Awesome Penetration Testing

> A collection of awesome penetration testing and offensive cybersecurity resources.

Penetration testing is the practice of launching authorized, simulated attacks against computer systems and their physical infrastructure to expose potential security weaknesses and vulnerabilities. Should you discover a vulnerability, please follow this guidance to report it responsibly.

Contents

- Windows Utilities

Android Utilities

- cSploit - Advanced IT security professional toolkit on Android featuring an integrated Metasploit daemon and MITM capabilities.
- Fing - Network scanning and host enumeration app that performs NetBIOS, UPnP, Bonjour, SNMP, and various other advanced device fingerprinting techniques.

Anonymity Tools

- I2P - The Invisible Internet Project.
- Metadata Anonymization Toolkit (MAT) - Metadata removal tool, supporting a wide range of commonly used file formats, written in Python3.
- What Every Browser Knows About You - Comprehensive detection page to test your own Web browser's configuration for privacy and identity leaks.

Tor Tools

See also awesome-tor.

- Nipe - Script to redirect all traffic from the machine to the Tor network.
- OnionScan - Tool for investigating the Dark Web by finding operational security issues introduced by Tor hidden service operators.
- Tails - Live operating system aiming to preserve your privacy and anonymity.
- Tor - Free software and onion routed overlay network that helps you defend against traffic analysis.
- dos-over-tor - Proof of concept denial of service over Tor stress test tool.
- kalitorify - Transparent proxy through Tor for Kali Linux OS.

Anti-virus Evasion Tools

- AntiVirus Evasion Tool (AVET) - Post-process exploits containing executable files targeted for Windows machines to avoid being recognized by antivirus software.
- CarbonCopy - Tool that creates a spoofed certificate of any online website and signs an Executable for AV evasion.
- Hyperion - Runtime encryptor for 32-bit portable executables ("PE `.exe` s").
- Shellter - Dynamic shellcode injection tool, and the first truly dynamic PE infector ever

created.

- UniByAv - Simple obfuscator that takes raw shellcode and generates Anti-Virus friendly executables by using a brute-forcable, 32-bit XOR key.
- Veil - Generate metasploit payloads that bypass common anti-virus solutions.
- peCloakCapstone - Multi-platform fork of the peCloak.py automated malware antivirus evasion tool.

Books

See also DEF CON Suggested Reading.

- Advanced Penetration Testing by Wil Allsopp, 2017
- Advanced Penetration Testing for Highly-Secured Environments by Lee Allen, 2012
- Advanced Persistent Threat Hacking: The Art and Science of Hacking Any Organization by Tyler Wrightson, 2014
- Android Hacker's Handbook by Joshua J. Drake et al., 2014
- BTFM: Blue Team Field Manual by Alan J White & Ben Clark, 2017
- Black Hat Python: Python Programming for Hackers and Pentesters by Justin Seitz, 2014
- Bug Hunter's Diary by Tobias Klein, 2011
- Car Hacker's Handbook by Craig Smith, 2016
- Fuzzing: Brute Force Vulnerability Discovery by Michael Sutton et al., 2007
- Metasploit: The Penetration Tester's Guide by David Kennedy et al., 2011
- Penetration Testing: A Hands-On Introduction to Hacking by Georgia Weidman, 2014
- Penetration Testing: Procedures & Methodologies by EC-Council, 2010
- Professional Penetration Testing by Thomas Wilhelm, 2013
- RTFM: Red Team Field Manual by Ben Clark, 2014
- The Art of Exploitation by Jon Erickson, 2008
- The Basics of Hacking and Penetration Testing by Patrick Engebretson, 2013
- The Database Hacker's Handbook, David Litchfield et al., 2005
- The Hacker Playbook by Peter Kim, 2014
- The Mac Hacker's Handbook by Charlie Miller & Dino Dai Zovi, 2009
- The Mobile Application Hacker's Handbook by Dominic Chell et al., 2015
- Unauthorised Access: Physical Penetration Testing For IT Security Teams by Wil Allsopp, 2010
- Violent Python by TJ O'Connor, 2012
- iOS Hacker's Handbook by Charlie Miller et al., 2012

Malware Analysis Books

See awesome-malware-analysis § Books.

CTF Tools

- CTF Field Guide - Everything you need to win your next CTF competition.
- Ciphey - Automated decryption tool using artificial intelligence and natural language processing.
- RsaCtfTool - Decrypt data enciphered using weak RSA keys, and recover private keys from public keys using a variety of automated attacks.
- ctf-tools - Collection of setup scripts to install various security research tools easily and quickly deployable to new machines.
- shellpop - Easily generate sophisticated reverse or bind shell commands to help you save time during penetration tests.

Cloud Platform Attack Tools

See also *HackingThe.cloud*.

- Cloud Container Attack Tool (CCAT) - Tool for testing security of container environments.
- CloudHunter - Looks for AWS, Azure and Google cloud storage buckets and lists permissions for vulnerable buckets.
- Cloudsplaining - Identifies violations of least privilege in AWS IAM policies and generates a pretty HTML report with a triage worksheet.
- Endgame - AWS Pentesting tool that lets you use one-liner commands to backdoor an AWS account's resources with a rogue AWS account.
- GCPBucketBrute - Script to enumerate Google Storage buckets, determine what access you have to them, and determine if they can be privilege escalated.

Collaboration Tools

- Dradis - Open-source reporting and collaboration tool for IT security professionals.
- Lair - Reactive attack collaboration framework and web application built with meteor.
- Pentest Collaboration Framework (PCF) - Open source, cross-platform, and portable toolkit for automating routine pentest processes with a team.
- Reconmap - Open-source collaboration platform for InfoSec professionals that streamlines the pentest process.

- RedELK - Track and alarm about Blue Team activities while providing better usability in long term offensive operations.

Conferences and Events

- BSides - Framework for organising and holding security conferences.
- CTFTime.org - Directory of upcoming and archive of past Capture The Flag (CTF) competitions with links to challenge writeups.

Asia

- HITB - Deep-knowledge security conference held in Malaysia and The Netherlands.
- HITCON - Hacks In Taiwan Conference held in Taiwan.
- Nullcon - Annual conference in Delhi and Goa, India.
- SECUINSIDE - Security Conference in Seoul.

