7 AMAZING SECURITY TOOLS THAT MOST PEOPLE DON'T KNOW EXIST!

CanaryTokens

stunnel

Sysdig

osquery

uMatrix

grsecurity

JonDoNym

STATIONX

CanaryTokens

https://www.stationx.net/canarytokens/

The art of security through deception to detect malware and hackers is a very underutilized technique. With CanaryTokens you can detect threats poking around on file systems, email, databases and pretty much anywhere by laying traps that trigger alerts. Head over to Station X and generate yourself some CanaryTokens and leave them in locations where you want to catch unauthorized activity.

No installation necessary.

stunnel

https://www.stunnel.org/index.html

Have you ever wanted to get a protocol through a deep packet inspection proxy or firewall but were unable? With Stunnel you can wrap TLS around most protocols to get your traffic through the firewall and over a TLS port. Stunnel is a proxy designed to add TLS encryption functionality to existing clients and servers without any changes in the programs' code. Its architecture is optimized for security, portability, and scalability (including load-balancing), making it suitable for large deployments.

Stunnel uses the OpenSSL library for cryptography, so it supports whatever cryptographic algorithms are compiled into the library.

JonDoNym

https://anonymous-proxy-servers.net/

Everyone has heard of Tor, but have you heard of JonDoNym? If you're looking for anonymity and the ability to hide your IP at a faster speed, with lower latency you might want to look at JonDoNym. This is a smaller network than Tor that you need to pay for (anonymously) to get access to.

It acts similar to a VPN in that it’s a paid service, but it adds anonymity by hiding your IP through mixing cascades which VPNs are not able to do. Giving you anonymity at high speed and low latency, which Tor or a VPN cannot do.

grsecurity

https://grsecurity.net/

The Linux kernel is in need of a total rethink or recoding to cope with today’s attack types. Continually patching core kernel and vendor driver bugs isn't a practical defense anymore due to the very long lifetime of these bugs.

Grsecurity is an extensive security enhancement to the Linux kernel that defends against a wide range of security threats through intelligent access control, memory corruption-based exploit prevention, and a host of other system hardening that generally requires no configuration. Available in commercial and non-commercial versions.

Sysdig

https://www.sysdig.org

All Linux users and system administrators need to be aware of Sysdig and its terminal UI version Csysdig.

Sysdig is an open source, system-level exploration: capture system state and activity from a running Linux instance, then save, filter and analyze. Sysdig is scriptable in Lua and includes a command line interface and a powerful interactive UI, csysdig, that runs in your terminal. Think of sysdig as strace + tcpdump + htop + iftop + lsof + transaction tracing + awesome sauce. With state of the art container visibility on top.

uMatrix

https://github.com/gorhill/uMatrix

Most people today are familiar with browser ad blockers which remove adverts, help prevent web based attacks and speed up your downloads.

Take your protection to the next level with the advanced browser add-on uMatrix. Think of it as a point-and-click matrix-based http firewall, with many privacy-enhancing tools.

uMatrix puts you in full control of where your browser is allowed to connect, what type of data it is allowed to download, and what it is allowed to execute. Nobody else decides for you: You choose. You are in full control of your privacy and security.

osquery

https://osquery.io/

A game changer for threat detection is osquery, which allows you to easily ask questions about your Linux, Windows, and OS X infrastructure. Whether your goal is intrusion detection, infrastructure reliability, or compliance, osquery gives you the ability to empower and inform a broad set of organizations within your company.

osquery exposes operating system information via SQL tables. The best way to think of it is that osquery allows you to ask questions of your operating system as if it was a database, by running SQL queries it. Giving you a fast, automatable and uniform way to discover OS information across your entire estate.

Nathan House BSc. CISSP. CISM. CISA. SCF. ISO 27001 LA has over 24 years experience in cyber security, where he has advised many of the largest companies in the world, assuring the security on multi-million and multi-billion pound projects. He is the CEO and founder of Station X, a cyber security consultancy.

More recently he acted as the lead security consultant on a number of the UKs mobile banking and payment solutions, helping secure to date over £71 billion in transactions.

Over the years he has spoken at a number of conferences, developed free security tools, and discovered serious security vulnerabilities in leading applications.

Nathan is also the author of the popular "The Complete Cyber Security Course" which is highly reviewed by tens of thousands of students in over 170 countries.