Lista unelte Penetration Testing

Name	Purpose
Nexpose	Nexpose vulnerability scanner proactively scans the infrastructure for misconfigurations, vulnerabilities and malware.
IDA Pro	The IDA Pro disassembler and debugger is an interactive, programmable, extendible, multi-processor disassembler hosted on the Windows platform.
ZAP	An easy-to-use, integrated penetration testing tool. It locates vulnerabilities in web applications, and helps you build secure apps.
SoftIce	SoftICE is a system-wide debugger that supports source level debugging of any software, driver, service, and most bios code on either a single or dual machine configuration. SoftICE not only debugs SYS files and VxDs, but also can debug Ring 3 applications as well as system internals and through-ring transitions.
OllyDebug	A 32-bit assembler level analyzing debugger for Microsoft® Windows®. Emphasis on binary code analysis makes it particularly useful in cases where source is unavailable.
Nessus	The Nessus vulnerability scanner features high speed discovery, configuration auditing, asset profiling, sensitive data discovery and vulnerability analysis of your security posture.
Nikto	Nikto is an Open Source web server scanner which performs comprehensive tests against web servers for multiple items, including over 3500 potentially dangerous files/CGIs, versions on over 900 servers, and version specific problems on over 250 servers.
Burp Suite	Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.
Reflector	Free .Net assembly decompiler and inspector.
Web Developer Firefox Ext.	Extension with numerous features that facilitate web app testing
IE DocMon	IE plug-in that lets you view the DOM tree for any page.
Sysinternals Tools	Variety of monitoring tools to view files, registry, process, memory, etc.
PE Explorer	IE plug-in that lets you view the DOM tree for any page.
SigCheck	Displays the digital signature attached to binaries. Can be useful in determining what binaries are installed by a given product (if they use signatures)
AccessCheck	Displays who has what writes on a given file or regkey

Wireshark	The gold standard of network sniffers and analysis (Name changed from Ethereal)
NetCat	The TCP/IP swiss-army knife. Converts a TCP/UDP port into a stdin/stdout pipe. Very useful for creating simple spoofed network servers.
TCPView	Enumerates all open TCP connections on the system along with the corresponding process.
OleView	Enumerates all open TCP connections on the system along with the corresponding process.
COMRaider	Fuzzer utility for COM interfaces. Also finds all 'safe for scripting' controls installed on a machine (those that are available in IE)
Morf	Encoder and decoder for all kinds of stuff. UTF, base64, hash formats, URL, HTML, etc. Great tool for getting past blacklist filtering.
Livehttpheaders	Easily view HTTP headers of a webpage and while browsing.
Metasploit Framework	Tool for developing and executing exploit code against a remote target machine. Other important sub-projects include the Opcode Database, shellcode archive and related research. It t is well known for its anti-forensic and evasion tool.
SQLMap	Sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.
Recon-ng	Recon-ng is a full-featured Web Reconnaissance framework written in Python. Complete with independent modules, database interaction, built in convenience functions, interactive help, and command completion, Recon-ng provides a powerful environment in which open source web-based reconnaissance can be conducted quickly and thoroughly.
wfuzz	Utility to bruteforce web applications to find their not linked resources.
peach	Peach Fuzzer™ is an advanced and extensible fuzzing platform. This software has been developed to enable security consultants, product testers, and enterprise quality assurance teams to find vulnerabilities in software using automated generative and mutational methods.
Hydra	This tool is a proof of concept code, to give researchers and security consultants the possiblity to show how easy it would be to gain unauthorized access from remote to a system.
John	John the Ripper is a free password cracking software tool. Initially developed for the Unix operating system, it now runs on fifteen different platforms (eleven of which are architecture-specific versions of Unix, DOS, Win32, BeOS, and OpenVMS). It is one of the most popular password testing and breaking programs as it combines a number of password crackers into one package, autodetects password hash types, and includes a customizable cracker. It can be run against various encrypted password formats including several crypt password hash types most commonly found