Europe

- 44Con - Annual Security Conference held in London.
- BalCCon - Balkan Computer Congress, annually held in Novi Sad, Serbia.
- BruCON - Annual security conference in Belgium.
- CCC - Annual meeting of the international hacker scene in Germany.
- DeepSec - Security Conference in Vienna, Austria.
- DefCamp - Largest Security Conference in Eastern Europe, held annually in Bucharest, Romania.
- FSec - FSec - Croatian Information Security Gathering in Varaždin, Croatia.
- Hack.lu - Annual conference held in Luxembourg.
- Infosecurity Europe - Europe's number one information security event, held in London, UK.
- SteelCon - Security conference in Sheffield UK.
- Swiss Cyber Storm - Annual security conference in Lucerne, Switzerland.
- Troopers - Annual international IT Security event with workshops held in Heidelberg, Germany.
- HoneyCON - Annual Security Conference in Guadalajara, Spain. Organized by the HoneySEC association.

North America

- AppSecUSA - Annual conference organized by OWASP.

- Black Hat - Annual security conference in Las Vegas.
- CarolinaCon - Infosec conference, held annually in North Carolina.
- DEF CON - Annual hacker convention in Las Vegas.
- DerbyCon - Annual hacker conference based in Louisville.
- Hackers Next Door - Cybersecurity and social technology conference held in New York City.
- Hackers On Planet Earth (HOPE) - Semi-annual conference held in New York City.
- Hackfest - Largest hacking conference in Canada.
- LayerOne - Annual US security conference held every spring in Los Angeles.
- National Cyber Summit - Annual US security conference and Capture the Flag event, held in Huntsville, Alabama, USA.
- PhreakNIC - Technology conference held annually in middle Tennessee.
- RSA Conference USA - Annual security conference in San Francisco, California, USA.
- ShmooCon - Annual US East coast hacker convention.
- SkyDogCon - Technology conference in Nashville.
- SummerCon - One of the oldest hacker conventions in America, held during Summer.
- ThotCon - Annual US hacker conference held in Chicago.
- Virus Bulletin Conference - Annual conference going to be held in Denver, USA for 2016.

South America

- Ekoparty - Largest Security Conference in Latin America, held annually in Buenos Aires, Argentina.
- Hackers to Hackers Conference (H2HC) - Oldest security research (hacking) conference in Latin America and one of the oldest ones still active in the world.

Zealandia

- CHCon - Christchurch Hacker Con, Only South Island of New Zealand hacker con.

Exfiltration Tools

- DET - Proof of concept to perform data exfiltration using either single or multiple channel(s) at the same time.
- Iodine - Tunnel IPv4 data through a DNS server; useful for exfiltration from networks where Internet access is firewalled, but DNS queries are allowed.
- TrevorC2 - Client/server tool for masking command and control and data exfiltration through a normally browsable website, not typical HTTP POST requests.

- dnscat2 - Tool designed to create an encrypted command and control channel over the DNS protocol, which is an effective tunnel out of almost every network.
- pwnat - Punches holes in firewalls and NATs.
- tgcd - Simple Unix network utility to extend the accessibility of TCP/IP based network services beyond firewalls.
- QueenSono - Client/Server Binaries for data exfiltration with ICMP. Useful in a network where ICMP protocol is less monitored than others (which is a common case).

Exploit Development Tools

See also *Reverse Engineering Tools*.

- Magic Unicorn - Shellcode generator for numerous attack vectors, including Microsoft Office macros, PowerShell, HTML applications (HTA), or `certutil` (using fake certificates).
- Pwntools - Rapid exploit development framework built for use in CTFs.
- peda - Python Exploit Development Assistance for GDB.
- Wordpress Exploit Framework - Ruby framework for developing and using modules which aid in the penetration testing of WordPress powered websites and systems.

File Format Analysis Tools

- ExifTool - Platform-independent Perl library plus a command-line application for reading, writing and editing meta information in a wide variety of files.
- Hachoir - Python library to view and edit a binary stream as tree of fields and tools for metadata extraction.
- Kaitai Struct - File formats and network protocols dissection language and web IDE, generating parsers in C++, C#, Java, JavaScript, Perl, PHP, Python, Ruby.
- peepdf - Python tool to explore PDF files in order to find out if the file can be harmful or not.
- Veles - Binary data visualization and analysis tool.

GNU/Linux Utilities

- Hwacha - Post-exploitation tool to quickly execute payloads via SSH on one or more Linux systems simultaneously.
- Linux Exploit Suggester - Heuristic reporting on potentially viable exploits for a given GNU/Linux system.
- Lynis - Auditing tool for UNIX-based systems.
- checksec.sh - Shell script designed to test what standard Linux OS and PaX security

features are being used.

Hash Cracking Tools

- BruteForce Wallet - Find the password of an encrypted wallet file (i.e. `wallet.dat`).
- CeWL - Generates custom wordlists by spidering a target's website and collecting unique words.
- duplicut - Quickly remove duplicates, without changing the order, and without getting OOM on huge wordlists.
- GoCrack - Management Web frontend for distributed password cracking sessions using hashcat (or other supported tools) written in Go.
- Hashcat - The more fast hash cracker.
- hate_crack - Tool for automating cracking methodologies through Hashcat.
- JWT Cracker - Simple HS256 JSON Web Token (JWT) token brute force cracker.
- John the Ripper - Fast password cracker.
- Rar Crack - RAR bruteforce cracker.

Hex Editors

- Bless - High quality, full featured, cross-platform graphical hex editor written in Gtk#.
- Frhed - Binary file editor for Windows.
- Hex Fiend - Fast, open source, hex editor for macOS with support for viewing binary diffs.
- HexEdit.js - Browser-based hex editing.
- Hexinator - World's finest (proprietary, commercial) Hex Editor.
- hexedit - Simple, fast, console-based hex editor.
- wxHexEditor - Free GUI hex editor for GNU/Linux, macOS, and Windows.

Industrial Control and SCADA Systems

See also awesome-industrial-control-system-security.

- Industrial Exploitation Framework (ISF) - Metasploit-like exploit framework based on routersploit designed to target Industrial Control Systems (ICS), SCADA devices, PLC firmware, and more.
- s7scan - Scanner for enumerating Siemens S7 PLCs on a TCP/IP or LLC network.

