Cybersecurity Tools And Websites

Tools

GitHub - cyberguideme/Tools: Cyber Security Tools
Cyber Security Tools. Contribute to cyberguideme/Tools development by creating an account on GitHub.
https://github.com/cyberguideme/Tools

Cyber Security Tools

SecTools.Org: Top 125 Network Security Tools

- List of SecTools.Org: Top 125 Network Security Tools - For more than a decade, the Nmap Project has been cataloguing the network security community's favorite tools.

Kali Tools

- Kali Tool List - Kali Linux Tools Listing.

Multi-paradigm Frameworks

- Metasploit - Software 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.
- 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.

Network Vulnerability Scanners

- 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.
- Nessus - Commercial vulnerability management, configuration, and compliance assessment platform, sold by Tenable.
- OpenVAS - Free software implementation of the popular Nessus vulnerability assessment system.

created with craft

- 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.
- Progpilot - Static security analysis tool for PHP code.
- RegEx-DoS - Analyzes source code for Regular Expressions susceptible to Denial of Service attacks.

Web Vulnerability Scanners

- Netsparker Application Security Scanner - Application security scanner to automatically find security flaws.
- Nikto - Noisy but fast black box web server and web application vulnerability scanner.
- Arachni - Scriptable framework for evaluating the security of web applications.
- w3af - 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 - 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 - Joomla vulnerability scanner.
- ACSTIS - Automated client-side template injection (sandbox escape/bypass) detection for AngularJS.
- SQLmate - A friend of sqlmap that identifies sqli vulnerabilities based on a given dork and website (optional).
- JCS - Joomla Vulnerability Component Scanner with automatic database updater from exploitdb and packetstorm.

Network Tools

- pig - GNU/Linux packet crafting tool.
- Network-Tools.com - Website offering an interface to numerous basic network utilities like `ping`, `traceroute`, `whois`, and more.
- Intercepter-NG - Multifunctional network toolkit.
- SPARTA - Graphical interface offering scriptable, configurable access to existing network infrastructure scanning and enumeration tools.
- Zarp - Network attack tool centered around the exploitation of local networks.

created with craft

- dsniff - Collection of tools for network auditing and pentesting.
- scapy - Python-based interactive packet manipulation program & library.
- 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.
- 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.
- CrackMapExec - Swiss army knife for pentesting networks.
- impacket - Collection of Python classes for working with network protocols.
- dnstwist - Domain name permutation engine for detecting typo squatting, phishing and corporate espionage.
- 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.
- IKEForce - Command line IPSEC VPN brute forcing tool for Linux that allows group name/ID enumeration and XAUTH brute forcing capabilities.
- hping3 - Network tool able to send custom TCP/IP packets.
- rshijack - TCP connection hijacker, Rust rewrite of `shijack`.
- NetworkMiner - A Network Forensic Analysis Tool (NFAT).
- Paros - A Java-based HTTP/HTTPS proxy for assessing web application vulnerability.
- mitmsocks4j - Man-in-the-middle SOCKS Proxy for Java.
- Charles Proxy - A cross-platform GUI web debugging proxy to view intercepted HTTP and HTTPS/SSL live traffic.
- Habu - Python Network Hacking Toolkit.
- Wifi Jammer - Free program to jam all wifi clients in range.
- Firesheep - Free program for HTTP session hijacking attacks.

Forensic

- Autopsy - A digital forensics platform and graphical interface to The Sleuth Kit and other digital forensics tools
- sleuthkit - A library and collection of command-line digital forensics tools
- EnCase - The shared technology within a suite of digital investigations products by Guidance Software
- malzilla - Malware hunting tool
- PEview - A quick and easy way to view the structure and content of 32-bit Portable Executable (PE) and Component Object File Format (COFF) files
- HxD - A hex editor which, additionally to raw disk editing and modifying of main memory (RAM), handles files of any size
- WinHex - A hexadecimal editor, helpful in the realm of computer forensics, data recovery, low-level data processing, and IT security

created with craft

- BinText - A small, very fast and powerful text extractor that will be of particular interest to programmers

Cryptography

- xortool - A tool to analyze multi-byte XOR cipher

Exfiltration Tools

- 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.
- tgcd - Simple Unix network utility to extend the accessibility of TCP/IP based network services beyond firewalls.
- Iodine - Tunnel IPv4 data through a DNS server; useful for exfiltration from networks where Internet access is firewalled, but DNS queries are allowed.

Network Reconnaissance 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.
- scanless - Utility for using websites to perform port scans on your behalf so as not to reveal your own IP.
- DNSDumpster - 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 - 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.
- 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 - TCP port scanner, spews SYN packets asynchronously, scanning entire Internet in under 5 minutes.
- smbmap - Handy SMB enumeration tool.
- XRay - Network (sub)domain discovery and reconnaissance automation tool.
- ACLight - Script for advanced discovery of sensitive Privileged Accounts - includes Shadow Admins.
- ScanCannon - Python 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.
- fierce - Python3 port of the original `fierce.pl` DNS reconnaissance tool for locating non-contiguous IP space.

created with craft

Protocol Analyzers and Sniffers

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

Proxies and MITM Tools

- dnschef - Highly configurable DNS proxy for pentesters.
- mitmproxy - Interactive TLS-capable intercepting HTTP proxy for penetration testers and software developers.
- Morpheus - Automated ettercap TCP/IP Hijacking tool.
- mallory - HTTP/HTTPS proxy over SSH.
- SSH MITM - Intercept SSH connections with a proxy; all plaintext passwords and sessions are logged to disk.
- evilgrade - Modular framework to take advantage of poor upgrade implementations by injecting fake updates.
- Ettercap - Comprehensive, mature suite for machine-in-the-middle attacks.
- BetterCAP - Modular, portable and easily extensible MITM framework.
- MITMf - Framework for Man-In-The-Middle attacks.
- Lambda-Proxy - Utility for testing SQL Injection vulnerabilities on AWS Lambda serverless functions.

Wireless Network Tools

- Aircrack-ng - Set of tools 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.
- Airgeddon - Multi-use bash script for Linux systems to audit wireless networks.
- Cowpatty - Brute-force dictionary attack against WPA-PSK.
- BoopSuite - Suite of tools written in Python for wireless auditing.
- Bully - Implementation of the WPS brute force attack, written in C.
- infernal-twin - Automated wireless hacking tool.
- krackattacks-scripts - WPA2 Krack attack scripts.
- KRACK Detector - Detect and prevent KRACK attacks in your network.

created with craft

- wifi-arsenal - Resources for Wi-Fi Pentesting.
- WiFi-Pumpkin - Framework for rogue Wi-Fi access point attack.

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.
- crackpkcs12 - Multithreaded program to crack PKCS#12 files (`.p12` and `.pfx` extensions), such as TLS/SSL certificates.