	on various Unix versions (based on DES, MD5, or Blowfish), Kerberos AFS, and Windows NT/2000/XP/2003 LM hash.
Maltego	Maltego is an open source intelligence and forensics application. It will offer you timous mining and gathering of information as well as the representation of this information in a easy to understand format.
NMap	Nmap (Network Mapper) is a security scanner used to discover hosts and services on a computer network, thus creating a "map" of the network. To accomplish its goal, Nmap sends specially crafted packets to the target host and then analyzes the responses.
Aircrack-ng	Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless LANs. It works with any wireless network interface controller whose driver supports raw monitoring mode and can sniff 802.11a, 802.11b and 802.11g traffic.
Reaver-wps	Reaver performs a brute force attack against an access point's WiFi Protected Setup pin number. Once the WPS pin is found, the WPA PSK can be recovered and alternately the AP's wireless settings can be reconfigured. While Reaver does not support reconfiguring the AP, this can be accomplished with wpa_supplicant once the WPS pin is known.
Bully	Bully is a new implementation of the WPS brute force attack, written in C. It is conceptually identical to other programs, in that it exploits the (now well known) design flaw in the WPS specification. It has several advantages over the original reaver code. These include fewer dependencies, improved memory and cpu performance, correct handling of endianness, and a more robust set of options. It runs on Linux, and was specifically developed to run on embedded Linux systems (OpenWrt, etc) regardless of architecture.
Wpscan	WPScan is a black box WordPress Security Scanner written in Ruby which attempts to find known security weaknesses within WordPress installations. This app was developed by Alessio Dalla Piazza. Its intended use is to be for security professionals or WordPress administrators to assess the security posture of their WordPress installations. WPScan includes user enumeration and will detect timthumb file, theme and WordPress version.
Joomscan	"Joomla! is probably the most widely-used CMS out there due to its flexibility, user-friendlinesss, extensibility to name a few.So, watching its vulnerabilities and adding such vulnerabilities as KB to Joomla scanner takes ongoing activity.It will help web developers and web masters to help identify possible security weaknesses on their deployed Joomla! sites. No web security scanner is dedicated only one CMS."
Scapy	Scapy is a packet manipulation tool for computer networks,[1][2] written in Python by Philippe Biondi. It can forge or decode packets, send them on the wire, capture them, and match requests and replies. It can also handle tasks like scanning, tracerouting, probing, unit tests, attacks, and network discovery.

SSLScan	SSLScan determines what ciphers are supported on SSL-based services, such as HTTPS. Furthermore, SSLScan will determine the prefered ciphers of the SSL service.
OpenVAS	The Open Vulnerability Assessment System (OpenVAS) is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution.
Fast-Track	Fast-Track is a python based open-source project aimed at helping Penetration Testers in an effort to identify, exploit, and further penetrate a network. Fast-Track was originally conceived when I was on a penetration test and found that there was generally a lack of tools or automation in certain attacks that were normally extremely advanced and time consuming.
Socat	Socat is a command line based utility that establishes two bidirectional byte streams and transfers data between them. Because the streams can be constructed from a large set of different types of data sinks and sources (see address types), and because lots of address options may be applied to the streams, socat can be used for many different purposes.
Wifite	To attack multiple WEP, WPA, and WPS encrypted networks in a row. This tool is customizable to be automated with only a few arguments. Wifite aims to be the "set it and forget it" wireless auditing tool.
HPing	This handy little utility assembles and sends custom ICMP, UDP, or TCP packets and then displays any replies. It was inspired by the ping command, but offers far more control over the probes sent. It also has a handy traceroute mode and supports IP fragmentation. Hping is particularly useful when trying to traceroute/ping/probe hosts behind a firewall that blocks attempts using the standard utilities.
Paros Proxy	A Java-based web proxy for assessing web application vulnerability. It supports editing/viewing HTTP/HTTPS messages on-the-fly to change items such as cookies and form fields. It includes a web traffic recorder, web spider, hash calculator, and a scanner for testing common web application attacks such as SQL injection and cross-site scripting.
Webscarab	In its simplest form, WebScarab records the conversations (requests and responses) that it observes, and allows the operator to review them in various ways. WebScarab is designed to be a tool for anyone who needs to expose the workings of an HTTP(S) based application, whether to allow the developer to debug otherwise difficult problems, or to allow a security specialist to identify vulnerabilities in the way that the application has been designed or implemented.
W3af	W3af is an extremely popular, powerful, and flexible framework for finding and exploiting web application vulnerabilities. It is easy to use and extend and features dozens of web assessment and exploitation plugins.
Sqlninja	sqlininja exploits web applications that use Microsoft SQL Server as a database backend. Its focus is on getting a running shell on the remote host. sqlninja doesn't find an SQL injection in the first place, but automates the exploitation process once one has been discovered.
BeEF	BeEF is a browser exploitation framework. This tool will demonstrate the collecting of zombie browsers and browser vulnerabilities in real-time. It provides a command and control interface which facilitates the targeting of individual or groups of zombie browsers. It is designed to make the creation of new exploit modules easy.

