VA/PT Tools

[GitHub - GhostPack/PSPKIAudit: PowerShell toolkit for AD CS auditing based on the PSPKI toolkit.](https://github.com/GhostPack/PSPKIAudit#setup)

[The Mirai Botnet – Threats and Mitigations](https://www.cisecurity.org/blog/the-mirai-botnet-threats-and-mitigations/)

[Twitch](https://m.twitch.tv/clip/ScaryGiftedRingPupper-K0I6lgN3cvKDJHGR)

[SSH Sniffing (SSH Spying) Methods and Defense - InfosecMatter](https://www.infosecmatter.com/ssh-sniffing-ssh-spying-methods-and-defense/)

[Keytap2 - acoustic keyboard eavesdropping based on language n-gram frequencies · Discussion #31 · ggerganov/kbd-audio · GitHub](https://github.com/ggerganov/kbd-audio/discussions/31)

[Building A Test Lab For Pentesting Guide | White Oak Security](https://www.whiteoaksecurity.com/blog/building-a-test-lab-for-pentesting/)

[GitHub - hashtaginfosec/vagrantlab: Testing out vagrant to spin up an AD lab](https://github.com/hashtaginfosec/vagrantlab)

[GitHub - hashtaginfosec/vagrantlab: Testing out vagrant to spin up an AD lab](https://github.com/hashtaginfosec/vagrantlab)

[Building A Test Lab For Pentesting Guide | White Oak Security](https://www.whiteoaksecurity.com/blog/building-a-test-lab-for-pentesting/)

[GitHub - hashtaginfosec/vagrantlab: Testing out vagrant to spin up an AD lab](https://github.com/hashtaginfosec/vagrantlab)

[rapid7 - Vagrant Cloud](https://app.vagrantup.com/rapid7)

[Airstrike Attack - FDE bypass and EoP on domain joined Windows workstations (CVE-2021-28316) | Shenanigans Labs](https://shenaniganslabs.io/2021/04/13/Airstrike.html)

[Trape OSINT tool: People tracker on the Internet](https://hakin9.org/people-tracker-on-the-internet-osint-analysis-and-research-tool/)

[GitHub - c6fc/npk: A mostly-serverless distributed hash cracking platform](https://github.com/c6fc/npk)

[Active Directory Lab Setup Tool](https://browninfosecguy.com/Active-Directory-Lab-Setup-Tool)

[Download | SonarQube](https://www.sonarqube.org/downloads/?gads_campaign=Europe-1-SonarQube&gads_ad_group=SonarQube&gads_keyword=sonarqube&gclid=Cj0KCQiA_JWOBhDRARIsANymNOZnurJlhC8mjvrjI1zEFv2iRFOMtoi5FwzxVxq4SkvnJQFdURec114aAh6gEALw_wcB)

[GitHub - VbScrub/Rubeus-GUI: GUI alternative to the Rubeus command line tool, for all your Kerberos exploit requirements](https://github.com/VbScrub/Rubeus-GUI)

[GitHub - Ignitetechnologies/Wireless-Penetration-Testing](https://github.com/Ignitetechnologies/Wireless-Penetration-Testing)

[GitHub - Lipton2777/cloud-nuke: A tool for cleaning up your cloud accounts by nuking (deleting) all resources within it](https://github.com/Lipton2777/cloud-nuke)

[GitHub - kacos2000/Evtx\_Log\_Browser: Evtx Log (xml) Browser](https://github.com/kacos2000/Evtx_Log_Browser)

[GitHub - klezVirus/CandyPotato: Pure C++, weaponized, fully automated implementation of RottenPotatoNG](https://github.com/klezVirus/CandyPotato)

[EndpointManagement/OSD-ComboRadioFrontendHTA.ps1 at master · Love-A/EndpointManagement · GitHub](https://github.com/Love-A/EndpointManagement/blob/master/MECM/OSD-ComboRadioFrontendHTA.ps1)

[(99+) Post | LinkedIn](https://www.linkedin.com/posts/meisameslahi_all-in-one-file-less-malware-hunt-via-memory-activity-6867360900282773505-sXkx/)

[(99+) Post | LinkedIn](https://www.linkedin.com/posts/meisameslahi_cybersecurity-threathunting-malwaredetection-activity-6859776455908438016-ORJq/)

[(99+) Post | LinkedIn](https://www.linkedin.com/posts/meisameslahi_cybersecurity-threathunting-malwaredetection-activity-6882211511402676224-f7UK/)

[GitHub - optiv/Ivy: Ivy is a payload creation framework for the execution of arbitrary VBA (macro) source code directly in memory. Ivy’s loader does this by utilizing programmatical access in the VBA object environment to load, decrypt and execute shellcode.](https://github.com/optiv/Ivy)

[Pentest Box](https://pentestbox.org/)

[Obfuscating Malicious Macro-Enabled Word Docs](https://depthsecurity.com/blog/obfuscating-malicious-macro-enabled-word-docs)

[GitHub - sottlmarek/DevSecOps: Ultimate DevSecOps library](https://github.com/sottlmarek/DevSecOps)

[GitHub - CyberSecurityUP/OSCE-Complete-Guide: OSWE, OSEP, OSED](https://github.com/CyberSecurityUP/OSCE-Complete-Guide)

[GitHub - thiagomayllart/Harvis: Harvis is designed to automate your C2 Infrastructure.](https://github.com/thiagomayllart/Harvis)

[GitHub - gquere/pwn\_jenkins: Notes about attacking Jenkins servers](https://github.com/gquere/pwn_jenkins)

[GitHub - dievus/lnkbomb: Malicious shortcut generator for collecting NTLM hashes from insecure file shares.](https://github.com/dievus/lnkbomb)

[GitHub - cert-ee/cuckoo3: Cuckoo 3 is a Python 3 open source automated malware analysis system.](https://github.com/cert-ee/cuckoo3)

[GitHub - JavierOlmedo/OWASP-Calculator: 🧮 An online calculator to assess the risk of web vulnerabilities based on OWASP Risk Assessment](https://github.com/JavierOlmedo/OWASP-Calculator)

[GitHub - rung/threat-matrix-cicd: Threat matrix for CI/CD Pipeline](https://github.com/rung/threat-matrix-cicd)

[GitHub - jafarlihi/serpentine: C++/Win32/Boost Windows RAT (Remote Administration Tool) with a multiplatform Java/Spring RESTful C2 server and Go, C++/Qt5 frontends](https://github.com/jafarlihi/serpentine)

[guelfoweb/knock: Knock Subdomain Scan](https://github.com/guelfoweb/knock)

[Web Server Penetration Testing Checklist - GBHackers](https://gbhackers.com/web-server-penetration-testing-checklist/)

[Cloud Computing Penetration Testing Checklist & Important Considerations](https://gbhackers.com/cloud-computing-penetration-testing-checklist-important-considerations/)

[infosec-jupyterthon/workshops/2021 at master · OTRF/infosec-jupyterthon · GitHub](https://github.com/OTRF/infosec-jupyterthon/tree/master/workshops/2021)

[PeTeReport - PeTeReport](https://1modm.github.io/petereport/)

[KitPloit - PenTest & Hacking Tools](https://www.kitploit.com/?m=1)

[PR0CESS/miniGhosting at main · aaaddress1/PR0CESS](https://github.com/aaaddress1/PR0CESS/tree/main/miniGhosting)

[t94j0/gophish-notifier: Notification webhook for GoPhish](https://github.com/t94j0/gophish-notifier)

[Inf0sec - Initial Access - File Smuggling](https://inf0sec.fr/article-21.php)

[Demon's Cries vulnerability (some NETGEAR smart switches) - gynvael.coldwind//vx.log](https://gynvael.coldwind.pl/?id=740)

[Release v1.3 · FourCoreLabs/EDRHunt · GitHub](https://github.com/FourCoreLabs/EDRHunt/releases/tag/v1.3)

[7 Threat Hunting Tools Everyone in the Industry Should Be Using | Cyborg Security](https://www.cyborgsecurity.com/blog/7-threat-hunting-tools-everyone-in-the-industry-should-be-using/)

[mandiant/commando-vm: Complete Mandiant Offensive VM (Commando VM), a fully customizable Windows-based pentesting virtual machine distribution. commandovm@fireeye.com](https://github.com/mandiant/commando-vm)

[DracOS GNU/Linux Remastered](https://github.com/dracos-linux)

[Publications | Outflank](https://outflank.nl/blog/2020/03/30/mark-of-the-web-from-a-red-teams-perspective/)

[ZDI-21-1053: Bypassing Windows Lock Screen | Abdelhamid Blog](https://halove23.blogspot.com/2021/09/zdi-21-1053-bypassing-windows-lock.html?m=1)

[knight0x07/ImpulsiveDLLHijack: C# based tool which automates the process of discovering and exploiting DLL Hijacks in target binaries. The Hijacked paths discovered can later be weaponized during Red Team Operations to evade EDR's.](https://github.com/knight0x07/ImpulsiveDLLHijack)

[Farming for Red Teams: Harvesting NetNTLM - MDSec](https://www.mdsec.co.uk/2021/02/farming-for-red-teams-harvesting-netntlm/)

[Bypassing Signature-Based AV | Red Siege Information Security](https://www.redsiege.com/blog/2021/08/bypass-sig-av/)

[vx-underground](https://www.vx-underground.org/)

[Audit Azure Web App against NotLegit vulnerability -Notes of Azure Security + Governance](https://azsec.azurewebsites.net/2021/12/23/audit-azure-web-app-against-notlegit-vulnerability/)

[Detecting LDAP enumeration and Bloodhound‘s Sharphound collector using AD Decoys | by Madhukar Raina | Securonix Tech Blog | Medium](https://medium.com/securonix-tech-blog/detecting-ldap-enumeration-and-bloodhound-s-sharphound-collector-using-active-directory-decoys-dfc840f2f644)

[bats3c/shad0w: A post exploitation framework designed to operate covertly on heavily monitored environments](https://github.com/bats3c/shad0w?utm_campaign=2021_Social%20Misc&utm_content=179460463&utm_medium=social&utm_source=twitter&hss_channel=tw-1376153113)

[Open Source Security Foundation (OpenSSF)](https://github.com/ossf)

( San Francisco, CA)

[Parrot Security](https://www.parrotsec.org/)

[Hack The Box: Hacking Training For The Best | Individuals & Companies](https://www.hackthebox.com/)

[Hardware Penetration Testing tools - SecureTechware](https://securetechware.com/video/hardware-penetration-testing-tools/)

[Cyber Security Consulting & Testing | Pen Test Partners](https://www.pentestpartners.com/)

[GitHub - mufeedvh/moonwalk: Cover your tracks during Linux Exploitation by leaving zero traces on system logs and filesystem timestamps. 👻🐚](https://github.com/mufeedvh/moonwalk)

[Fsociety Hacking Tools Pack - A Penetration Testing Framework](https://hakin9.org/fsociety-hacking-tools-pack-a-penetration-testing-framework/)

[Photon - Incredibly fast crawler designed for OSINT](https://hakin9.org/photon-incredibly-fast-crawler-designed-for-osint/)

[GitHub - frankwxu/digital-forensics-lab: Free hands-on digital forensics labs for students and faculty](https://github.com/frankwxu/digital-forensics-lab)

[Security Automation and Orchestration - Theat Intelligence](https://www.threatintelligence.com/)

[Top 30+ Most Popular Red Team Tools (Updated 2021)](https://securitytrails.com/blog/red-team-tools)

[Introduction - Red Team Notes 2.0](https://dmcxblue.gitbook.io/red-team-notes-2-0/)

[CVE STALKER -The most viral CVE(vulnerability) ranking chart-](https://cvestalker.com/)

[GitHub - bigb0sss/RedTeam-OffensiveSecurity: Tools & Interesting Things for RedTeam Ops](https://github.com/bigb0sss/RedTeam-OffensiveSecurity)

[Drop support for Python 3.6 · Issue #238 · microsoft/msticpy · GitHub](https://github.com/microsoft/msticpy/issues/238)

[Offensive Security Tool: log4j-scan | Black Hat Ethical Hacking](https://www.blackhatethicalhacking.com/tools/log4j-scan/)

[Log4Shell Scanner - PortSwigger](https://portswigger.net/bappstore/b011be53649346dd87276bca41ce8e8f)

[4 Free Easy Wins That Make Red Teams Harder - TrustedSec](https://www.trustedsec.com/blog/4-free-easy-wins-that-make-red-teams-harder/)

[NTLM Relaying via Cobalt Strike – Rasta Mouse](https://rastamouse.me/ntlm-relaying-via-cobalt-strike/)

[DarkSide - Tool Information Gathering & social engineering](https://hakin9.org/darkside-tool-information-gathering-social-engineering/)

[GitHub - TheWover/CertStealer: A .NET tool for exporting and importing certificates without touching disk.](https://github.com/TheWover/CertStealer)

[Pentest-Tools-Collection/portscan.ps1 at main · LuemmelSec/Pentest-Tools-Collection · GitHub](https://github.com/LuemmelSec/Pentest-Tools-Collection/blob/main/tools/portscan.ps1)

[Reverse Shell Generator by Ryan Montgomery](https://hakin9.org/reverse-shell-generator-by-ryan-montgomery/)

[GitHub - logpresso/CVE-2021-44228-Scanner: Vulnerability scanner and mitigation patch for Log4j2 CVE-2021-44228](https://github.com/logpresso/CVE-2021-44228-Scanner)

[saeeddhqan's profile - asciinema](https://asciinema.org/~saeeddhqan)

[GitHub - YfryTchsGD/Log4jAttackSurface](https://github.com/YfryTchsGD/Log4jAttackSurface)

[GitHub - Neo23x0/log4shell-detector: Detector for Log4Shell exploitation attempts](https://github.com/Neo23x0/log4shell-detector)

[Trape OSINT tool: People tracker on the Internet](https://hakin9.org/people-tracker-on-the-internet-osint-analysis-and-research-tool/)

[GitHub - foyzulkarim/linux-playbook](https://github.com/foyzulkarim/linux-playbook)

[GitHub - HyCraftHD/Log4J-RCE-Proof-Of-Concept: Log4j-RCE (CVE-2021-44228) Proof of Concept with additional information](https://github.com/HyCraftHD/Log4J-RCE-Proof-Of-Concept)

[GitHub - Gopro336/PSA-MINERCRAFT-RCE-EXPLOIT: Minecraft exploit allowing remote code execution via Minecraft chat](https://github.com/Gopro336/PSA-MINERCRAFT-RCE-EXPLOIT)

[GitHub - feihong-cs/JNDIExploit: A malicious LDAP server for JNDI injection attacks](https://github.com/feihong-cs/JNDIExploit)

[GitHub - 0x727/JNDIExploit: 一款用于JNDI注入利用的工具，大量参考/引用了Rogue JNDI项目的代码，支持直接植入内存shell，并集成了常见的bypass 高版本JDK的方式，适用于与自动化工具配合使用。](https://github.com/0x727/JNDIExploit)

[GitHub - welk1n/JNDI-Injection-Exploit: JNDI注入测试工具（A tool which generates JNDI links can start several servers to exploit JNDI Injection vulnerability,like Jackson,Fastjson,etc）](https://github.com/welk1n/JNDI-Injection-Exploit)

[GitHub - jas502n/Log4j2-CVE-2021-44228: Remote Code Injection In Log4j](https://github.com/jas502n/Log4j2-CVE-2021-44228)

