average person can pick deadbolt locks in less than five minutes
  - After only a week or two of practice
- Experienced hackers can pick deadbolt locks in under 30 seconds
- Bump keys are even easier (Link Ch 3o)

Card Reader Locks

- Keep a log of who enters and leaves the room
- Security cards can be used instead of keys for better security
  - Image from link Ch 3p