


PENTESTING

A Complete Penetration Testing & Hacking Tools List for Hackers & Security Professionals

By **BALAJI N** - January 20, 2020  2



Newsletter

Signup to get Hacking
News & Tutorials to your
Inbox

Name

Email*

Subscribe

Penetration Testing as a Service

Penetration testing & **Hacking Tools** are more often used by security industries to test the vulnerabilities in network and applications. Here you can find the Comprehensive Penetration testing & **Hacking Tools** list that covers Performing Penetration testing Operation in all the Environment.

Penetration testing and ethical hacking tools are very essential part for every organization to test the vulnerabilities and patch the vulnerable system.

[New York's SHIELD Act](#)

[Also Read: Penetration Testing Cheat Sheet For Windows Machine – Intrusion Detection](#)

[Cyber Security Courses](#)

[Also Read Most Important Tools and Resources For Security Researcher, Malware Analyst, Reverse Engineer and Security](#)

Penetration Testing & Hacking Tools List

Online Resources – Hacking Tools

Penetration Testing Resources

- Metasploit Unleashed – Free Offensive Security Metasploit course.
- [Penetration Testing Execution Standard \(PTES\)](#) – Documentation designed to provide a common language and scope for performing and reporting the results of a penetration test.
- [Open Web Application Security Project \(OWASP\)](#) – Worldwide not-for-profit charitable organization focused on improving the security of especially Web-based and Application-layer software.
- [PENTEST-WIKI](#) – Free online security knowledge library for pentesters and researchers.
- [Penetration Testing Framework \(PTF\)](#) – Outline for performing penetration tests compiled as a general framework usable by vulnerability analysts and penetration testers alike.
- [XSS-Payloads](#) – Ultimate resource for all things cross-site including payloads, tools, games and documentation.
- [Open Source Security Testing Methodology Manual \(OSSTMM\)](#) – Framework for providing test cases that result in verified facts on

Computer Security

Hackers Use Fake Zoom
Installers to Install
Backdoor and Devil
Shadow...

May 22, 2020

which to base decisions that impact an organization's security.

- [MITRE's Adversarial Tactics, Techniques & Common Knowledge \(ATT&CK\)](#) – Curated knowledge base and model for cyber adversary behavior.

Exploit Development

- [Shellcode Tutorial](#) – Tutorial on how to write shellcode.
- [Shellcode Examples](#) – Shellcodes database.
- [Exploit Writing Tutorials](#) – Tutorials on how to develop exploits.

OSINT Resources

- [OSINT Framework](#) – Collection of various OSINT Hacking Tools broken out by category.
- [Intel Techniques](#) – Collection of OSINT tools. Menu on the left can be used to navigate through the categories.
- [NetBootcamp OSINT Tools](#) – Collection of OSINT links and custom Web interfaces to other services such as [Facebook Graph Search](#) and [various paste sites](#).
- [WiGLE.net](#) – Information about wireless networks world-wide, with user-friendly desktop and web applications.

Social Engineering Resources

Critical Bluetooth BIAS
Attack Let Hackers
Access Billions of
Devices

May 20, 2020

Best Ways to Detect and
Handle Suspicious Email
Attachments

May 20, 2020

Ramsay – A
cyber-espionage Toolkit
Attack Steal Sensitive
Document From
Air-Gapped...

May 19, 2020

Reverse RDP – Microsoft
Patch for RDP client
Opens Room for...

May 15, 2020

Load more ▾

- [Social Engineering Framework](#) – Information resource for social engineers.

Lock Picking Resources

- [Schuyler Towne channel](#) – Lockpicking videos and security talks.
- [bosnianbill](#) – More lockpicking videos.
- [/r/lockpicking](#) – Resources for learning lockpicking, equipment recommendations.

Operating Systems

- [Security related Operating Systems @ Rawsec](#) – Penetration testing tools & Hacking Tools list Related Complete list of security operating systems.
- [Best Linux Penetration Testing Distributions @ CyberPunk](#) – Description of main penetration testing distributions.
- [Security @ Distrowatch](#) – Website dedicated to talking about, reviewing, and keeping up to date with open source operating systems.
- [cuckoo](#) – Open source automated malware analysis system.
- [Computer Aided Investigative Environment \(CAINE\)](#) – Italian GNU/Linux live distribution created as a digital forensics project.
- [Digital Evidence & Forensics Toolkit \(DEFT\)](#) – Live CD for forensic analysis runnable without tampering or corrupting connected devices where the boot process takes place.

- [Tails](#) – Live OS aimed at preserving privacy and anonymity.

Hacking Tools

Penetration Testing Distributions

- [Kali](#) – GNU/Linux distribution designed for digital forensics and penetration testing Hacking Tools
- [ArchStrike](#) – Arch GNU/Linux repository for security professionals and enthusiasts.
- [BlackArch](#) – Arch GNU/Linux-based distribution with best Hacking Tools for penetration testers and security researchers.
- [Network Security Toolkit \(NST\)](#) – Fedora-based bootable live operating system designed to provide easy access to best-of-breed open source network security applications.
- [Pentoo](#) – Security-focused live CD based on Gentoo.
- [BackBox](#) – Ubuntu-based distribution for penetration tests and security assessments.
- [Parrot](#) – Distribution similar to Kali, with multiple architectures with 100 of Hacking Tools.
- [Buscador](#) – GNU/Linux virtual machine that is pre-configured for online investigators.
- [Fedora Security Lab](#) – Provides a safe test environment to work on security auditing, forensics, system rescue and teaching security testing methodologies.