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 - 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 tool.
- 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.

created with craft

- GitTools - Automatically find and download Web-accessible `.git` repositories.
- sslstrip - 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.
- recursebuster - Content discovery tool to perform directory and file bruteforcing.
- Raccoon - High performance offensive security tool for reconnaissance and vulnerability scanning.
- WhatWaf - Detect and bypass web application firewalls and protection systems.
- badtouch - Scriptable network authentication cracker.

Hex Editors

- HexEdit.js - Browser-based hex editing.
- Hexinator - World's finest (proprietary, commercial) Hex Editor.
- Frhed - Binary file editor for Windows.
- 0xED - Native macOS hex editor that supports plug-ins to display custom data types.
- Hex Fiend - Fast, open source, hex editor for macOS with support for viewing binary diffs.
- Bless - High quality, full featured, cross-platform graphical hex editor written in Gtk#.
- wxHexEditor - Free GUI hex editor for GNU/Linux, macOS, and Windows.
- `hexedit` - Simple, fast, console-based hex editor.

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.

Anti-virus 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").

created with craft

- 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.
- Shellter - Dynamic shellcode injection tool, and the first truly dynamic PE infector ever created.

Hash Cracking Tools

- John the Ripper - Fast password cracker.
- Hashcat - 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`).
- StegCracker - Steganography brute-force utility to uncover hidden data inside files.

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 - Link-Local Multicast Name Resolution (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.
- RID_ENUM - Python script that can enumerate all users from a Windows Domain Controller and crack those user's passwords using brute-force.

created with craft

- 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.
- 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.
- LaZagne - Credentials recovery project.
- 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.

GNU/Linux Utilities

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

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.

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.
- Memcrashed - DDoS attack tool for sending forged UDP packets to vulnerable Memcached servers obtained using Shodan API.

Social Engineering Tools

created with craft

- 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 - 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.
- Evilginx2 - Standalone man-in-the-middle attack framework.
- wifiphisher - Automated phishing attacks against WiFi networks.
- Catphish - Tool for phishing and corporate espionage written in Ruby.
- Beelogger - Tool for generating keylooger.
- FiercePhish - Full-fledged phishing framework to manage all phishing engagements.
- SocialFish - Social media phishing framework that can run on an Android phone or in a Docker container.
- ShellPhish - Social media site cloner and phishing tool built atop SocialFish.
- Gophish - Open-source phishing framework.
- phishery - TLS/SSL enabled Basic Auth credential harvester.
- ReelPhish - Real-time two-factor phishing tool.
- Modlishka - Flexible and powerful reverse proxy with real-time two-factor authentication.

OSINT Tools

- Maltego - Proprietary software for open source intelligence and forensics, from Paterva.
- theHarvester - E-mail, subdomain and people names harvester.
- SimplyEmail - Email recon made fast and easy.
- creepy - Geolocation OSINT tool.
- metagoofil - Metadata harvester.
- Google Hacking Database - Database of Google dorks; can be used for recon.
- 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 - Full-featured Web Reconnaissance framework written in Python.
- sn0int - Semi-automatic OSINT framework and package manager.
- github-dorks - CLI tool to scan GitHub repos/organizations for potential sensitive information leaks.
- 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.

created with craft

- Sn1per - Automated Pentest Recon Scanner.
- 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.
- PacketTotal - Simple, free, high-quality packet capture file analysis facilitating the quick detection of network-borne malware (using Bro and Suricata IDS signatures under the hood).
- 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.
- gOSINT - OSINT tool with multiple modules and a telegram scraper.
- OWASP Amass - Subdomain enumeration via scraping, web archives, brute forcing, permutations, reverse DNS sweeping, TLS certificates, passive DNS data sources, etc.
- Hunter.io - Data broker providing a Web search interface for discovering the email addresses and other organizational details of a company.
- FOCA (Fingerprinting Organizations with Collected Archives) - Automated document harvester that searches Google, Bing, and DuckDuckGo to find and extrapolate internal company organizational structures.
- dorks - Google hack database automation tool.
- image-match - Quickly search over billions of images.
- OSINT-SPY - Performs OSINT scan on email addresses, domain names, IP addresses, or organizations.
- pagodo - Automate Google Hacking Database scraping.
- surfraw - Fast UNIX command line interface to a variety of popular WWW search engines.
- GyoiThon - GyoiThon is an Intelligence Gathering tool using Machine Learning.

Anonymity Tools

- Tor - Free software and onion routed overlay network that helps you defend against traffic analysis.
- OnionScan - Tool 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.
- dos-over-tor - Proof of concept denial of service over Tor stress test tool.
- oregano - Python module that runs as a machine-in-the-middle (MITM) accepting Tor client requests.

created with craft

- kalitorify - Transparent proxy through Tor for Kali Linux OS.

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 - Tool 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.
- boxxy - Linkable sandbox explorer.
- 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.

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.

created with craft

- PCILeech - Uses PCIe hardware devices to read and write from the target system memory via Direct Memory Access (DMA) over PCIe.
- 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.
- Packet Squirrel - Ethernet multi-tool designed to enable covert remote access, painless packet captures, and secure VPN connections with the flip of a switch.

Industrial Control and SCADA Systems

- 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.

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.
- shellpop - Easily generate sophisticated reverse or bind shell commands to help you save time during penetration tests.

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.

More Tools

- Target Scanner - Target Scanner is a penetration testing utility that quickly automates common tasks when assessing a target.
- exploit-db-search - Exploitdb Search.
- punk.py - unix SSH post-exploitation 1337 tool.

