

Useful Links

Useful Links for education, training, CTFs and News

- [Cyber Security Training](#)
- [Youtube](#)
- [Nice Links](#)
- [Clear Brainfog](#)
- [Tools, OSINT & Open Source](#)

Cyber Security Training

This is a curated list of interactive platforms, games, CTFs, open-source intelligence tools, and educational resources for anyone interested in cybersecurity, threat hunting, or ethical hacking.

Source:

https://www.linkedin.com/posts/mohessa511_cybersecurity-incidentresponse-playgames-activity-7132644163556114432-xC67?utm_source=share&utm_medium=member_desktop&rcm=ACoAAB4yqIYBh8d6l6lWTW6bdVPynH4m3OpMRZI

And own additions

📚 Learning Platforms

- [INE](#) – Free cybersecurity and networking courses.
 - [Immersive Labs](#) – Advanced interactive cybersecurity labs.
 - [RangeForce](#) – Interactive and scalable cyber training.
 - [Pluralsight](#) – Developer & security skill-building platform.
 - [Haiku, Inc](#) – Platform for hosting cybersecurity ranges and challenges.
 - [Pentest Cheat Sheets](#) – Collection of red team tactics and commands.
 - [Darkstar7471](#) – Blog of a TryHackMe admin with various security insights.
 - [Gian's GitHub Page](#) – Personal write-ups and insights from a LinkedIn security expert.
-

📚 Learning Platforms & CTFs

- [Hacksplaining](#)
Interactive lessons explaining common web vulnerabilities and their mitigations.
- [picoCTF](#)
Beginner-friendly CTF (Capture The Flag) competition platform created by cybersecurity experts at Carnegie Mellon.

- [**Let's Defend**](#)
Blue team-focused simulation platform with SOC analyst tasks.
 - [**OverTheWire**](#)
Classic wargames to learn Linux security, shell scripting, and exploitation.
 - [**HackerOne CTF**](#)
A hacking playground hosted by HackerOne for web vulnerability training.
 - [**Splunk Boss of the SOC**](#)
Realistic SOC analyst challenges using Splunk data.
 - [**CyberDefenders**](#)
Blue team-oriented challenges and training platform.
 - [**CyberDefenders Blue Team CTFs**](#)
Archive of practical detection and analysis challenges.
 - [**EchoCTF**](#)
Competitive red/blue team CTF environment.
 - [**Exploitation Education**](#)
Linux-based exploitation challenges covering stack overflows, heap, and format strings.
 - [**Google CTF**](#)
Official Google-hosted cybersecurity CTFs.
 - [**W3Challs**](#)
Various hacking challenges: web, forensics, and crypto.
 - [**WeChall**](#)
Meta-CTF aggregator that tracks your challenge progress across sites.
 - [**Webgoat**](#)
OWASP's deliberately insecure web app for learning web vulnerabilities.
 - [**CMD Challenge**](#)
Solve problems using only Linux command line knowledge.
 - [**CryptoHack**](#)
Learn cryptography by solving Python-based challenges.
 - [**CTFtime**](#)
CTF competition calendar and team ranking tracker.
 - [**Vulnmachines**](#)
Vulnerable machines and labs to practice penetration testing.
 - [**Alert to Win**](#)
Fun JavaScript-based hacking challenge.
 - [**TCM Security Academy**](#)
Practical cybersecurity courses including ethical hacking and OSINT.
-

☐☐ Hacking-Themed Games

- [**Duskers**](#)
Sci-fi tactical game using command-line-like interface.
 - [**TIS-100**](#)
Assembly language puzzle game that simulates reverse engineering.
 - [**ThreatGen Red vs. Blue**](#)
Turn-based strategy game teaching cyber offensive/defensive skills.
 - [**Spudnet Board Game**](#)
Fun family board game teaching cybersecurity concepts.
 - [**Nite Team 4**](#)
A tactical hacking simulation game with real-world inspired missions.
 - [**Hacknet**](#)
Terminal-based hacking simulation game.
-

☐☐ Reports & Insights

- [**2024 State of the Security Team - TrendMicro**](#)
Research report on challenges faced by security teams.
- [**Backdoors & Breaches Card Game**](#)
A fun tabletop game to simulate incident response and detection.