- [The Pentesters Framework](#) – Distro organized around the Penetration Testing Execution Standard (PTES), providing a curated collection of utilities that eliminates often unused toolchains.
- [AttifyOS](#) – GNU/Linux distribution focused on tools useful during Internet of Things (IoT) security assessments.

Docker for Penetration Testing

- `docker pull kalilinux/kali-linux-docker` [official Kali Linux](#)
- `docker pull owasp/zap2docker-stable` – [official OWASP ZAP](#)
- `docker pull wpscanteam/wpscan` – [official WPScan](#)
- `docker pull citizenstig/dvwa` – [Damn Vulnerable Web Application \(DVWA\)](#)
- `docker pull wpscanteam/vulnerablewordpress` – [Vulnerable WordPress Installation](#)
- `docker pull hmllo/vaas-cve-2014-6271` – [Vulnerability as a service: Shellshock](#)
- `docker pull hmllo/vaas-cve-2014-0160` – [Vulnerability as a service: Heartbleed](#)
- `docker pull opendns/security-ninjas` – [Security Ninjas](#)
- `docker pull diogomonica/docker-bench-security` – [Docker Bench for Security](#)

- `docker pull ismisepaul/securityshepherd` – [OWASP Security Shepherd](#)
- `docker pull danmx/docker-owasp-webgoat` – [OWASP WebGoat Project docker image](#)
- `docker-compose build && docker-compose up` – [OWASP NodeGoat](#)
- `docker pull citizenstig/nowasp` – [OWASP Mutillidae II Web Pen-Test Practice Application](#)
- `docker pull bkimminich/juice-shop` – [OWASP Juice Shop](#)
- `docker pull kalilinux/kali-linux-docker` – [Kali Linux Docker Image](#)
- `docker pull phocean/msf` – [docker-metasploit](#)

Multi-paradigm Frameworks

- [Metasploit](#) – post exploitation Hacking Tools for offensive security teams to help verify vulnerabilities and manage security assessments.
- [Armitage](#) – Java-based GUI front-end for the Metasploit Framework.
- [Faraday](#) – Multiuser integrated pentesting environment for red teams performing cooperative penetration tests, security audits, and risk assessments.
- [ExploitPack](#) – Graphical tool for automating penetration tests that ships with many pre-packaged exploits.

- [Pupy](#) – Cross-platform (Windows, Linux, macOS, Android) remote administration and post-exploitation tool,

Also Read

DEFCON

– [2017 Hackers Presentation Complete PDF](#)

[Lists with Advance Hacking Techniques](#)

Vulnerability Scanners

- [Nexpose](#) – Commercial vulnerability and risk management assessment engine that integrates with Metasploit, sold by Rapid7.
- [Nessus](#) – Commercial vulnerability management, configuration, and compliance assessment platform, sold by Tenable.
- [OpenVAS](#) – Free software implementation of the popular Nessus vulnerability assessment system.
- [Vuls](#) – Agentless vulnerability scanner for GNU/Linux and FreeBSD, written in Go.

Static Analyzers

- [Brakeman](#) – Static analysis security vulnerability scanner for Ruby on Rails applications.
- [cppcheck](#) – Extensible C/C++ static analyzer focused on finding bugs.
- [FindBugs](#) – Free software static analyzer to look for bugs in Java code.

- [sobelow](#) – Security-focused static analysis for the Phoenix Framework.
- [bandit](#) – Security oriented static analyser for python code.

Web Scanners

- [Nikto](#) – Noisy but fast black box web server and web application vulnerability scanner.
- [Arachni](#) – Scriptable framework for evaluating the security of web applications.
- [w3af](#) – Hacking Tools for Web application attack and audit framework.
- [Wapiti](#) – Black box web application vulnerability scanner with built-in fuzzer.
- [SecApps](#) – In-browser web application security testing suite.
- [WebReaver](#) – Commercial, graphical web application vulnerability scanner designed for macOS.
- [WPScan](#) – Hacking Tools of Black box WordPress vulnerability scanner.
- [cms-explorer](#) – Reveal the specific modules, plugins, components and themes that various websites powered by content management systems are running.
- [joomscan](#) – on of the best Hacking Tools for Joomla vulnerability scanner.
- [ACSTIS](#) – Automated client-side template injection (sandbox escape/bypass) detection for AngularJS.

Network Tools

- [zmap](#) – Open source network scanner that enables researchers to easily perform Internet-wide network studies.
- [nmap](#) – Free security scanner for network exploration & security audits.
- [pig](#) – one of the Hacking Tools for GNU/Linux packet crafting .
- [scanless](#) – Utility for using websites to perform port scans on your behalf so as not to reveal your own IP.
- [tcpdump/libpcap](#) – Common packet analyzer that runs under the command line.
- [Wireshark](#) – Widely-used graphical, cross-platform network protocol analyzer.
- [Network-Tools.com](#) – Website offering an interface to numerous basic network utilities like `ping` , `traceroute` , `whois` , and more.
- [netsniff-ng](#) – Swiss army knife for for network sniffing.
- [Interceptor-NG](#) – Multifunctional network toolkit.
- [SPARTA](#) – Graphical interface offering scriptable, configurable access to existing network infrastructure scanning and enumeration tools.
- [dnschef](#) – Highly configurable DNS proxy for pentesters.
- [DNSDumpster](#) – one of the Hacking Tools for Online DNS recon and search service.
- [CloudFail](#) – Unmask server IP addresses hidden behind Cloudflare by searching old database records and detecting misconfigured DNS.