created with craft

- tulpar - Web Vulnerability Scanner.
- dcrawl - Simple, but smart, multi-threaded web crawler for randomly gathering huge lists of unique domain names.
- V3n0m Scanner - Popular Pentesting scanner in Python3.6 for SQLi/XSS/LFI/RFI and other Vulns.
- golismero - The Web Knife.
- sqliv - Massive SQL injection vulnerability scanner.
- gitminer - Tool for advanced mining for content on Github.
- Cr3d0v3r - Know the dangers of credential reuse attacks.
- Striker - Striker is an offensive information and vulnerability scanner.
- emailHarvester - Email addresses harvester.
- BruteX - Automatically brute force all services running on a target.
- BlackWidow - A Python based web application scanner to gather OSINT and fuzz for OWASP vulnerabilities on a target website.
- Shiva - Improved DOS exploit for wordpress websites (CVE-2018-6389).
- ctfr - Domain enumeration, it just abuses of Certificate Transparency logs.
- twa - A **t**iny **w**eb **a**uditor with strong opinions.
- Photon - Incredibly fast crawler designed for OSINT.
- CMSeek - CMS Detection and Exploitation suite - Scan WordPress, Joomla, Drupal and 130 other CMSs.
- HashBuster - Crack hashes in seconds.
- Invoke-Apex - PowerShell-based toolkit consisting of a collection of techniques and tradecraft for use in red team, post-exploitation, adversary simulation, or other offensive security tasks.
- RapidScan - The Multi-Tool Web Vulnerability Scanner.
- Freedom Fighting Mode (FFM) - FFM is a hacking harness that you can use during the post-exploitation phase of a red-teaming engagement.
- vault - Swiss army knife for hackers.
- badkarma - badKarma is an open source GUI based network reconnaissance toolkit which aims to assist penetration testers during network infrastructure assessments..
- EaST - «Exploits And Security Tools» penetration testing framework.
- Vanquish - Vanquish is a Kali Linux based Enumeration Orchestrator built in Python. Vanquish leverages the opensource enumeration tools on Kali to perform multiple active information gathering phases.
- Reconnoitre - A security tool for multithreaded information gathering and service enumeration whilst building directory structures to store results, along with writing out recommendations for further testing.
- nudge4j - Java tool to let the browser talk to the JVM.
- dex2jar - Tools to work with Android .dex and Java .class files.
- JD-GUI - A standalone graphical utility that displays Java source codes of ".class" files.
- procyon - A modern open-source Java decompiler.
- androguard - Reverse engineering, malware and goodware analysis of Android applications.

created with craft

- JAD - JAD Java Decompiler (closed-source, unmaintained).
- dotPeek - a free-of-charge .NET decompiler from JetBrains.
- ILSpy - an open-source .NET assembly browser and decompiler.
- de4dot - .NET deobfuscator and unpacker.
- antinet - .NET anti-managed debugger and anti-profiler code.
- UPX - the Ultimate Packer for eXecutables.
- radare2 - A portable reversing framework.
- Hopper - A OS X and Linux Disassembler/Decompiler for 32/64-bit Windows/Mac/Linux/iOS executables.
- ScratchABit - Easily retargetable and hackable interactive disassembler with IDAPython-compatible plugin API.

GitHub - SpectralOps/netz: Discover internet-wide misconfigurations while drinking coffee
Discover internet-wide misconfigurations while drinking coffee - GitHub - SpectralOps/netz: Discover internet-wide mi...
https://github.com/spectralops/netz

GitHub - yeti-platform/yeti: Your Everyday Threat Intelligence
Your Everyday Threat Intelligence. Contribute to yeti-platform/yeti development by creating an account on GitHub.
https://github.com/yeti-platform/yeti

GitHub - hakluke/hakrawler: Simple, fast web crawler designed for easy, quick discovery of
Simple, fast web crawler designed for easy, quick discovery of endpoints and assets within a web application - GitHub...
https://github.com/hakluke/hakrawler

GitHub - caffix/amass: In-depth Attack Surface Mapping and Asset Discovery
In-depth Attack Surface Mapping and Asset Discovery - GitHub - caffix/amass: In-depth Attack Surface Mapping and...
https://github.com/caffix/amass

GitHub - chris408/ct-exposer: An OSINT tool that discovers sub-domains by searching
An OSINT tool that discovers sub-domains by searching Certificate Transparency logs - GitHub - chris408/ct-exposer...
https://github.com/chris408/ct-exposer

GitHub - thehappydinoa/awesome-censys-queries: A collection of fascinating and bizarre
A collection of fascinating and bizarre Censys Search Queries - GitHub - thehappydinoa/awesome-censys-queries: A...
https://github.com/thehappydinoa/awesome-censys-queries

GitHub - evilsocket/xray: XRay is a tool for recon, mapping and OSINT gathering from
XRay is a tool for recon, mapping and OSINT gathering from public networks. - GitHub - evilsocket/xray: XRay is a tool...
https://github.com/evilsocket/xray

GitHub - michenriksen/aquatone: A Tool for Domain Flyovers
A Tool for Domain Flyovers. Contribute to michenriksen/aquatone development by creating an account on GitHub.
https://github.com/michenriksen/aquatone#installation

metasploit-payloads/README.md at master · rapid7/metasploit-payloads
Unified repository for different Metasploit Framework payloads - metasploit-payloads/README.md at master · rapid7/...
https://github.com/rapid7/metasploit-payloads/blob/master/README.md

created with craft

Amass/tutorial.md at master · OWASP/Amass
In-depth Attack Surface Mapping and Asset Discovery - Amass/tutorial.md at master · OWASP/Amass
https://github.com/OWASP/Amass/blob/master/doc/tutorial.md

GitHub - blechschmidt/massdns: A high-performance DNS stub resolver for bulk lookups
A high-performance DNS stub resolver for bulk lookups and reconnaissance (subdomain enumeration) - GitHub - blec...
https://github.com/blechschmidt/massdns

GitHub - robertdavidgraham/masscan: TCP port scanner, spews SYN packets
TCP port scanner, spews SYN packets asynchronously, scanning entire Internet in under 5 minutes. - GitHub - robertd...
https://github.com/robertdavidgraham/masscan

Download to get list of tools from sans.org

Free_Faculty_Tools_2.pdf
PDF Document
1006.0 KB

Awesome AWS S3 Security

Collection of tools, techniques and useful links concerning security and exposed AWS S3 Buckets

Tools

- Grayhat Warfare - A free tool that lists open s3 buckets and helps you search for interesting files
- Slurp - Evaluate the security of S3 buckets
- AWSBucketDump - AWSBucketDump is a tool to quickly enumerate AWS S3 buckets to look for loot
- S3Scanner - Scan for open AWS S3 buckets and dump the contents - By sa7mon
- s3enum - Fast Amazon S3 bucket enumeration tool for pentesters
- s3-buckets-finder - PHP tool to brute force Amazon S3 bucket - By gwen001
- s3-buckets-finder - PHP tool to brute force Amazon S3 bucket - By gold1029
- Sandcastle - a Python script for AWS S3 bucket enumeration, formerly known as bucketCrawler
- mubrute - The tool uses the response code returned by s3.amazonaws.com to determine if a bucket exists and its list permissions
- PyLazyS3 - Enumerate AWS S3 buckets using different permutations
- RoboBucketeer - Robot Framework Library for Buckteer - S3 Buckets & Subdomain Enumeration
- s3-inspector - Tool to check AWS S3 bucket permissions
- inSp3ctor - AWS S3 Bucket/Object Finder
- bucketkicker - A tool to quickly enumerate AWS S3 buckets verify whether or not they exist and to look for loot
- s3recon - Amazon S3 bucket finder and crawler

created with craft

- s3finder - Can search using a wordlist or by monitoring the certstream network for domain names from certificate transparency logs
- kicks3 - S3 bucket finder from html,js and bucket misconfiguration testing tool
- bucket_finder - DigiNinja's bucket_finder utility - By mattweidner
- Bucket_Finder - Leaky Buckets - By hazana
- haka_toni_bucket_finder - Yet another S3 Bucket finder (*No official description provided*)
- s3-open-bucket-finder - Yet another S3 Bucket finder (*No official description provided*)
- s3scanner - Scan for open public S3 buckets - By miguelmota
- bucket-scraper - Command-line application for scraping, indexing and downloading of Amazon S3 buckets
- bucket-hunter - Amazon AWS Exposed Bucket Hunter - Security research
- bucket-stream - Find interesting Amazon S3 Buckets by watching certificate transparency logs
- goGetBucket - A penetration testing tool to enumerate and analyse Amazon S3 Buckets owned by a domain
- bucket_finder - Trawl Amazon S3 buckets for interesting files

