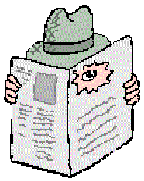


Computer Security

Tools

Tools

- Here is a list of potentially useful tools and utilities with which to fight the onslaught of viruses, worms, Trojan horses, and other malware.
- Don't consider it in any way a complete list! There are lots of other tools out there, which you can find easily via Google, et. al.
- Also, I've tended to focus on Windows-based tools (with some mention of Unix/Linux-based tools), because most of you have Windows machines. Also, I don't really have access to a Unix/Linux machine.

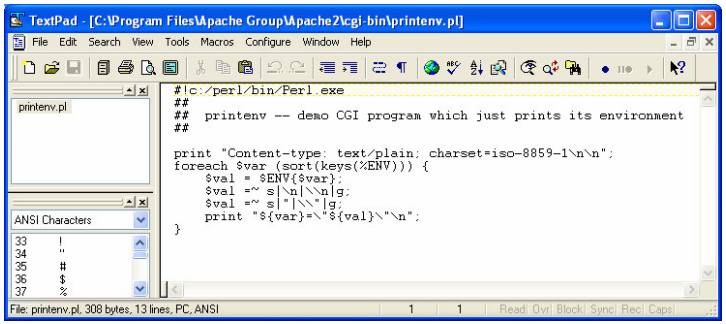
Resources

- **Malware: Fighting Malicious Code,** by Ed Skoudis, Lenny Zeltser, Prentice Hall PTR, 2003, **ISBN:** 0131014056
- **Counter Hack: A Step-by-Step Guide to Computer Attacks and Effective Defenses** by Ed Skoudis, Prentice Hall PTR , 2001, **ISBN:** 0130332739
- **How to Break Web Software : Functional and Security Testing of Web Applications and Web Services**, by Mike Andrews, James A. Whittaker, Addison-Wesley Professional, 2006, **ISBN:** 0321369440
- **The Software Vulnerability Guide (Programming Series) (Programming Series) (Paperback),** by Herbert H Thompson, Scott G Chase, Charles River Media, 2005, **ISBN:** 1584503580
- **Web Security, Privacy and Commerce, 2nd Edition (Paperback)**, by Simson Garfinkel, O'Reilly Media, Inc., 2002, **ISBN:** 0596000456
- **Hands-On Ethical Hacking and Network Defense (Paperback),** by Michael T. Simpson, Thomson Course Technology, 2005, **ISBN:** 0619217081