- [dnsenum](#) – Perl script that enumerates DNS information from a domain, attempts zone transfers, performs a brute force dictionary style attack, and then performs reverse look-ups on the results.
- [dnsmap](#) – One of the Hacking Tools for Passive DNS network mapper.
- [dnsrecon](#) – One of the Hacking Tools for DNS enumeration script.
- [dnstracer](#) – Determines where a given DNS server gets its information from, and follows the chain of DNS servers.
- [passivedns-client](#) – Library and query tool for querying several passive DNS providers.
- [passivedns](#) – Network sniffer that logs all DNS server replies for use in a passive DNS setup.
- [Mass Scan](#) – best Hacking Tools for TCP port scanner, spews SYN packets asynchronously, scanning entire Internet in under 5 minutes.
- [Zarp](#) – Network attack tool centered around the exploitation of local networks.
- [mitmproxy](#) – Interactive TLS-capable intercepting HTTP proxy for penetration testers and software developers.
- [Morpheus](#) – Automated ettercap TCP/IP Hacking Tools .
- [mallory](#) – HTTP/HTTPS proxy over SSH.
- [SSH MITM](#) – Intercept SSH connections with a proxy; all plaintext passwords and sessions are logged to disk.
- [Netzob](#) – Reverse engineering, traffic generation and fuzzing of communication protocols.
- [DET](#) – Proof of concept to perform data exfiltration using either single or multiple channel(s) at the same time.

- [pwnat](#) – Punches holes in firewalls and NATs.
- [dsniff](#) – Collection of tools for network auditing and pentesting.
- [tgcd](#) – Simple Unix network utility to extend the accessibility of TCP/IP based network services beyond firewalls.
- [smbmap](#) – Handy SMB enumeration tool.
- [scapy](#) – Python-based interactive packet manipulation program & library.
- [Dshell](#) – Network forensic analysis framework.
- [Debookey](#) – Simple and powerful network traffic analyzer for macOS.
- [Dripcap](#) – Caffeinated packet analyzer.
- [Printer Exploitation Toolkit \(PRET\)](#) – Tool for printer security testing capable of IP and USB connectivity, fuzzing, and exploitation of PostScript, PDL, and PCL printer language features.
- [Praeda](#) – Automated multi-function printer data harvester for gathering usable data during security assessments.
- [routersploit](#) – Open source exploitation framework similar to Metasploit but dedicated to embedded devices.
- [evilgrade](#) – Modular framework to take advantage of poor upgrade implementations by injecting fake updates.
- [XRay](#) – Network (sub)domain discovery and reconnaissance automation tool.
- [Ettercap](#) – Comprehensive, mature suite for machine-in-the-middle attacks.
- [BetterCAP](#) – Modular, portable and easily extensible MITM framework.
- [CrackMapExec](#) – A swiss army knife for pentesting networks.

- [impacket](#) – A collection of Python classes for working with network protocols.

Wireless Network Hacking Tools

- [Aircrack-ng](#) – Set of Penetration testing & Hacking Tools list for auditing wireless networks.
- [Kismet](#) – Wireless network detector, sniffer, and IDS.
- [Reaver](#) – Brute force attack against WiFi Protected Setup.
- [Wifite](#) – Automated wireless attack tool.
- [Fluxion](#) – Suite of automated social engineering based WPA attacks.

Transport Layer Security Tools

- [SSLyze](#) – Fast and comprehensive TLS/SSL configuration analyzer to help identify security mis-configurations.
- [tls_prober](#) – Fingerprint a server's SSL/TLS implementation.
- [testssl.sh](#) – Command line tool which checks a server's service on any port for the support of TLS/SSL ciphers, protocols as well as some cryptographic flaws.

Web Exploitation

- [OWASP Zed Attack Proxy \(ZAP\)](#) – Feature-rich, scriptable HTTP intercepting proxy and fuzzer for penetration testing web applications.

- [Fiddler](#) – Free cross-platform web debugging proxy with user-friendly companion tools.
- [Burp Suite](#) – One of the Hacking Tools integrated platform for performing security testing of web applications.
- [autochrome](#) – Easy to install a test browser with all the appropriate setting needed for web application testing with native Burp support, from NCCGroup.
- [Browser Exploitation Framework \(BeEF\)](#) – Command and control server for delivering exploits to commandeered Web browsers.
- [Offensive Web Testing Framework \(OWTF\)](#) – Python-based framework for pentesting Web applications based on the OWASP Testing Guide.
- [WordPress Exploit Framework](#) – Ruby framework for developing and using modules which aid in the penetration testing of WordPress powered websites and systems.
- [WPSploit](#) – Exploit WordPress-powered websites with Metasploit.
- [SQLmap](#) – Automatic SQL injection and database takeover tool.
- [tplmap](#) – Automatic server-side template injection and Web server takeover Hacking Tools .
- [weevely3](#) – Weaponized web shell.
- [Wappalyzer](#) – Wappalyzer uncovers the technologies used on websites.
- [WhatWeb](#) – Website fingerprinter.
- [BlindElephant](#) – Web application fingerprinter.
- [wafw00f](#) – Identifies and fingerprints Web Application Firewall (WAF) products.