Youtube

Youtube Channels

NetworkChuck

<https://www.youtube.com/user/NetworkChuck>



David Bombal

<https://www.youtube.com/user/ConfigTerm>



LiveOverflow

<https://www.youtube.com/channel/UCIcE-kVhqyiHCcjYwcpfj9w>



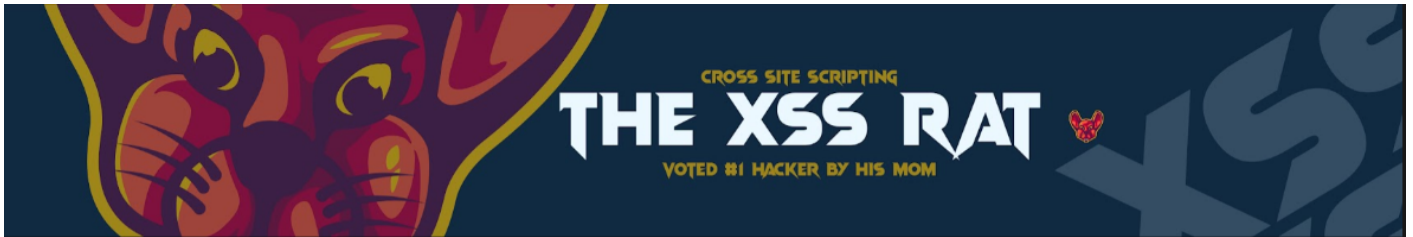
John Hammond

<https://www.youtube.com/user/RootOfTheNull>



The XSS rat

<https://www.youtube.com/channel/UCjBhCIJ59W4hfUly51i11hg>



HackerSploit

<https://www.youtube.com/channel/UC0ZTPkdxIAKf-V33tqXwi3Q>



freeCodeCamp Talks

<https://www.youtube.com/c/freeCodeCampTalks>



The Net Ninja

<https://www.youtube.com/c/TheNetNinja>



Loi Liang Yang

<https://www.youtube.com/channel/UC1szFCBUWXY3ESff8dJjzW>



Cyber Insecurity

<https://www.youtube.com/c/CyberInsecurity>

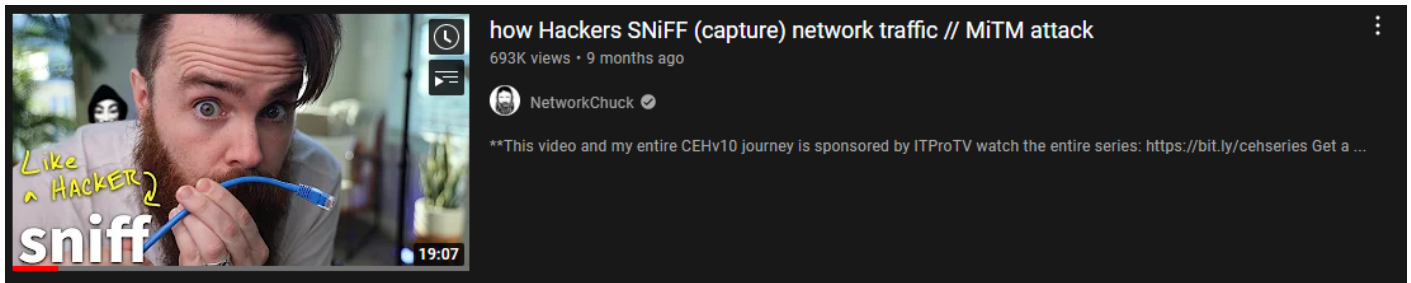
Former NSA Hacker



Youtube Videos

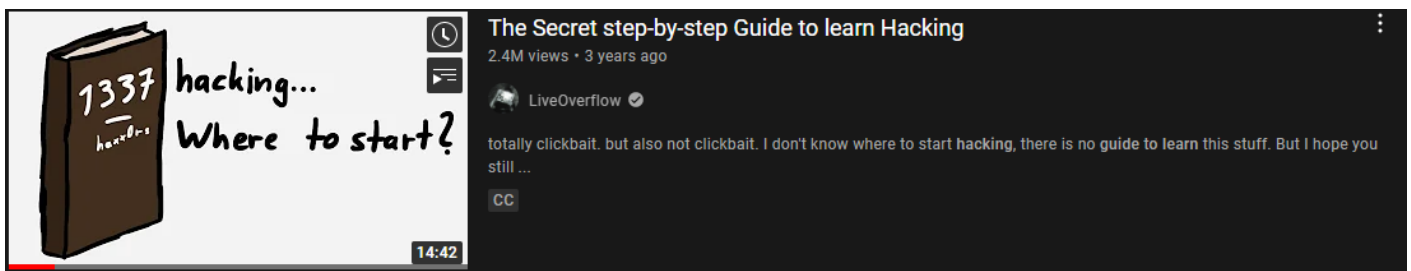
MiTM attack

<https://www.youtube.com/watch?v=-rSqbgI7oZM>



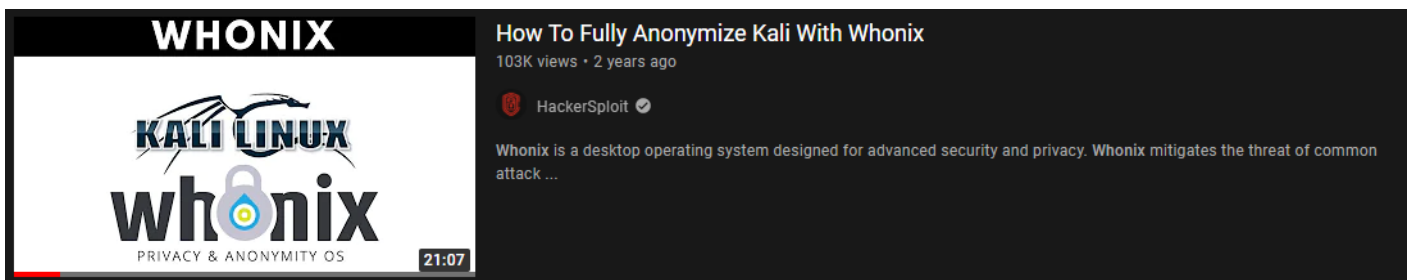
Hacking step-by-step

<https://www.youtube.com/watch?v=2TofunAI6fU>



Whonix anonymize kali

<https://www.youtube.com/watch?v=g8SzRhA8NXI&t=1s>



CTFs explained

<https://www.youtube.com/watch?v=Lus7aNf2xDg&t=84s>



Wildcard injection

<https://www.youtube.com/watch?v=HXikLrFVIXc&t=1844s>



Get yourself free Membership

<https://www.youtube.com/watch?v=MEyyegfvhwM>



Make your LinkedIn better

<https://www.youtube.com/watch?v=GcISqwKWCPE>

Tipps how to boost your profile in the topic



Hack Your LinkedIn Part 1

6.1K views · 5 months ago



Cyber Insecurity

cybersecurity #linkedin #mentoring #hiring #career In part 1 of our 2 part LinkedIn hacking series, we do a deep dive on several ...