Use a Powerful Editor to be Able to Look at Lots of Different File Formats

The TextPad Editor

http://www.textpad.com/



Safer Browsing

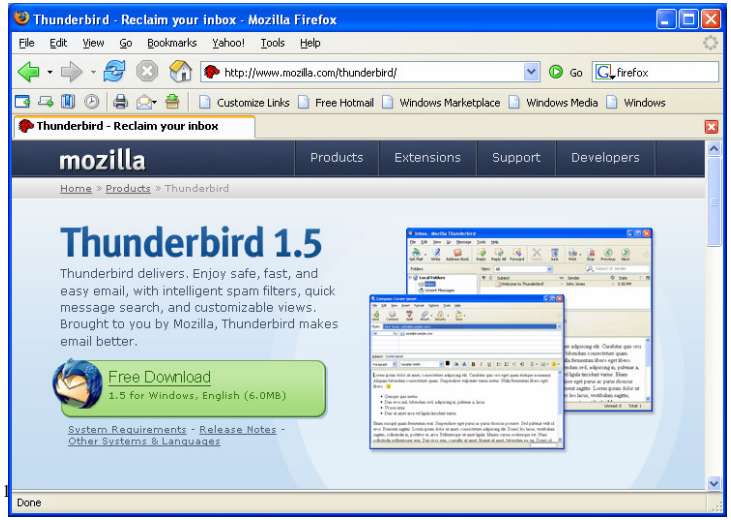
The Mozilla Firefox Browser

http://www.mozilla.com/firefox/

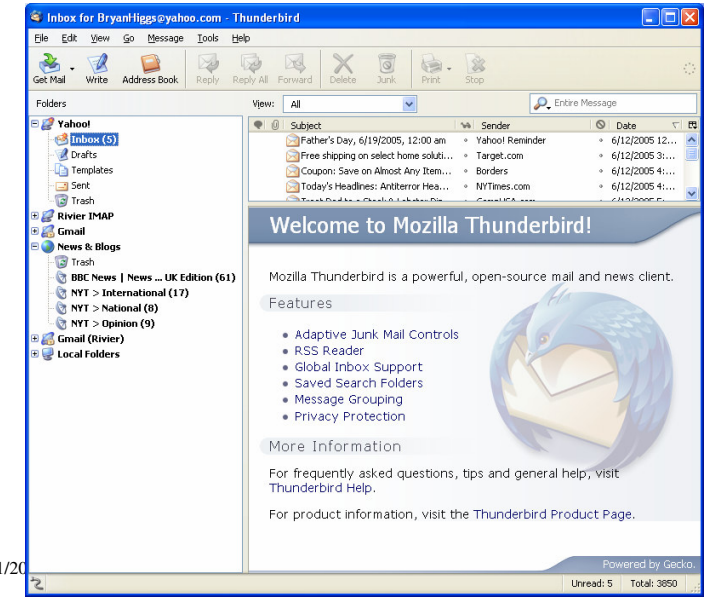
Safer eMail

The Mozilla Thunderbird Mail Client

http://www.mozilla.com/thunderbird/



The Mozilla Thunderbird Mail Client



Anti-Virus Protection

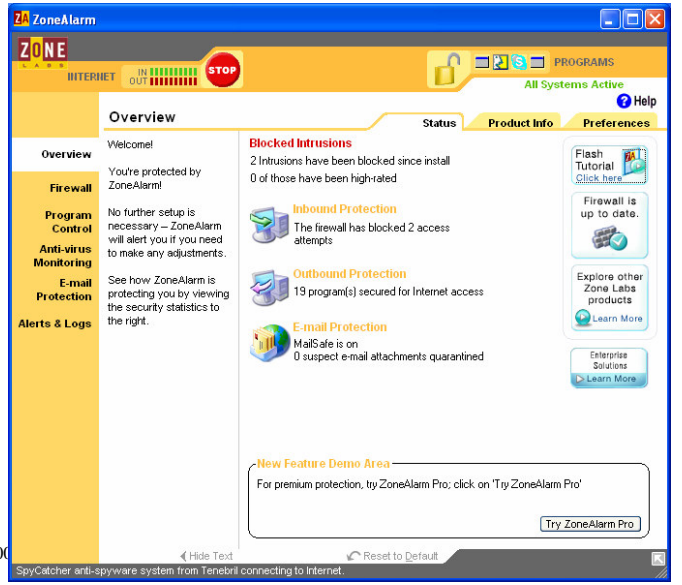
AVG Anti-Virus

http://free.grisoft.com/doc/2/lng/us/tpl/v5

Firewall

ZoneAlarm Firewall

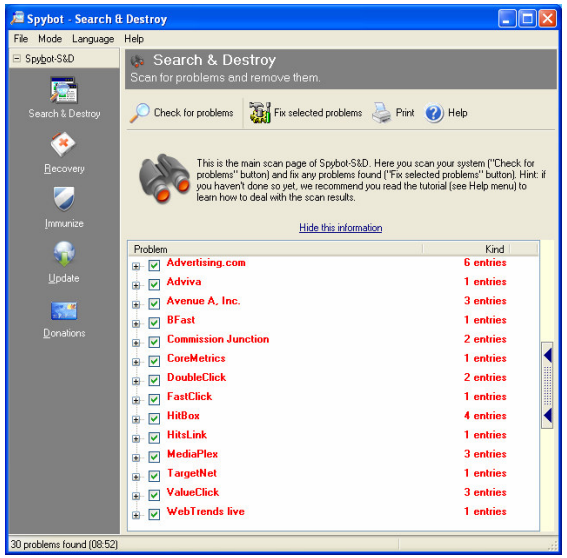
http://www.zonelabs.com/store/content/catalog/products/sku_list_za.jsp?dc=12bms&ctry=US&lang=en&lid=dbtopnav_zaav