- [fimap](#) – Find, prepare, audit, exploit and even Google automatically for LFI/RFI bugs.
- [Kadabra](#) – Automatic LFI exploiter and scanner.
- [Kadimus](#) – LFI scan and exploit tool.
- [liffy](#) – LFI exploitation tool.
- [Commix](#) – Automated all-in-one operating system command injection and exploitation tool.
- [DVCS Ripper](#) – Rip web accessible (distributed) version control systems: SVN/GIT/HG/BZR.
- [GitTools](#) – One of the Hacking Tools that Automatically find and download Web-accessible `.git` repositories.
- [sslstrip](#) –
One of the Hacking Tools Demonstration of the HTTPS stripping attacks.
- [sslstrip2](#) – SSLStrip version to defeat HSTS.
- [NoSQLmap](#) – Automatic NoSQL injection and database takeover tool.
- [VHostScan](#) – A virtual host scanner that performs reverse lookups, can be used with pivot tools, detect catch-all scenarios, aliases and dynamic default pages.
- [FuzzDB](#) – Dictionary of attack patterns and primitives for black-box application fault injection and resource discovery.
- [EyeWitness](#) – Tool to take screenshots of websites, provide some server header info, and identify default credentials if possible.
- [webscreenshot](#) – A simple script to take screenshots of list of websites.

Hex Editors

- [HexEdit.js](#) – Browser-based hex editing.
- [Hexinator](#) – World's finest (proprietary, commercial) Hex Editor.
- [Frrhed](#) – Binary file editor for Windows.
- [0xED](#) – Native macOS hex editor that supports plug-ins to display custom data types.

File Format Analysis Tools

- [Kaitai Struct](#) – File formats and network protocols dissection language and web IDE, generating parsers in C++, C#, Java, JavaScript, Perl, PHP, Python, Ruby.
- [Veles](#) – Binary data visualization and analysis tool.
- [Hachoir](#) – Python library to view and edit a binary stream as tree of fields and tools for metadata extraction.

Defense Evasion Tools

- [Veil](#) – Generate metasploit payloads that bypass common anti-virus solutions.
- [shellsploit](#) – Generates custom shellcode, backdoors, injectors, optionally obfuscates every byte via encoders.
- [Hyperion](#) – Runtime encryptor for 32-bit portable executables ("PE .exe s").

- [AntiVirus Evasion Tool \(AVET\)](#) – Post-process exploits containing executable files targeted for Windows machines to avoid being recognized by antivirus software.
- [peCloak.py](#) – Automates the process of hiding a malicious Windows executable from antivirus (AV) detection.
- [peCloakCapstone](#) – Multi-platform fork of the peCloak.py automated malware antivirus evasion tool.
- [UniByAv](#) – Simple obfuscator that takes raw shellcode and generates Anti-Virus friendly executables by using a brute-forcable, 32-bit XOR key.

Hash Cracking Hacking Tools

- [John the Ripper](#) – One of the best Hacking Tools for Fast password cracker.
- [Hashcat](#) – Another One of the Hacking Tools The more fast hash cracker.
- [CeWL](#) – Generates custom wordlists by spidering a target's website and collecting unique words.
- [JWT Cracker](#) – Simple HS256 JWT token brute force cracker.
- [Rar Crack](#) – RAR bruteforce cracker.
- [BruteForce Wallet](#) – Find the password of an encrypted wallet file (i.e. `wallet.dat`).

Windows Utilities

- [Sysinternals Suite](#) – The Sysinternals Troubleshooting Utilities.
- [Windows Credentials Editor](#) – Inspect logon sessions and add, change, list, and delete associated credentials, including Kerberos tickets.
- [mimikatz](#) – Credentials extraction tool for Windows operating system.
- [PowerSploit](#) – PowerShell Post-Exploitation Framework.
- [Windows Exploit Suggester](#) – Detects potential missing patches on the target.
- [Responder](#) – LLMNR, NBT-NS and MDNS poisoner.
- [Bloodhound](#) – Graphical Active Directory trust relationship explorer.
- [Empire](#) – Pure PowerShell post-exploitation agent.
- [Fibratus](#) – Tool for exploration and tracing of the Windows kernel.
- [wePWNise](#) – Generates architecture independent VBA code to be used in Office documents or templates and automates bypassing application control and exploit mitigation software.
- [redsnarf](#) – Post-exploitation tool for retrieving password hashes and credentials from Windows workstations, servers, and domain controllers.
- [Magic Unicorn](#) – Shellcode generator for numerous attack vectors, including Microsoft Office macros, PowerShell, HTML applications (HTA), or `certutil` (using fake certificates).
- [DeathStar](#) – Python script that uses Empire's RESTful API to automate gaining Domain Admin rights in Active Directory environments.

GNU/Linux Utilities

- [Linux Exploit Suggester](#) – Heuristic reporting on potentially viable exploits for a given GNU/Linux system.

macOS Utilities

- [Bella](#) – Pure Python post-exploitation data mining and remote administration tool for macOS.

DDoS Tools

- [LOIC](#) – Open source network stress tool for Windows.
- [JS LOIC](#) – JavaScript in-browser version of LOIC.
- [SlowLoris](#) – DoS tool that uses low bandwidth on the attacking side.
- [HOIC](#) – Updated version of Low Orbit Ion Cannon, has ‘boosters’ to get around common counter measures.
- [T50](#) – Faster network stress tool.
- [UFONet](#) – Abuses OSI layer 7 HTTP to create/manage ‘zombies’ and to conduct different attacks using; `GET / POST`, multithreading, proxies, origin spoofing methods, cache evasion techniques, etc.

