

Forum: [Hack Forums](#)

Thread: [\[Mega List\] Free Red Team Tools \[2023\]](#)

source - April 9, 2023, 11:35 am

A collection of open-source and commercial Red Team tools that aid in red team operations. This repository will help you with the majority part of red team engagement

Red Team Field Manual PDF: <https://r00t.live/pdf/rtfm-red-team-field-manual.pdf>

[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.

[spoocheck](#) a program that checks if a domain can be spoofed. The program checks SPF and DMARC records for weak configurations that allow spoofing.

[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.

[Social Mapper](#) 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 payroll 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.

[Maltego](#) is a unique platform developed to deliver a clear threat picture to the environment that an organization owns and operates.

[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.

[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.

[CheckPlease](#) Sandbox evasion modules written in PowerShell, Python, Go, Ruby, C, C#, Perl, and Rust.

[Invoke-PSImage](#) is a tool to embed 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.

[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.

[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_Paranoide_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.

[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.

[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.

[BeEF](#) is short for The Browser Exploitation Framework. It is a penetration testing tool that focuses on the web browser.

[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.

[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.

[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 infrastructure.

[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.

[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.

[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 techniques.

[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.

[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 Isass.

[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.

[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.

[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 Subscriptions.

[DAMP](#) The Discretionary ACL Modification Project: Persistence Through Host-based Security Descriptor Modification.

Too be continued when I can use my wrists again.

Pikachuu - April 9, 2023, 11:37 am

Root, thank you for suffering and pouring out hours of your life to type this beautiful piece of work for us. You are awesome.

ALEDIO - April 9, 2023, 11:42 am

Heck you really worked hard to make this collection available, I congratulate you because it's absolutely fantastic. You did an excellent job, congratulations.

source - April 9, 2023, 11:42 am

(Apr 9, 2023 11:42 AM)ALEDIO Wrote: [\[CITE\]](#) Heck you really worked hard to make this collection available, I congratulate you because it's absolutely fantastic. You did an excellent job,

congratulations.

I am only a messenger, the real artists are the ones who created the tools!

Dread.Reaper - April 9, 2023, 12:08 pm

Amazing collection. Thanks for the time compiling.

The_unknown - April 9, 2023, 12:50 pm

Thank you a lot this is one of the best lists I have ever seen

source - April 9, 2023, 2:05 pm

[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.

[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).

[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.

Yuno - April 9, 2023, 3:38 pm

Thank you for sharing this collection. I'm sure many users will find this useful, including myself.

source - April 9, 2023, 3:39 pm

(Apr 9, 2023 03:38 PM)Yuno Wrote: [\[CITE\]](#) Thank you for sharing this collection. I'm sure many users will find this useful, including myself.

Wish I planned it out better, Had to put part of it as a late reply due to max characters lol, should have had whole thread ready for the replies right away.

3nvyc0r3 - April 9, 2023, 4:30 pm

Amazing collection, thank you for sharing the list.

source - April 11, 2023, 8:50 am

(Apr 9, 2023 04:30 PM)3nvyc0r3 Wrote: [\[CITE\]](#) Amazing collection, thank you for sharing the list. Glad I could help, Enjoy

jxhacker - April 15, 2023, 11:26 am

Red Team Field Manual PDF won t open

source - April 15, 2023, 11:27 am

(Apr 15, 2023 11:26 AM)jxhacker Wrote: [\[CITE\]](#) Red Team Field Manual PDF won t openUpdated, sorry <https://r00t.live/Hackforums/rtfm-red-team-field-manual.pdf>

jxhacker - April 15, 2023, 11:33 am

Thank you for your sharing, I hope to have a detailed steps or usage guide for osint

kosithu - April 15, 2023, 2:20 pm

Amazing collection. Thanks for the time compiling.

source - April 16, 2023, 7:18 pm

(Apr 15, 2023 02:20 PM)kosithu Wrote: [\[CITE\]](#) Amazing collection. Thanks for the time compiling. If you have any troubles feel free to PM me

x0rk - April 18, 2023, 7:55 am

Good job for what you have done here!

source - April 21, 2023, 4:09 pm

(Apr 18, 2023 07:55 AM)x0rk Wrote: [\[CITE\]](#) Good job for what you have done here! Dont thank me, Thank the folks who created these tools.

M1XX - May 22, 2023, 2:14 am

Thx, i'm happy. Good post

source - May 22, 2023, 7:32 pm

(May 22, 2023 02:14 AM)M1XX Wrote: [\[CITE\]](#) Thx, i'm happy. Good post Glad it was useful for you!

mögg - May 23, 2023, 10:58 pm

I'm extremely new to all of this, and never knew what to search for. You've made things alot easier for me. Much appreciated!

Colioo - May 25, 2023, 12:26 am

Alot of these tools will come in handy!