Intentionally Vulnerable Systems

See also awesome-vulnerable.

Intentionally Vulnerable Systems as Docker Containers

- Damn Vulnerable Web Application (DVWA) - `docker pull citizenstig/dvwa .`
- OWASP Juice Shop - `docker pull bkimminich/juice-shop .`
- OWASP Mutillidae II Web Pen-Test Practice Application - `docker pull citizenstig/nowasp .`
- OWASP NodeGoat - `docker-compose build && docker-compose up .`
- OWASP Security Shepherd - `docker pull ismisepaul/securityshepherd .`
- OWASP WebGoat Project 7.1 docker image - `docker pull webgoat/webgoat-7.1 .`
- OWASP WebGoat Project 8.0 docker image - `docker pull webgoat/webgoat-8.0 .`
- Vulnerability as a service: Heartbleed - `docker pull hmlio/vaas-cve-2014-0160 .`
- Vulnerability as a service: SambaCry - `docker pull vulnerables/cve-2017-7494 .`
- Vulnerability as a service: Shellshock - `docker pull hmlio/vaas-cve-2014-6271 .`
- Vulnerable WordPress Installation - `docker pull wpscanteam/vulnerablewordpress .`

Lock Picking

See awesome-lockpicking.

macOS Utilities

- Bella - Pure Python post-exploitation data mining and remote administration tool for macOS.
- EvilOSX - Modular RAT that uses numerous evasion and exfiltration techniques out-of-the-box.

Multi-paradigm Frameworks

- Armitage - Java-based GUI front-end for the Metasploit Framework.
- AutoSploit - Automated mass exploiter, which collects target by employing the Shodan.io API and programmatically chooses Metasploit exploit modules based on the Shodan query.
- Decker - Penetration testing orchestration and automation framework, which allows writing declarative, reusable configurations capable of ingesting variables and using outputs of tools it has run as inputs to others.
- Faraday - Multiuser integrated pentesting environment for red teams performing cooperative penetration tests, security audits, and risk assessments.

- Metasploit - Software for offensive security teams to help verify vulnerabilities and manage security assessments.
- Pupy - Cross-platform (Windows, Linux, macOS, Android) remote administration and post-exploitation tool.

Network Tools

- CrackMapExec - Swiss army knife for pentesting networks.
- IKEForce - Command line IPSEC VPN brute forcing tool for Linux that allows group name/ID enumeration and XAUTH brute forcing capabilities.
- Intercepter-NG - Multifunctional network toolkit.
- Legion - Graphical semi-automated discovery and reconnaissance framework based on Python 3 and forked from SPARTA.
- Network-Tools.com - Website offering an interface to numerous basic network utilities like `ping`, `traceroute`, `whois`, and more.
- Ncrack - High-speed network authentication cracking tool built to help companies secure their networks by proactively testing all their hosts and networking devices for poor passwords.
- Praeda - Automated multi-function printer data harvester for gathering usable data during security assessments.
- Printer Exploitation Toolkit (PRET) - Tool for printer security testing capable of IP and USB connectivity, fuzzing, and exploitation of PostScript, PJL, and PCL printer language features.
- SPARTA - Graphical interface offering scriptable, configurable access to existing network infrastructure scanning and enumeration tools.
- SigPloit - Signaling security testing framework dedicated to telecom security for researching vulnerabilites in the signaling protocols used in mobile (cellular phone) operators.
- Smart Install Exploitation Tool (SIET) - Scripts for identifying Cisco Smart Install-enabled switches on a network and then manipulating them.
- THC Hydra - Online password cracking tool with built-in support for many network protocols, including HTTP, SMB, FTP, telnet, ICQ, MySQL, LDAP, IMAP, VNC, and more.
- Tsunami - General purpose network security scanner with an extensible plugin system for detecting high severity vulnerabilities with high confidence.
- Zarp - Network attack tool centered around the exploitation of local networks.
- dnstwist - Domain name permutation engine for detecting typo squatting, phishing and corporate espionage.
- dsniff - Collection of tools for network auditing and pentesting.

- impacket - Collection of Python classes for working with network protocols.
- pivotsuite - Portable, platform independent and powerful network pivoting toolkit.
- routersploit - Open source exploitation framework similar to Metasploit but dedicated to embedded devices.
- rshijack - TCP connection hijacker, Rust rewrite of `shijack`.

DDoS Tools

- Anevicon - Powerful UDP-based load generator, written in Rust.
- D(HE)ater - D(HE)ater sends forged cryptographic handshake messages to enforce the Diffie-Hellman key exchange.
- HOIC - Updated version of Low Orbit Ion Cannon, has 'boosters' to get around common counter measures.
- Low Orbit Ion Canon (LOIC) - Open source network stress tool written for Windows.
- Memcrashed - DDoS attack tool for sending forged UDP packets to vulnerable Memcached servers obtained using Shodan API.
- SlowLoris - DoS tool that uses low bandwidth on the attacking side.
- 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.

Network Reconnaissance Tools

- ACLight - Script for advanced discovery of sensitive Privileged Accounts - includes Shadow Admins.
- AQUATONE - Subdomain discovery tool utilizing various open sources producing a report that can be used as input to other tools.
- CloudFail - Unmask server IP addresses hidden behind Cloudflare by searching old database records and detecting misconfigured DNS.
- DNSDumpster - Online DNS recon and search service.
- Mass Scan - TCP port scanner, spews SYN packets asynchronously, scanning entire Internet in under 5 minutes.
- OWASP Amass - Subdomain enumeration via scraping, web archives, brute forcing, permutations, reverse DNS sweeping, TLS certificates, passive DNS data sources, etc.
- ScanCannon - POSIX-compliant BASH script to quickly enumerate large networks by calling `masscan` to quickly identify open ports and then `nmap` to gain details on the systems/services on those ports.