Social Engineering Tools

- [Social Engineer Toolkit \(SET\)](#) – Open source pentesting framework designed for social engineering featuring a number of custom attack

vectors to make believable attacks quickly.

- [King Phisher](#) – One of the Hacking Tools for Phishing campaign toolkit used for creating and managing multiple simultaneous phishing attacks with custom email and server content.
- [Evilginx](#) – MITM attack framework used for phishing credentials and session cookies from any Web service.
- [wifiphisher](#) – Automated phishing attacks against WiFi networks.
- [Catphish](#) – Tool for phishing and corporate espionage written in Ruby.
- [Beelogger](#) – Tool for generating keylogger.

OSINT Tools

- [Maltego](#) – One of the Hacking Tools and Proprietary software for open source intelligence and forensics, from Paterva.
- [theHarvester](#) – E-mail, subdomain and people names harvester.
- [creepy](#) – Geolocation OSINT tool.
- [metagoofil](#) – Metadata harvester.
- [Google Hacking Database](#) – Database of Google dorks; can be used for recon.
- [Google-dorks](#) – Common Google dorks and others you probably don't know.
- [GooDork](#) – Command line Google dorking tool.
- [dork-cli](#) – Command line Google dork tool.
- [Censys](#) – Collects data on hosts and websites through daily ZMap and ZGrab scans.

- [Shodan](#) – World's first search engine for Internet-connected devices.
- [recon-ng](#) – One of the Hacking Tools Full-featured Web Reconnaissance framework written in Python.
- [github-dorks](#) – CLI tool to scan Github repos/organizations for potential sensitive information leak.
- [vcsmap](#) – Plugin-based tool to scan public version control systems for sensitive information.
- [Spiderfoot](#) – Multi-source OSINT automation tool with a Web UI and report visualizations
- [BinGoo](#) – GNU/Linux bash based Bing and Google Dorking Tool.
- [fast-recon](#) – Perform Google dorks against a domain.
- [snitch](#) – Information gathering via dorks.
- [Sn1per](#) – ons of the Hacking Tools for Automated Pentest Recon Scanner.
- [Threat Crowd](#) – Search engine for threats.
- [Virus Total](#) – VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.
- [DataSploit](#) – OSINT visualizer utilizing Shodan, Censys, Clearbit, EmailHunter, FullContact, and Zoomeye behind the scenes.
- [AQUATONE](#) – Subdomain discovery tool utilizing various open sources producing a report that can be used as input to other tools.
- [Intrigue](#) – Automated OSINT & Attack Surface discovery framework with powerful API, UI and CLI.
- [ZoomEye](#) – Search engine for cyberspace that lets the user find specific network components.

Anonymity Tools

- [Tor](#) – Free software and onion routed overlay network that helps you defend against traffic analysis.
- [OnionScan](#) – One of the Hacking Tools for investigating the Dark Web by finding operational security issues introduced by Tor hidden service operators.
- [I2P](#) – The Invisible Internet Project.
- [Nipe](#) – Script to redirect all traffic from the machine to the Tor network.
- [What Every Browser Knows About You](#) – Comprehensive detection page to test your own Web browser's configuration for privacy and identity leaks.

Reverse Engineering Tools

- [Interactive Disassembler \(IDA Pro\)](#) – Proprietary multi-processor disassembler and debugger for Windows, GNU/Linux, or macOS; also has a free version, [IDA Free](#).
- [WDK/WinDbg](#) – Windows Driver Kit and WinDbg.
- [OllyDbg](#) – x86 debugger for Windows binaries that emphasizes binary code analysis.
- [Radare2](#) – Open source, crossplatform reverse engineering framework.
- [x64dbg](#) – Open source x64/x32 debugger for windows.

- [Immunity Debugger](#) – Powerful way to write exploits and analyze malware.
- [Evan's Debugger](#) – OllyDbg-like debugger for GNU/Linux.
- [Medusa](#) – Open source, cross-platform interactive disassembler.
- [plasma](#) – Interactive disassembler for x86/ARM/MIPS. Generates indented pseudo-code with colored syntax code.
- [peda](#) – Python Exploit Development Assistance for GDB.
- [dnSpy](#) – one of the Hacking Tools to reverse engineer .NET assemblies.
- [binwalk](#) – Fast, easy to use tool for analyzing, reverse engineering, and extracting firmware images.
- [PyREBox](#) – Python scriptable Reverse Engineering sandbox by Cisco-Talos.
- [Voltron](#) – Extensible debugger UI toolkit written in Python.
- [Capstone](#) – Lightweight multi-platform, multi-architecture disassembly framework.
- [rVMI](#) – Debugger on steroids; inspect userspace processes, kernel drivers, and preboot environments in a single tool.
- [Frida](#) – Dynamic instrumentation toolkit for developers, reverse-engineers, and security researchers.

Physical Access Tools

- [LAN Turtle](#) – Covert “USB Ethernet Adapter” that provides remote access, network intelligence gathering, and MITM capabilities when installed in a local network.

- [USB Rubber Ducky](#) – Customizable keystroke injection attack platform masquerading as a USB thumbdrive.
- [PoisonTap](#) – Siphons cookies, exposes internal (LAN-side) router and installs web backdoor on locked computers.
- [WiFi Pineapple](#) – Wireless auditing and penetration testing platform.
- [Proxmark3](#) – RFID/NFC cloning, replay, and spoofing toolkit often used for analyzing and attacking proximity cards/readers, wireless keys/keyfobs, and more.