Anti-Spyware

Spybot Search & Destroy

http://www.safer-networking.org/

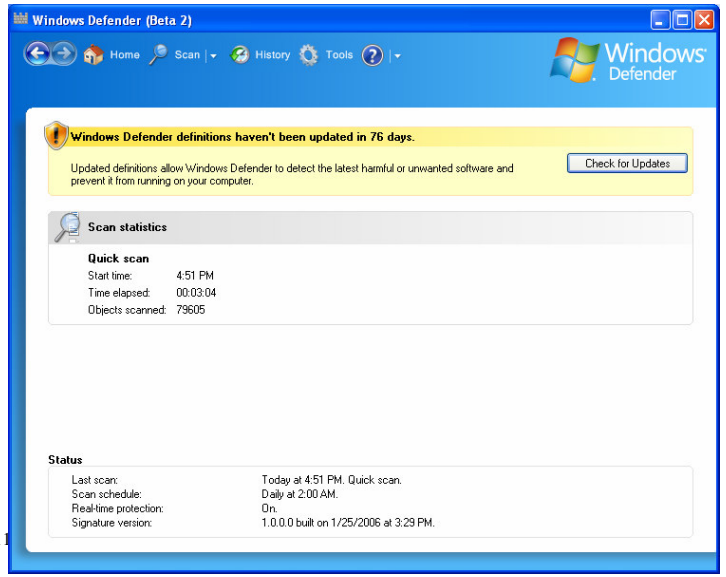


Ad-Aware

http://www.lavasoft.de/software/adaware/

Microsoft Windows Defender

http://www.microsoft.com/athome/security/spyware/software/default.mspx



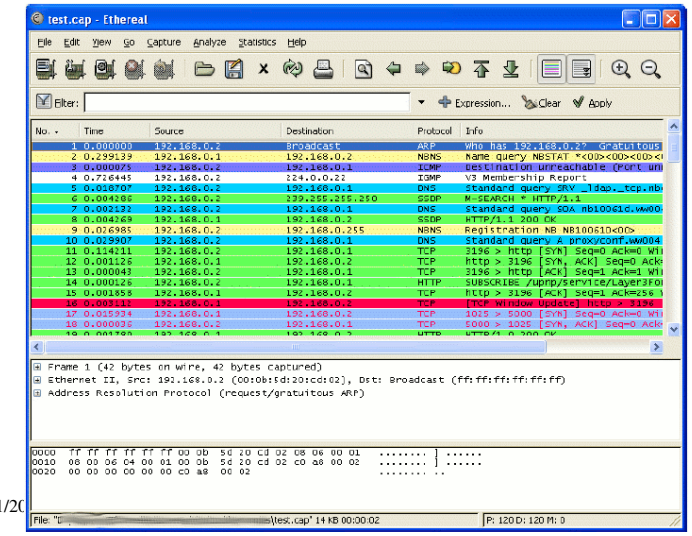
SpyCatcher Express

http://www.tenebril.com/consumer/spyware/spycatcher-express.php

Tracing HTTP and Other Protocols

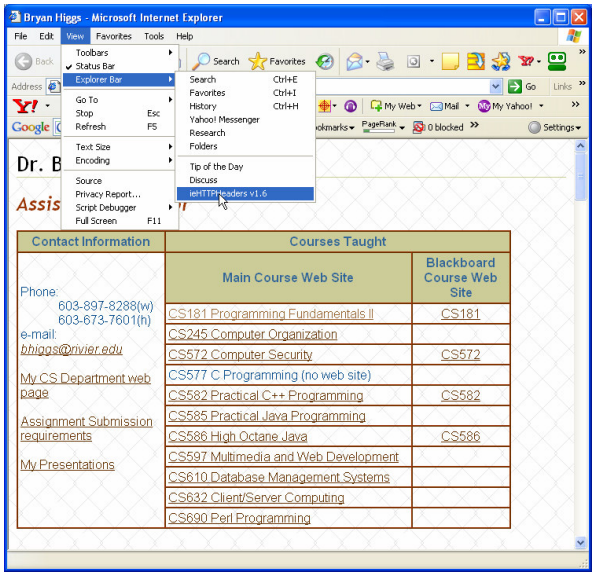
The Ethereal Network Protocol Analyzer

http://www.ethereal.com/

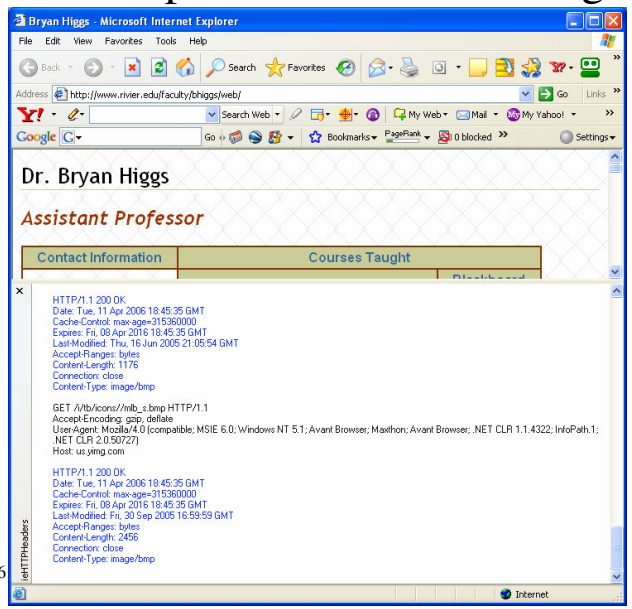


The IEHttpHeaders Browser Plug-in

http://www.blunck.info/iehttpheaders.html