[GitHub - CrowdStrike/automactc: AutoMacTC: Automated Mac Forensic Triage Collector](https://github.com/CrowdStrike/automactc)

[GitHub - floodsung/Deep-Learning-Papers-Reading-Roadmap: Deep Learning papers reading roadmap for anyone who are eager to learn this amazing tech!](https://github.com/floodsung/Deep-Learning-Papers-Reading-Roadmap)

[SIEM Monitoring using Wazuh by Francis Jeremiah](https://hakin9.org/siem-monitoring-using-wazuh-by-francis-jeremiah/)

[Exploit in the Wild: #drupalgeddon2 - Analysis of CVE-2018-7600](https://unit42.paloaltonetworks.com/unit42-exploit-wild-drupalgeddon2-analysis-cve-2018-7600/)

[AV Evasion Part 1 · Hop Infosec](https://0xhop.github.io/evasion/2021/04/19/evasion-pt1/)

[Vulnerability Assessment & Penetration Testing | Infocratus](https://www.infocratus.com/vulnerability-assessment-penetration-testing/)

[The Difference Between a Vulnerability Assessment and a Penetration Test - Daniel Miessler](https://danielmiessler.com/study/vulnerability-assessment-penetration-test/)

[Vulnerability Assessment and Penetration Testing](https://www.csa.gov.sg/gosafeonline/go-safe-for-business/smes/vulnerability-assessment-and-penetration-testing)

[What’s the difference between a vulnerability assessment and a penetration test? - PGI](https://www.pgitl.com/blog/whats-the-difference-between-a-vulnerability-assessment-and-a-penetration-test/)

[The Ultimate Guide to Vulnerability Scanning](https://www.intruder.io/guides/the-ultimate-guide-to-vulnerability-scanning?utm_campaign=The%20Hacker%20News&utm_source=thehackernews)

[GitHub - CyberSecurityUP/Awesome-Blue-Team-Operations](https://github.com/CyberSecurityUP/Awesome-Blue-Team-Operations)

[GitHub - CyberSecurityUP/Awesome-Red-Team-Operations](https://github.com/CyberSecurityUP/Awesome-Red-Team-Operations)

[Microsoft-Defender-for-Cloud/Workbooks/AzureSecurityBenchmark at main · Azure/Microsoft-Defender-for-Cloud · GitHub](https://github.com/Azure/Microsoft-Defender-for-Cloud/tree/main/Workbooks/AzureSecurityBenchmark)

[Threat Hunting AWS CloudTrail with Sentinel: Part 3 - Binary Defense](https://www.binarydefense.com/threat-hunting-aws-cloudtrail-with-sentinel-part-3/)

[Microsoft-Defender-for-Cloud/Workbooks/Network Security Dashboard at main · Azure/Microsoft-Defender-for-Cloud · GitHub](https://github.com/Azure/Microsoft-Defender-for-Cloud/tree/main/Workbooks/Network%20Security%20Dashboard)

[Login | Let's Defend](https://app.letsdefend.io/accounts/login/?next=/)

[GitHub - LeCoqHardi/WolverineFramework: WolverineFramework - Free, OpenSource and easy to use Cybersecurity Framework.](https://github.com/LeCoqHardi/WolverineFramework)

[GitHub - darkquasar/AzureHunter: A Cloud Forensics Powershell module to run threat hunting playbooks on data from Azure and O365](https://github.com/darkquasar/AzureHunter)

[GitHub - rung/threat-matrix-cicd: Threat matrix for CI/CD Pipeline](https://github.com/rung/threat-matrix-cicd)

[Windows 11 Security. Our Hacker-in-Chief Runs Attacks and… | by Mechanics Team | Medium](https://officegarageitpro.medium.com/windows-11-security-53f927bab652)

[Best Security Practices for Mitigating Secure Shell Attacks - Security Investigation](https://www.socinvestigation.com/best-security-practices-for-mitigating-secure-shell-attacks/)

[Spraykatz - retrieve credentials on Windows machines](https://hakin9.org/spraykatz-retrieve-credentials-on-windows-machines/)

[#1249583 Authenticated kubernetes principal with restricted permissions can retrieve ingress-nginx serviceaccount token and secrets across all namespaces](https://hackerone.com/reports/1249583)

[Offensive Security Tool: GoMapEnum | Black Hat Ethical Hacking](https://www.blackhatethicalhacking.com/tools/gomapenum/)

[GitHub - codeyourweb/fastfinder: Incident Response - Fast suspicious file finder](https://github.com/codeyourweb/fastfinder)

[What is a DDoS Attack? Why are DDoS Attacks Dangerous | Indusface](https://www.indusface.com/learning/what-is-a-ddos-attack/?_gl=1*gxo5n0*_ga*TEFuWkIxZXdlUF8wdHlLWXJFSURvNGZIYUdVTk40ZjgxeV8wR3diTWh5TlNEOUt3a0xwdVFFUmNvM3lRaHd3VQ..)

[p0f - A Forensics Tool for Passive Traffic Analysis OS Fingerprinting](https://gbhackers-com.cdn.ampproject.org/c/s/gbhackers.com/os-fingerprinting-forensics-tool/amp/)

[GitHub - IvanGlinkin/AutoSUID: AutoSUID application is the Open-Source project, the main idea of which is to automate harvesting the SUID executable files and to find a way for further escalating the privileges.](https://github.com/IvanGlinkin/AutoSUID/)

[Compromising Email Supply Chains | CanIPhish](https://caniphish.com/phishing-resources/blog/compromised-australian-email-infrastructure)

[Airstrike Attack - FDE bypass and EoP on domain joined Windows workstations (CVE-2021-28316) | Shenanigans Labs](https://shenaniganslabs.io/2021/04/13/Airstrike.html)

[Tools - Intelligence X](https://intelx.io/tools)

[GitHub - CyberSecurityUP/Awesome-Malware-Analysis-Reverse-Engineering](https://github.com/CyberSecurityUP/Awesome-Malware-Analysis-Reverse-Engineering)

(, 1970)

[Kit\_Hunter - A Basic Phishing Kit Scanner For Dedicated And Semi-Dedicated Hosting](https://amp.kitploit.com/2021/11/kithunter-basic-phishing-kit-scanner.html?amp=1&m=1)

[PeTeReport - open-source application vulnerability reporting tool](https://hakin9.org/petereport-open-source-application-vulnerability-reporting-tool/)

[GitHub - Ignitetechnologies/HackTheBox-CTF-Writeups: This cheasheet is aimed at the CTF Players and Beginners to help them sort Hack The Box Labs on the basis of Operating System and Difficulty.](https://github.com/Ignitetechnologies/HackTheBox-CTF-Writeups)

[GitHub - ahmedkhlief/APT-Hunter: APT-Hunter is Threat Hunting tool for windows event logs which made by purple team mindset to provide detect APT movements hidden in the sea of windows event logs to decrease the time to uncover suspicious activity](https://github.com/ahmedkhlief/APT-Hunter)

[GitHub - AppThreat/dep-scan: Fully open-source security audit for project dependencies based on known vulnerabilities and advisories. Supports both local repos and container images. Integrates with various CI environments such as Azure Pipelines, CircleCI](https://github.com/AppThreat/dep-scan#usage)

[From AWAE to OSWE: The Preperation Guide – HanseSecure](https://hansesecure.de/2019/08/from-awae-to-oswe-the-preperation-guide/?lang=en)

[GitHub - Dheerajmadhukar/karma\_v2: ⡷⠂𝚔𝚊𝚛𝚖𝚊 𝚟𝟸⠐⢾ is a Passive Open Source Intelligence (OSINT) Automated Reconnaissance (framework)](https://github.com/Dheerajmadhukar/karma_v2)

[GitHub - inodee/threathunting-spl: Splunk code (SPL) for serious threat hunters and detection engineers.](https://github.com/inodee/threathunting-spl)

[Active Directory Lab Setup Tool](https://browninfosecguy.com/Active-Directory-Lab-Setup-Tool)

[Fsociety Hacking Tools Pack - A Penetration Testing Framework](https://hakin9.org/fsociety-hacking-tools-pack-a-penetration-testing-framework/)

[Offensive Security Tool: Hashcat | Black Hat Ethical Hacking](https://www.blackhatethicalhacking.com/tools/hashcat/)

[Invoke-winPEAS - Empire Module - InfosecMatter](https://www.infosecmatter.com/empire-module-library/?mod=powershell/privesc/winPEAS)

[Exploiting OAuth: Journey to Account Takeover | Bugs and Writeups](https://blog.dixitaditya.com/2021/11/19/account-takeover-chain.html)

[GitHub - chvancooten/OSEP-Code-Snippets: A repository with my notable code snippets for Offensive Security's PEN-300 (OSEP) course.](https://github.com/chvancooten/OSEP-Code-Snippets)

[Golden Certificate – Penetration Testing Lab](https://pentestlab.blog/2021/11/15/golden-certificate/)

[GitHub - S4R1N/AlternativeShellcodeExec: Alternative Shellcode Execution Via Callbacks](https://github.com/S4R1N/AlternativeShellcodeExec)

[GitHub - tokyoneon/Chimera: Chimera is a PowerShell obfuscation script designed to bypass AMSI and commercial antivirus solutions.](https://github.com/tokyoneon/Chimera)

[Guarding against DCSync attacks - Help Net Security](https://www.helpnetsecurity.com/2021/11/23/dcsync-attacks/)

[GitHub - S3cur3Th1sSh1t/WinPwn: Automation for internal Windows Penetrationtest / AD-Security](https://github.com/S3cur3Th1sSh1t/WinPwn)

[GitHub - praetorian-inc/trident: automated password spraying tool](https://github.com/praetorian-inc/trident)

[GitHub - CyberSecurityUP/Awesome-Cloud-PenTest](https://github.com/CyberSecurityUP/Awesome-Cloud-PenTest)

[GitHub - klinix5/InstallerFileTakeOver](https://github.com/klinix5/InstallerFileTakeOver)

[Realtek HD Audio Driver Package - DLL Preloading and Potential Abuses](https://www.safebreach.com/blog/2020/realtek-hd-audio-driver-package-dll-preloading-and-potential-abuses/)

[GitHub - shubham0d/UAC-bypass-using-dll-injection: A small project to bypass UAC in windows 10/8/7 using dll injection technique](https://github.com/shubham0d/UAC-bypass-using-dll-injection)

[The difference between Powershell only & process specific AMSI bypasses | S3cur3Th1sSh1t](https://s3cur3th1ssh1t.github.io/Powershell-and-the-.NET-AMSI-Interface/)

[GitHub - cloudquery/cloudquery: The open-source cloud asset inventory powered by SQL.](https://github.com/cloudquery/cloudquery)

[Advance Mitre Threat Mapping - Attack Navigator & TRAM Tools](https://www.socinvestigation.com/advance-mitre-threat-mapping-attack-navigator-tram-tools/)

[Welcome to ThreatPursuit VM: A Threat Intelligence and Hunting Virtual Machine | Mandiant](https://www.mandiant.com/resources/threatpursuit-vm-threat-intelligence-and-hunting-virtual-machine)

[GitHub - RedCursorSecurityConsulting/PPLKiller: Tool to bypass LSA Protection (aka Protected Process Light)](https://github.com/RedCursorSecurityConsulting/PPLKiller)

[GitHub - D4RK-4RMY/DARKARMY: DARKARMY Hacking Tools Pack - A Penetration Testing Framework .](https://github.com/D4RK-4RMY/DARKARMY)

[What is old is new again: The Relay Attack – SecureAuth](https://www.secureauth.com/blog/what-is-old-is-new-again-the-relay-attack/)

[DNS Shell - Tool to Compromise and Maintain control Over Victim Machine](https://gbhackers-com.cdn.ampproject.org/c/s/gbhackers.com/dns-shell-command-control-dns/amp/)

[GitHub - 3CORESec/MAL-CL: MAL-CL (Malicious Command-Line)](https://github.com/3CORESec/MAL-CL)

[GitHub - S3cur3Th1sSh1t/MultiPotato](https://github.com/S3cur3Th1sSh1t/MultiPotato)

[NERVE - Network Exploitation, Reconnaissance & Vulnerability Engine](https://hakin9.org/nerve-network-exploitation-reconnaissance-vulnerability-engine/)

[Detecting Office365 Azure AD Environment Backdoors](https://www.socinvestigation.com/detecting-office365-azure-ad-environment-backdoors/)

[Releases · horsicq/DIE-engine · GitHub](https://github.com/horsicq/DIE-engine/releases)

[GitHub - cobbr/PSAmsi: PSAmsi is a tool for auditing and defeating AMSI signatures.](https://github.com/cobbr/PSAmsi)

[Known Exploited Vulnerabilities Catalog | CISA](https://www.cisa.gov/known-exploited-vulnerabilities-catalog)

[Release Pre-Release: RiskIQ, Sentinel Incident Explorer, Kusto and MS Defender · microsoft/msticpy · GitHub](https://github.com/microsoft/msticpy/releases/tag/v.1.5.0pre3)

[GitHub - wagga40/Zircolite: A standalone SIGMA-based detection tool for EVTX.](https://github.com/wagga40/Zircolite)

[DFIR-ORC · GitHub](https://github.com/dfir-orc)

[Windows & Active Directory Exploitation Cheat Sheet and Command Reference :: Cas van Cooten — I ramble about security stuff, mostly](https://casvancooten.com/posts/2020/11/windows-active-directory-exploitation-cheat-sheet-and-command-reference/)

[GitHub - superhero1/OSCP-Prep](https://github.com/superhero1/OSCP-Prep)

(, 2020)

[What is AS-REP Roasting? | Cracking Active Directory Passwords](https://stealthbits.com/blog/cracking-active-directory-passwords-with-as-rep-roasting/)

[Public SSH keys can leak your private infrastructure | Artem Golubin](https://rushter.com/blog/public-ssh-keys/)

[GitHub - CravateRouge/bloodyAD: BloodyAD is an Active Directory Privilege Escalation Framework](https://github.com/CravateRouge/bloodyAD)

[How to Tackle SaaS Security Misconfigurations](https://thehackernews.com/2021/11/how-to-tackle-saas-security.html?m=1)

[GitHub - AmirHoseinTangsiriNET/SSQAuto](https://github.com/AmirHoseinTangsiriNET/SSQAuto)

[APT-Hunter V2.0 - Threat Hunting Tool For Windows Event Logs](https://www.socinvestigation.com/apt-hunter-v2-0-threat-hunting-tool-for-windows-event-logs/)

[GitHub - bmuschko/ckad-crash-course: In-depth and hands-on practice for acing the exam.](https://github.com/bmuschko/ckad-crash-course)

[GenesisBlock3301/product\_delivery\_fastapi: Product delivery api](https://github.com/GenesisBlock3301/product_delivery_fastapi)

[Process Lineage Analysis - Technique D3-PLA | MITRE D3FEND™](https://d3fend.mitre.org/technique/d3f:ProcessLineageAnalysis/)

[Intrusion Prevention System(IPS) and Its Detailed Function - SOC/SIEM](https://gbhackers-com.cdn.ampproject.org/c/s/gbhackers.com/intrusion-prevention-systemips-and-its-detailed-funtion-socsiem/amp/)

[IRP-Phishing · main · Public Incident Response Ressources / Public Playbooks · GitLab](https://gitlab.com/syntax-ir/playbooks/-/tree/main/IRP-Phishing)

[GitHub - horsicq/Detect-It-Easy: Program for determining types of files for Windows, Linux and MacOS.](https://github.com/horsicq/Detect-It-Easy)