Side-channel Tools

- [ChipWhisperer](#) – Complete open-source toolchain for side-channel power analysis and glitching attacks.

CTF Tools

- [ctf-tools](#) – Collection of setup scripts to install various security research tools easily and quickly deployable to new machines.
- [Pwntools](#) – Rapid exploit development framework built for use in CTFs.
- [RsaCtfTool](#) – Decrypt data enciphered using weak RSA keys, and recover private keys from public keys using a variety of automated attacks.

Penetration Testing Report Templates

- [Public Pentesting Reports](#) – Curated list of public penetration test reports released by several consulting firms and academic security groups.
- [Pentesting Report Template](#) – testandverification.com template.
- [Pentesting Report Template](#) – hitachi-systems-security.com template.
- [Pentesting Report Template](#) – lucideus.com template.
- [Pentesting Report Template](#) – crest-approved.org template.
- [Pentesting Report Template](#) – pcisecuritystandards.org template.

Books

Penetration Testing Books

- [The Art of Exploitation](#) by Jon Erickson, 2008
- [Metasploit: The Penetration Tester's Guide](#) by David Kennedy et al., 2011
- [Penetration Testing: A Hands-On Introduction to Hacking](#) by Georgia Weidman, 2014
- [Rtfm: Red Team Field Manual](#) by Ben Clark, 2014
- [The Hacker Playbook](#) by Peter Kim, 2014
- [The Basics of Hacking and Penetration Testing](#) by Patrick Engebretson, 2013
- [Professional Penetration Testing](#) by Thomas Wilhelm, 2013

- [Advanced Penetration Testing for Highly-Secured Environments](#) by Lee Allen, 2012
- [Violent Python](#) by TJ O'Connor, 2012
- [Fuzzing: Brute Force Vulnerability Discovery](#) by Michael Sutton et al., 2007
- [Black Hat Python: Python Programming for Hackers and Pentesters](#) by Justin Seitz, 2014
- [Penetration Testing: Procedures & Methodologies](#) by EC-Council, 2010
- [Unauthorised Access: Physical Penetration Testing For IT Security Teams](#) by Wil Allsopp, 2010
- [Advanced Persistent Threat Hacking: The Art and Science of Hacking Any Organization](#) by Tyler Wrightson, 2014
- [Bug Hunter's Diary](#) by Tobias Klein, 2011
- [Advanced Penetration Testing](#) by **Wil Allsopp, 2017**

Hackers Handbook Series

- [The Database Hacker's Handbook](#), David Litchfield et al., 2005
- [The Shellcoders Handbook](#) by Chris Anley et al., 2007
- [The Mac Hacker's Handbook](#) by Charlie Miller & Dino Dai Zovi, 2009
- [The Web Application Hackers Handbook](#) by D. Stuttard, M. Pinto, 2011
- [iOS Hackers Handbook](#) by Charlie Miller et al., 2012
- [Android Hackers Handbook](#) by Joshua J. Drake et al., 2014
- [The Browser Hackers Handbook](#) by Wade Alcorn et al., 2014

- [The Mobile Application Hackers Handbook](#) by Dominic Chell et al., 2015
- [Car Hacker's Handbook](#) by Craig Smith, 2016

Defensive Development

- [Holistic Info-Sec for Web Developers \(Fascicle 0\)](#)
- [Holistic Info-Sec for Web Developers \(Fascicle 1\)](#)

Network Analysis Books

- [Nmap Network Scanning](#) by Gordon Fyodor Lyon, 2009
- [Practical Packet Analysis](#) by Chris Sanders, 2011
- [Wireshark Network Analysis](#) by by Laura Chappell & Gerald Combs, 2012
- [Network Forensics: Tracking Hackers through Cyberspace](#) by Sherri Davidoff & Jonathan Ham, 2012

Reverse Engineering Books

- [Reverse Engineering for Beginners](#) by Dennis Yurichev
- [Hacking the Xbox](#) by Andrew Huang, 2003
- [The IDA Pro Book](#) by Chris Eagle, 2011
- [Practical Reverse Engineering](#) by Bruce Dang et al., 2014
- [Gray Hat Hacking The Ethical Hacker's Handbook](#) by Daniel Regalado et al., 2015

Malware Analysis Books

- [Practical Malware Analysis](#) by Michael Sikorski & Andrew Honig, 2012
- [The Art of Memory Forensics](#) by Michael Hale Ligh et al., 2014
- [Malware Analyst's Cookbook and DVD](#) by Michael Hale Ligh et al., 2010

Windows Books

- [Windows Internals](#) by Mark Russinovich et al., 2012
- [Troubleshooting with the Windows Sysinternals Tools](#) by Mark Russinovich & Aaron Margosis, 2016

Social Engineering Books

- [The Art of Deception](#) by Kevin D. Mitnick & William L. Simon, 2002
- [The Art of Intrusion](#) by Kevin D. Mitnick & William L. Simon, 2005
- [Ghost in the Wires](#) by Kevin D. Mitnick & William L. Simon, 2011
- [No Tech Hacking](#) by Johnny Long & Jack Wiles, 2008
- [Social Engineering: The Art of Human Hacking](#) by Christopher Hadnagy, 2010
- [Unmasking the Social Engineer: The Human Element of Security](#) by Christopher Hadnagy, 2014
- [Social Engineering in IT Security: Tools, Tactics, and Techniques](#) by Sharon Conheady, 2014