NBTScan	NBTScan is a program for scanning IP networks for NetBIOS name information (similar to what the Windows nbtstat tool provides against single hosts). It sends a NetBIOS status query to each address in a supplied range and lists received information in human readable form.
Acunetix WVS	Acunetix WVS (web vulnerability scanner) automatically checks web applications for vulnerabilities such as SQL Injections, cross site scripting, arbitrary file creation/deletion, and weak password strength on authentication pages. It boasts a comfortable GUI, an ability to create professional security audit and compliance reports, and tools for advanced manual webapp testing.
Netsparker	Netsparker is a web application security scanner, with support for both detection and exploitation of vulnerabilities. It aims to be false positive–free by only reporting confirmed vulnerabilities after successfully exploiting or otherwise testing them.
Firebug	Firebug is an add-on for Firefox that provides access to browser internals. It features live editing of HTML and CSS, a DOM viewer, and a JavaScript debugger. Web application security testers appreciate the ability to see what's happening behind the scenes of the browser.
Grendel-Scan	Grendel-Scan is an open-source web application security testing tool. It has automated testing module for detecting common web application vulnerabilities, and features geared at aiding manual penetration tests.
DirBuster	DirBuster searches for hidden pages and directories on a web server. Sometimes developers will leave a page accessible, but unlinked; DirBuster is meant to find these potential vulnerabilities.
Wapiti	Wapiti allows you to audit the security of your web applications. It performs "black-box" scans; i.e., it does not study the source code of the application but will scans the webpages of the deployed webapp, looking for scripts and forms where it can inject data. Once it gets this list, Wapiti acts like a fuzzer, injecting payloads to see if a script is vulnerable.
Kismet	Kismet is a console (ncurses) based 802.11 layer-2 wireless network detector, sniffer, and intrusion detection system. It identifies networks by passively sniffing (as opposed to more active tools such as NetStumbler), and can even decloak hidden (non-beaconing) networks if they are in use. It can automatically detect network IP blocks by sniffing TCP, UDP, ARP, and DHCP packets, log traffic in Wireshark/tcpdump compatible format, and even plot detected networks and estimated ranges on downloaded maps.
inSSIDer	inSSIDer is a wireless network scanner for Windows, OS X, and Android. It was designed to overcome limitations of NetStumbler, namely not working well on 64-bit Windows and Windows Vista. inSSIDer can find open wireless access points, track signal strength over time, and save logs with GPS records.
Immunity Debugger	Immunity Debugger is a debugger whose design reflects the need to write exploits, analyze malware, and reverse engineer binary files. It builds on a solid user interface with function graphing, the industry's first heap analysis tool built specifically for heap creation, and a large and well supported Python API for easy extensibility.
GDB	DB is the GNU Project's debugger. Security folks use it to analyze unknown binaries, by getting disassemblies and stepping through a program

	instruction by instruction. GDB can debug programs written in Ada, C, C++, Objective-C, Pascal, and other languages.