[GitHub - 3CORESec/MAL-CL: MAL-CL (Malicious Command-Line)](https://github.com/3CORESec/MAL-CL)

[IRP-Phishing · main · Public Incident Response Ressources / Public Playbooks · GitLab](https://gitlab.com/syntax-ir/playbooks/-/tree/main/IRP-Phishing)

[Offensive Security Tool: Pentesting Tools | Black Hat Ethical Hacking](https://www.blackhatethicalhacking.com/tools/pentesting-tools/)

[PeTeReport - open-source application vulnerability reporting tool](https://hakin9.org/petereport-open-source-application-vulnerability-reporting-tool/?fbclid=IwAR0f1mrHBZPRDXQUv1yP-vUUWguOaCHGnoYfvIDew27Jg4xOPIAPcc1xldE)

[What is an Evil Twin Attack - Example, Procedure, and Preventive Methods](https://cybersecuritynews.com/evil-twin/)

[GitHub - OALabs/hashdb-ida: HashDB API hash lookup plugin for IDA Pro](https://github.com/OALabs/hashdb-ida)

[Winitor](https://www.winitor.com/)

[BloodHound-Tools/Ransomulator at main · zeronetworks/BloodHound-Tools · GitHub](https://github.com/zeronetworks/BloodHound-Tools/tree/main/Ransomulator)

[ADenum: find misconfiguration through the protocol LDAP](https://securityonline.info/adenum-find-misconfiguration-through-the-protocol-ldap/)

[Initial Access Broker Landscape](https://www.curatedintel.org/2021/10/initial-access-broker-landscape.html?m=1)

[Initial-Access-Broker-Landscape/InitialAccessBrokers.png at main · curated-intel/Initial-Access-Broker-Landscape · GitHub](https://github.com/curated-intel/Initial-Access-Broker-Landscape/blob/main/InitialAccessBrokers.png)

[IronNetTR/cobalt\_strike at main · IronNetCybersecurity/IronNetTR · GitHub](https://github.com/IronNetCybersecurity/IronNetTR/tree/main/cobalt_strike)

[GitHub - OmerYa/Invisi-Shell: Hide your Powershell script in plain sight. Bypass all Powershell security features](https://github.com/OmerYa/Invisi-Shell)

[GitHub - nyxgeek/o365recon: retrieve information via O365 and AzureAD with a valid cred](https://github.com/nyxgeek/o365recon)

[GitHub - ahmedkhlief/APT-Hunter: APT-Hunter is Threat Hunting tool for windows event logs which made by purple team mindset to provide detect APT movements hidden in the sea of windows event logs to decrease the time to uncover suspicious activity](https://github.com/ahmedkhlief/APT-Hunter)

[BHEH1337 - Twitch](https://m.twitch.tv/bheh1337)

[Nim on the Attack: Process Injection Using Nim and the Windows API – HuskyHacks](https://huskyhacks.dev/2021/07/17/nim-exploit-dev/amp/)

[This is how I bypassed almost every EDR! | by Omri Baso | Nov, 2021 | Medium](https://medium.com/@omribaso/this-is-how-i-bypassed-almost-every-edr-6e9792cf6c44)

[Aircrack-ng](https://www.aircrack-ng.org/)

[John the Ripper password cracker](https://www.openwall.com/john/)

[Most Common Windows Event IDs to Hunt - Mind Map](https://www.socinvestigation.com/most-common-windows-event-ids-to-hunt-mind-map/)

[GitHub - derv82/wifite2: Rewrite of the popular wireless network auditor, "wifite"](https://github.com/derv82/wifite2)

[start [hashcat wiki]](https://hashcat.net/wiki/)

[Offensive Security Tool: DotDotPwn – The Directory Traversal Fuzzer | Black Hat Ethical Hacking](https://www.blackhatethicalhacking.com/tools/dotdotpwn/)

[THC-Hydra | Penetration Testing Tools](https://tools.kali.org/password-attacks/hydra)

[GitHub - Matheus-Garbelini/braktooth\_esp32\_bluetooth\_classic\_attacks: A Series of Baseband & LMP Exploits against Bluetooth Classic Controllers](https://github.com/Matheus-Garbelini/braktooth_esp32_bluetooth_classic_attacks)

[GitHub - stuhli/awesome-event-ids: Collection of Event ID ressources useful for Digital Forensics and Incident Response](https://github.com/stuhli/awesome-event-ids)

[TryHackMe | CC: Pen Testing](https://tryhackme.com/room/ccpentesting)

[TruffleHog — Truffle Security](https://trufflesecurity.com/trufflehog)

[Threat Hunting and Detection with Web Proxy Logs | by Mehmet Ergene | Medium](https://posts.bluraven.io/threat-hunting-and-detection-with-web-proxy-logs-58094cae3537)

[Offensive Security Tool: Discover | Black Hat Ethical Hacking](https://www.blackhatethicalhacking.com/tools/discover/)

[Windows Management Instrumentation Attacks - Detection & Response](https://www.socinvestigation.com/windows-management-instrumentation-attacks-detection-response/)

[Blinding EDR On Windows - Red Team Blog](https://synzack.github.io/Blinding-EDR-On-Windows/)

[toutatis: extract information from instagrams accounts such as e-mails, phone numbers](https://securityonline.info/toutatis-extract-information-from-instagrams-accounts/)

[GitHub - ufrisk/MemProcFS: The Memory Process File System](https://github.com/ufrisk/MemProcFS)

[The Official Social Engineering Hub - Security Through Education](https://www.social-engineer.org/)

[Positive Technologies - vulnerability assessment, compliance management and threat analysis solutions](https://www.ptsecurity.com/ww-en/)

[Mama Always Told Me Not to Trust Strangers without Certificates](https://blog.grimm-co.com/2021/09/mama-always-told-me-not-to-trust.html?m=1)

[GitHub - Narasimha1997/fake-sms: A simple command line tool using which you can skip phone number based SMS verification by using a temporary phone number that acts like a proxy.](https://github.com/Narasimha1997/fake-sms)

[GitHub - penetrarnya-tm/WeaponizeKali.sh: Automate installation of extra pentest tools on Kali Linux](https://github.com/penetrarnya-tm/WeaponizeKali.sh)

[Linux-CatScale IR Collection Script • Penetration Testing](https://securityonline.info/linux-catscale-ir-collection-script/)

[GitHub - ForbiddenProgrammer/conti-pentester-guide-leak: Leaked pentesting manuals given to Conti ransomware crooks](https://github.com/ForbiddenProgrammer/conti-pentester-guide-leak)

[PT Network Attack Discovery](https://www.ptsecurity.com/ww-en/products/network-attack-discovery/)

[vx-underground.orghttps://tinyurl.com/ygtydr57https://tinyurl.com/yzuxt8dw - Pastebin.com](https://pastebin.com/U71YVjjy)

[APT-Hunter - Threat Hunting Tool For Windows Event Logs](https://www.socinvestigation.com/apt-hunter-threat-hunting-tool-for-windows-event-logs/)

[GitHub - kitabisa/mubeng: An incredibly fast proxy checker & IP rotator with ease.](https://github.com/kitabisa/mubeng)

[GitHub - Mamun-swe/Node\_mssql\_crud\_api: Node.JS and MSSQL CRUD API application.](https://github.com/Mamun-swe/Node_mssql_crud_api)

[GitHub - HightechSec/scarce-apache2: A framework for bug hunting or pentesting targeting websites that have CVE-2021-41773 Vulnerability in public](https://github.com/HightechSec/scarce-apache2)

[GitHub - frankwxu/digital-forensics-lab: Free hands-on digital forensics labs for students and faculty](https://github.com/frankwxu/digital-forensics-lab)

[19 Powerful Penetration Testing Tools Used By Pros in 2021](https://www.softwaretestinghelp.com/penetration-testing-tools/)

[10 Best Free Penetration Testing Tools 2021 - Cyber Security News](https://cybersecuritynews-com.cdn.ampproject.org/c/s/cybersecuritynews.com/penetration-testing-tools/?amp)

[Information Technology Sector | CISA](https://www.cisa.gov/publication/information-technology-sector)

[10 Best Tools to Scan Linux Servers for Vulnerability & Malware](https://cybersecuritynews-com.cdn.ampproject.org/c/s/cybersecuritynews.com/scan-linux-servers/?amp)

[» Attack Methods for Gaining Domain Admin Rights in Active Directory » Active Directory Security](https://adsecurity.org/?p=2362)

[Introduction — Threat Hunter Playbook](https://threathunterplaybook.com/introduction.html)

[GitHub - xct/xc: A small reverse shell for Linux & Windows](https://github.com/xct/xc)

[GitHub - SimpleBoilerplates/Flutter: A boilerplate project for Flutter using RiverPod, Dio, auto\_route, Freezed and generated with very\_good\_cli](https://github.com/SimpleBoilerplates/Flutter)

[GitHub - iamthefrogy/frogy: My subdomain enumeration script. It's unique in the way it is built upon.](https://github.com/iamthefrogy/frogy/)

[GitHub - waydroid/waydroid](https://github.com/waydroid/waydroid)

[Pentest oriented collaborative tool - Smersh documentation](https://docs.smersh.app/)

[Active Directory Checklist - Attack & Defense Cheatsheet](https://cybersecuritynews-com.cdn.ampproject.org/c/s/cybersecuritynews.com/active-directory-checklist/?amp)

[GitHub - 0xInfection/TIDoS-Framework: The Offensive Manual Web Application Penetration Testing Framework.](https://github.com/0xInfection/TIDoS-Framework)

[GitHub - austinsonger/Incident-Playbook: GOAL: Incident Response Playbooks Mapped to MITRE Attack Tactics and Techniques. [Contributors Friendly]](https://github.com/austinsonger/Incident-Playbook)

[Grype - Vulnerability Scanner For Container Images & Filesystems](https://www.darknet.org.uk/2021/04/grype-vulnerability-scanner-for-container-images-filesystems/?utm_source=dlvr.it&utm_medium=linkedin&utm_campaign=darknetfeed)

[GitHub - Azure/Stormspotter: Azure Red Team tool for graphing Azure and Azure Active Directory objects](https://github.com/Azure/Stormspotter?utm_campaign=2021_Social%20Misc&utm_content=152053973&utm_medium=social&utm_source=twitter&hss_channel=tw-1376153113)

[No Logs? No Problem! Incident Response without Windows Event Logs - JUMPSEC LABS](https://labs.jumpsec.com/no-logs-no-problem-incident-response-without-windows-event-logs/)

[GitHub - S3cur3Th1sSh1t/WinPwn: Automation for internal Windows Penetrationtest / AD-Security](https://github.com/S3cur3Th1sSh1t/WinPwn)

[DNS Lookup Viewer for Windows 10](http://www.nirsoft.net/utils/dns_lookup_view.html)

[OWASP Zed Attack Proxy How-To](https://chrisdecairos.ca/intercepting-traffic-with-zaproxy/)

[GitHub - ANSSI-FR/DFIR-O365RC: PowerShell module for Office 365 and Azure log collection](https://github.com/ANSSI-FR/DFIR-O365RC)

[GitHub - TRSTN4/EagleShell: EagleShell is a high-quality tool that aims to improve your pentest.](https://github.com/TRSTN4/EagleShell)

[GitHub - boku7/spawn: Cobalt Strike BOF that spawns a sacrificial process, injects it with shellcode, and executes payload. Built to evade EDR/UserLand hooks by spawning sacrificial process with Arbitrary Code Guard (ACG), BlockDll, and PPID spoofing.](https://github.com/boku7/spawn)

[GitHub - p3nt4/PowerShdll: Run PowerShell with rundll32. Bypass software restrictions.](https://github.com/p3nt4/PowerShdll)

[GitHub - intelowlproject/IntelOwl: Intel Owl: analyze files, domains, IPs in multiple ways from a single API at scale](https://github.com/intelowlproject/IntelOwl)

[Release DRAKVUF Sandbox v0.17.0 · CERT-Polska/drakvuf-sandbox · GitHub](https://github.com/CERT-Polska/drakvuf-sandbox/releases/tag/v0.17.0)

[GitHub - byt3bl33d3r/CrackMapExec: A swiss army knife for pentesting networks](https://github.com/byt3bl33d3r/CrackMapExec)

[Go-Shellcode : A Repository Of W S R And Supporting Utilities.](https://kalilinuxtutorials-com.cdn.ampproject.org/c/s/kalilinuxtutorials.com/go-shellcode/amp/)

[GitHub - Kevin-Robertson/Sharpmad: C# version of Powermad](https://github.com/Kevin-Robertson/Sharpmad)

[GitHub - f0wl/MalwareLab\_VM-Setup: Setup scripts for my Malware Analysis VMs](https://github.com/f0wl/MalwareLab_VM-Setup)

[GitHub - six2dez/reconftw: reconFTW is a tool designed to perform automated recon on a target domain by running the best set of tools to perform scanning and finding out vulnerabilities](https://github.com/six2dez/reconftw)

[GitHub - goichot/CVE-2020-3433: PoCs and technical analysis of three vulnerabilities found on Cisco AnyConnect for Windows: CVE-2020-3433, CVE-2020-3434 and CVE-2020-3435](https://github.com/goichot/CVE-2020-3433)

[GitHub - Fahrj/reverse-ssh: Statically-linked ssh server with reverse shell functionality for CTFs and such](https://github.com/Fahrj/reverse-ssh#requirements)

<https://osint.link/>

[GitHub - dfirtrack/dfirtrack: DFIRTrack - The Incident Response Tracking Application](https://github.com/dfirtrack/dfirtrack#installation-and-dependencies)

[GitHub - mitre/caldera: Scalable Automated Adversary Emulation Platform](https://github.com/mitre/caldera)

[Scorpiones Group | Lateral Movement using DCOM Objects - Guide to using DCOM Objects in order to Move Laterally in the Network.](https://www.scorpiones.io/articles/lateral-movement-using-dcom-objects)

[GitHub - shubham0d/UAC-bypass-using-dll-injection: A small project to bypass UAC in windows 10/8/7 using dll injection technique](https://github.com/shubham0d/UAC-bypass-using-dll-injection)

[GitHub - iphelix/dnschef: DNSChef - DNS proxy for Penetration Testers and Malware Analysts](https://github.com/iphelix/dnschef)

[Comprehensive Guide to Local File Inclusion (LFI)](https://www.hackingarticles.in/comprehensive-guide-to-local-file-inclusion/)

[10 (more) free security tools worth a look | CSO Online](https://www.csoonline.com/article/3563872/10-more-free-security-tools-worth-a-look.html?utm_source=Adestra&utm_medium=email&utm_content=Title%3A%2010%20%28more%29%20free%20security%20tools%20worth%20a%20look&utm_campaign=CSO%20US%20Update&utm_term=CSO%20US%20Editorial%20Newsletters&utm_date=20200625151040)

[Router Security](https://www.routersecurity.org/index.php)

[Active Directory Enumeration With BloodHound](https://www.youtube.com/watch?v=sGO4F23Xik4)

[Android Rat - An Advanced Hacking Tool to Hack Targeted Android Phone](https://gbhackers-com.cdn.ampproject.org/c/s/gbhackers.com/android-rat-kali-linux-tutorial/amp/)

[GitHub - tanc7/EXOCET-AV-Evasion: EXOCET - AV-evading, undetectable, payload delivery tool](https://github.com/tanc7/EXOCET-AV-Evasion)