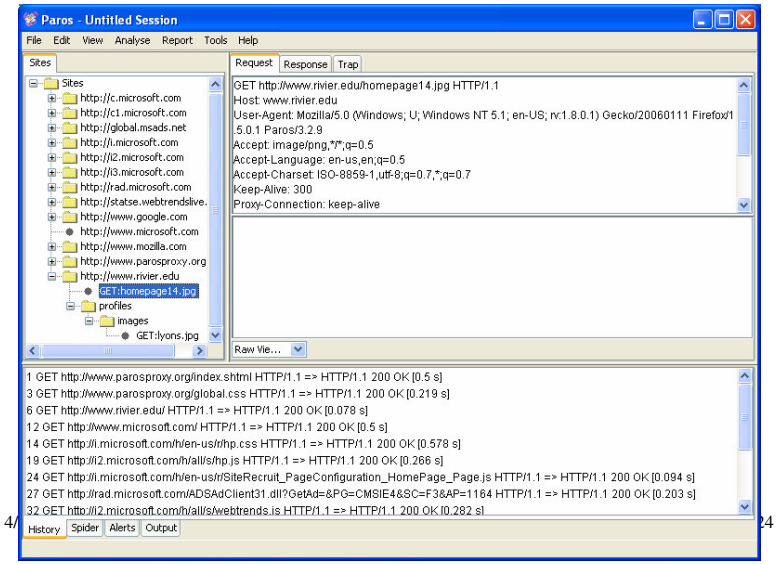


The IEHttpHeaders Browser Plug-in



The Paros HTTP Proxy

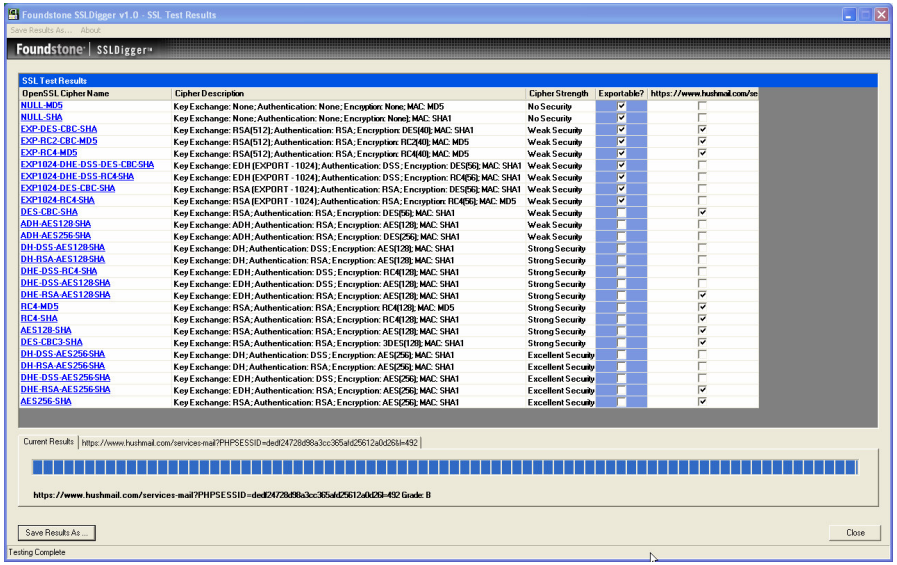
http://www.parosproxy.org/index.shtml



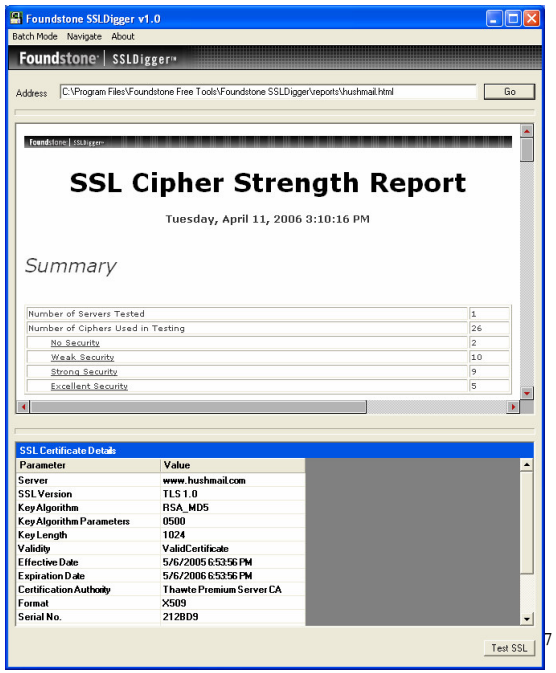
Checking the Security of Web Site SSL

SSLDigger

http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/proddesc/ssldigger.htm



SSLDigger



Security/Vulnerability Scanners

The Nessus Security Scanner

http://www.nessus.org/

- Nessus is a vulnerability scanner, originally for Unix/Linux systems.
- It is being ported to other systems, such as MacOS and Windows.
- There is a version of Nessus for Windows called NeWT.

NeWT

http://www.tenablesecurity.com/products/newt.shtml