- XRay - Network (sub)domain discovery and reconnaissance automation tool.
- 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 - Passive DNS network mapper.
- dnsrecon - DNS enumeration script.
- dnstracer - Determines where a given DNS server gets its information from, and follows the chain of DNS servers.
- fierce - Python3 port of the original `fierce.pl` DNS reconnaissance tool for locating non-contiguous IP space.
- netdiscover - Network address discovery scanner, based on ARP sweeps, developed mainly for those wireless networks without a DHCP server.
- nmap - Free security scanner for network exploration & security audits.
- 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.
- RustScan - Lightweight and quick open-source port scanner designed to automatically pipe open ports into Nmap.
- scanless - Utility for using websites to perform port scans on your behalf so as not to reveal your own IP.
- smbmap - Handy SMB enumeration tool.
- subbrute - DNS meta-query spider that enumerates DNS records, and subdomains.
- zmap - Open source network scanner that enables researchers to easily perform Internet-wide network studies.

Protocol Analyzers and Sniffers

See also awesome-pcaptools.

- Debookee - Simple and powerful network traffic analyzer for macOS.
- Dshell - Network forensic analysis framework.
- Netzob - Reverse engineering, traffic generation and fuzzing of communication protocols.
- Wireshark - Widely-used graphical, cross-platform network protocol analyzer.
- netsniff-ng - Swiss army knife for network sniffing.
- sniffglue - Secure multithreaded packet sniffer.
- tcpdump/libpcap - Common packet analyzer that runs under the command line.

Network Traffic Replay and Editing Tools

- TraceWrangler - Network capture file toolkit that can edit and merge `pcap` or `pcapng` files with batch editing features.
- WireEdit - Full stack WYSIWYG pcap editor (requires a free license to edit packets).
- bittwist - Simple yet powerful libpcap-based Ethernet packet generator useful in simulating networking traffic or scenario, testing firewall, IDS, and IPS, and troubleshooting various network problems.
- hping3 - Network tool able to send custom TCP/IP packets.
- pig - GNU/Linux packet crafting tool.
- scapy - Python-based interactive packet manipulation program and library.
- tcpreplay - Suite of free Open Source utilities for editing and replaying previously captured network traffic.

Proxies and Machine-in-the-Middle (MITM) Tools

See also *Intercepting Web proxies*.

- BetterCAP - Modular, portable and easily extensible MITM framework.
- Ettercap - Comprehensive, mature suite for machine-in-the-middle attacks.
- Habu - Python utility implementing a variety of network attacks, such as ARP poisoning, DHCP starvation, and more.
- Lambda-Proxy - Utility for testing SQL Injection vulnerabilities on AWS Lambda serverless functions.
- MITMf - Framework for Man-In-The-Middle attacks.
- Morpheus - Automated ettercap TCP/IP Hijacking tool.
- SSH MITM - Intercept SSH connections with a proxy; all plaintext passwords and sessions are logged to disk.
- dnschef - Highly configurable DNS proxy for pentesters.
- evilgrade - Modular framework to take advantage of poor upgrade implementations by injecting fake updates.
- mallory - HTTP/HTTPS proxy over SSH.
- oregano - Python module that runs as a machine-in-the-middle (MITM) accepting Tor client requests.
- sylkie - Command line tool and library for testing networks for common address spoofing security vulnerabilities in IPv6 networks using the Neighbor Discovery Protocol.

Transport Layer Security Tools

- SSLyze - Fast and comprehensive TLS/SSL configuration analyzer to help identify security

mis-configurations.

- crackpkcs12 - Multithreaded program to crack PKCS#12 files (`.p12` and `.pfx` extensions), such as TLS/SSL certificates.
- 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.
- tls_prober - Fingerprint a server's SSL/TLS implementation.

Wireless Network Tools

- Aircrack-ng - Set of tools for auditing wireless networks.
- Airgeddon - Multi-use bash script for Linux systems to audit wireless networks.
- BoopSuite - Suite of tools written in Python for wireless auditing.
- Bully - Implementation of the WPS brute force attack, written in C.
- Cowpatty - Brute-force dictionary attack against WPA-PSK.
- Fluxion - Suite of automated social engineering based WPA attacks.
- KRACK Detector - Detect and prevent KRACK attacks in your network.
- Kismet - Wireless network detector, sniffer, and IDS.
- PSKracker - Collection of WPA/WPA2/WPS default algorithms, password generators, and PIN generators written in C.
- Reaver - Brute force attack against WiFi Protected Setup.
- WiFi Pineapple - Wireless auditing and penetration testing platform.
- WiFi-Pumpkin - Framework for rogue Wi-Fi access point attack.
- Wifite - Automated wireless attack tool.
- infernal-twin - Automated wireless hacking tool.
- krackattacks-scripts - WPA2 Krack attack scripts.
- pwnagotchi - Deep reinforcement learning based AI that learns from the Wi-Fi environment and instruments BetterCAP in order to maximize the WPA key material captured.
- wifi-arsenal - Resources for Wi-Fi Pentesting.

Network Vulnerability Scanners

- celerystalk - Asynchronous enumeration and vulnerability scanner that "runs all the tools on all the hosts" in a configurable manner.
- kube-hunter - Open-source tool that runs a set of tests ("hunters") for security issues in Kubernetes clusters from either outside ("attacker's view") or inside a cluster.
- Nessus - Commercial vulnerability management, configuration, and compliance assessment platform, sold by Tenable.

- Netsparker Application Security Scanner - Application security scanner to automatically find security flaws.
- Nexpose - Commercial vulnerability and risk management assessment engine that integrates with Metasploit, sold by Rapid7.
- OpenVAS - Free software implementation of the popular Nessus vulnerability assessment system.
- Vuls - Agentless vulnerability scanner for GNU/Linux and FreeBSD, written in Go.

Web Vulnerability Scanners

- ACSTIS - Automated client-side template injection (sandbox escape/bypass) detection for AngularJS.
- Arachni - Scriptable framework for evaluating the security of web applications.
- JCS - Joomla Vulnerability Component Scanner with automatic database updater from exploitdb and packetstorm.
- Nikto - Noisy but fast black box web server and web application vulnerability scanner.
- SQLmate - Friend of `sqlmap` that identifies SQLi vulnerabilities based on a given dork and (optional) website.
- SecApps - In-browser web application security testing suite.
- WPScan - Black box WordPress vulnerability scanner.
- Wapiti - Black box web application vulnerability scanner with built-in fuzzer.
- WebReaver - Commercial, graphical web application vulnerability scanner designed for macOS.
- cms-explorer - Reveal the specific modules, plugins, components and themes that various websites powered by content management systems are running.
- joomscan - Joomla vulnerability scanner.
- skipfish - Performant and adaptable active web application security reconnaissance tool.
- w3af - Web application attack and audit framework.