[OSINT Tool: Osintgram | Black Hat Ethical Hacking](https://www.blackhatethicalhacking.com/tools/osintgram/)

[GitHub - t94j0/gophish-notifier: Notification webhook for GoPhish](https://github.com/t94j0/gophish-notifier)

[GitHub - carlospolop/PEASS-ng: PEASS - Privilege Escalation Awesome Scripts SUITE (with colors)](https://github.com/carlospolop/PEASS-ng)

[Hunt the Beasts in the Bits A Proactive Approach | Meisam Eslahi | BSides Singapore Conference 2021](https://www.youtube.com/watch?v=KT8LGDl74Tw&t=1761s)

[The flexible management system | monday.com Work OS](https://www.youtube.com/watch?v=39DGVpMt7eQ)

[Hunting Malware in Process Memory | Icegrave](https://icegrave0391.github.io/2020/03/10/memfor-8/)

[Offensive WMI - Exploring Namespaces, Classes & Methods (Part 2) :: 0xInfection's Blog — Random ramblings of an Infected Geek.](https://0xinfection.github.io/posts/wmi-classes-methods-part-2/)

[Mind Maps | Never Ending Security](https://neverendingsecurity.wordpress.com/2015/02/20/mind-maps/)

[FinFisher malware hijacks Windows Boot Manager with UEFI bootkit | Black Hat Ethical Hacking](https://www.blackhatethicalhacking.com/news/finfisher-malware-hijacks-windows-boot-manager-with-uefi-bootkit/)

[GitHub - thomast1906/DevOps-The-Hard-Way-Azure: This repository contains free labs for setting up an entire workflow and DevOps environment from a real-world perspective in Azure](https://github.com/thomast1906/DevOps-The-Hard-Way-Azure)

[Twitch](https://m.twitch.tv/clip/CoweringAstuteOryxRaccAttack-VhhP6VT_vir0ZJ6P)

[Taking Hunting to the Next Level: Hunting in Memory - SANS Threat Hunting Summit 2017 - YouTube](https://m.youtube.com/watch?v=EVBCoV8lpWc&feature=youtu.be)

[GitHub - mgeeky/ShellcodeFluctuation: An in-memory evasion technique fluctuating shellcode memory protection between RW & RX and encrypting/decrypting contents](https://github.com/mgeeky/ShellcodeFluctuation)

[GitHub - punk-security/pwnspoof](https://github.com/punk-security/pwnspoof)

[Network traffic analysis using Wireshark | AT&T Cybersecurity](https://cybersecurity.att.com/blogs/security-essentials/network-traffic-analysis-using-wireshark)

[GitHub - outflanknl/PrintNightmare](https://github.com/outflanknl/PrintNightmare)

[ImpulsiveDLLHijack - C# Based Tool Which Automates The Process Of Discovering And Exploiting DLL Hijacks In Target Binaries](https://www.kitploit.com/2021/10/impulsivedllhijack-c-based-tool-which.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+PentestTools+%28PenTest+Tools%29)

[Do Your Best Schoolwork Faster | Better Results With Grammarly](https://www.youtube.com/watch?v=nbZ0xs6LKrE)

[Karma\_V2 - A Passive Open Source Intelligence (OSINT) Automated Reconnaissance (Framework)](https://amp.kitploit.com/2021/10/karmav2-passive-open-source.html?amp=1&m=1)

[GitHub - p0dalirius/LDAPmonitor: Monitor creation, deletion and changes to LDAP objects live during your pentest or system administration!](https://github.com/p0dalirius/LDAPmonitor)

[GitHub - OWASP/Python-Honeypot: OWASP Honeypot, Automated Deception Framework.](https://github.com/OWASP/Python-Honeypot)

[Winshark - Wireshark plugin to work with Event Tracing for Windows](https://hakin9.org/winshark-wireshark-plugin-to-work-with-event-tracing-for-windows/)

[Winshark - Wireshark plugin to work with Event Tracing for Windows](https://hakin9.org/winshark-wireshark-plugin-to-work-with-event-tracing-for-windows/)

[writeups/Confluence-RCE.md at main · httpvoid/writeups · GitHub](https://github.com/httpvoid/writeups/blob/main/Confluence-RCE.md)

[Huan: Encrypted PE Loader Generator • Penetration Testing](https://securityonline.info/huan-encrypted-pe-loader-generator/)

[ImpulsiveDLLHijack - C# Based Tool Which Automates The Process Of Discovering And Exploiting DLL Hijacks In Target Binaries](https://amp.kitploit.com/2021/10/impulsivedllhijack-c-based-tool-which.html?amp=1&m=1)

[GitHub - hak5/omg-payloads](https://github.com/hak5/omg-payloads)

[GitHub - Arinerron/heaptrace: helps visualize heap operations for pwn and debugging](https://github.com/Arinerron/heaptrace)

[GitHub - ly4k/CallbackHell: PoC (DoS) for CVE-2021-40449 - Win32k Elevation of Privilege Vulnerability (LPE)](https://github.com/ly4k/CallbackHell)

[Tor Rootkit: Python 3 standalone Windows 10 / Linux Rootkit](https://securityonline.info/tor-rootkit-python-3-standalone-windows-10-linux-rootkit/)

[Networkit - A Growing Open-Source Toolkit For Large-Scale Network Analysis](https://www.kitploit.com/2021/10/networkit-growing-open-source-toolkit.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+PentestTools+(PenTest+Tools)&m=1)

[GitHub - Vinum-Security/kubernetes-security-checklist: Kubernetes Security Checklist and Requirements - All in One (authentication, authorization, logging, secrets, configuration, network, workloads, dockerfile)](https://github.com/Vinum-Security/kubernetes-security-checklist)

[GitHub - its-a-feature/Mythic: A collaborative, multi-platform, red teaming framework](https://github.com/its-a-feature/Mythic)

[GitHub - matamorphosis/Scrummage: The Ultimate OSINT and Threat Hunting Framework](https://github.com/matamorphosis/Scrummage)

[GitHub - summitt/burp-ysoserial: YSOSERIAL Integration with burp suite](https://github.com/summitt/burp-ysoserial)

[DarkSide Ransomware Reverse Engineering - YouTube](https://m.youtube.com/watch?v=NIiEcOryLpI&feature=youtu.be)

[Silent Breach - Cyber Security Experts](https://silentbreach.com/)

[GitHub - nsacyber/Hardware-and-Firmware-Security-Guidance: Guidance for the Spectre, Meltdown, Speculative Store Bypass, Rogue System Register Read, Lazy FP State Restore, Bounds Check Bypass Store, TLBleed, and L1TF/Foreshadow vulnerabilities as well as](https://github.com/nsacyber/Hardware-and-Firmware-Security-Guidance)

[GitHub - OWASP/owasp-mstg: The Mobile Security Testing Guide (MSTG) is a comprehensive manual for mobile app security development, testing and reverse engineering.](https://github.com/OWASP/owasp-mstg)

[0-Day Hunting (Chaining Bugs/Methodology)](https://blog.riotsecurityteam.com/0day-chains)

[GitHub - dhondta/dronesploit: Drone pentesting framework console](https://github.com/dhondta/dronesploit)

[Active Directory Checklist - Attack & Defense Cheatsheet](https://cybersecuritynews-com.cdn.ampproject.org/c/s/cybersecuritynews.com/active-directory-checklist/?amp)

[GitHub - seajaysec/cypheroth: Automated, extensible toolset that runs cypher queries against Bloodhound's Neo4j backend and saves output to spreadsheets.](https://github.com/seajaysec/cypheroth/)

[Orbitaldump - a simple multi-threaded distributed SSH brute-forcing tool written in Python](https://hakin9.org/orbitaldump-a-simple-multi-threaded-distributed-ssh-brute-forcing-tool-written-in-python/)

[GitHub - xFreed0m/RDPassSpray: Python3 tool to perform password spraying using RDP](https://github.com/xFreed0m/RDPassSpray)

[Hacker Associate - Cyber Security Training, Certification and Services](https://hackerassociate.com/)

[Pentest-Tools.com | 25+ Online Penetration Testing Tools](https://pentest-tools.com/home)

[Reverse engineering and decrypting CyberArk vault credential files – NCC Group Research](https://research.nccgroup.com/2021/10/08/reverse-engineering-and-decrypting-cyberark-vault-credential-files/amp/)

[Justin Bieber Linux](http://biebian.sourceforge.net/)

[What is a Honeypot and How it Improves Network security?](https://cybersecuritynews-com.cdn.ampproject.org/c/s/cybersecuritynews.com/what-is-a-honeypot/?amp)

[Detecting CONTI CobaltStrike Lateral Movement Techniques - Part 1 - CYB3RSN0RLAX](https://www.unh4ck.com/detection-engineering-and-threat-hunting/lateral-movement/detecting-conti-cobaltstrike-lateral-movement-techniques-part-1)

[Inside TeamTNT’s Impressive Arsenal](https://www.anomali.com/blog/inside-teamtnts-impressive-arsenal-a-look-into-a-teamtnt-server)

[Wireshark Tutorial: Wireshark Workshop Videos Now Available](https://unit42.paloaltonetworks.com/wireshark-workshop-videos/)

[Masscan -Worlds Fastest Scanner - Scan the Entire Internet Under 6 Min](https://gbhackers-com.cdn.ampproject.org/c/s/gbhackers.com/masscan-worlds-fastest-scanner/amp/)

[GitHub - Cloud-Architekt/AzureAD-Attack-Defense: This publication is a collection of various common attack scenarios on Azure Active Directory and how they can be mitigated or detected.](https://github.com/Cloud-Architekt/AzureAD-Attack-Defense)

[Investigating an Office 365 account compromise – CIAOPS](https://blog.ciaops.com/2018/12/22/investigating-an-office-365-account-compromise/amp/)

[Offensive Security Tool: URL Hunter | Black Hat Ethical Hacking](https://www.blackhatethicalhacking.com/tools/url-hunter/)

[GitHub - ollypwn/PrintNightmare: Python implementation for PrintNightmare (CVE-2021-1675 / CVE-2021-34527)](https://github.com/ollypwn/PrintNightmare)

[Release v1.6.1 - Sentinel APIs, Folium, VirusTotal, ProcessTree, and more · microsoft/msticpy · GitHub](https://github.com/microsoft/msticpy/releases/tag/v1.6.1)

[Release v1.6.1 - Sentinel APIs, Folium, VirusTotal, ProcessTree, and more · microsoft/msticpy · GitHub](https://github.com/microsoft/msticpy/releases/tag/v1.6.1)

[GitHub - CyberSecurityUP/Awesome-Red-Team-Operations](https://github.com/CyberSecurityUP/Awesome-Red-Team-Operations)

[GitHub - CyberSecurityUP/eWPTX-Preparation](https://github.com/CyberSecurityUP/eWPTX-Preparation)

[GitHub - CyberSecurityUP/OSCP-Survival-Guide](https://github.com/CyberSecurityUP/OSCP-Survival-Guide)

[GitHub - CyberSecurityUP/eCXD-Preparation: eLearnSecurity Certified Exploit Development](https://github.com/CyberSecurityUP/eCXD-Preparation)

[LFI Cheat Sheet](https://highon.coffee/blog/lfi-cheat-sheet/)

[GitHub - usnistgov/oscal-content: NIST SP 800-53 content and other OSCAL content examples](https://github.com/usnistgov/oscal-content)

[The Ultimate Guide to Vulnerability Scanning](https://www.intruder.io/guides/the-ultimate-guide-to-vulnerability-scanning?utm_campaign=The%20Hacker%20News&utm_source=thehackernews)

[GitHub - AlgoSecure/Pollenisator: Collaborative pentest tool with highly customizable tools](https://github.com/AlgoSecure/Pollenisator)

[Warming Up. Using ATT&CK for Self Advancement - SOC Prime](https://socprime.com/blog/warming-up-using-attck-for-self-advancement/)

[GitHub - horsicq/Nauz-File-Detector: Linker/Compiler/Tool detector for Windows, Linux and MacOS.](https://github.com/horsicq/Nauz-File-Detector)

[Hacking CloudKit - How I accidentally deleted your Apple Shortcuts - Detectify Labs](https://labs.detectify.com/2021/09/13/hacking-cloudkit-how-i-accidentally-deleted-your-apple-shortcuts/)

[GitHub - adstuart/azure-expressroute-migration: How to approach migrating from one ExpressRoute circuit to another ExpressRoute circuit, with a focus on methodical transition of the ExpressRoute Private Peering.](https://github.com/adstuart/azure-expressroute-migration)

[Dystopia - a low to medium multithreaded Ubuntu Core honeypot coded in Python -](https://hakin9.org/dystopia-a-low-to-medium-multithreaded-ubuntu-core-honeypot-coded-in-python/)

[Most Important Android Application Penetration Testing Checklist](https://gbhackers-com.cdn.ampproject.org/c/s/gbhackers.com/penetration-testing-android-application-checklist/amp/)

[DNSTake - A Fast Tool To Check Missing Hosted DNS Zones That Can Lead To Subdomain Takeover](https://www.kitploit.com/2021/09/dnstake-fast-tool-to-check-missing.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+PentestTools+%28PenTest+Tools%29)

[GitHub - countercept/chainsaw: Rapidly Search and Hunt through Windows Event Logs](https://github.com/countercept/chainsaw#getting-started)

[Chainsaw](https://labs.f-secure.com/tools/chainsaw/)

[Breaking The Browser - A tale of IPC, credentials and backdoors - MDSec](https://www.mdsec.co.uk/2021/01/breaking-the-browser-a-tale-of-ipc-credentials-and-backdoors/)

[Malware Analysis Use Cases with ANY.RUN Sandbox](https://www.socinvestigation.com/malware-analysis-use-cases-with-any-run-sandbox/)

[Capoae Malware Attacking Linux systems & Web Apps](https://gbhackers-com.cdn.ampproject.org/c/s/gbhackers.com/capoae-malware/amp/)

[Airstrike Attack - FDE bypass and EoP on domain joined Windows workstations (CVE-2021-28316) | Shenanigans Labs](https://shenaniganslabs.io/2021/04/13/Airstrike.html)

[AD CS relay attack - practical guide · Ex Android Dev](https://www.exandroid.dev/2021/06/23/ad-cs-relay-attack-practical-guide/)

[Online - Reverse Shell Generator](https://www.revshells.com/)

[Release age v1.0.0 🏁 · FiloSottile/age · GitHub](https://github.com/FiloSottile/age/releases/tag/v1.0.0)

[GitHub - brightio/penelope: Penelope Shell Handler](https://github.com/brightio/penelope)

[Hiding Your Syscalls | PassTheHashBrowns](https://passthehashbrowns.github.io/hiding-your-syscalls)

[peirates: Kubernetes Penetration Testing tool • Penetration Testing](https://securityonline.info/peirates-kubernetes-penetration-testing-tool/)

[GitHub - kacos2000/MFT\_Browser: $MFT directory tree reconstruction & record info](https://github.com/kacos2000/MFT_Browser)

[GitHub - waleedassar/RestrictedKernelLeaks](https://github.com/waleedassar/RestrictedKernelLeaks)

[Offensive Security Tool: Jenkins Attack Framework | Black Hat Ethical Hacking](https://www.blackhatethicalhacking.com/tools/jenkins-attack-framework/?__cf_chl_jschl_tk__=pmd_S9BaKo9pFUmGaZw2qBWWs2GMZq8.kL6jCHeF2ZXLBj8-1631291171-0-gqNtZGzNAfujcnBszQdl)