Nice Links

Research & Academic Tools

- [Sci-Hub](#) - Provides free access to millions of research papers.
- [Gutenberg](#) - Offers a library of over 70,000 free eBooks.
- [Cymath](#) - Solves any math problem.
- [OceanofPDF](#) - Provides access to free PDFs of books.
- [MyBib](#) - Creates citations in seconds, all in one place.
- [UnstuckStudy](#) - Chat with all of the files in your class at once and get cited answers.
- [Scholarcy](#) - Summarize any paper, article, or textbook. You can summarize videos too.
- [Perplexity.ai](#) - A free AI-powered answer engine providing accurate, trusted, and real-time answers to any question.
- [Bookai.chat](#) - Chat with your books in over 30 languages.

AI Tools

- [Paperz.ai](#) - Write your research paper 10x faster with AI.
- [Flashka.ai](#) - Writing flashcards with AI.
- [Dende.ai](#) - Turn your study notes into exam quizzes in seconds.
- [Gamma.app](#) - A new medium for presenting ideas, powered by AI.
- [Otter.ai](#) - Get transcripts, automated summaries, action items, and chat with Otter to get answers from your meetings.
- [Krea.ai](#) - The easiest way to generate with AI.
- [Twaingpt](#) - AI humanizer.
- [Ryne.ai](#) - Another AI tool.
- [Sketch Meta Demo Lab](#) - AI animation tool.
- [Otio.ai](#) - Understand & chat with your docs, links & videos. Automate complex research workflows with AI.
- [Logomark.ai](#) - Limitless creativity with prompt-based logo creation.
- [Audioread](#) - Use AI to listen to articles, PDFs, emails, etc., in your podcast player.
- [AgentGPT](#) - Allows you to configure and deploy autonomous AI agents.