Online Resources

Online Operating Systems Resources

- DistroWatch.com's Security Category - Website dedicated to talking about, reviewing, and keeping up to date with open source operating systems.

Online Penetration Testing Resources

- MITRE's Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) - Curated knowledge base and model for cyber adversary behavior.
- Metasploit Unleashed - Free Offensive Security Metasploit course.
- 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 Execution Standard (PTES) - Documentation designed to provide a common language and scope for performing and reporting the results of a penetration test.
- Penetration Testing Framework (PTF) - Outline for performing penetration tests compiled as a general framework usable by vulnerability analysts and penetration testers alike.
- XSS-Payloads - Resource dedicated to all things XSS (cross-site), including payloads, tools, games, and documentation.

Other Lists Online

- .NET Programming - Software framework for Microsoft Windows platform development.
- Infosec/hacking videos recorded by cooper - Collection of security conferences recorded by Cooper.
- Android Exploits - Guide on Android Exploitation and Hacks.
- Android Security - Collection of Android security related resources.
- AppSec - Resources for learning about application security.
- Awesome Awesomness - The List of the Lists.
- Awesome Malware - Curated collection of awesome malware, botnets, and other post-exploitation tools.
- Awesome Shodan Queries - Awesome list of useful, funny, and depressing search queries for Shodan.
- AWS Tool Arsenal - List of tools for testing and securing AWS environments.
- Blue Team - Awesome resources, tools, and other shiny things for cybersecurity blue teams.
- C/C++ Programming - One of the main language for open source security tools.
- CTFs - Capture The Flag frameworks, libraries, etc.
- Forensics - Free (mostly open source) forensic analysis tools and resources.
- Hacking - Tutorials, tools, and resources.
- Honeypots - Honeypots, tools, components, and more.
- InfoSec § Hacking challenges - Comprehensive directory of CTFs, wargames, hacking challenge websites, pentest practice lab exercises, and more.
- Infosec - Information security resources for pentesting, forensics, and more.

- JavaScript Programming - In-browser development and scripting.
- Kali Linux Tools - List of tools present in Kali Linux.
- Node.js Programming by @sindresorhus - Curated list of delightful Node.js packages and resources.
- Pentest Cheat Sheets - Awesome Pentest Cheat Sheets.
- Python Programming by @svaksha - General Python programming.
- Python Programming by @vinta - General Python programming.
- Python tools for penetration testers - Lots of pentesting tools are written in Python.
- Rawsec's CyberSecurity Inventory - An open-source inventory of tools, resources, CTF platforms and Operating Systems about CyberSecurity. (Source)
- Red Teaming - List of Awesome Red Teaming Resources.
- Ruby Programming by @Sdogruyol - The de-facto language for writing exploits.
- Ruby Programming by @dreikanter - The de-facto language for writing exploits.
- Ruby Programming by @markets - The de-facto language for writing exploits.
- SecLists - Collection of multiple types of lists used during security assessments.
- SecTools - Top 125 Network Security Tools.
- Security Talks - Curated list of security conferences.
- Security - Software, libraries, documents, and other resources.
- Serverless Security - Curated list of awesome serverless security resources such as (e)books, articles, whitepapers, blogs and research papers.
- Shell Scripting - Command line frameworks, toolkits, guides and gizmos.
- YARA - YARA rules, tools, and people.

Penetration Testing Report Templates

- Public Pentesting Reports - Curated list of public penetration test reports released by several consulting firms and academic security groups.
- T&VS Pentesting Report Template - Pentest report template provided by Test and Verification Services, Ltd.
- Web Application Security Assessment Report Template - Sample Web application security assessment reporting template provided by Lucideus.

Open Sources Intelligence (OSINT)

See also awesome-osint.

- DataSploit - OSINT visualizer utilizing Shodan, Censys, Clearbit, EmailHunter, FullContact,

and Zoomeye behind the scenes.
- Depix - Tool for recovering passwords from pixelized screenshots (by de-pixelating text).
- GyoiThon - GyoiThon is an Intelligence Gathering tool using Machine Learning.
- Intrigue - Automated OSINT & Attack Surface discovery framework with powerful API, UI and CLI.
- Maltego - Proprietary software for open sources intelligence and forensics.
- PacketTotal - Simple, free, high-quality packet capture file analysis facilitating the quick detection of network-borne malware (using Zeek and Suricata IDS signatures under the hood).
- Skiptracer - OSINT scraping framework that utilizes basic Python webscraping (BeautifulSoup) of PII paywall sites to compile passive information on a target on a ramen noodle budget.
- Sn1per - Automated Pentest Recon Scanner.
- Spiderfoot - Multi-source OSINT automation tool with a Web UI and report visualizations.
- creepy - Geolocation OSINT tool.
- gOSINT - OSINT tool with multiple modules and a telegram scraper.
- image-match - Quickly search over billions of images.
- recon-ng - Full-featured Web Reconnaissance framework written in Python.
- sn0int - Semi-automatic OSINT framework and package manager.
- Facebook Friend List Scraper - Tool to scrape names and usernames from large friend lists on Facebook, without being rate limited.

Data Broker and Search Engine Services

- Hunter.io - Data broker providing a Web search interface for discovering the email addresses and other organizational details of a company.
- Threat Crowd - Search engine for threats.
- Virus Total - Free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.
- surfraw - Fast UNIX command line interface to a variety of popular WWW search engines.

Dorking tools

- BinGoo - GNU/Linux bash based Bing and Google Dorking Tool.
- dorkbot - Command-line tool to scan Google (or other) search results for vulnerabilities.
- github-dorks - CLI tool to scan GitHub repos/organizations for potential sensitive information leaks.
- GooDork - Command line Google dorking tool.

- Google Hacking Database - Database of Google dorks; can be used for recon.
- dork-cli - Command line Google dork tool.
- dorks - Google hack database automation tool.
- fast-recon - Perform Google dorks against a domain.
- pagodo - Automate Google Hacking Database scraping.
- snitch - Information gathering via dorks.

Email search and analysis tools

- SimplyEmail - Email recon made fast and easy.
- WhatBreach - Search email addresses and discover all known breaches that this email has been seen in, and download the breached database if it is publicly available.