[GitHub - COSSAS/dgad: DGA Detective](https://github.com/COSSAS/dgad)

[IMQ Minded Security Blog: A Journey Into the Beauty of DNSRebinding - Part 2](https://blog.mindedsecurity.com/2021/08/a-journey-into-beauty-of-dnsrebinding.html?m=1)

[GitHub - hoppscotch/hoppscotch: 👽 Open source API development ecosystem https://hoppscotch.io](https://github.com/hoppscotch/hoppscotch)

[How to apply Sun Tzu’s ‘The Art of War’ to cybersecurity | Security Magazine](https://www.securitymagazine.com/articles/96072-how-to-apply-sun-tzus-the-art-of-war-to-cybersecurity)

[MacOS Security & Privilege Escalation - HackTricks](https://book.hacktricks.xyz/macos/macos-security-and-privilege-escalation)

[GitHub - GhostPack/ForgeCert: "Golden" certificates](https://github.com/GhostPack/ForgeCert)

[Cyberwox Academy | Cybersecurity Community](https://www.cyberwoxacademy.com/)

[How to Install · JPCERTCC/MalConfScan Wiki · GitHub](https://github.com/JPCERTCC/MalConfScan/wiki/how-to-install)

[DogWhisperer’s SharpHound Cheat Sheet – Insinuator.net](https://insinuator.net/2021/05/dogwhisperers-sharphound-cheat-sheet/)

[GitHub - CMatri/Gotato: Generic impersonation and privilege escalation with Golang. Like GenericPotato both named pipes and HTTP are supported.](https://github.com/CMatri/Gotato)

[Detecting DNS Tunnels with Packetbeat and Watcher | Elastic Blog](https://www.elastic.co/blog/detecting_dns_tunnels_with_packetbeat_and_watcher)

[GitHub - dirkjanm/ROADtools: The Azure AD exploration framework.](https://github.com/dirkjanm/ROADtools)

[Twitch](https://m.twitch.tv/clip/WildScrumptiousGarbageHotPokket-ayXXnsI-LuNXoveS)

[5 ways to check if a Port is open on a remote Linux PC | FOSS Linux](https://www.fosslinux.com/35730/5-ways-to-check-if-a-port-is-open-on-a-remote-linux-pc.htm)

[GitHub - Sentinel-One/CobaltStrikeParser](https://github.com/Sentinel-One/CobaltStrikeParser)

[FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild - The Citizen Lab](https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/)

[GitHub - JoelGMSec/Invoke-DNSteal: Simple & Customizable DNS Data Exfiltrator](https://github.com/JoelGMSec/Invoke-DNSteal)

[Active Directory Checklist - Attack & Defense Cheatsheet](https://cybersecuritynews-com.cdn.ampproject.org/c/s/cybersecuritynews.com/active-directory-checklist/?amp)

[IAM Vulnerable - An AWS IAM Privilege Escalation Playground](https://labs.bishopfox.com/tech-blog/iam-vulnerable-an-aws-iam-privilege-escalation-playground)

[RedTeam-Tactics-and-Techniques/offensive-security at master · mantvydasb/RedTeam-Tactics-and-Techniques · GitHub](https://github.com/mantvydasb/RedTeam-Tactics-and-Techniques/tree/master/offensive-security)

[kubescape: testing if Kubernetes is deployed securely as defined in Kubernetes Hardening Guidance](https://securityonline.info/kubescape-kubernetes-hardening-guidance/)

[S.O.V.A. - A new Android Banking trojan with fowl intentions — ThreatFabric](https://www.threatfabric.com/blogs/sova-new-trojan-with-fowl-intentions.html)

[Admin’s Nightmare: Combining HiveNightmare/SeriousSAM and AD CS Attack Path’s for Profit - Black Hills Information Security](https://www.blackhillsinfosec.com/admins-nightmare-combining-hivenightmare-serioussam-and-ad-cs-attack-paths-for-profit/)

[From Pearl to Pegasus: Bahraini Government Hacks Activists with NSO Group Zero-Click iPhone Exploits - The Citizen Lab](https://citizenlab.ca/2021/08/bahrain-hacks-activists-with-nso-group-zero-click-iphone-exploits/)

[SIFT Workstation | SANS Institute](https://www.sans.org/tools/sift-workstation/)

[pagodo (Passive Google Dork) - Automate Google Hacking Database scraping and searching -](https://hakin9.org/pagodo-passive-google-dork-automate-google-hacking-database-scraping-and-searching/)

[Offensive Security Guide to SSH Tunnels and Proxies | by Russel Van Tuyl | Posts By SpecterOps Team Members](https://posts.specterops.io/offensive-security-guide-to-ssh-tunnels-and-proxies-b525cbd4d4c6)

[Entity Based Detection Engineering with BloodHound Enterprise | by Joshua Prager | Aug, 2021 | Posts By SpecterOps Team Members](https://posts.specterops.io/entity-based-detection-engineering-with-bloodhound-enterprise-b4dce3963d66)

[AV Evasion Part 2, The disk is lava · Hop Infosec](https://0xhop.github.io/evasion/2021/05/26/evasion-pt2/)

[GitHub - PetrusViet/CVE-2021-39115: Template Injection in Email Templates leads to code execution on Jira Service Management Server](https://github.com/PetrusViet/CVE-2021-39115)

[Objective-See's Blog](https://objective-see.com/blog/blog_0x67.html)

[CISSP PRACTICE QUESTIONS – 20211116 @ WUSON Private School](https://wentzwu.com/2021/11/16/cissp-practice-questions-20211116/)

[Understanding Cobalt Strike Profiles | ZeroSec - Adventures In Information Security](https://blog.zsec.uk/cobalt-strike-profiles/)

[Offensive Security Tool: Starkiller | Black Hat Ethical Hacking](https://www.blackhatethicalhacking.com/tools/starkiller/?__cf_chl_jschl_tk__=pmd_A72ppm4OtDi5OGqXtHTdt6kviwLRnZ15RdlhCvnTSCY-1630000895-0-gqNtZGzNAeWjcnBszQc9)

[How to start an AppSec program with the OWASP Top 10 - OWASP Top 10:2021 (DRAFT FOR PEER REVIEW)](https://owasp.org/Top10/A00_2021-How_to_start_an_AppSec_program_with_the_OWASP_Top_10/)

[GitHub - VoidSec/CVE-2020-1472: Exploit Code for CVE-2020-1472 aka Zerologon](https://github.com/VoidSec/CVE-2020-1472)

[IMAPLoginTester - a simple Python script that reads a text file with e-mails and passwords, and checks if those credentials are valid by logging to the respective IMAP](https://hakin9.org/imaplogintester-a-simple-python-script/)

[GitHub - threathunters-io/laurel: Transform Linux Audit logs for SIEM usage](https://github.com/threathunters-io/laurel)

[Active Directory Computer Account SMB Relaying Attack - Praetorian](https://www.praetorian.com/blog/active-directory-computer-account-smb-relaying-attack/)

[Cooking Malicious Documents with Cyberchef - Detect & Respond](https://www.socinvestigation.com/cooking-malicious-documents-with-cyberchef-detect-respond/)

[From RpcView to PetitPotam | itm4n's blog](https://itm4n.github.io/from-rpcview-to-petitpotam/)

[Cobalt Strike, a Defender's Guide](https://thedfirreport.com/2021/08/29/cobalt-strike-a-defenders-guide/)

[THOR Lite - Nextron Systems](https://www.nextron-systems.com/thor-lite/)

[WARCannon - catastrophically powerful parallel WARC processing -](https://hakin9.org/warcannon-catastrophically-powerful-parallel-warc-processing/)

[LittleCorporal: C# Automated Maldoc Generator • Penetration Testing](https://securityonline.info/littlecorporal-c-automated-maldoc-generator/)

[Pentest-Tools.com | 25+ Online Penetration Testing Tools](https://pentest-tools.com/home)

[Clickjacking Attack - How to Detect & Prevent this Attack ?](https://www.socinvestigation.com/clickjacking-attack-how-to-detect-prevent-this-attack/)

[10 Best Cyber Attack Simulation Tools For Organization Security 2021](https://cybersecuritynews-com.cdn.ampproject.org/c/s/cybersecuritynews.com/cyber-attack-simulation-tools/?amp)

[GitHub - Velocidex/velociraptor: Digging Deeper....](https://github.com/Velocidex/velociraptor)

[BITS for Script Kiddies | TrustedSec](https://www.trustedsec.com/blog/bits-for-script-kiddies/?utm_campaign=Blog%20Posts&utm_content=162204304&utm_medium=social&utm_source=linkedin&hss_channel=lcp-9478538)

[Lynis – Open source security auditing tool Detailed Explanation](https://gbhackers-com.cdn.ampproject.org/c/s/gbhackers.com/lynis-open-source-security-auditing-tool-a-detailed-explanation/amp/)

[Pentesting\_Active\_directory - XMind - Mind Mapping Software](https://www.xmind.net/m/5dypm8/)

[GitHub - 4n0nyx/bugBountyTools](https://github.com/4n0nyx/bugBountyTools)

[ICMP Attacks - Types & Codes For Log Analysis , Detection & Defense](https://www.socinvestigation.com/icmp-attacks-types-codes-for-log-analysis-detection-defense/)

[Post Compromise Active Directory Checklist – PwnDefend](https://www.pwndefend.com/2021/09/15/post-compromise-active-directory-checklist/)

[DNS Security: How to Reduce the Risk of a DNS Attack](https://gbhackers-com.cdn.ampproject.org/c/s/gbhackers.com/dns-security-risk-dns-attack/amp/)

[GitHub - rathbuna/DFIRMindMaps: A repository of DFIR-related Mind Maps geared towards the visual learners!](https://github.com/rathbuna/DFIRMindMaps)

[LockFile Ransomware Uses Never-Before Seen Encryption to Avoid Detection | Threatpost](https://threatpost.com/lockfile-ransomware-avoid-detection/169042/?)

[From Stranger to DA // Using PetitPotam to NTLM relay to Domain Administrator - TRUESEC Blog](https://blog.truesec.com/2021/08/05/from-stranger-to-da-using-petitpotam-to-ntlm-relay-to-active-directory/)

[Deception in Depth - LSASS Injection](https://blog.spookysec.net/DnD-LSASS-Injection/)

[GitHub - knqyf263/CVE-2021-40346: CVE-2021-40346 PoC (HAProxy HTTP Smuggling)](https://github.com/knqyf263/CVE-2021-40346)

[Investigating Kubernetes Attack Scenarios in Threat Stack (part 1) | Threat Stack](https://www.threatstack.com/blog/kubernetes-attack-scenarios-part-1)

[Netcat for Pentester](https://www.hackingarticles.in/netcat-for-pentester/)

[From Stranger to DA // Using PetitPotam to NTLM relay to Domain Administrator - TRUESEC Blog](https://blog.truesec.com/2021/08/05/from-stranger-to-da-using-petitpotam-to-ntlm-relay-to-active-directory/)

[Investigating Kubernetes Attack Scenarios in Threat Stack (part 2) | Threat Stack](https://www.threatstack.com/blog/investigating-kubernetes-attack-scenarios-in-threat-stack-part-2)

[Most Important A- Z Kali Linux Commands](https://ethicalhackersacademy.com/blogs/ethical-hackers-academy/kali-linux-commands)

[Android Pentesting Archives - GBHackers On Security](https://gbhackers.com/category/android/?_gl=1*1umgtca*_ga*YVV6VXhFTDMxOHVaaW5rVnF5VGFtd0VjbVlOZE5wVThPeDFFOUxGVnBjWE4xOHhQUlctS1dUMHJ6dW9mc0plSA..)

[Threat Alert: Mirai/Gafgyt Fork with New DDoS Modules Discovered - CUJO AI](https://cujo.com/mirai-gafgyt-with-new-ddos-modules-discovered/)

[Oh, Behave! Figuring Out User Behavior | TrustedSec](https://www.trustedsec.com/blog/oh-behave-figuring-out-user-behavior/)

[Offensive Security Tool: SniperPhish | Black Hat Ethical Hacking](https://www.blackhatethicalhacking.com/tools/sniperphish/?__cf_chl_managed_tk__=pmd_p13owe2abdWOK92d_dwVvDy_3szSDO0Pxt8WHBTwHAU-1631899093-0-gqNtZGzNArujcnBszRKl)

[[Atlassian Confluence CVE-2021–26084]::: The other side of bug report! | by PeterJson | Sep, 2021 | tradahacking](https://tradahacking.vn/atlassian-confluence-cve-2021-26084-the-other-side-of-bug-bounty-45ed19c814f6?gi=713f171907b0)

[Introduction - Red Team Notes](https://dmcxblue.gitbook.io/red-team-notes/)

[AnyDesk Silent Installation Detected · GitHub](https://gist.github.com/Shivammalaviya/5e9d133045c3b24d323c873e5ba8689a)

[Armourbird - Container Security Framework - Haxf4rall](https://haxf4rall.com/2019/09/04/armourbird-container-security-framework/)

[Ntlm\_Theft - A Tool For Generating Multiple Types Of NTLMv2 Hash Theft Files](https://www.kitploit.com/2021/09/ntlmtheft-tool-for-generating-multiple.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+PentestTools+(PenTest+Tools)&m=1)

[Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit](https://www.metasploit.com/)

[GitHub - AnErrupTion/LoGiC.NET: A more advanced free and open .NET obfuscator using dnlib.](https://github.com/AnErrupTion/LoGiC.NET)

[code white | Blog: RCE in Citrix ShareFile Storage Zones Controller (CVE-2021-22941) – A Walk-Through](https://codewhitesec.blogspot.com/2021/09/citrix-sharefile-rce-cve-2021-22941.html?m=1)

[Nebula - Cloud C2 Framework, which offers reconnaissance, enumeration, exploitation, post exploitation on AWS -](https://hakin9.org/nebula-cloud-c2-framework-which-offers-reconnaissance-enumeration-exploitation-post-exploitation-on-aws/)

[GitHub - FortyNorthSecurity/EDD: Enumerate Domain Data](https://github.com/FortyNorthSecurity/EDD)

[What is Spoofing? How It Works? - Cyber Security News](https://cybersecuritynews.com/spoofing/?amp)

[Burp Suite and Beyond: Exploring non-HTTP protocols using MITM\_RELAY | JUMPSEC LABS](https://labs.jumpsec.com/burpsuite-and-beyond/)

[Security Onion: Quick Malware Analysis: malware-traffic-analysis.net BazaCall-BazaLoader pcap from 2021-04-16](https://blog.securityonion.net/2021/08/quick-malware-analysis-malware-traffic_30.html?m=1)

[Indicator of Attack vs Indicator of Compromise | IOA vs IOC](https://www.youtube.com/watch?v=KPHVg-oeI9w)

[Creating the WhereAmI Cobalt Strike BOF - Boku](https://0xboku.com/2021/08/19/Bof-WhereAmI.html)

[CVE-2020-24581 D-Link DSL-2888A Remote Command Execution - Penetration Testing Tools, ML and Linux Tutorials](https://reconshell.com/cve-2020-24581-d-link-dsl-2888a-remote-command-execution/)

[GitHub - TheWover/CertStealer: A .NET tool for exporting and importing certificates without touching disk.](https://github.com/TheWover/CertStealer)

[h3xStream's blog: Emails Disclosure on WordPress](http://blog.h3xstream.com/2021/03/emails-disclosure-on-wordpress.html?m=1)