Thank you for putting this collection together!

naomigfsxz - May 25, 2023, 8:34 am

nice! looks very good

source - May 26, 2023, 8:07 pm

(May 25, 2023 12:26 AM)Colioo Wrote: [\[CITE\]](#) Alot of these tools will come in handy!
Thank you for putting this collection together!If you find any youd like added let me know

\$u®°°T - May 28, 2023, 1:11 am

I would imagine my eyes are almost as tired as your wrists lol
We appreciate the gifts. Gracias

source - May 28, 2023, 5:02 pm

(May 28, 2023 01:11 AM)\$u®°°T Wrote: [\[CITE\]](#) I would imagine my eyes are almost as tired as your wrists lol

We appreciate the gifts. Gracias

Wrists are well recovered, I tried to add more info but cant edit post because of characters that got merged with my second reply...

OMSPK - May 28, 2023, 5:24 pm

404 not found on this link!

<https://r00t.live/Hackforums/rtfm-red-team-field-manual.pdf>

source - May 28, 2023, 5:53 pm

(May 28, 2023 05:24 PM)OMSPK Wrote: [\[CITE\]](#) 404 not found on this link!

<https://r00t.live/Hackforums/rtfm-red-team-field-manual.pdf>

Fixed the issue.

KrypteX - July 2, 2023, 4:32 pm

Amazing collection of tools, massive thank you for the share!!

source - July 2, 2023, 4:54 pm

(Jul 2, 2023 04:32 PM)KrypteX Wrote: [\[CITE\]](#) Amazing collection of tools, massive thank you for the share!!

Glad you found it useful and thank you for reporting the link down, I have now fixed it.

Advaitoz - July 4, 2023, 9:58 am

Great job buddy.Nice compilation ???

source - July 4, 2023, 10:13 am

(Jul 4, 2023 09:58 AM)Advaitoz Wrote: [\[CITE\]](#) Great job buddy.Nice compilation ???

Hope you found it useful!

dexter007 - July 4, 2023, 2:56 pm

Wow, your post is fantastic

NEED - July 5, 2023, 1:40 pm

Awesome list, used a couple of these on the PJPT

enthusiasticMonkey777 - July 6, 2023, 7:55 pm

Thank you for sharing!

sijacz - July 7, 2023, 11:59 am

thanks for your time and effort to give us this collection!

Scifer - July 7, 2023, 8:34 pm

kinda really need this my friend
would love to see whats in store

IndefenseCat - July 15, 2023, 4:35 pm

I wish I could you invite a beer for that. Thanks you a lot, amazing community.

MrMaddTraxx - August 13, 2023, 3:46 pm

The link is dead unfortunately :(

emmabee - August 15, 2023, 2:36 am

Great collection of links...many thanks

hh3545 - August 22, 2023, 3:57 am

Hello i get an error 404 when trying to acces the link can you help please

rww1510 - September 4, 2023, 12:33 pm

Getting a 404 error as well.

juras13 - September 4, 2023, 5:06 pm

thanks bro to sent file nice work

PandaEyes23 - October 4, 2023, 6:25 pm

This is truly a masterclass post thank you so much

07days - October 11, 2023, 8:10 am

Thank you so much for this. I'm pretty new to all of this, so this list will come up handy. Thanks again!

source - October 28, 2023, 5:57 pm

(Oct 4, 2023 06:25 PM)PandaEyes23 Wrote: [\[CITE\]](#) This is truly a masterclass post thank you so much

Hope it helped in some way!

athanatoi - November 2, 2023, 3:17 am

Can't access the link but we don't need it you wrote it all!
Really thanks :)

KrissTV - November 2, 2023, 9:01 am

Thank you, very usefull

tx303 - November 3, 2023, 11:57 pm

thank you master!These tools are awesome

Bastille - November 4, 2023, 2:13 am

Nice share, I wasn't aware of this thread, added to my favs

Thanks source :)

source - November 4, 2023, 8:51 am

(Nov 4, 2023 02:13 AM)Yseurk Wrote: [\[CITE\]](#) Nice share, I wasn't aware of this thread, added to my favs

Thanks source :)
More recent used tools can be found on source.lol/

Cooligan - November 17, 2023, 7:09 pm

[source](#)

The PDF link is broken it seems like :/

source - November 17, 2023, 8:02 pm

(Nov 17, 2023 08:09 PM)Cooligan Wrote: [\[CITE\]](#) [source](#)

The PDF link is broken it seems like :/

Yes I removed it from my web host, I will see what I can do.

fatahino - November 18, 2023, 5:03 am

thank you Amazing collection. Thanks for the time compiling.

Cooligan - November 18, 2023, 7:30 am

(Nov 17, 2023 09:02 PM)source Wrote: [\[CITE\]](#) Yes I removed it from my web host, I will see what I can do.

You could always add a 3rd party PDF download link and just link the URL on one of your resource pages on r00t.live itself.

source - November 18, 2023, 9:44 am

(Nov 18, 2023 08:30 AM)Cooligan Wrote: [\[CITE\]](#) You could always add a 3rd party PDF download link and just link the URL on one of your resource pages on r00t.live itself.

meh, I removed it when I got banned so I have re added it now.