Metadata harvesting and analysis

- FOCA (Fingerprinting Organizations with Collected Archives) - Automated document harvester that searches Google, Bing, and DuckDuckGo to find and extrapolate internal company organizational structures.
- metagoofil - Metadata harvester.
- theHarvester - E-mail, subdomain and people names harvester.

Network device discovery tools

- Censys - Collects data on hosts and websites through daily ZMap and ZGrab scans.
- Shodan - World's first search engine for Internet-connected devices.
- ZoomEye - Search engine for cyberspace that lets the user find specific network components.

OSINT Online Resources

- CertGraph - Crawls a domain's SSL/TLS certificates for its certificate alternative names.
- GhostProject - Searchable database of billions of cleartext passwords, partially visible for free.
- NetBootcamp OSINT Tools - Collection of OSINT links and custom Web interfaces to other services.
- OSINT Framework - Collection of various OSINT tools broken out by category.
- WiGLE.net - Information about wireless networks world-wide, with user-friendly desktop and web applications.

Source code repository searching tools

See also *Web-accessible source code ripping tools*.

- vcsmap - Plugin-based tool to scan public version control systems for sensitive information.
- Yar - Clone git repositories to search through the whole commit history in order of commit time for secrets, tokens, or passwords.

Web application and resource analysis tools

- BlindElephant - Web application fingerprinter.
- EyeWitness - Tool to take screenshots of websites, provide some server header info, and identify default credentials if possible.
- VHostScan - Virtual host scanner that performs reverse lookups, can be used with pivot tools, detect catch-all scenarios, aliases and dynamic default pages.
- Wappalyzer - Wappalyzer uncovers the technologies used on websites.
- WhatWaf - Detect and bypass web application firewalls and protection systems.
- WhatWeb - Website fingerprinter.
- wafw00f - Identifies and fingerprints Web Application Firewall (WAF) products.
- webscreenshot - Simple script to take screenshots of websites from a list of sites.

Operating System Distributions

- Android Tamer - Distribution built for Android security professionals that includes tools required for Android security testing.
- ArchStrike - Arch GNU/Linux repository for security professionals and enthusiasts.
- AttifyOS - GNU/Linux distribution focused on tools useful during Internet of Things (IoT) security assessments.
- BlackArch - Arch GNU/Linux-based distribution for penetration testers and security researchers.
- Buscador - GNU/Linux virtual machine that is pre-configured for online investigators.
- Kali - Rolling Debian-based GNU/Linux distribution designed for penetration testing and digital forensics.
- Network Security Toolkit (NST) - Fedora-based GNU/Linux bootable live Operating System designed to provide easy access to best-of-breed open source network security applications.
- Parrot - Distribution similar to Kali, with support for multiple hardware architectures.
- PentestBox - Open source pre-configured portable penetration testing environment for the

Windows Operating System.

- The Pentesters Framework - Distro organized around the Penetration Testing Execution Standard (PTES), providing a curated collection of utilities that omits less frequently used utilities.

Periodicals

- 2600: The Hacker Quarterly - American publication about technology and computer "underground" culture.
- Phrack Magazine - By far the longest running hacker zine.

Physical Access Tools

- AT Commands - Use AT commands over an Android device's USB port to rewrite device firmware, bypass security mechanisms, exfiltrate sensitive information, perform screen unlocks, and inject touch events.
- Bash Bunny - Local exploit delivery tool in the form of a USB thumbdrive in which you write payloads in a DSL called BunnyScript.
- LAN Turtle - Covert "USB Ethernet Adapter" that provides remote access, network intelligence gathering, and MITM capabilities when installed in a local network.
- PCILeech - Uses PCIe hardware devices to read and write from the target system memory via Direct Memory Access (DMA) over PCIe.
- Packet Squirrel - Ethernet multi-tool designed to enable covert remote access, painless packet captures, and secure VPN connections with the flip of a switch.
- Poisontap - Siphons cookies, exposes internal (LAN-side) router and installs web backdoor on locked computers.
- Proxmark3 - RFID/NFC cloning, replay, and spoofing toolkit often used for analyzing and attacking proximity cards/readers, wireless keys/keyfobs, and more.
- Thunderclap - Open source I/O security research platform for auditing physical DMA-enabled hardware peripheral ports.
- USB Rubber Ducky - Customizable keystroke injection attack platform masquerading as a USB thumbdrive.

Privilege Escalation Tools

- Active Directory and Privilege Escalation (ADAPE) - Umbrella script that automates numerous useful PowerShell modules to discover security misconfigurations and attempt privilege escalation against Active Directory.

- GTFOBins - Curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems.
- LOLBAS (Living Off The Land Binaries and Scripts) - Documents binaries, scripts, and libraries that can be used for "Living Off The Land" techniques, i.e., binaries that can be used by an attacker to perform actions beyond their original purpose.
- LinEnum - Scripted local Linux enumeration and privilege escalation checker useful for auditing a host and during CTF gaming.
- Postenum - Shell script used for enumerating possible privilege escalation opportunities on a local GNU/Linux system.
- unix-privesc-check - Shell script to check for simple privilege escalation vectors on UNIX systems.

Password Spraying Tools

- DomainPasswordSpray - Tool written in PowerShell to perform a password spray attack against users of a domain.
- SprayingToolkit - Scripts to make password spraying attacks against Lync/S4B, Outlook Web Access (OWA) and Office 365 (O365) a lot quicker, less painful and more efficient.

Reverse Engineering

See also awesome-reversing, *Exploit Development Tools*.

Reverse Engineering Books

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

Reverse Engineering Tools

- angr - Platform-agnostic binary analysis framework.
- Capstone - Lightweight multi-platform, multi-architecture disassembly framework.
- Detect It Easy(DiE) - Program for determining types of files for Windows, Linux and MacOS.
- Evan's Debugger - OllyDbg-like debugger for GNU/Linux.
- Frida - Dynamic instrumentation toolkit for developers, reverse-engineers, and security researchers.