[Introducing: Azure Sentinel Data Exploration Toolset (ASDET) - Microsoft Tech Community](https://techcommunity.microsoft.com/t5/azure-sentinel/introducing-azure-sentinel-data-exploration-toolset-asdet/ba-p/2712728)

[How to analyze mobile malware: a Cabassous/FluBot Case study – NVISO Labs](https://blog.nviso.eu/2021/04/19/how-to-analyze-mobile-malware-a-cabassous-flubot-case-study/?amp)

[How DKIM SPF & DMARC Work to Prevent Email Spoofing and Phishing](https://www.socinvestigation.com/what-are-spf-dkim-and-dmarc-protection-against-spoofing-and-phishing/)

[ip-scripts/acl-converter.py at main · ddib-ccde/ip-scripts · GitHub](https://github.com/ddib-ccde/ip-scripts/blob/main/acl-converter.py)

[Unobtainium: Hack The Box Walkthrough](https://hackso.me/unobtainium-htb-walkthrough/)

[4 Open Source Tools to Add to Your Security Arsenal](https://www.darkreading.com/application-security/4-open-source-tools-to-add-to-your-security-arsenal/a/d-id/1340487?_mc=rss_x_drr_edt_aud_dr_x_x-rss-simple&utm_source=dlvr.it&utm_medium=linkedin)

[capa 2.0: Better, Faster, Stronger | FireEye Inc](https://www.fireeye.com/blog/threat-research/2021/07/capa-2-better-stronger-faster.html)

[Pentest-Tools-Collection/portscan.ps1 at main · LuemmelSec/Pentest-Tools-Collection · GitHub](https://github.com/LuemmelSec/Pentest-Tools-Collection/blob/main/tools/portscan.ps1)

[Offensive Security Tool: FFUF | Black Hat Ethical Hacking](https://www.blackhatethicalhacking.com/tools/ffuf/?__cf_chl_jschl_tk__=pmd_7Ssu07RZtbhe5acu_ZbhU0YlVZA_kXMEsB_31ndLIIs-1629514925-0-gqNtZGzNAeWjcnBszQdl)

[4 Free Easy Wins That Make Red Teams Harder | TrustedSec](https://www.trustedsec.com/blog/4-free-easy-wins-that-make-red-teams-harder/)

[DNSTake - A Fast Tool To Check Missing Hosted DNS Zones That Can Lead To Subdomain Takeover](https://www.kitploit.com/2021/09/dnstake-fast-tool-to-check-missing.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+PentestTools+%28PenTest+Tools%29)

[GitHub - mdecrevoisier/Windows-auditing-mindmap: Set of Mindmaps providing a detailed overview of the different #Windows auditing capacities and event log files.](https://github.com/mdecrevoisier/Windows-auditing-mindmap)

[Yuki Chan - Automated Penetration Testing and Auditing Tool](https://gbhackers.com/yuki-chan-automated-penetration-testing/)

[Using Reflection for AMSI Bypass - Intruder](https://www.redteam.cafe/red-team/powershell/using-reflection-for-amsi-bypass)

[GitHub - MartinSohn/Office-phish-templates](https://github.com/MartinSohn/Office-phish-templates)

[SQL Injection Scanner - Online Scan for SQL Injection (SQLi) Vulnerabilities | Pentest-Tools.com](https://pentest-tools.com/website-vulnerability-scanning/sql-injection-scanner-online)

[GitHub - angus-y/PyIris-backdoor: PyIris-backdoor is a modular, stealthy and flexible remote-access-toolkit written completely in python used to command and control other systems. It is now in the beta stage, possibly perpetually. There are bugs still pre](https://github.com/angus-y/PyIris-backdoor#getting-started)

[GitHub - sans-blue-team/DeepBlueCLI](https://github.com/sans-blue-team/DeepBlueCLI)

[AV Evasion Part 1 · Hop Infosec](https://0xhop.github.io/evasion/2021/04/19/evasion-pt1/)

[GitHub - lockedbyte/CVE-2021-40444: CVE-2021-40444 PoC](https://github.com/lockedbyte/CVE-2021-40444)

[GitHub - Azure/Stormspotter: Azure Red Team tool for graphing Azure and Azure Active Directory objects](https://github.com/Azure/Stormspotter)

[Cobalt Strike, a Defender's Guide](https://thedfirreport.com/2021/08/29/cobalt-strike-a-defenders-guide/)

[Labs | CyberDefenders® | Blue Team CTF Challenges](https://cyberdefenders.org/labs/)

[GitHub - wagiro/BurpBounty: Burp Bounty (Scan Check Builder in BApp Store) is a extension of Burp Suite that allows you, in a quick and simple way, to improve the active and passive scanner by means of personalized rules through a very intuitive graphical](https://github.com/wagiro/BurpBounty)

[Releases · beefproject/beef · GitHub](https://github.com/beefproject/beef/releases)

[GitHub - Aetsu/OffensivePipeline: OffensivePipeline allows to download, compile (without Visual Studio) and obfuscate C# tools for Red Team exercises.](https://github.com/Aetsu/OffensivePipeline)

[The difference between Powershell only & process specific AMSI bypasses | S3cur3Th1sSh1t](https://s3cur3th1ssh1t.github.io/Powershell-and-the-.NET-AMSI-Interface/)

[Practical Compromise Recovery Guidance for Active Directory – Microsoft 365 Security](https://m365internals.com/2021/04/27/practical-compromise-recovery-guidance-for-active-directory/amp/)

[GitHub - sensepost/ruler: A tool to abuse Exchange services](https://github.com/sensepost/ruler)

[Top 30+ Most Popular Red Team Tools (Updated 2021)](https://securitytrails.com/blog/red-team-tools)

[GitHub - duc-nt/RCE-0-day-for-GhostScript-9.50: RCE 0-day for GhostScript 9.50 - Payload generator](https://github.com/duc-nt/RCE-0-day-for-GhostScript-9.50)

[GitHub - oslabs-beta/KUR8: A visual overview of Kubernetes architecture and Prometheus metrics](https://github.com/oslabs-beta/KUR8)

[Mapping AD relationship using BloodHound | VK9 Security](https://vk9-sec.com/mapping-ad-relationship-using-bloodhound/)

[GitHub - APTortellini/unDefender: Killing your preferred antimalware by abusing native symbolic links and NT paths.](https://github.com/APTortellini/unDefender)

[Security Onion: Quick Malware Analysis: malware-traffic-analysis.net TA551/SHATHAK + URSNIF/GOZI/ISFB pcap from 2021-04-28](https://blog.securityonion.net/2021/08/quick-malware-analysis-malware-traffic_25.html?m=1)

[GitHub - bvoris/PSNetMon: PSNetMon - PowerShell Network Resource Monitoring Tool](https://github.com/bvoris/PSNetMon)

References

#1249583 Authenticated kubernetes principal with restricted permissions can retrieve ingress-nginx serviceaccount token and secrets across all namespaces

(99+) Post | LinkedIn

0-Day Hunting (Chaining Bugs/Methodology)

10 (more) free security tools worth a look | CSO Online

10 Best Cyber Attack Simulation Tools For Organization Security 2021

10 Best Free Penetration Testing Tools 2021 - Cyber Security News

10 Best Tools to Scan Linux Servers for Vulnerability & Malware

19 Powerful Penetration Testing Tools Used By Pros in 2021

4 Free Easy Wins That Make Red Teams Harder - TrustedSec

4 Free Easy Wins That Make Red Teams Harder | TrustedSec

4 Open Source Tools to Add to Your Security Arsenal

5 ways to check if a Port is open on a remote Linux PC | FOSS Linux

7 Threat Hunting Tools Everyone in the Industry Should Be Using | Cyborg Security

[Atlassian Confluence CVE-2021–26084]::: The other side of bug report! | by PeterJson | Sep, 2021 | tradahacking

bats3c/shad0w: A post exploitation framework designed to operate covertly on heavily monitored environments

Best Security Practices for Mitigating Secure Shell Attacks - Security Investigation

BHEH1337 - Twitch

BITS for Script Kiddies | TrustedSec

Blinding EDR On Windows - Red Team Blog

BloodHound-Tools/Ransomulator at main · zeronetworks/BloodHound-Tools · GitHub

Breaking The Browser - A tale of IPC, credentials and backdoors - MDSec

Building A Test Lab For Pentesting Guide | White Oak Security

Burp Suite and Beyond: Exploring non-HTTP protocols using MITM\_RELAY | JUMPSEC LABS

Bypassing Signature-Based AV | Red Siege Information Security

capa 2.0: Better, Faster, Stronger | FireEye Inc

Capoae Malware Attacking Linux systems & Web Apps

Chainsaw

CISSP PRACTICE QUESTIONS – 20211116 @ WUSON Private School

Clickjacking Attack - How to Detect & Prevent this Attack ?

Cloud Computing Penetration Testing Checklist & Important Considerations

Cobalt Strike, a Defender's Guide

code white | Blog: RCE in Citrix ShareFile Storage Zones Controller (CVE-2021-22941) – A Walk-Through

Comprehensive Guide to Local File Inclusion (LFI)

Compromising Email Supply Chains | CanIPhish

Cooking Malicious Documents with Cyberchef - Detect & Respond

Creating the WhereAmI Cobalt Strike BOF - Boku

Active Directory Checklist - Attack & Defense Cheatsheet

Active Directory Computer Account SMB Relaying Attack - Praetorian

Active Directory Enumeration With BloodHound

Active Directory Lab Setup Tool

CVE STALKER -The most viral CVE(vulnerability) ranking chart-

CVE-2020-24581 D-Link DSL-2888A Remote Command Execution - Penetration Testing Tools, ML and Linux Tutorials

Cyber Security Consulting & Testing | Pen Test Partners

Cyberwox Academy | Cybersecurity Community

AD CS relay attack - practical guide · Ex Android Dev

DarkSide - Tool Information Gathering & social engineering

DarkSide Ransomware Reverse Engineering - YouTube

Deception in Depth - LSASS Injection

Demon's Cries vulnerability (some NETGEAR smart switches) - gynvael.coldwind//vx.log

ADenum: find misconfiguration through the protocol LDAP

Detecting CONTI CobaltStrike Lateral Movement Techniques - Part 1 - CYB3RSN0RLAX

Detecting DNS Tunnels with Packetbeat and Watcher | Elastic Blog

Detecting LDAP enumeration and Bloodhound‘s Sharphound collector using AD Decoys | by Madhukar Raina | Securonix Tech Blog | Medium

Detecting Office365 Azure AD Environment Backdoors

DFIR-ORC · GitHub

The Difference Between a Vulnerability Assessment and a Penetration Test - Daniel Miessler

The difference between Powershell only & process specific AMSI bypasses | S3cur3Th1sSh1t

Admin’s Nightmare: Combining HiveNightmare/SeriousSAM and AD CS Attack Path’s for Profit - Black Hills Information Security

DNS Lookup Viewer for Windows 10

DNS Security: How to Reduce the Risk of a DNS Attack

DNS Shell - Tool to Compromise and Maintain control Over Victim Machine

DNSTake - A Fast Tool To Check Missing Hosted DNS Zones That Can Lead To Subdomain Takeover

Do Your Best Schoolwork Faster | Better Results With Grammarly

DogWhisperer’s SharpHound Cheat Sheet – Insinuator.net

Download | SonarQube

DracOS GNU/Linux Remastered

Drop support for Python 3.6 · Issue #238 · microsoft/msticpy · GitHub

Advance Mitre Threat Mapping - Attack Navigator & TRAM Tools

Dystopia - a low to medium multithreaded Ubuntu Core honeypot coded in Python -

EndpointManagement/OSD-ComboRadioFrontendHTA.ps1 at master · Love-A/EndpointManagement · GitHub

Entity Based Detection Engineering with BloodHound Enterprise | by Joshua Prager | Aug, 2021 | Posts By SpecterOps Team Members

Exploit in the Wild: #drupalgeddon2 - Analysis of CVE-2018-7600

Exploiting OAuth: Journey to Account Takeover | Bugs and Writeups

Farming for Red Teams: Harvesting NetNTLM - MDSec

FinFisher malware hijacks Windows Boot Manager with UEFI bootkit | Black Hat Ethical Hacking

The flexible management system | monday.com Work OS

FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild - The Citizen Lab

From AWAE to OSWE: The Preperation Guide – HanseSecure

From Pearl to Pegasus: Bahraini Government Hacks Activists with NSO Group Zero-Click iPhone Exploits - The Citizen Lab

From RpcView to PetitPotam | itm4n's blog

From Stranger to DA // Using PetitPotam to NTLM relay to Domain Administrator - TRUESEC Blog

Fsociety Hacking Tools Pack - A Penetration Testing Framework

GenesisBlock3301/product\_delivery\_fastapi: Product delivery api

GitHub - 0x727/JNDIExploit: 一款用于JNDI注入利用的工具，大量参考/引用了Rogue JNDI项目的代码，支持直接植入内存shell，并集成了常见的bypass 高版本JDK的方式，适用于与自动化工具配合使用。

GitHub - 0xInfection/TIDoS-Framework: The Offensive Manual Web Application Penetration Testing Framework.

GitHub - 3CORESec/MAL-CL: MAL-CL (Malicious Command-Line)

GitHub - 4n0nyx/bugBountyTools

GitHub - adstuart/azure-expressroute-migration: How to approach migrating from one ExpressRoute circuit to another ExpressRoute circuit, with a focus on methodical transition of the ExpressRoute Private Peering.

GitHub - Aetsu/OffensivePipeline: OffensivePipeline allows to download, compile (without Visual Studio) and obfuscate C# tools for Red Team exercises.

GitHub - ahmedkhlief/APT-Hunter: APT-Hunter is Threat Hunting tool for windows event logs which made by purple team mindset to provide detect APT movements hidden in the sea of windows event logs to decrease the time to uncover suspicious activity

GitHub - AlgoSecure/Pollenisator: Collaborative pentest tool with highly customizable tools

GitHub - AmirHoseinTangsiriNET/SSQAuto

GitHub - AnErrupTion/LoGiC.NET: A more advanced free and open .NET obfuscator using dnlib.

GitHub - angus-y/PyIris-backdoor: PyIris-backdoor is a modular, stealthy and flexible remote-access-toolkit written completely in python used to command and control other systems. It is now in the beta stage, possibly perpetually. There are bugs still pre

GitHub - ANSSI-FR/DFIR-O365RC: PowerShell module for Office 365 and Azure log collection

GitHub - AppThreat/dep-scan: Fully open-source security audit for project dependencies based on known vulnerabilities and advisories. Supports both local repos and container images. Integrates with various CI environments such as Azure Pipelines, CircleCI

GitHub - APTortellini/unDefender: Killing your preferred antimalware by abusing native symbolic links and NT paths.

GitHub - Arinerron/heaptrace: helps visualize heap operations for pwn and debugging

GitHub - austinsonger/Incident-Playbook: GOAL: Incident Response Playbooks Mapped to MITRE Attack Tactics and Techniques. [Contributors Friendly]

GitHub - Azure/Stormspotter: Azure Red Team tool for graphing Azure and Azure Active Directory objects

GitHub - bigb0sss/RedTeam-OffensiveSecurity: Tools & Interesting Things for RedTeam Ops

GitHub - bmuschko/ckad-crash-course: In-depth and hands-on practice for acing the exam.