<https://r00t.live/pdf/rtfm-red-team-field-manual.pdf>

Cooligan - November 18, 2023, 10:08 am

(Nov 18, 2023 10:44 AM)source Wrote: [\[CITE\]](#) meh, I removed it when I got banned so I have re added it now. <https://r00t.live/pdf/rtfm-red-team-field-manual.pdf>

Yup, it's working now ?

Bookmarked. Definitely a useful list of resources.

Thanks for the share brotha

source - November 18, 2023, 10:09 am

(Nov 18, 2023 11:08 AM)Cooligan Wrote: [\[CITE\]](#) Yup, it's working now ?

Bookmarked. Definitely a useful list of resources.

Thanks for the share brotha

Enjoy!

PwnHunter - November 20, 2023, 11:22 pm

This collection is really interesting i am saving it for letter bro hats off for your work you should also creat a git repo

source - November 21, 2023, 1:38 pm

(Nov 21, 2023 12:22 AM)PwnHunter Wrote: [\[CITE\]](#) This collection is really interesting i am saving it for letter bro hats off for your work you should also creat a git repo

I do not take full credit for this list, I did however compile it in a nice format. Credit goes to the creators of the tools!

martin1981 - May 22, 2024, 1:13 pm

Hello link with pdf not works for me. Could you send mi private message?Thanks

SIM-5523692 - May 23, 2024, 2:02 pm

thanks man

it is of great help

source - May 29, 2024, 4:08 pm

(May 22, 2024 01:13 PM)martin1981 Wrote: [\[CITE\]](#) Hello link with pdf not works for me. Could you send mi private message?Thanks

I discontinued that part now, sorry!

jm0524895 - June 8, 2024, 6:55 pm

the PDF is not working .

Alastor@ - June 10, 2024, 3:10 am

Red Team Field Manual PDF won t open

Coringa - June 13, 2024, 2:57 pm

Realmente sensacional

Parabéns brother

GBanks - June 13, 2024, 5:09 pm

Thorough, detailed and comprehensive

Thank you for your efforts

source - September 14, 2024, 9:50 am

(Jun 10, 2024 03:10 AM)Alastor@ Wrote: [\[CITE\]](#) Red Team Field Manual PDF won t open

the link is dead sorry and I no longer have pdf, a v2 version is out also so the v1 wouldnt be useful.

Bozak - September 14, 2024, 1:46 pm

The perfect list for a lazy person like me, thanks boss

HF.Psych - September 16, 2024, 10:36 am

Nice HQ share <3 Hopefully this will benefit some users.

Hect0r - September 16, 2024, 11:17 am

Awesome collection, thanks for sharing it with the community.

SuperAlpaca - September 17, 2024, 8:46 am

Saved and bookmarked, ty

elocuente - September 18, 2024, 4:38 am

Thank! ?

Stanley - October 9, 2024, 7:49 pm

I'm Stanley HF's helper bot. The OP (original poster) of this thread wants everyone to see this page

and has elected to bump it to the top of the showthread listing. Since HF doesn't want a ton of LQP (Low Quality Posts) this is the best method of bumping your content. There is a small ?yte fee for each bump. Any OP can bump any of their threads on HF from the linked icon on the top of their first post.

If you haven't already read the first post of this thread we encourage you to do so.

Thanks,
Stanley

cynmaynard - November 27, 2024, 8:37 am

Where is the v2 version

cebef - March 5, 2025, 6:56 am

thank you so much for this!

samasugeti - March 6, 2025, 6:48 am

I was looking for a long time for this! thanks

T0XIC - March 6, 2025, 6:57 pm

Thank you for sharing!

ixeberg - March 7, 2025, 11:50 pm

My friend, I am waiting for your little help, thank you in advance. :)

Klausssss - March 11, 2025, 9:43 am

some still works....

PoneyyX - March 16, 2025, 9:31 am

nice topic thanks for your sharing

vectorjerigo - March 17, 2025, 6:56 am

Thank you for sharing

Cmiamiz - July 5, 2025, 9:20 am

bro like redteam

emp202 - July 5, 2025, 12:18 pm

wow, this is really awesome. thanks for the effort

luxmburg - July 9, 2025, 7:08 am

thank you man you such a good man

R00tziLLa - July 9, 2025, 2:00 pm

nice buddy excellent post

sdfhtg777 - July 12, 2025, 9:50 am

Thank you so much for your kind words—I really appreciate it! ? Helping out is always a pleasure, and I'm glad you found it useful. Let me know if you need anything else—I'm happy to assist! Stay awesome! ?

num3riz - September 29, 2025, 4:03 am

Thank you for sharing this collection.

klody.32 - *October 2, 2025, 4:14 pm*
thanx bro

Sergiarr - *October 5, 2025, 5:05 pm*
thanks!!

Dr4k0xKaRTeL - *October 7, 2025, 7:34 am*
This is actually a really good list.. thank you. Bookmarked