- Fridax - Read variables and intercept/hook functions in Xamarin/Mono JIT and AOT compiled iOS/Android applications.
- Ghidra - Suite of free software reverse engineering tools developed by NSA's Research Directorate originally exposed in WikiLeaks's "Vault 7" publication and now maintained as open source software.
- Immunity Debugger - Powerful way to write exploits and analyze malware.
- Interactive Disassembler (IDA Pro) - Proprietary multi-processor disassembler and debugger for Windows, GNU/Linux, or macOS; also has a free version, IDA Free.
- Medusa - Open source, cross-platform interactive disassembler.
- OllyDbg - x86 debugger for Windows binaries that emphasizes binary code analysis.
- PyREBox - Python scriptable Reverse Engineering sandbox by Cisco-Talos.
- Radare2 - Open source, crossplatform reverse engineering framework.
- UEFITool - UEFI firmware image viewer and editor.
- Voltron - Extensible debugger UI toolkit written in Python.
- WDK/WinDbg - Windows Driver Kit and WinDbg.
- binwalk - Fast, easy to use tool for analyzing, reverse engineering, and extracting firmware images.
- boxxy - Linkable sandbox explorer.
- dnSpy - Tool to reverse engineer .NET assemblies.
- plasma - Interactive disassembler for x86/ARM/MIPS. Generates indented pseudo-code with colored syntax code.
- pwndbg - GDB plug-in that eases debugging with GDB, with a focus on features needed by low-level software developers, hardware hackers, reverse-engineers, and exploit developers.
- rVMI - Debugger on steroids; inspect userspace processes, kernel drivers, and preboot environments in a single tool.
- x64dbg - Open source x64/x32 debugger for windows.

Security Education Courses

- 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'.
- European Union Agency for Network and Information Security - ENISA Cyber Security Training material.

- Offensive Security Training - Training from BackTrack/Kali developers.
- Open Security Training - Training material for computer security classes.
- Roppers Academy Training - Free courses on computing and security fundamentals designed to train a beginner to crush their first CTF.
- SANS Security Training - Computer Security Training & Certification.

Shellcoding Guides and Tutorials

- Exploit Writing Tutorials - Tutorials on how to develop exploits.
- Shellcode Examples - Shellcodes database.
- Shellcode Tutorial - Tutorial on how to write shellcode.
- The Shellcoder's Handbook by Chris Anley et al., 2007

Side-channel Tools

- ChipWhisperer - Complete open-source toolchain for side-channel power analysis and glitching attacks.
- SGX-Step - Open-source framework to facilitate side-channel attack research on Intel x86 processors in general and Intel SGX (Software Guard Extensions) platforms in particular.
- TRRespass - Many-sided rowhammer tool suite able to reverse engineer the contents of DDR3 and DDR4 memory chips protected by Target Row Refresh mitigations.

Social Engineering

See also awesome-social-engineering.

Social Engineering Books

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

Social Engineering Online Resources

- Social Engineering Framework - Information resource for social engineers.

Social Engineering Tools

- Beelogger - Tool for generating keylooger.
- Catphish - Tool for phishing and corporate espionage written in Ruby.
- Evilginx2 - Standalone Machine-in-the-Middle (MitM) reverse proxy attack framework for setting up phishing pages capable of defeating most forms of 2FA security schemes.
- FiercePhish - Full-fledged phishing framework to manage all phishing engagements.
- Gophish - Open-source phishing framework.
- King Phisher - Phishing campaign toolkit used for creating and managing multiple simultaneous phishing attacks with custom email and server content.
- Modlishka - Flexible and powerful reverse proxy with real-time two-factor authentication.
- ReelPhish - Real-time two-factor phishing tool.
- Social Engineer Toolkit (SET) - Open source pentesting framework designed for social engineering featuring a number of custom attack vectors to make believable attacks quickly.
- SocialFish - Social media phishing framework that can run on an Android phone or in a Docker container.
- phishery - TLS/SSL enabled Basic Auth credential harvester.
- wifiphisher - Automated phishing attacks against WiFi networks.

Static Analyzers

- Brakeman - Static analysis security vulnerability scanner for Ruby on Rails applications.
- FindBugs - Free software static analyzer to look for bugs in Java code.
- Progpilot - Static security analysis tool for PHP code.
- RegEx-DoS - Analyzes source code for Regular Expressions susceptible to Denial of Service attacks.
- bandit - Security oriented static analyser for Python code.
- cppcheck - Extensible C/C++ static analyzer focused on finding bugs.
- sobelow - Security-focused static analysis for the Phoenix Framework.
- cwe_checker - Suite of tools built atop the Binary Analysis Platform (BAP) to heuristically detect CWEs in compiled binaries and firmware.

Steganography Tools

- Cloakify - Textual steganography toolkit that converts any filetype into lists of everyday

strings.

- StegOnline - Web-based, enhanced, and open-source port of StegSolve.
- StegCracker - Steganography brute-force utility to uncover hidden data inside files.

Vulnerability Databases

- Bugtraq (BID) - Software security bug identification database compiled from submissions to the SecurityFocus mailing list and other sources, operated by Symantec, Inc.
- CXSecurity - Archive of published CVE and Bugtraq software vulnerabilities cross-referenced with a Google dork database for discovering the listed vulnerability.
- China National Vulnerability Database (CNNVD) - Chinese government-run vulnerability database analoguous to the United States's CVE database hosted by Mitre Corporation.
- Common Vulnerabilities and Exposures (CVE) - Dictionary of common names (i.e., CVE Identifiers) for publicly known security vulnerabilities.
- Exploit-DB - Non-profit project hosting exploits for software vulnerabilities, provided as a public service by Offensive Security.
- Full-Disclosure - Public, vendor-neutral forum for detailed discussion of vulnerabilities, often publishes details before many other sources.
- GitHub Advisories - Public vulnerability advisories published by or affecting codebases hosted by GitHub, including open source projects.
- HPI-VDB - Aggregator of cross-referenced software vulnerabilities offering free-of-charge API access, provided by the Hasso-Plattner Institute, Potsdam.
- Inj3ct0r - Exploit marketplace and vulnerability information aggregator. (Onion service.)
- Microsoft Security Advisories and Bulletins - Archive and announcements of security advisories impacting Microsoft software, published by the Microsoft Security Response Center (MSRC).
- Mozilla Foundation Security Advisories - Archive of security advisories impacting Mozilla software, including the Firefox Web Browser.
- 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.
- Open Source Vulnerabilities (OSV) - Database of vulnerabilities affecting open source software, queryable by project, Git commit, or version.
- Packet Storm - Compendium of exploits, advisories, tools, and other security-related resources aggregated from across the industry.
- SecuriTeam - Independent source of software vulnerability information.
- Snyk Vulnerability DB - Detailed information and remediation guidance for vulnerabilities

known by Snyk.