General Purpose Tools

- CloudScraper - CloudScraper: Tool to enumerate targets in search of cloud resources. S3 Buckets, Azure Blobs, Digital Ocean Storage Space
- CloudStorageFinder - A collection of tools to find data that has been made public in cloud storage systems such as S3 Buckets and Digital Ocean Spaces
- exif-scraper - Grab photos from an S3 bucket and store their EXIF data in a database
- mlb-dfs-scrapers - Web scraping library for dumping MLB stats in S3 bucket csv files

Techniques

- enum_wayback - Metasploit module that pulls and parses the URLs stored by Archive.org for the purpose of replaying during a web assessment. Finding unlinked and old pages.

camo.githubusercontent.com
https://camo.githubusercontent.com/500fd7e68db2af2d7638c4f5d01b73e0e5e95ee61819f9c203c8784d665034e2/6874...

created with craft

```
msf5 > use auxiliary/scanner/http/enum_wayback
msf5 auxiliary(scanner/http/enum_wayback) > set domain s3.amazonaws.com
domain => s3.amazonaws.com
msf5 auxiliary(scanner/http/enum_wayback) > set outfile buckets
outfile => buckets
msf5 auxiliary(scanner/http/enum_wayback) > run

[*] Pulling urls from Archive.org
[*] Located 254782 addresses for s3.amazonaws.com
[*] Writing URLs list to buckets...
[*] OUTFILE did not exist, creating..
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/enum_wayback) >
```

Red Team Tools Operations:

- Reconnaissance
- Weaponization
- Delivery
- Command and Control
- Lateral Movement
- Establish Foothold
- Escalate Privileges
- Data Exfiltration
- Misc
- References

Best Red Team Tools 2023

Reconnaissance

Active Intelligence Gathering

- **EyeWitness** is designed to take screenshots of websites, provide some server header info, and identify default credentials if possible.
- **AWSBucketDump** is a tool to quickly enumerate AWS S3 buckets to look for loot.
- **AQUATONE** is a set of tools for performing reconnaissance on domain names.
- **spoofcheck** a program that checks if a domain can be spoofed. The program checks SPF and DMARC records for weak configurations that allow spoofing.

created with craft

- **Nmap** is used to discover hosts and services on a computer network, thus building a “map” of the network.
- **dnsrecon** a tool DNS Enumeration Script.
- **dirsearch** is a simple command line tool designed to brute force directories and files in websites.
- **Sn1per** automated pentest recon scanner.

Passive Intelligence Gathering

- **Social Mapper** OSINT Social Media Mapping Tool, takes a list of names & images (or LinkedIn company name) and performs automated target searching on a huge scale across multiple social media sites. Not restricted by APIs as it instruments a browser using Selenium. Outputs reports to aid in correlating targets across sites.
- **skiptracer** OSINT scraping framework, utilizes some basic python webscraping (BeautifulSoup) of PII paywall sites to compile passive information on a target on a ramen noodle budget.
- **FOCA** (Fingerprinting Organizations with Collected Archives) is a tool used mainly to find metadata and hidden information in the documents its scans.
- **theHarvester** is a tool for gathering subdomain names, e-mail addresses, virtual hosts, open ports/ banners, and employee names from different public sources.
- **Metagoofil** is a tool for extracting metadata of public documents (pdf,doc,xls,ppt,etc) availables in the target websites.
- **SimplyEmail** Email recon made fast and easy, with a framework to build on.
- **truffleHog** searches through git repositories for secrets, digging deep into commit history and branches.
- **Just-Metadata** is a tool that gathers and analyzes metadata about IP addresses. It attempts to find relationships between systems within a large dataset.
- **typofinder** a finder of domain typos showing country of IP address.
- **pwnedOrNot** is a python script which checks if the email account has been compromised in a data breach, if the email account is compromised it proceeds to find passwords for the compromised account.
- **GitHarvester** This tool is used for harvesting information from GitHub like google dork.
- **pwndb** is a python command-line tool for searching leaked credentials using the Onion service with the same name.
- **LinkedInt** LinkedIn Recon Tool.
- **CrossLinked** LinkedIn enumeration tool to extract valid employee names from an organization through search engine scraping.
- **findomain** is a fast domain enumeration tool that uses Certificate Transparency logs and a selection of APIs. h

Frameworks

- **Maltego** is a unique platform developed to deliver a clear threat picture to the environment that an organization owns and operates.

created with craft

- **SpiderFoot** the open source footprinting and intelligence-gathering tool.
- **datasploit** is an OSINT Framework to perform various recon techniques on Companies, People, Phone Number, Bitcoin Addresses, etc., aggregate all the raw data, and give data in multiple formats.
- **Recon-ng** is a full-featured Web Reconnaissance framework written in Python.

Weaponization

- **WinRAR Remote Code Execution** Proof of Concept exploit for CVE-2018-20250.
- **Composite Moniker** Proof of Concept exploit for CVE-2017-8570.
- **Exploit toolkit CVE-2017-8759** is a handy python script which provides pentesters and security researchers a quick and effective way to test Microsoft .NET Framework RCE.
- **CVE-2017-11882 Exploit** accepts over 17k bytes long command/code in maximum.
- **Adobe Flash Exploit** CVE-2018-4878.
- **Exploit toolkit CVE-2017-0199** is a handy python script which provides pentesters and security researchers a quick and effective way to test Microsoft Office RCE.
- **demiguise** is a HTA encryption tool for RedTeams.
- **Office-DDE-Payloads** collection of scripts and templates to generate Office documents embedded with the DDE, macro-less command execution technique.
- **CACTUSTORCH** Payload Generation for Adversary Simulations.
- **SharpShooter** is a payload creation framework for the retrieval and execution of arbitrary CSharp source code.
- **Don't kill my cat** is a tool that generates obfuscated shellcode that is stored inside of polyglot images. The image is 100% valid and also 100% valid shellcode.
- **Malicious Macro Generator Utility** Simple utility design to generate obfuscated macro that also include a AV / Sandboxes escape mechanism.
- **SCT Obfuscator** Cobalt Strike SCT payload obfuscator.
- **Invoke-Obfuscation** PowerShell Obfuscator.
- **Invoke-CradleCrafter** PowerShell remote download cradle generator and obfuscator.
- **Invoke-DOSfuscation** cmd.exe Command Obfuscation Generator & Detection Test Harness.
- **morphHTA** Morphing Cobalt Strike's evil.HTA.
- **Unicorn** is a simple tool for using a PowerShell downgrade attack and inject shellcode straight into memory.
- **Shellter** is a dynamic shellcode injection tool, and the first truly dynamic PE infector ever created.
- **EmbedInHTML** Embed and hide any file in an HTML file.
- **SigThief** Stealing Signatures and Making One Invalid Signature at a Time.
- **Veil** is a tool designed to generate metasploit payloads that bypass common anti-virus solutions.