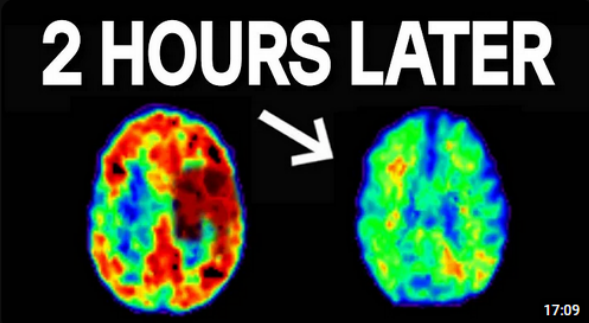
- [BlackBox.ai](#) - Best AI model for code.
- [InVideo.io](#) - Unlock your creativity and turn any idea into a full-length video.

Miscellaneous Tools

- [Stremio](#) - Freedom to stream movies and TV shows.
- [NuclearPlayer](#) - Supports YouTube, SoundCloud, Bandcamp, and your local library to stream music.
- [PlayPhrase](#) - Search for movie and TV show dialogue clips using keywords.
- [Tldraw](#) - A free and instant collaborative whiteboarding tool.
- [ChatDoc](#) - Chat with documents and get instant answers with cited sources.
- [Hissab.io](#) - A text-based calculator app that does much more than calculations.

Clear Brainfog

<https://www.youtube.com/watch?v=QNKhtQpboU>



2 HOURS LATER

17:09

Clearing Your Allostatic Load Makes Laziness Impossible

1M views • 1 year ago

Rian Doris

ABOUT ME Rian Doris is the Co-Founder & CEO of Flow Research Collective, the world's leading peak performance research ...

7 chapters Intro | What is Allostatic Load | Executive Athlete | Recovery | Active Recovery | Is it working | Live Lik

<https://www.youtube.com/watch?v=Wk9p3dhMYdk>



PERFECT SLEEP

10:12

How I FIXED My Terrible Sleep - 10 Habits

1.7M views • 7 months ago

Bryan Johnson

Sleep will give you superpowers. It's the cornerstone of my Blueprint routine, and the most important thing I do every day. Order ...

4K

10 chapters 8 months of perfect sleep | 1. Identify as a professional sleeper | 2. Consistent bedtime | 3. Wind dow...

<https://www.youtube.com/watch?v=ISwHxE9LohA>



BEFORE AFTER

14:10

5X Your BRAIN CELLS

2M views • 1 year ago

Dr. Eric Berg DC

It's been thought that brain cells don't regenerate—but is that actually true? Learn more! Support brain health—check out ...

4 chapters Introduction: Boost brainpower | Understanding neurogenesis | How to increase brain cells | Learn mor...

<https://www.youtube.com/watch?v=zwmX4ADLjuE>



Now playing

How To Clear Up Brain Fog & Feel Mentally Sharper - Dr. Rhonda Patrick

244K views • 8 months ago

Chris Williamson

Chris and Dr Rhonda Patrick discuss how you can reduce brain fog. What is Dr Rhonda Patrick's protocol for

4K

8 chapters What is brain fog | Exercise snacks | Food order | Starter | Deans Bread Crown | Prio

Tools, OSINT & Open Source

▣▣ OSINT & Data Discovery Tools

These tools are useful for uncovering publicly accessible information, exposed data, malware indicators, code leaks, documents, and file indexing across the internet.

▣▣ Privacy Search Engines

- [DuckDuckGo](#) – Privacy-focused search engine that doesn't track users.
 - [Startpage](#) – Google results with privacy protection and no tracking.
-

▣▣ Paste, Code, and Source Scanning

- [psbdmp](#) – Largest archive of leaked {paste} dumps from pastebin-style sites.
 - [Search-Pastebin](#) – Google CSE-powered meta-search across 33 paste sites.
 - [RedHuntlabs Online IDE Search](#) – Search keywords across online IDEs, code sharing platforms, and pastebins.
 - [NerdyData](#) – Find websites using specific technologies or HTML/JavaScript code.
 - [Publicwww](#) – Source code search engine indexing 480+ million pages.
 - [CybDetective Code Search](#) – Custom search across 20+ code hosting platforms.
 - [grep.app](#) – Fast regex-capable search engine for 500k+ Git repos.
 - [searchcode](#) – Search 75 billion lines of code from 40 million public projects.
-

▣▣ File & Directory Indexing

- [Open Directory Search Tool](#) – Search files in unprotected open directories.
- [Mamont FTP](#) – Largest public FTP search engine.
- [NAPALM FTP Indexer](#) – Index of over 894 million FTP files across thousands of servers.

