PENETRATION TOOLS

STANDARDS

The National Institute of Standards and Technology (NIST) discusses penetration testing in Special Publication 800-42, Guideline on Network Security Testing. NIST's methodology is less comprehensive than the OSSTMM; however, it is more likely to be accepted by regulatory agencies. For this reason NIST refers to the OSSTMM.

The Open Source Security Testing Methodology Manual (OSSTMM)is a peer-reviewed methodology for performing security tests and metrics. The OSSTMM test cases are divided into five channels which collectively test: information and data controls, personnel security awareness levels, fraud and social engineering control levels, computer and telecommunications networks, wireless devices, mobile devices, physical security access controls, security processes, and physical locations such as buildings, perimeters, and military bases. http://www.isecom.org/osstmm/

here is a new Methodology known as the Information Systems Security Assessment Framework (ISSAF) by the Open Information Systems Security Group (OISSG). http://www.oissg.org/

CORE IMPACT :

An automated, comprehensive penetration testing product

http://www.coresecurity.com/

Core Impact isn't cheap (be prepared to spend tens of thousands of dollars), but it is widely considered to be the most powerful exploitation tool available. It sports a large, regularly updated database of professional exploits, and can do neat tricks like exploiting one machine and then establishing an encrypted tunnel through that machine to reach and exploit other boxes. If you can't afford Impact, take a look at the cheaper Canvas or the excellent and free Metasploit Framework. Your best bet is to use all three.

CANVAS :

A Comprehensive Exploitation Framework

http://www.immunitysec.com/company-info.shtml

Canvas is a commercial vulnerability exploitation tool from Dave Aitel's ImmunitySec. It includes more than 150 exploits and is less expensive than Core Impact, though it still costs thousands of dollars. You can also buy the optional VisualSploit Plugin for drag and drop GUI exploit creation. Zero-day exploits can occasionally be found within Canvas.

Top 3 Vulnerability Exploitation Tools

http://sectools.org/sploits.html

Top 4 Packet Crafting Tools

http://sectools.org/packet-crafters.html

Top 10 Web Vulnerability Scanners

http://sectools.org/web-scanners.html

x-Scan

http://www.xfocus.net/tools/200507/1057.html

A list of open source single CD tools can be found at

http://www.darknet.org.uk/2006/03/10-best-security-live-cd-distros-pen-test-forensics-recovery/

Backtrack:

http://www.remote-exploit.org/backtrack_download.html

KNOPPIX

http://www.knopper.net/knoppix-info/

Operator

http://www.ussysadmin.com/operator/

Hacking Tools

Hack Tools, Utilities and Exploits

http://www.darknet.org.uk/hack-tools-exploits-feeds/

Top 100 Network Security Tools

http://sectools.org/