GitHub - boku7/spawn: Cobalt Strike BOF that spawns a sacrificial process, injects it with shellcode, and executes payload. Built to evade EDR/UserLand hooks by spawning sacrificial process with Arbitrary Code Guard (ACG), BlockDll, and PPID spoofing.

GitHub - brightio/penelope: Penelope Shell Handler

GitHub - bvoris/PSNetMon: PSNetMon - PowerShell Network Resource Monitoring Tool

GitHub - byt3bl33d3r/CrackMapExec: A swiss army knife for pentesting networks

GitHub - c6fc/npk: A mostly-serverless distributed hash cracking platform

GitHub - carlospolop/PEASS-ng: PEASS - Privilege Escalation Awesome Scripts SUITE (with colors)

GitHub - cert-ee/cuckoo3: Cuckoo 3 is a Python 3 open source automated malware analysis system.

GitHub - chvancooten/OSEP-Code-Snippets: A repository with my notable code snippets for Offensive Security's PEN-300 (OSEP) course.

GitHub - Cloud-Architekt/AzureAD-Attack-Defense: This publication is a collection of various common attack scenarios on Azure Active Directory and how they can be mitigated or detected.

GitHub - cloudquery/cloudquery: The open-source cloud asset inventory powered by SQL.

GitHub - CMatri/Gotato: Generic impersonation and privilege escalation with Golang. Like GenericPotato both named pipes and HTTP are supported.

GitHub - cobbr/PSAmsi: PSAmsi is a tool for auditing and defeating AMSI signatures.

GitHub - codeyourweb/fastfinder: Incident Response - Fast suspicious file finder

GitHub - COSSAS/dgad: DGA Detective

GitHub - countercept/chainsaw: Rapidly Search and Hunt through Windows Event Logs

GitHub - CravateRouge/bloodyAD: BloodyAD is an Active Directory Privilege Escalation Framework

GitHub - CrowdStrike/automactc: AutoMacTC: Automated Mac Forensic Triage Collector

GitHub - CyberSecurityUP/Awesome-Blue-Team-Operations

GitHub - CyberSecurityUP/Awesome-Cloud-PenTest

(1970). *Awesome-Malware-Analysis-Reverse-Engineering.*

GitHub - CyberSecurityUP/Awesome-Red-Team-Operations

GitHub - CyberSecurityUP/eCXD-Preparation: eLearnSecurity Certified Exploit Development

GitHub - CyberSecurityUP/eWPTX-Preparation

GitHub - CyberSecurityUP/OSCE-Complete-Guide: OSWE, OSEP, OSED

GitHub - CyberSecurityUP/OSCP-Survival-Guide

GitHub - D4RK-4RMY/DARKARMY: DARKARMY Hacking Tools Pack - A Penetration Testing Framework .

GitHub - darkquasar/AzureHunter: A Cloud Forensics Powershell module to run threat hunting playbooks on data from Azure and O365

GitHub - derv82/wifite2: Rewrite of the popular wireless network auditor, "wifite"

GitHub - dfirtrack/dfirtrack: DFIRTrack - The Incident Response Tracking Application

GitHub - Dheerajmadhukar/karma\_v2: ⡷⠂𝚔𝚊𝚛𝚖𝚊 𝚟𝟸⠐⢾ is a Passive Open Source Intelligence (OSINT) Automated Reconnaissance (framework)

GitHub - dhondta/dronesploit: Drone pentesting framework console

GitHub - dievus/lnkbomb: Malicious shortcut generator for collecting NTLM hashes from insecure file shares.

GitHub - dirkjanm/ROADtools: The Azure AD exploration framework.

GitHub - duc-nt/RCE-0-day-for-GhostScript-9.50: RCE 0-day for GhostScript 9.50 - Payload generator

GitHub - f0wl/MalwareLab\_VM-Setup: Setup scripts for my Malware Analysis VMs

GitHub - Fahrj/reverse-ssh: Statically-linked ssh server with reverse shell functionality for CTFs and such

GitHub - feihong-cs/JNDIExploit: A malicious LDAP server for JNDI injection attacks

GitHub - floodsung/Deep-Learning-Papers-Reading-Roadmap: Deep Learning papers reading roadmap for anyone who are eager to learn this amazing tech!

GitHub - ForbiddenProgrammer/conti-pentester-guide-leak: Leaked pentesting manuals given to Conti ransomware crooks

GitHub - FortyNorthSecurity/EDD: Enumerate Domain Data

GitHub - foyzulkarim/linux-playbook

GitHub - frankwxu/digital-forensics-lab: Free hands-on digital forensics labs for students and faculty

GitHub - GhostPack/ForgeCert: "Golden" certificates

GitHub - GhostPack/PSPKIAudit: PowerShell toolkit for AD CS auditing based on the PSPKI toolkit.

GitHub - goichot/CVE-2020-3433: PoCs and technical analysis of three vulnerabilities found on Cisco AnyConnect for Windows: CVE-2020-3433, CVE-2020-3434 and CVE-2020-3435

GitHub - Gopro336/PSA-MINERCRAFT-RCE-EXPLOIT: Minecraft exploit allowing remote code execution via Minecraft chat

GitHub - gquere/pwn\_jenkins: Notes about attacking Jenkins servers

GitHub - hak5/omg-payloads

GitHub - hashtaginfosec/vagrantlab: Testing out vagrant to spin up an AD lab

GitHub - HightechSec/scarce-apache2: A framework for bug hunting or pentesting targeting websites that have CVE-2021-41773 Vulnerability in public

GitHub - hoppscotch/hoppscotch: 👽 Open source API development ecosystem https://hoppscotch.io

GitHub - horsicq/Detect-It-Easy: Program for determining types of files for Windows, Linux and MacOS.

GitHub - horsicq/Nauz-File-Detector: Linker/Compiler/Tool detector for Windows, Linux and MacOS.

GitHub - HyCraftHD/Log4J-RCE-Proof-Of-Concept: Log4j-RCE (CVE-2021-44228) Proof of Concept with additional information

GitHub - iamthefrogy/frogy: My subdomain enumeration script. It's unique in the way it is built upon.

GitHub - Ignitetechnologies/HackTheBox-CTF-Writeups: This cheasheet is aimed at the CTF Players and Beginners to help them sort Hack The Box Labs on the basis of Operating System and Difficulty.

GitHub - Ignitetechnologies/Wireless-Penetration-Testing

GitHub - inodee/threathunting-spl: Splunk code (SPL) for serious threat hunters and detection engineers.

GitHub - intelowlproject/IntelOwl: Intel Owl: analyze files, domains, IPs in multiple ways from a single API at scale

GitHub - iphelix/dnschef: DNSChef - DNS proxy for Penetration Testers and Malware Analysts

GitHub - its-a-feature/Mythic: A collaborative, multi-platform, red teaming framework

GitHub - IvanGlinkin/AutoSUID: AutoSUID application is the Open-Source project, the main idea of which is to automate harvesting the SUID executable files and to find a way for further escalating the privileges.

GitHub - jafarlihi/serpentine: C++/Win32/Boost Windows RAT (Remote Administration Tool) with a multiplatform Java/Spring RESTful C2 server and Go, C++/Qt5 frontends

GitHub - jas502n/Log4j2-CVE-2021-44228: Remote Code Injection In Log4j

GitHub - JavierOlmedo/OWASP-Calculator: 🧮 An online calculator to assess the risk of web vulnerabilities based on OWASP Risk Assessment

GitHub - JoelGMSec/Invoke-DNSteal: Simple & Customizable DNS Data Exfiltrator

GitHub - kacos2000/Evtx\_Log\_Browser: Evtx Log (xml) Browser

GitHub - kacos2000/MFT\_Browser: $MFT directory tree reconstruction & record info

GitHub - Kevin-Robertson/Sharpmad: C# version of Powermad

GitHub - kitabisa/mubeng: An incredibly fast proxy checker & IP rotator with ease.

GitHub - klezVirus/CandyPotato: Pure C++, weaponized, fully automated implementation of RottenPotatoNG

GitHub - klinix5/InstallerFileTakeOver

GitHub - knqyf263/CVE-2021-40346: CVE-2021-40346 PoC (HAProxy HTTP Smuggling)

GitHub - LeCoqHardi/WolverineFramework: WolverineFramework - Free, OpenSource and easy to use Cybersecurity Framework.

GitHub - Lipton2777/cloud-nuke: A tool for cleaning up your cloud accounts by nuking (deleting) all resources within it

GitHub - lockedbyte/CVE-2021-40444: CVE-2021-40444 PoC

GitHub - logpresso/CVE-2021-44228-Scanner: Vulnerability scanner and mitigation patch for Log4j2 CVE-2021-44228

GitHub - ly4k/CallbackHell: PoC (DoS) for CVE-2021-40449 - Win32k Elevation of Privilege Vulnerability (LPE)

GitHub - Mamun-swe/Node\_mssql\_crud\_api: Node.JS and MSSQL CRUD API application.

GitHub - MartinSohn/Office-phish-templates

GitHub - matamorphosis/Scrummage: The Ultimate OSINT and Threat Hunting Framework

GitHub - Matheus-Garbelini/braktooth\_esp32\_bluetooth\_classic\_attacks: A Series of Baseband & LMP Exploits against Bluetooth Classic Controllers

GitHub - mdecrevoisier/Windows-auditing-mindmap: Set of Mindmaps providing a detailed overview of the different #Windows auditing capacities and event log files.

GitHub - mgeeky/ShellcodeFluctuation: An in-memory evasion technique fluctuating shellcode memory protection between RW & RX and encrypting/decrypting contents

GitHub - mitre/caldera: Scalable Automated Adversary Emulation Platform

GitHub - mufeedvh/moonwalk: Cover your tracks during Linux Exploitation by leaving zero traces on system logs and filesystem timestamps. 👻🐚

GitHub - Narasimha1997/fake-sms: A simple command line tool using which you can skip phone number based SMS verification by using a temporary phone number that acts like a proxy.

GitHub - Neo23x0/log4shell-detector: Detector for Log4Shell exploitation attempts

GitHub - nsacyber/Hardware-and-Firmware-Security-Guidance: Guidance for the Spectre, Meltdown, Speculative Store Bypass, Rogue System Register Read, Lazy FP State Restore, Bounds Check Bypass Store, TLBleed, and L1TF/Foreshadow vulnerabilities as well as

GitHub - nyxgeek/o365recon: retrieve information via O365 and AzureAD with a valid cred

GitHub - OALabs/hashdb-ida: HashDB API hash lookup plugin for IDA Pro

GitHub - ollypwn/PrintNightmare: Python implementation for PrintNightmare (CVE-2021-1675 / CVE-2021-34527)

GitHub - OmerYa/Invisi-Shell: Hide your Powershell script in plain sight. Bypass all Powershell security features

GitHub - optiv/Ivy: Ivy is a payload creation framework for the execution of arbitrary VBA (macro) source code directly in memory. Ivy’s loader does this by utilizing programmatical access in the VBA object environment to load, decrypt and execute shellcode.

GitHub - oslabs-beta/KUR8: A visual overview of Kubernetes architecture and Prometheus metrics

GitHub - outflanknl/PrintNightmare

GitHub - OWASP/owasp-mstg: The Mobile Security Testing Guide (MSTG) is a comprehensive manual for mobile app security development, testing and reverse engineering.

GitHub - OWASP/Python-Honeypot: OWASP Honeypot, Automated Deception Framework.

GitHub - p0dalirius/LDAPmonitor: Monitor creation, deletion and changes to LDAP objects live during your pentest or system administration!

GitHub - p3nt4/PowerShdll: Run PowerShell with rundll32. Bypass software restrictions.

GitHub - penetrarnya-tm/WeaponizeKali.sh: Automate installation of extra pentest tools on Kali Linux

GitHub - PetrusViet/CVE-2021-39115: Template Injection in Email Templates leads to code execution on Jira Service Management Server

GitHub - praetorian-inc/trident: automated password spraying tool

GitHub - punk-security/pwnspoof

GitHub - rathbuna/DFIRMindMaps: A repository of DFIR-related Mind Maps geared towards the visual learners!

GitHub - RedCursorSecurityConsulting/PPLKiller: Tool to bypass LSA Protection (aka Protected Process Light)

GitHub - rung/threat-matrix-cicd: Threat matrix for CI/CD Pipeline

GitHub - S3cur3Th1sSh1t/MultiPotato

GitHub - S3cur3Th1sSh1t/WinPwn: Automation for internal Windows Penetrationtest / AD-Security

GitHub - S4R1N/AlternativeShellcodeExec: Alternative Shellcode Execution Via Callbacks

GitHub - sans-blue-team/DeepBlueCLI

GitHub - seajaysec/cypheroth: Automated, extensible toolset that runs cypher queries against Bloodhound's Neo4j backend and saves output to spreadsheets.

GitHub - sensepost/ruler: A tool to abuse Exchange services

GitHub - Sentinel-One/CobaltStrikeParser

GitHub - shubham0d/UAC-bypass-using-dll-injection: A small project to bypass UAC in windows 10/8/7 using dll injection technique

GitHub - SimpleBoilerplates/Flutter: A boilerplate project for Flutter using RiverPod, Dio, auto\_route, Freezed and generated with very\_good\_cli

GitHub - six2dez/reconftw: reconFTW is a tool designed to perform automated recon on a target domain by running the best set of tools to perform scanning and finding out vulnerabilities

GitHub - sottlmarek/DevSecOps: Ultimate DevSecOps library

GitHub - stuhli/awesome-event-ids: Collection of Event ID ressources useful for Digital Forensics and Incident Response

GitHub - summitt/burp-ysoserial: YSOSERIAL Integration with burp suite

(2020). *superhero1 / OSCP-Prep.*

GitHub - t94j0/gophish-notifier: Notification webhook for GoPhish

GitHub - tanc7/EXOCET-AV-Evasion: EXOCET - AV-evading, undetectable, payload delivery tool

GitHub - TheWover/CertStealer: A .NET tool for exporting and importing certificates without touching disk.

GitHub - thiagomayllart/Harvis: Harvis is designed to automate your C2 Infrastructure.

GitHub - thomast1906/DevOps-The-Hard-Way-Azure: This repository contains free labs for setting up an entire workflow and DevOps environment from a real-world perspective in Azure

GitHub - threathunters-io/laurel: Transform Linux Audit logs for SIEM usage

GitHub - tokyoneon/Chimera: Chimera is a PowerShell obfuscation script designed to bypass AMSI and commercial antivirus solutions.

GitHub - TRSTN4/EagleShell: EagleShell is a high-quality tool that aims to improve your pentest.

GitHub - ufrisk/MemProcFS: The Memory Process File System

GitHub - usnistgov/oscal-content: NIST SP 800-53 content and other OSCAL content examples

GitHub - VbScrub/Rubeus-GUI: GUI alternative to the Rubeus command line tool, for all your Kerberos exploit requirements

GitHub - Velocidex/velociraptor: Digging Deeper....

GitHub - Vinum-Security/kubernetes-security-checklist: Kubernetes Security Checklist and Requirements - All in One (authentication, authorization, logging, secrets, configuration, network, workloads, dockerfile)

GitHub - VoidSec/CVE-2020-1472: Exploit Code for CVE-2020-1472 aka Zerologon

GitHub - wagga40/Zircolite: A standalone SIGMA-based detection tool for EVTX.