- [**DeDigger**](#) – Discover publicly shared files in Google Drive.
 - [**UVRX**](#) – Search files from older hosting sites (e.g., Mega, Mediafire, Zshare).
-

☐☐ Document & Content Discovery

- [**PDF Drive**](#) – Download from a library of over 75 million free PDFs.
 - [**SlideShare**](#) – Explore millions of user-submitted presentations.
 - [**Scribd**](#) – Document repository with 195+ million user-uploaded files.
-

☐☐ Threat Intelligence & IOC Lookup

- [**VirusTotal**](#) – Multi-engine scanner and IOC search platform for files, hashes, domains, and URLs.
 - [**Hybrid Analysis**](#) – Free malware sandbox that performs hybrid static/dynamic analysis.
 - [**Sucuri SiteCheck**](#) – Website malware and security scanner.
 - [**URLhaus**](#) – Malicious URL tracker and database.
 - [**Feodo Tracker**](#) – Monitor and block IPs related to Feodo/Bugat/Dridex botnets.
 - [**SSL Blacklist**](#) – Collection of blacklisted SSL certificates and JA3 fingerprints.
 - [**MalwareBazaar**](#) – Repository for sharing malware samples.
 - [**Talos Reputation Center**](#) – IP, domain, and file reputation check.
 - [**PaloAlto URL Filtering**](#) – Link classification and reputation check.
 - [**OTX AlienVault**](#) – Threat sharing platform with global IOC and pulse feeds.
 - [**URLScan**](#) – Scan and analyze websites in a sandboxed environment.
 - [**McAfee Threat Center**](#) – Threat intelligence and malware information.
 - [**National Vulnerability Database \(NVD\)**](#) – US government vulnerability database with CVSS scores.
 - [**CVE Database**](#) – Public list of common vulnerabilities and exposures.
 - [**Website Reputation Checker \(URLVoid\)**](#) – Checks domain/IP reputation using multiple sources.
 - [**Google Safe Browsing Status**](#) – Checks if a site is flagged by Google Safe Browsing.
 - [**Looky Luu**](#) – Online Sandbox for Domain Checks
 - [**URLscan**](#) – Online Sandbox for Domain Checks
-

☐☐ Network, Routing, and Metadata Tools

- [Nmap](#) – Network scanner and host discovery tool.
 - [Yersinia](#) – Penetration testing tool for attacking network protocols.
 - [Passive OS Fingerprinter \(p0f\)](#) – Passive network OS fingerprinting tool.
-

☐☐ Offensive Security & Exploitation

- [Kali Linux](#) – Penetration testing and security auditing Linux distribution.
 - [Metasploit](#) – Exploit development and penetration testing framework.
 - [Aircrack-ng](#) – Wireless network security auditing tool.
 - [Powerfuzzer](#) – Automated web application vulnerability scanner.
 - [ShellNoob](#) – Shellcode writing toolkit.
 - [Backdoor Factory](#) – Patch binaries with custom backdoors.
 - [Capstone Engine](#) – Multi-architecture disassembly framework.
-

☐☐ Analysis & Development Utilities

- [CyberChef](#) – Web-based data transformation and analysis toolkit.
 - [CyberChef \(Offline\)](#) – Local instance for offline data analysis and transformation.
 - [JavaScript Beautifier](#) – Formats and beautifies JavaScript code for readability.
 - [UnPacker](#) – JavaScript deobfuscation/unpacking tool.
 - [Awesome Malware Analysis](#) – Curated list of malware analysis tools and resources.
-

☐☐ News & Security Feeds

- [Inside-IT](#) – Swiss IT and tech news.
 - [Heise Security - 7-Tage-News](#) – German IT security news overview (last 7 days).
 - [CERT-EU News Monitor](#) – EU cybersecurity news and advisories.
-

☐☐ Disposable Email Services

- [Trash-Mail](#) – Temporary disposable email inbox.
 - [Mailinator](#) – Public temporary email service.
-

☐☐ Internal/Local Resources

- [Sandbox](#) – Likely internal sandbox environment for testing malware or files.
 - [DPI \(NetWitness\)](#) – Network analysis and deep packet inspection tool (internal link).
-