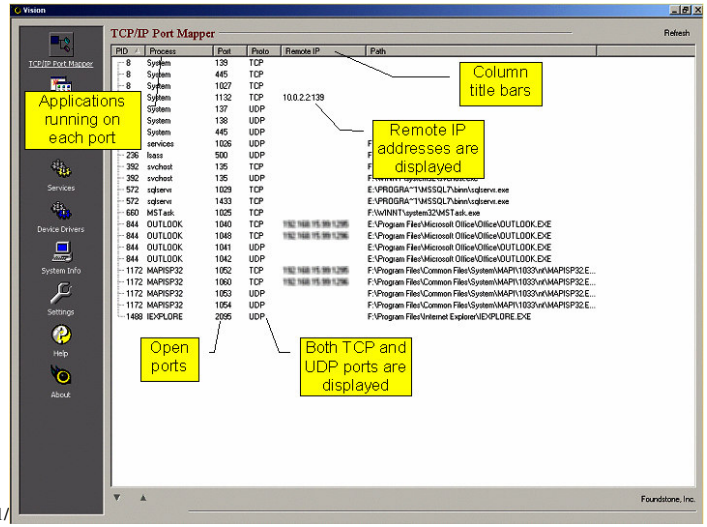
Microsoft Baseline Security Analyzer

http://www.microsoft.com/technet/security/tools/mbsahome.mspx

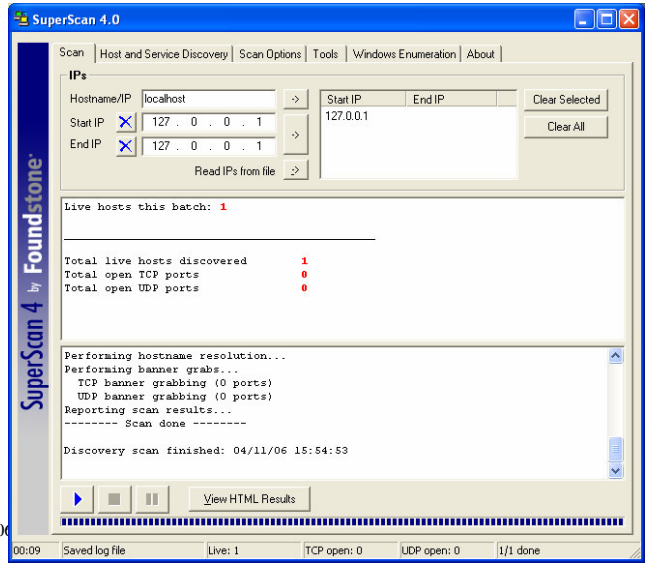
Port Scanning Tools

- Nmap (http://www.insecure.org/nmap/)
- Foundstone Vision (http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/proddesc/vision.htm)
- Foundstone Fport (http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/proddesc/fport.htm)
- Foundstone Superscan (http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/proddesc/superscan.htm)
- Others…

Foundstone Vision



Foundstone Superscan



That's Just a Sample!

There are lots more out there…