Lock Picking Books

- [Practical Lock Picking](#) by Deviant Ollam, 2012
- [Keys to the Kingdom](#) by Deviant Ollam, 2012
- [Lock Picking: Detail Overkill](#) by Solomon
- [Eddie the Wire](#) books

Defcon Suggested Reading – Hacking Tools

- [Defcon Suggested Reading](#)

Vulnerability Databases – Hacking Tools

- [Common Vulnerabilities and Exposures \(CVE\)](#) – Dictionary of common names (i.e., CVE Identifiers) for publicly known security vulnerabilities.
- [National Vulnerability Database \(NVD\)](#) – United States government's National Vulnerability Database provides additional meta-data (CPE, CVSS scoring) of the standard CVE List along with a fine-grained search engine.
- [US-CERT Vulnerability Notes Database](#) – Summaries, technical details, remediation information, and lists of vendors affected by software vulnerabilities, aggregated by the United States Computer Emergency Response Team (US-CERT).

- [Full-Disclosure](#) – Public, vendor-neutral forum for detailed discussion of vulnerabilities, often publishes details before many other sources.
- [Bugtraq \(BID\)](#) – Software security bug identification database compiled from submissions to the SecurityFocus mailing Penetration testing tools list and other sources, operated by Symantec, Inc.
- [Exploit-DB](#) – Non-profit project hosting exploits for software vulnerabilities, provided as a public service by Offensive Security.
- [Microsoft Security Bulletins](#) – Announcements of security issues discovered in Microsoft software, published by the Microsoft Security Response Center (MSRC).
- [Microsoft Security Advisories](#) – Archive of security advisories impacting Microsoft software.
- [Mozilla Foundation Security Advisories](#) – Archive of security advisories impacting Mozilla software, including the Firefox Web Browser.
- [Packet Storm](#) – Compendium of exploits, advisories, tools, and other security-related resources aggregated from across the industry.
- [CXSecurity](#) – Archive of published CVE and Bugtraq software vulnerabilities cross-referenced with a Google dork database for discovering the listed vulnerability.
- [SecuriTeam](#) – Independent source of software vulnerability information.
- [Vulnerability Lab](#) – Open forum for security advisories organized by category of exploit target.
- [Zero Day Initiative](#) – Bug bounty program with the publicly accessible archive of published security advisories, operated by TippingPoint.

- [Vulners](#) – Security database of software vulnerabilities.
- [Inj3ct0r \(Onion service\)](#) – Exploit marketplace and vulnerability information aggregator.
- [Open Source Vulnerability Database \(OSVDB\)](#) – Historical archive of security vulnerabilities in computerized equipment, no longer adding to its vulnerability database as of April, 2016.Hacking Tools
- [HPI-VDB](#) – Aggregator of cross-referenced software vulnerabilities offering free-of-charge API access, provided by the Hasso-Plattner Institute, Potsdam.Hacking Tools

Security Courses – Hacking Tools – Hacking Tools

- [Offensive Security Training](#) – Training from BackTrack/Kali developers.
- [SANS Security Training](#) – Computer Security Training & Certification.
- [Open Security Training](#) – Training material for computer security classes.
- [CTF Field Guide](#) – Everything you need to win your next CTF competition.
- [ARIZONA CYBER WARFARE RANGE](#) – 24x7 live fire exercises for beginners through real world operations; capability for upward progression into the real world of cyber warfare.
- [Cybrary](#) – Free courses in ethical hacking and advanced penetration testing. Advanced penetration testing courses are based on the book

'Penetration Testing for Highly-Secured Environments'.

- [Computer Security Student](#) – Many free tutorials, great for beginners, \$10/mo membership unlocks all content.
- [European Union Agency for Network and Information Security](#) – ENISA Cyber Security Training material.

Information Security Conferences – Hacking Tools

- [DEF CON](#) – Annual hacker convention in Las Vegas.
- [Black Hat](#) – Annual security conference in Las Vegas.
- [BSides](#) – Framework for organising and holding security conferences.
- [CCC](#) – Annual meeting of the international hacker scene in Germany.
- [DerbyCon](#) – Annual hacker conference based in Louisville.
- [PhreakNIC](#) – Technology conference held annually in middle Tennessee.
- [ShmooCon](#) – Annual US East coast hacker convention.
- [CarolinaCon](#) – Infosec conference, held annually in North Carolina.
- [CHCon](#) – Christchurch Hacker Con, Only South Island of New Zealand hacker con.
- [SummerCon](#) – One of the oldest hacker conventions, held during Summer.
- [Hack.lu](#) – Annual conference held in Luxembourg.
- [Hackfest](#) – Largest hacking conference in Canada.

- [HITB](#) – Deep-knowledge security conference held in Malaysia and The Netherlands.
- [Troopers](#) – Annual international IT Security event with workshops held in Heidelberg, Germany.
- [Hack3rCon](#) – Annual US hacker conference.
- [ThotCon](#) – Annual US hacker conference held in Chicago.
- [LayerOne](#) – Annual US security conference held every spring in Los Angeles.
- [DeepSec](#) – Security Conference in Vienna, Austria.
- [SkyDogCon](#) – Technology conference in Nashville.
- [SECUINSIDE](#) – Security Conference in [Seoul](#).
- [DefCamp](#) – Largest Security Conference in Eastern Europe, held annually in Bucharest, Romania.
- [AppSecUSA](#) – Annual conference organized by OWASP.
- [BruCON](#) – Annual security conference in Belgium.
- [Infosecurity Europe](#) – Europe's number one information security event, held in London, UK.
- [Nullcon](#) – Annual conference in Delhi and Goa, India.
- [RSA Conference USA](#) – Annual security conference in San Francisco, California, USA.
- [Swiss Cyber Storm](#) – Annual security conference in Lucerne, Switzerland.
- [Virus Bulletin Conference](#) – Annual conference going to be held in Denver, USA for 2016.
- [Ekoparty](#) – Largest Security Conference in Latin America, held annually in Buenos Aires, Argentina.

