Security Leftovers

By *Roy Schestowitz*
Created *25/05/2019 - 4:23am*
Submitted by Roy Schestowitz on Saturday 25th of May 2019 04:23:44 AM Filed under Security [1]

- **Security updates for Friday** **[2]**

- **Episode 19: Democratizing Cybersecurity** **[3]**

  Katherine Druckman and Doc Searls talk to Alex Gounares of Polyverse Linux about Cybersecurity for everyone.

- **Introducing the Librem Tunnel** **[4]**

  You probably know by now that the Librem Tunnel is part of Librem One, a suite of privacy-protecting, no-tracking apps and services created by our team at Purism, which also includes Librem Mail, Librem Chat and Librem Social.

  Librem Tunnel offers an encrypted, no-logging, virtual private network tunnel, making sure all your network traffic is secure and your privacy fully protected. This means you can safely and conveniently use any public hotspot and not have to worry about how private your connection really is, using standards-based OpenVPN with any compatible client. You are not the product in Librem Tunnel: you will not be tracked, we do not sell your data, and we don?t advertise.

- **Trump Explains Why He Banned Huawei, And It?s Not Convincing** **[5]**

  The world?s two biggest economies are indulged in a trade war and the toll is being paid by

the Chinese company Huawei, which is being erased from existence in the US.

The US government has already blacklisted Huawei, causing a big blow to its growing smartphone business across the globe. After the temporary license ends in August, it won?t be able to do any business with US-based companies unless the ban is lifted.

- **Snort Alerts [6]**

  It was previously explained on LinuxHint how to install Snort Intrusion Detection System and how to create Snort rules. Snort is an Intrusion Detection System designed to detect and alert on irregular activities within a network. Snort is integrated by sensors delivering information to the server according to rules instructions.
  In this tutorial Snort alert modes will be explained to instruct Snort to report over incidents in 5 different ways (ignoring the ?no alert? mode), fast, full, console, cmg and unsock.

  If you didn?t read the articles mentioned above and you don?t have previous experience with snort please get started with the tutorial on Snort installation and usage and continue with the article on rules before continuing this lecture. This tutorial assumes you have Snort already running.

Security

Source URL: http://www.tuxmachines.org/node/124220

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://lwn.net/Articles/789353/rss
[3] https://www.linuxjournal.com/podcast/episode-19-democratizing-cybersecurity
[4] https://puri.sm/posts/introducing-the-librem-tunnel/
[5] https://fossbytes.com/trump-explains-banned-huawei-dangerous/
[6] https://linuxhint.com/snort_alerts/