created with craft

- **CheckPlease** Sandbox evasion modules written in PowerShell, Python, Go, Ruby, C, C#, Perl, and Rust.
- **Invoke-PSImage** is a tool to embeded a PowerShell script in the pixels of a PNG file and generates a oneliner to execute.
- **LuckyStrike** a PowerShell based utility for the creation of malicious Office macro documents. To be used for pentesting or educational purposes only.
- **ClickOnceGenerator** Quick Malicious ClickOnceGenerator for Red Team. The default application a simple WebBrowser widget that point to a website of your choice.
- **macro_pack** is a tool by @EmericNasi used to automatize obfuscation and generation of MS Office documents, VB scripts, and other formats for pentest, demo, and social engineering assessments.
- **StarFighters** a JavaScript and VBScript Based Empire Launcher.
- **nps_payload** this script will generate payloads for basic intrusion detection avoidance. It utilizes publicly demonstrated techniques from several different sources.
- **SocialEngineeringPayloads** a collection of social engineering tricks and payloads being used for credential theft and spear phishing attacks.
- **The Social-Engineer Toolkit** is an open-source penetration testing framework designed for social engineering.
- **Phishery** is a Simple SSL Enabled HTTP server with the primary purpose of phishing credentials via Basic Authentication.
- **PowerShdll** run PowerShell with rundll32. Bypass software restrictions.
- **Ultimate AppLocker ByPass List** The goal of this repository is to document the most common techniques to bypass AppLocker.
- **Ruler** is a tool that allows you to interact with Exchange servers remotely, through either the MAPI/HTTP or RPC/HTTP protocol.
- **Generate-Macro** is a standalone PowerShell script that will generate a malicious Microsoft Office document with a specified payload and persistence method.
- **Malicious Macro MSBuild Generator** Generates Malicious Macro and Execute Powershell or Shellcode via MSBuild Application Whitelisting Bypass.
- **Meta Twin** is designed as a file resource cloner. Metadata, including digital signature, is extracted from one file and injected into another.
- **WePWNise** generates architecture-independent VBA code to be used in Office documents or templates and automates bypassing application control and exploit mitigation software.
- **DotNetToJScript** a tool to create a JScript file which loads a .NET v2 assembly from memory.
- **PSAmsi** is a tool for auditing and defeating AMSI signatures.
- **Reflective DLL injection** is a library injection technique in which the concept of reflective programming is employed to perform the loading of a library from memory into a host process.
- **ps1encode** use to generate and encode a powershell based metasploit payloads.
- **Worse PDF** turn a normal PDF file into malicious. Use to steal Net-NTLM Hashes from windows machines.

created with craft

- **SpookFlare** has a different perspective to bypass security measures and it gives you the opportunity to bypass the endpoint countermeasures at the client-side detection and network-side detection.
- **GreatSCT** is an open source project to generate application white list bypasses. This tool is intended for BOTH red and blue team.
- **nps** running powershell without PowerShell.
- **Meterpreter_Paranoid_Mode.sh** allows users to secure their staged/stageless connection for Meterpreter by having it check the certificate of the handler it is connecting to.
- **The Backdoor Factory (BDF)** is to patch executable binaries with user desired shellcode and continue normal execution of the prepatched state.
- **MacroShop** a collection of scripts to aid in delivering payloads via Office Macros.
- **UnmanagedPowerShell** Executes PowerShell from an unmanaged process.
- **evil-ssdp** Spoof SSDP replies to phish for NTLM hashes on a network. Creates a fake UPNP device, tricking users into visiting a malicious phishing page.
- **Ebowla** Framework for Making Environmental Keyed Payloads.
- **make-pdf-embedded** a tool to create a PDF document with an embedded file.
- **avet** (AntiVirusEvasionTool) is targeting windows machines with executable files using different evasion techniques.
- **EvilClippy** A cross-platform assistant for creating malicious MS Office documents. Can hide VBA macros, stomp VBA code (via P-Code) and confuse macro analysis tools. Runs on Linux, OSX and Windows.
- **CallObfuscator** Obfuscate windows apis from static analysis tools and debuggers.
- **Donut** is a shellcode generation tool that creates position-independant shellcode payloads from .NET Assemblies. This shellcode may be used to inject the Assembly into arbitrary Windows processes.

Red Team Tools – Delivery

Phishing

- **King Phisher** is a tool for testing and promoting user awareness by simulating real-world phishing attacks.
- **FiercePhish** is a full-fledged phishing framework to manage all phishing engagements. It allows you to track separate phishing campaigns, schedule sending of emails, and much more.
- **ReelPhish** is a Real-Time Two-Factor Phishing Tool.
- **Gophish** is an open-source phishing toolkit designed for businesses and penetration testers. It provides the ability to quickly and easily set up and execute phishing engagements and security awareness training.
- **CredSniper** is a phishing framework written with the Python micro-framework Flask and Jinja2 templating which supports capturing 2FA tokens.
- **PwnAuth** is a web application framework for launching and managing OAuth abuse campaigns.

created with craft

- **Phishing Frenzy** Ruby on Rails Phishing Framework.
- **Phishing Pretexts** are a library of pretexts to use on offensive phishing engagements.
- **Modlishka** is a flexible and powerful reverse proxy, that will take your ethical phishing campaigns to the next level.
- **Evilginx2** is a man-in-the-middle attack framework for phishing credentials and session cookies of any web service.

Watering Hole Attack

- **BeEF** is short for The Browser Exploitation Framework. It is a penetration testing tool that focuses on the web browser.