- [44Con](#) – Annual Security Conference held in London.
- [BalCCon](#) – Balkan Computer Congress, annually held in Novi Sad, Serbia.
- [FSec](#) – FSec – Croatian Information Security Gathering in Varaždin, Croatia.

Information Security Magazines – Hacking Tools

- [2600: The Hacker Quarterly](#) – American publication about technology and computer “underground.”
- [Phrack Magazine](#) – By far the longest running hacker zine.

Awesome Lists – Hacking Tools –

- [Kali Linux Tools](#) – List of Hacking tools present in Kali Linux.
- [SecTools](#) – Top 125 Network Security Hacking Tools.
- [Pentest Cheat Sheets](#) – Awesome Pentest Cheat Sheets.
- [C/C++ Programming](#) – One of the main language for open source security tools.
- [.NET Programming](#) – Software framework for Microsoft Windows platform development.
- [Shell Scripting](#) – Command line frameworks, toolkits, guides and gizmos.

- [Ruby Programming by @dreikanter](#) – The de-facto language for writing exploits.
- [Ruby Programming by @markets](#) – The de-facto language for writing exploits.
- [Ruby Programming by @Sdogruyol](#) – The de-facto language for writing exploits.
- [JavaScript Programming](#) – In-browser development and scripting.
- [Node.js Programming by @sindresorhus](#) – Curated list of delightful Node.js packages and resources.
- [Python tools for penetration testers](#) – Lots of pentesting tools are written in Python.
- [Python Programming by @svaksha](#) – General Python programming.
- [Python Programming by @vinta](#) – General Python programming.
- [Android Security](#) – Collection of Android security-related resources.
- [Awesome Awesomness](#) – The List of the Lists.
- [AppSec](#) – Resources for learning about application security.
- [CTFs](#) – Capture The Flag frameworks, libraries, etc.
- [InfoSec § Hacking challenges](#) – Comprehensive directory of CTFs, wargames, hacking challenge websites, Penetration testing tools list practice lab exercises, and more.
- [Hacking](#) – Tutorials, tools, and resources.
- [Honeypots](#) – Honeypots, tools, components, and more.
- [Infosec](#) – Information security resources for pentesting, forensics, and more.
- [Forensics](#) – Free (mostly open source) forensic analysis tools and resources.

- [Malware Analysis](#) – Tools and resources for analysts.
- [PCAP Tools](#) – Tools for processing network traffic.
- [Security](#) – Software, libraries, documents, and other resources.
- [Awesome Lockpicking](#) – Awesome guides, tools, and other resources about the security and compromise of locks, safes, and keys.
- [SecLists](#) – Collection of multiple types of lists used during security assessments.
- [Security Talks](#) – Curated list of security conferences.
- [OSINT](#) – Awesome OSINT list containing great resources.
- [YARA](#) – YARA rules, tools, and people.

These Awesome Penetration testing Tools collection created with the help of [Following Contributors](#). GBHackers on Security won't take any credits.

You can follow us on [Linkedin](#), [Twitter](#), [Facebook](#) for daily Cybersecurity updates also you can take the [Best Cybersecurity courses online](#) to keep your self-updated.

Share and Support Us :



SOURCE

ENAQX - AWESOME-PENTEST

TAGS

Hacking

Pentesting Tools

Security

Testing

Tools

BALAJI N

<http://www.gbhackers.com>

BALAJI is a Security Researcher (Threat Research Labs) at Comodo Cybersecurity. Editor-in-Chief, Author & Co-Creator of GBHackers On Security



RELATED ARTICLES

MORE FROM AUTHOR

PENTESTING

Most Important Mobile Application Penetration Testing Cheat sheet with Tools & Resources for Security Professionals

Cloud

Cloud Computing Penetration Testing Checklist & Important Considerations

Computer Security

Modern CyberSOC – A Brief Implementation Of Building a Collaborative Cyber Security Infrastructure



2 COMMENTS

Mrs. Doe December 19, 2019 at 12:44 pm

I miss Linux Smart Enumeration
(<https://github.com/diego-treitos/linux-smart-enumeration>) from the GNU/Linux section. Linux Exploit
Suggester is rather old...

Reply

divyanshu January 20, 2020 at 7:08 am

Nice Blog

Reply

Leave a Reply

Enter your comment here...



ABOUT US

GBHackers on security is a Cyber Security platform that covers daily Cyber Security News, Hacking News, Technology updates

FOLLOW US

and Kali Linux tutorials. Our mission is to keep the community up to date with happenings in the Cyber World.

Contact us: admin@gbhackers.com



[Home](#) [TECH NEWS](#) [Infosec- Resources](#) [OWASP – Top 10](#) [Privacy Policy](#) [Contact Us](#) [About Us](#)

© GBHackers on Security 2016 - 2019. All Rights Reserved