GitHub - wagiro/BurpBounty: Burp Bounty (Scan Check Builder in BApp Store) is a extension of Burp Suite that allows you, in a quick and simple way, to improve the active and passive scanner by means of personalized rules through a very intuitive graphical

GitHub - waleedassar/RestrictedKernelLeaks

GitHub - waydroid/waydroid

GitHub - welk1n/JNDI-Injection-Exploit: JNDI注入测试工具（A tool which generates JNDI links can start several servers to exploit JNDI Injection vulnerability,like Jackson,Fastjson,etc）

GitHub - xct/xc: A small reverse shell for Linux & Windows

GitHub - xFreed0m/RDPassSpray: Python3 tool to perform password spraying using RDP

GitHub - YfryTchsGD/Log4jAttackSurface

Go-Shellcode : A Repository Of W S R And Supporting Utilities.

Golden Certificate – Penetration Testing Lab

Grype - Vulnerability Scanner For Container Images & Filesystems

Guarding against DCSync attacks - Help Net Security

guelfoweb/knock: Knock Subdomain Scan

h3xStream's blog: Emails Disclosure on WordPress

Hack The Box: Hacking Training For The Best | Individuals & Companies

Hacker Associate - Cyber Security Training, Certification and Services

Hacking CloudKit - How I accidentally deleted your Apple Shortcuts - Detectify Labs

Hardware Penetration Testing tools - SecureTechware

Hiding Your Syscalls | PassTheHashBrowns

How DKIM SPF & DMARC Work to Prevent Email Spoofing and Phishing

How to analyze mobile malware: a Cabassous/FluBot Case study – NVISO Labs

How to apply Sun Tzu’s ‘The Art of War’ to cybersecurity | Security Magazine

How to Install · JPCERTCC/MalConfScan Wiki · GitHub

How to start an AppSec program with the OWASP Top 10 - OWASP Top 10:2021 (DRAFT FOR PEER REVIEW)

How to Tackle SaaS Security Misconfigurations

https://osint.link/

Huan: Encrypted PE Loader Generator • Penetration Testing

Hunt the Beasts in the Bits A Proactive Approach | Meisam Eslahi | BSides Singapore Conference 2021

Hunting Malware in Process Memory | Icegrave

IAM Vulnerable - An AWS IAM Privilege Escalation Playground

ICMP Attacks - Types & Codes For Log Analysis , Detection & Defense

IMAPLoginTester - a simple Python script that reads a text file with e-mails and passwords, and checks if those credentials are valid by logging to the respective IMAP

ImpulsiveDLLHijack - C# Based Tool Which Automates The Process Of Discovering And Exploiting DLL Hijacks In Target Binaries

IMQ Minded Security Blog: A Journey Into the Beauty of DNSRebinding - Part 2

Indicator of Attack vs Indicator of Compromise | IOA vs IOC

Inf0sec - Initial Access - File Smuggling

Information Technology Sector | CISA

infosec-jupyterthon/workshops/2021 at master · OTRF/infosec-jupyterthon · GitHub

Initial Access Broker Landscape

Initial-Access-Broker-Landscape/InitialAccessBrokers.png at main · curated-intel/Initial-Access-Broker-Landscape · GitHub

Inside TeamTNT’s Impressive Arsenal

Introducing: Azure Sentinel Data Exploration Toolset (ASDET) - Microsoft Tech Community

Introduction - Red Team Notes

Introduction - Red Team Notes 2.0

Introduction — Threat Hunter Playbook

Intrusion Prevention System(IPS) and Its Detailed Function - SOC/SIEM

Investigating an Office 365 account compromise – CIAOPS

Investigating Kubernetes Attack Scenarios in Threat Stack (part 1) | Threat Stack

Investigating Kubernetes Attack Scenarios in Threat Stack (part 2) | Threat Stack

Invoke-winPEAS - Empire Module - InfosecMatter

ip-scripts/acl-converter.py at main · ddib-ccde/ip-scripts · GitHub

Aircrack-ng

IronNetTR/cobalt\_strike at main · IronNetCybersecurity/IronNetTR · GitHub

IRP-Phishing · main · Public Incident Response Ressources / Public Playbooks · GitLab

Airstrike Attack - FDE bypass and EoP on domain joined Windows workstations (CVE-2021-28316) | Shenanigans Labs

John the Ripper password cracker

Justin Bieber Linux

Karma\_V2 - A Passive Open Source Intelligence (OSINT) Automated Reconnaissance (Framework)

Keytap2 - acoustic keyboard eavesdropping based on language n-gram frequencies · Discussion #31 · ggerganov/kbd-audio · GitHub

Kit\_Hunter - A Basic Phishing Kit Scanner For Dedicated And Semi-Dedicated Hosting

KitPloit - PenTest & Hacking Tools

knight0x07/ImpulsiveDLLHijack: C# based tool which automates the process of discovering and exploiting DLL Hijacks in target binaries. The Hijacked paths discovered can later be weaponized during Red Team Operations to evade EDR's.

Known Exploited Vulnerabilities Catalog | CISA

kubescape: testing if Kubernetes is deployed securely as defined in Kubernetes Hardening Guidance

Labs | CyberDefenders® | Blue Team CTF Challenges

LFI Cheat Sheet

Linux-CatScale IR Collection Script • Penetration Testing

LittleCorporal: C# Automated Maldoc Generator • Penetration Testing

LockFile Ransomware Uses Never-Before Seen Encryption to Avoid Detection | Threatpost

Log4Shell Scanner - PortSwigger

Login | Let's Defend

Lynis – Open source security auditing tool Detailed Explanation

MacOS Security & Privilege Escalation - HackTricks

Malware Analysis Use Cases with ANY.RUN Sandbox

Mama Always Told Me Not to Trust Strangers without Certificates

mandiant/commando-vm: Complete Mandiant Offensive VM (Commando VM), a fully customizable Windows-based pentesting virtual machine distribution. commandovm@fireeye.com

Mapping AD relationship using BloodHound | VK9 Security

Masscan -Worlds Fastest Scanner - Scan the Entire Internet Under 6 Min

Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit

Microsoft-Defender-for-Cloud/Workbooks/AzureSecurityBenchmark at main · Azure/Microsoft-Defender-for-Cloud · GitHub

Microsoft-Defender-for-Cloud/Workbooks/Network Security Dashboard at main · Azure/Microsoft-Defender-for-Cloud · GitHub

Mind Maps | Never Ending Security

The Mirai Botnet – Threats and Mitigations

Most Common Windows Event IDs to Hunt - Mind Map

Most Important A- Z Kali Linux Commands

Most Important Android Application Penetration Testing Checklist

Android Pentesting Archives - GBHackers On Security

Android Rat - An Advanced Hacking Tool to Hack Targeted Android Phone

Nebula - Cloud C2 Framework, which offers reconnaissance, enumeration, exploitation, post exploitation on AWS -

NERVE - Network Exploitation, Reconnaissance & Vulnerability Engine

Netcat for Pentester

Network traffic analysis using Wireshark | AT&T Cybersecurity

Networkit - A Growing Open-Source Toolkit For Large-Scale Network Analysis

Nim on the Attack: Process Injection Using Nim and the Windows API – HuskyHacks

No Logs? No Problem! Incident Response without Windows Event Logs - JUMPSEC LABS

NTLM Relaying via Cobalt Strike – Rasta Mouse

Ntlm\_Theft - A Tool For Generating Multiple Types Of NTLMv2 Hash Theft Files

AnyDesk Silent Installation Detected · GitHub

Obfuscating Malicious Macro-Enabled Word Docs

Objective-See's Blog

Offensive Security Guide to SSH Tunnels and Proxies | by Russel Van Tuyl | Posts By SpecterOps Team Members

Offensive Security Tool: Discover | Black Hat Ethical Hacking

Offensive Security Tool: DotDotPwn – The Directory Traversal Fuzzer | Black Hat Ethical Hacking

Offensive Security Tool: FFUF | Black Hat Ethical Hacking

Offensive Security Tool: GoMapEnum | Black Hat Ethical Hacking

Offensive Security Tool: Hashcat | Black Hat Ethical Hacking

Offensive Security Tool: Jenkins Attack Framework | Black Hat Ethical Hacking

Offensive Security Tool: log4j-scan | Black Hat Ethical Hacking

Offensive Security Tool: Pentesting Tools | Black Hat Ethical Hacking

Offensive Security Tool: SniperPhish | Black Hat Ethical Hacking

Offensive Security Tool: Starkiller | Black Hat Ethical Hacking

Offensive Security Tool: URL Hunter | Black Hat Ethical Hacking

Offensive WMI - Exploring Namespaces, Classes & Methods (Part 2) :: 0xInfection's Blog — Random ramblings of an Infected Geek.

The Official Social Engineering Hub - Security Through Education

Oh, Behave! Figuring Out User Behavior | TrustedSec

Online - Reverse Shell Generator

San Francisco, CA *Open Source Security Foundation (OpenSSF).*

Orbitaldump - a simple multi-threaded distributed SSH brute-forcing tool written in Python

OSINT Tool: Osintgram | Black Hat Ethical Hacking

OWASP Zed Attack Proxy How-To

p0f - A Forensics Tool for Passive Traffic Analysis OS Fingerprinting

pagodo (Passive Google Dork) - Automate Google Hacking Database scraping and searching -

Parrot Security

peirates: Kubernetes Penetration Testing tool • Penetration Testing

Pentest Box

Pentest oriented collaborative tool - Smersh documentation

Pentest-Tools-Collection/portscan.ps1 at main · LuemmelSec/Pentest-Tools-Collection · GitHub

Pentest-Tools.com | 25+ Online Penetration Testing Tools

Pentesting\_Active\_directory - XMind - Mind Mapping Software

PeTeReport - open-source application vulnerability reporting tool

PeTeReport - PeTeReport

Photon - Incredibly fast crawler designed for OSINT

Positive Technologies - vulnerability assessment, compliance management and threat analysis solutions

Post Compromise Active Directory Checklist – PwnDefend

PR0CESS/miniGhosting at main · aaaddress1/PR0CESS

Practical Compromise Recovery Guidance for Active Directory – Microsoft 365 Security

Process Lineage Analysis - Technique D3-PLA | MITRE D3FEND™

PT Network Attack Discovery

APT-Hunter - Threat Hunting Tool For Windows Event Logs

APT-Hunter V2.0 - Threat Hunting Tool For Windows Event Logs

Public SSH keys can leak your private infrastructure | Artem Golubin

Publications | Outflank

rapid7 - Vagrant Cloud

Realtek HD Audio Driver Package - DLL Preloading and Potential Abuses

RedTeam-Tactics-and-Techniques/offensive-security at master · mantvydasb/RedTeam-Tactics-and-Techniques · GitHub

Release age v1.0.0 🏁 · FiloSottile/age · GitHub

Release DRAKVUF Sandbox v0.17.0 · CERT-Polska/drakvuf-sandbox · GitHub

Release Pre-Release: RiskIQ, Sentinel Incident Explorer, Kusto and MS Defender · microsoft/msticpy · GitHub

Release v1.3 · FourCoreLabs/EDRHunt · GitHub

Release v1.6.1 - Sentinel APIs, Folium, VirusTotal, ProcessTree, and more · microsoft/msticpy · GitHub

Releases · beefproject/beef · GitHub

Releases · horsicq/DIE-engine · GitHub

Reverse engineering and decrypting CyberArk vault credential files – NCC Group Research

Reverse Shell Generator by Ryan Montgomery

Armourbird - Container Security Framework - Haxf4rall

Router Security

S.O.V.A. - A new Android Banking trojan with fowl intentions — ThreatFabric

saeeddhqan's profile - asciinema

Scorpiones Group | Lateral Movement using DCOM Objects - Guide to using DCOM Objects in order to Move Laterally in the Network.

Security Automation and Orchestration - Theat Intelligence

Security Onion: Quick Malware Analysis: malware-traffic-analysis.net BazaCall-BazaLoader pcap from 2021-04-16

Security Onion: Quick Malware Analysis: malware-traffic-analysis.net TA551/SHATHAK + URSNIF/GOZI/ISFB pcap from 2021-04-28

SIEM Monitoring using Wazuh by Francis Jeremiah

SIFT Workstation | SANS Institute

Silent Breach - Cyber Security Experts

Spraykatz - retrieve credentials on Windows machines

SQL Injection Scanner - Online Scan for SQL Injection (SQLi) Vulnerabilities | Pentest-Tools.com

SSH Sniffing (SSH Spying) Methods and Defense - InfosecMatter

start [hashcat wiki]

t94j0/gophish-notifier: Notification webhook for GoPhish

Taking Hunting to the Next Level: Hunting in Memory - SANS Threat Hunting Summit 2017 - YouTube

THC-Hydra | Penetration Testing Tools

This is how I bypassed almost every EDR! | by Omri Baso | Nov, 2021 | Medium

THOR Lite - Nextron Systems

Threat Alert: Mirai/Gafgyt Fork with New DDoS Modules Discovered - CUJO AI

Threat Hunting and Detection with Web Proxy Logs | by Mehmet Ergene | Medium

Threat Hunting AWS CloudTrail with Sentinel: Part 3 - Binary Defense

Tools - Intelligence X

Top 30+ Most Popular Red Team Tools (Updated 2021)

Tor Rootkit: Python 3 standalone Windows 10 / Linux Rootkit

toutatis: extract information from instagrams accounts such as e-mails, phone numbers

Trape OSINT tool: People tracker on the Internet

TruffleHog — Truffle Security

TryHackMe | CC: Pen Testing

Twitch

Audit Azure Web App against NotLegit vulnerability -Notes of Azure Security + Governance

The Ultimate Guide to Vulnerability Scanning

Understanding Cobalt Strike Profiles | ZeroSec - Adventures In Information Security

Unobtainium: Hack The Box Walkthrough

Using Reflection for AMSI Bypass - Intruder

AV Evasion Part 1 · Hop Infosec

AV Evasion Part 2, The disk is lava · Hop Infosec

Vulnerability Assessment & Penetration Testing | Infocratus

Vulnerability Assessment and Penetration Testing

vx-underground

vx-underground.orghttps://tinyurl.com/ygtydr57https://tinyurl.com/yzuxt8dw - Pastebin.com

WARCannon - catastrophically powerful parallel WARC processing -

Warming Up. Using ATT&CK for Self Advancement - SOC Prime

Web Server Penetration Testing Checklist - GBHackers

Welcome to ThreatPursuit VM: A Threat Intelligence and Hunting Virtual Machine | Mandiant

What is a DDoS Attack? Why are DDoS Attacks Dangerous | Indusface

What is a Honeypot and How it Improves Network security?

What is an Evil Twin Attack - Example, Procedure, and Preventive Methods

What is AS-REP Roasting? | Cracking Active Directory Passwords

What is old is new again: The Relay Attack – SecureAuth

What is Spoofing? How It Works? - Cyber Security News

What’s the difference between a vulnerability assessment and a penetration test? - PGI

Windows & Active Directory Exploitation Cheat Sheet and Command Reference :: Cas van Cooten — I ramble about security stuff, mostly

Windows 11 Security. Our Hacker-in-Chief Runs Attacks and… | by Mechanics Team | Medium

Windows Management Instrumentation Attacks - Detection & Response

Winitor

Winshark - Wireshark plugin to work with Event Tracing for Windows

Wireshark Tutorial: Wireshark Workshop Videos Now Available

writeups/Confluence-RCE.md at main · httpvoid/writeups · GitHub

Yuki Chan - Automated Penetration Testing and Auditing Tool

ZDI-21-1053: Bypassing Windows Lock Screen | Abdelhamid Blog

» Attack Methods for Gaining Domain Admin Rights in Active Directory » Active Directory Security