Command and Control

Remote Access Tools

- **Cobalt Strike** is software for Adversary Simulations and Red Team Operations.
- **Empire** is a post-exploitation framework that includes a pure-PowerShell2.0 Windows agent, and a pure Python 2.6/2.7 Linux/OS X agent.
- **Metasploit Framework** is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.
- **SILENTTRINITY** A post-exploitation agent powered by Python, IronPython, C#/.NET.
- **Pupy** is an opensource, cross-platform (Windows, Linux, OSX, Android) remote administration and post-exploitation tool mainly written in python.
- **Koadic** or COM Command & Control, is a Windows post-exploitation rootkit similar to other penetration testing tools such as Meterpreter and Powershell Empire.
- **PoshC2** is a proxy aware C2 framework written completely in PowerShell to aid penetration testers with red teaming, post-exploitation and lateral movement.
- **Merlin** is a cross-platform post-exploitation HTTP/2 Command & Control server and agent written in golang.
- **Quasar** is a fast and light-weight remote administration tool coded in C#. Providing high stability and an easy-to-use user interface, Quasar is the perfect remote administration solution for you.
- **Covenant** is a .NET command and control framework that aims to highlight the attack surface of .NET, make the use of offensive .NET tradecraft easier, and serve as a collaborative command and control platform for red teamers.
- **FactionC2** is a C2 framework which use websockets based API that allows for interacting with agents and transports.
- **DNScat2** is a tool is designed to create an encrypted command-and-control (C&C) channel over the DNS protocol.
- **Sliver** is a general purpose cross-platform implant framework that supports C2 over Mutual-TLS, HTTP(S), and DNS.

created with craft

- **EvilOSX** An evil RAT (Remote Administration Tool) for macOS / OS X.
- **EggShell** is a post exploitation surveillance tool written in Python. It gives you a command line session with extra functionality between you and a target machine.
- **Gcat** a stealthy Python based backdoor that uses Gmail as a command and control server.
- **TrevorC2** is a legitimate website (browsable) that tunnels client/server communications for covert command execution.

Staging

- **Rapid Attack Infrastructure (RAI)** Red Team Infrastructure... Quick... Fast... Simplified One of the most tedious phases of a Red Team Operation is usually the infrastructure setup. This usually entails a teamserver or controller, domains, redirectors, and a Phishing server.
- **Red Baron** is a set of modules and custom/third-party providers for Terraform which tries to automate creating resilient, disposable, secure and agile infrastructure for Red Teams.
- **EvilURL** generate unicode evil domains for IDN Homograph Attack and detect them.
- **Domain Hunter** checks expired domains, bluecoat categorization, and Archive.org history to determine good candidates for phishing and C2 domain names.
- **PowerDNS** is a simple proof of concept to demonstrate the execution of PowerShell script using DNS only.
- **Chameleon** a tool for evading Proxy categorisation.
- **CatMyFish** Search for categorized domain that can be used during red teaming engagement. Perfect to setup whitelisted domain for your Cobalt Strike beacon C&C.
- **Malleable C2** is a domain specific language to redefine indicators in Beacon's communication.
- **Malleable-C2-Randomizer** This script randomizes Cobalt Strike Malleable C2 profiles through the use of a metalanguage, hopefully reducing the chances of flagging signature-based detection controls.
- **FindFrontableDomains** search for potential frontable domains.
- **Postfix-Server-Setup** Setting up a phishing server is a very long and tedious process. It can take hours to setup, and can be compromised in minutes.
- **DomainFrontingLists** a list of Domain Frontable Domains by CDN.
- **Apache2-Mod-Rewrite-Setup** Quickly Implement Mod-Rewrite in your infastructure.
- **mod_rewrite rule** to evade vendor sandboxes.
- **external_c2 framework** a python framework for usage with Cobalt Strike's External C2.
- **Malleable-C2-Profiles** A collection of profiles used in different projects using Cobalt Strike
- **ExternalC2** a library for integrating communication channels with the Cobalt Strike External C2 server.
- **cs2modrewrite** a tools for convert Cobalt Strike profiles to modrewrite scripts.
- **e2modrewrite** a tools for convert Empire profiles to Apache modrewrite scripts.
- **redi** automated script for setting up CobaltStrike redirectors (nginx reverse proxy, letsencrypt).
- **cat-sites** Library of sites for categorization.

created with craft

- **ycsm** is a quick script installation for resilient redirector using nginx reverse proxy and letsencrypt compatible with some popular Post-Ex Tools (Cobalt Strike, Empire, Metasploit, PoshC2).
- **Domain Fronting Google App Engine**.
- **DomainFrontDiscover** Scripts and results for finding domain frontable CloudFront domains.
- **Automated Empire Infrastructure**
- **Serving Random Payloads** with NGINX.
- **meek** is a blocking-resistant pluggable transport for Tor. It encodes a data stream as a sequence of HTTPS requests and responses.
- **CobaltStrike-ToolKit** Some useful scripts for CobaltStrike.
- **mkhtaccess_red** Auto-generate an HTaccess for payload delivery — automatically pulls ips/nets/etc from known sandbox companies/sources that have been seen before, and redirects them to a benign payload.
- **RedFile** a flask wsgi application that serves files with intelligence, good for serving conditional RedTeam payloads.
- **keyserver** Easily serve HTTP and DNS keys for proper payload protection.
- **DoHC2** allows the ExternalC2 library from Ryan Hanson to be leveraged for command and control (C2) via DNS over HTTPS (DoH). This is built for the popular Adversary Simulation and Red Team Operations Software Cobalt Strike
- **HTran** is a connection bouncer, a kind of proxy server. A "listener" program is hacked stealthily onto an unsuspecting host anywhere on the Internet.

Lateral Movement

- **CrackMapExec** is a swiss army knife for pentesting networks.
- **PowerLessShell** rely on MSBuild.exe to remotely execute PowerShell scripts and commands without spawning powershell.exe.
- **GoFetch** is a tool to automatically exercise an attack plan generated by the BloodHound application.
- **ANGRYPUPPY** a bloodhound attack path automation in CobaltStrike.
- **DeathStar** is a Python script that uses Empire's RESTful API to automate gaining Domain Admin rights in Active Directory environments using a variety of techinques.
- **SharpHound** C# Rewrite of the BloodHound Ingestor.
- **BloodHound.py** is a Python based ingestor for BloodHound, based on Impacket.
- **Responder** is a LLMNR, NBT-NS and MDNS poisoner, with built-in HTTP/SMB/MSSQL/FTP/LDAP rogue authentication server supporting NTLMv1/NTLMv2/LMv2, Extended Security NTLMSSP and Basic HTTP authentication.
- **SessionGopher** is a PowerShell tool that uses WMI to extract saved session information for remote access tools such as WinSCP, PuTTY, SuperPuTTY, FileZilla, and Microsoft Remote Desktop. It can be run remotely or locally.
- **PowerSploit** is a collection of Microsoft PowerShell modules that can be used to aid penetration testers during all phases of an assessment.