- 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).
- VulDB - Independent vulnerability database with user community, exploit details, and additional meta data (e.g. CPE, CVSS, CWE)
- Vulnerability Lab - Open forum for security advisories organized by category of exploit target.
- Vulners - Security database of software vulnerabilities.
- Vulmon - Vulnerability search engine with vulnerability intelligence features that conducts full text searches in its database.
- Zero Day Initiative - Bug bounty program with publicly accessible archive of published security advisories, operated by TippingPoint.

Web Exploitation

- FuzzDB - Dictionary of attack patterns and primitives for black-box application fault injection and resource discovery.
- Offensive Web Testing Framework (OWTF) - Python-based framework for pentesting Web applications based on the OWASP Testing Guide.
- Raccoon - High performance offensive security tool for reconnaissance and vulnerability scanning.
- WPSploit - Exploit WordPress-powered websites with Metasploit.
- autochrome - Chrome browser profile preconfigured with appropriate settings needed for web application testing.
- badtouch - Scriptable network authentication cracker.
- gobuster - Lean multipurpose brute force search/fuzzing tool for Web (and DNS) reconnaissance.
- sslstrip2 - SSLStrip version to defeat HSTS.
- sslstrip - Demonstration of the HTTPS stripping attacks.

Intercepting Web proxies

See also *Proxies and Machine-in-the-Middle (MITM) Tools*.

- Burp Suite - Integrated platform for performing security testing of web applications.
- Fiddler - Free cross-platform web debugging proxy with user-friendly companion tools.
- OWASP Zed Attack Proxy (ZAP) - Feature-rich, scriptable HTTP intercepting proxy and

fuzzer for penetration testing web applications.
- mitmproxy - Interactive TLS-capable intercepting HTTP proxy for penetration testers and software developers.

Web file inclusion tools

- Kadimus - LFI scan and exploit tool.
- LFISuite - Automatic LFI scanner and exploiter.
- fimap - Find, prepare, audit, exploit and even Google automatically for LFI/RFI bugs.
- liffy - LFI exploitation tool.

Web injection tools

- Commix - Automated all-in-one operating system command injection and exploitation tool.
- NoSQLmap - Automatic NoSQL injection and database takeover tool.
- SQLmap - Automatic SQL injection and database takeover tool.
- tplmap - Automatic server-side template injection and Web server takeover tool.

Web path discovery and bruteforcing tools

- DotDotPwn - Directory traversal fuzzer.
- dirsearch - Web path scanner.
- recursebuster - Content discovery tool to perform directory and file bruteforcing.

Web shells and C2 frameworks

- Browser Exploitation Framework (BeEF) - Command and control server for delivering exploits to commandeered Web browsers.
- DAws - Advanced Web shell.
- Merlin - Cross-platform post-exploitation HTTP/2 Command and Control server and agent written in Golang.
- PhpSploit - Full-featured C2 framework which silently persists on webserver via evil PHP oneliner.
- SharPyShell - Tiny and obfuscated ASP.NET webshell for C# web applications.
- weevely3 - Weaponized PHP-based web shell.

Web-accessible source code ripping tools

- DVCS Ripper - Rip web accessible (distributed) version control systems: SVN/GIT/HG/BZR.

- GitTools - Automatically find and download Web-accessible `.git` repositories.
- git-dumper - Tool to dump a git repository from a website.
- git-scanner - Tool for bug hunting or pentesting websites that have open `.git` repositories available in public.

Web Exploitation Books

- The Browser Hacker's Handbook by Wade Alcorn et al., 2014
- The Web Application Hacker's Handbook by D. Stuttard, M. Pinto, 2011

Windows Utilities

- Bloodhound - Graphical Active Directory trust relationship explorer.
- Commando VM - Automated installation of over 140 Windows software packages for penetration testing and red teaming.
- Covenant - ASP.NET Core application that serves as a collaborative command and control platform for red teamers.
- ctftool - Interactive Collaborative Translation Framework (CTF) exploration tool capable of launching cross-session edit session attacks.
- DeathStar - Python script that uses Empire's RESTful API to automate gaining Domain Admin rights in Active Directory environments.
- Empire - Pure PowerShell post-exploitation agent.
- Fibratus - Tool for exploration and tracing of the Windows kernel.
- Inveigh - Windows PowerShell ADIDNS/LLMNR/mDNS/NBNS spoofer/machine-in-the-middle tool.
- LaZagne - Credentials recovery project.
- MailSniper - Modular tool for searching through email in a Microsoft Exchange environment, gathering the Global Address List from Outlook Web Access (OWA) and Exchange Web Services (EWS), and more.
- PowerSploit - PowerShell Post-Exploitation Framework.
- RID_ENUM - Python script that can enumerate all users from a Windows Domain Controller and crack those user's passwords using brute-force.
- Responder - Link-Local Multicast Name Resolution (LLMNR), NBT-NS, and mDNS poisoner.
- Rubeus - Toolset for raw Kerberos interaction and abuses.
- Ruler - Abuses client-side Outlook features to gain a remote shell on a Microsoft Exchange server.
- SCOMDecrypt - Retrieve and decrypt RunAs credentials stored within Microsoft System

Center Operations Manager (SCOM) databases.

- Sysinternals Suite - The Sysinternals Troubleshooting Utilities.
- Windows Credentials Editor - Inspect logon sessions and add, change, list, and delete associated credentials, including Kerberos tickets.
- Windows Exploit Suggester - Detects potential missing patches on the target.
- mimikatz - Credentials extraction tool for Windows operating system.
- redsnarf - Post-exploitation tool for retrieving password hashes and credentials from Windows workstations, servers, and domain controllers.
- wePWNise - Generates architecture independent VBA code to be used in Office documents or templates and automates bypassing application control and exploit mitigation software.
- WinPwn - Internal penetration test script to perform local and domain reconnaissance, privilege escalation and exploitation.

License