created with craft

- **Nishang** is a framework and collection of scripts and payloads which enables usage of PowerShell for offensive security, penetration testing and red teaming. Nishang is useful during all phases of penetration testing.
- **Inveigh** is a Windows PowerShell LLMNR/mDNS/NBNS spoofer/man-in-the-middle tool.
- **PowerUpSQL** a PowerShell Toolkit for Attacking SQL Server.
- **MailSniper** is a penetration testing tool for searching through email in a Microsoft Exchange environment for specific terms (passwords, insider intel, network architecture information, etc.).
- **DomainPasswordSpray** is a tool written in PowerShell to perform a password spray attack against users of a domain.
- **WMIOps** is a powershell script that uses WMI to perform a variety of actions on hosts, local or remote, within a Windows environment. It's designed primarily for use on penetration tests or red team engagements.
- **Mimikatz** is an open-source utility that enables the viewing of credential information from the Windows lsass.
- **LaZagne** project is an open source application used to retrieve lots of passwords stored on a local computer.
- **mimipenguin** a tool to dump the login password from the current linux desktop user. Adapted from the idea behind the popular Windows tool mimikatz.
- **PsExec** is a light-weight telnet-replacement that lets you execute processes on other systems, complete with full interactivity for console applications, without having to manually install client software.
- **KeeThief** allows for the extraction of KeePass 2.X key material from memory, as well as the backdooring and enumeration of the KeePass trigger system.
- **PSAttack** combines some of the best projects in the infosec powershell community into a self contained custom PowerShell console.
- **Internal Monologue Attack** Retrieving NTLM Hashes without Touching LSASS.
- **Impacket** is a collection of Python classes for working with network protocols. Impacket is focused on providing low-level programmatic access to the packets and for some protocols (for instance NMB, SMB1-3 and MS-DCERPC) the protocol implementation itself.
- **icebreaker** gets plaintext Active Directory credentials if you're on the internal network but outside the AD environment.
- **Living Off The Land Binaries and Scripts (and now also Libraries)** The goal of these lists are to document every binary, script and library that can be used for other purposes than they are designed to.
- **WSUSpendu** for compromised WSUS server to extend the compromise to clients.
- **Evilgrade** is a modular framework that allows the user to take advantage of poor upgrade implementations by injecting fake updates.
- **NetRipper** is a post exploitation tool targeting Windows systems which uses API hooking in order to intercept network traffic and encryption related functions from a low privileged user, being able to capture both plain-text traffic and encrypted traffic before encryption/after decryption.
- **LethalHTA** Lateral Movement technique using DCOM and HTA.

created with craft

- **Invoke-PowerThIEf** an Internet Explorer Post Exploitation library.
- **RedSnarf** is a pen-testing / red-teaming tool for Windows environments.
- **HoneypotBuster** Microsoft PowerShell module designed for red teams that can be used to find honeypots and honeytokens in the network or at the host.
- **PAExec** lets you launch Windows programs on remote Windows computers without needing to install software on the remote computer first.

Establish Foothold

- **Tunna** is a set of tools which will wrap and tunnel any TCP communication over HTTP. It can be used to bypass network restrictions in fully firewalled environments.
- **reGeorg** the successor to reDuh, pwn a bastion webserver and create SOCKS proxies through the DMZ. Pivot and pwn.
- **Blade** is a webshell connection tool based on console, currently under development and aims to be a choice of replacement of Chooper.
- **TinyShell** Web Shell Framework.
- **PowerLurk** is a PowerShell toolset for building malicious WMI Event Subsriptions.
- **DAMP** The Discretionary ACL Modification Project: Persistence Through Host-based Security Descriptor Modification.

Domain Escalation

PowerView is a PowerShell tool to gain network situational awareness on Windows domains.

Get-GPPPassword Retrieves the plaintext password and other information for accounts pushed through Group Policy Preferences.

Invoke-ACLpwn is a tool that automates the discovery and pwnage of ACLs in Active Directory that are unsafe configured.

BloodHound uses graph theory to reveal the hidden and often unintended relationships within an Active Directory environment.

PyKEK (Python Kerberos Exploitation Kit), a python library to manipulate KRB5-related data.

Grouper a PowerShell script for helping to find vulnerable settings in AD Group Policy.

ADRecon is a tool which extracts various artifacts (as highlighted below) out of an AD environment in a specially formatted Microsoft Excel report that includes summary views with metrics to facilitate analysis.

ADACLScanner one script for ACL's in Active Directory.

ACLight a useful script for advanced discovery of Domain Privileged Accounts that could be targeted – including Shadow Admins.

LAPSToolkit a tool to audit and attack LAPS environments.

created with craft

PingCastle is a free, Windows-based utility to audit the risk level of your AD infrastructure and check for vulnerable practices.

RiskySPNs is a collection of PowerShell scripts focused on detecting and abusing accounts associated with SPNs (Service Principal Name).

Mystique is a PowerShell tool to play with Kerberos S4U extensions, this module can assist blue teams to identify risky Kerberos delegation configurations as well as red teams to impersonate arbitrary users by leveraging KCD with Protocol Transition.

Rubeus is a C# toolset for raw Kerberos interaction and abuses. It is heavily adapted from Benjamin Delpy's Kekeo project.

kekeo is a little toolbox I have started to manipulate Microsoft Kerberos in C (and for fun).

Local Escalation

UACMe is an open source assessment tool that contains many methods for bypassing Windows User Account Control on multiple versions of the operating system.

windows-kernel-exploits a collection windows kernel exploit.

PowerUp aims to be a clearinghouse of common Windows privilege escalation vectors that rely on misconfigurations.

The Elevate Kit demonstrates how to use third-party privilege escalation attacks with Cobalt Strike's Beacon payload.

Sherlock a powerShell script to quickly find missing software patches for local privilege escalation vulnerabilities.

Tokenvator a tool to elevate privilege with Windows Tokens.

Red Team Tools – Data Exfiltration

CloakifyFactory & the Cloakify Toolset – Data Exfiltration & Infiltration In Plain Sight; Evade DLP/MLS Devices; Social Engineering of Analysts; Defeat Data Whitelisting Controls; Evade AV Detection.

DET (is provided AS IS), is a proof of concept to perform Data Exfiltration using either single or multiple channel(s) at the same time.

DNSExfiltrator allows for transfering (exfiltrate) a file over a DNS request covert channel. This is basically a data leak testing tool allowing to exfiltrate data over a covert channel.

PyExfil a Python Package for Data Exfiltration.

Egress-Assess is a tool used to test egress data detection capabilities.

Powershell RAT python based backdoor that uses Gmail to exfiltrate data as an e-mail attachment.

Misc

Adversary Emulation

created with craft

MITRE CALDERA – An automated adversary emulation system that performs post-compromise adversarial behavior within Windows Enterprise networks.

APTSimulator – A Windows Batch script that uses a set of tools and output files to make a system look as if it was compromised.

Atomic Red Team – Small and highly portable detection tests mapped to the Mitre ATT&CK Framework.

Network Flight Simulator – flightsim is a lightweight utility used to generate malicious network traffic and help security teams to evaluate security controls and network visibility.

Metta – A security preparedness tool to do adversarial simulation.

Red Team Automation (RTA) – RTA provides a framework of scripts designed to allow blue teams to test their detection capabilities against malicious tradecraft, modeled after MITRE ATT&CK.

Wireless Networks

Wifiphisher is a security tool that performs Wi-Fi automatic association attacks to force wireless clients to unknowingly connect to an attacker-controlled Access Point.

mana toolkit for wifi rogue AP attacks and MitM.

Embedded & Peripheral Devices Hacking

magspoof a portable device that can spoof/emulate any magnetic stripe, credit card or hotel card "wirelessly", even on standard magstripe (non-NFC/RFID) readers.

WarBerryPi was built to be used as a hardware implant during red teaming scenarios where we want to obtain as much information as possible in a short period of time with being as stealth as possible.

P4wnP1 is a highly customizable USB attack platform, based on a low cost Raspberry Pi Zero or Raspberry Pi Zero W (required for HID backdoor).

malusb HID spoofing multi-OS payload for Teensy.

Fenrir is a tool designed to be used "out-of-the-box" for penetration tests and offensive engagements. Its main feature and purpose is to bypass wired 802.1x protection and to give you an access to the target network.

poisontap exploits locked/password protected computers over USB, drops persistent WebSocket-based backdoor, exposes internal router, and siphons cookies using Raspberry Pi Zero & Node.js.

WHID WiFi HID Injector – An USB Rubberducky / BadUSB On Steroids.

PhanTap is an 'invisible' network tap aimed at red teams. With limited physical access to a target building, this tap can be installed inline between a network device and the corporate network.

created with craft

Software For Team Communication

RocketChat is free, unlimited and open source. Replace email & Slack with the ultimate team chat software solution.

Etherpad is an open source, web-based collaborative real-time editor, allowing authors to simultaneously edit a text document

Log Aggregation

RedELK Red Team's SIEM – easy deployable tool for Red Teams used for tracking and alarming about Blue Team activities as well as better usability in long term operations.

CobaltSplunk Splunk Dashboard for CobaltStrike logs.

Red Team Telemetry A collection of scripts and configurations to enable centralized logging of red team infrastructure.

Elastic for Red Teaming Repository of resources for configuring a Red Team SIEM using Elastic.

Ghostwriter is a Django project written in Python 3.7 and is designed to be used by a team of operators.

C# Offensive Framework

- **SharpSploit** is a .NET post-exploitation library written in C# that aims to highlight the attack surface of .NET and make the use of offensive .NET easier for red teamers.
- **GhostPack** is (currently) a collection various C# implementations of previous PowerShell functionality, and includes six separate toolsets being released today- Seatbelt, SharpUp, SharpRoast, SharpDump, SafetyKatz, and SharpWMI.
- **SharpWeb** .NET 2.0 CLR project to retrieve saved browser credentials from Google Chrome, Mozilla Firefox and Microsoft Internet Explorer/Edge.
- **reconerator** C# Targeted Attack Reconnissance Tools.
- **SharpView** C# implementation of harmj0y's PowerView.
- **Watson** is a (.NET 2.0 compliant) C# implementation of Sherlock.

Labs

- **Detection Lab** This lab has been designed with defenders in mind. Its primary purpose is to allow the user to quickly build a Windows domain that comes pre-loaded with security tooling and some best practices when it comes to system logging configurations.
- **Modern Windows Attacks and Defense Lab** This is the lab configuration for the Modern Windows Attacks and Defense class that Sean Metcalf (@pyrotek3) and I teach.
- **Invoke-UserSimulator** Simulates common user behaviour on local and remote Windows hosts.

created with craft

- **Invoke-ADLabDeployer** Automated deployment of Windows and Active Directory test lab networks. Useful for red and blue teams.
- **Sheepl** Creating realistic user behaviour for supporting tradecraft development within lab environments.

References

- **MITRE's ATT&CK™** is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary's lifecycle and the platforms they are known to target.
- **Cheat Sheets** for various projects (Beacon/Cobalt Strike,PowerView, PowerUp, Empire, and PowerSploit).
- **PRE-ATT&CK** Adversarial Tactics, Techniques & Common Knowledge for Left-of-Exploit.
- **Adversary OPSEC** consists of the use of various technologies or 3rd party services to obfuscate, hide, or blend in with accepted network traffic or system behavior.
- **Adversary Emulation Plans** To showcase the practical use of ATT&CK for offensive operators and defenders, MITRE created Adversary Emulation Plans.
- **Red-Team-Infrastructure-Wiki** Wiki to collect Red Team infrastructure hardening resources.
- **Advanced Threat Tactics – Course and Notes** This is a course on red team operations and adversary simulations.
- **Red Team Tips** as posted by @vysecurity on Twitter.
- **Awesome Red Teaming** List of Awesome Red Team / Red Teaming Resources.
- **APT & CyberCriminal Campaign Collection** This is a collection of APT and CyberCriminal campaigns. Please fire issue to me if any lost APT/Malware events/campaigns.
- **ATT&CK for Enterprise Software** is a generic term for custom or commercial code, operating system utilities, open-source software, or other tools used to conduct behavior modeled in ATT&CK.
- **Planning a Red Team exercise** This document helps inform red team planning by contrasting against the very specific red team style described in Red Teams.
- **Awesome Lockpicking** a curated list of awesome guides, tools, and other resources related to the security and compromise of locks, safes, and keys.
- **Awesome Threat Intelligence** a curated list of awesome Threat Intelligence resources.
- **APT Notes** Need some scenario? APTnotes is a repository of publicly-available papers and blogs (sorted by year) related to malicious campaigns/activity/software that have been associated with vendor-defined APT (Advanced Persistent Threat) groups and/or tool-sets.
- **TIBER-EU FRAMEWORK** The European Framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU), which is the first Europe-wide framework for controlled and bespoke tests against cyber attacks in the financial market.
- **CBEST Implementation Guide** CBEST is a framework to deliver controlled, bespoke, intelligence-led cyber security tests. The tests replicate behaviours of threat actors, assessed by the UK Government and commercial intelligence providers as posing a genuine threat to systemically important financial institutions.

created with craft

- **Red Team: Adversarial Attack Simulation Exercise Guidelines for the Financial Industry in Singapore** The Association of Banks in Singapore (ABS), with support from the Monetary Authority of Singapore (MAS), has developed a set of cybersecurity assessment guidelines today to strengthen the cyber resilience of the financial sector in Singapore. Known as the Adversarial Attack Simulation Exercises (AASE) Guidelines or “Red Teaming” Guidelines, the Guidelines provide financial institutions (FIs) with best practices and guidance on planning and conducting Red Teaming exercises to enhance their security testing.

created with craft