UNIXSHADOW

- A Laptop, a Container, and $6.3 Billion: What the Binance Hack Means for Anyone Running Infrastructure (2026/11/04 01:58)
  On October 29, roughly $6.3 billion left Binance's hot wallets in minutes. Strip away the crypto, and this is the […]
- PwnEscape: One Checksum That Broke Out of the Guest [Under the Hood] (2026/11/03 01:16)
  PwnEscape is not a hypervisor bug. It is a host-kernel IPv4 flaw where a guest's checksum-offload metadata rewrites a header the kernel already acted on — leaking host memory, crashing the host, or, in the researcher's lab, running code as root.
- setuid, setgid, and the Sticky Bit: How Linux Permissions Really Work [Under the Hood] (2026/11/02 15:38)
  unixshadow — permissions setuid, setgid, and the Sticky Bit The three permission bits every sysadmin uses and few can explain […]
- The Cursor Marketplace Backdoor: How a svc-telemetry SSH Key Landed in authorized_keys (2026/11/02 15:38)
  unixshadow — cursor-backdoor The Cursor Marketplace Backdoor A trusted editor extension auto-updated, and a stranger’s SSH key quietly moved into […]
- Node2Shell: The Brotli Bug That Turned HTTP/2 Into Remote Code Execution (2026/10/28 14:56)
  node — CVE-2026-111497 ~ node –version # if this prints anything older than the fixed lines below, keep reading Node2Shell: […]
- The CVE Flood: Why 2026 Broke the Vulnerability Count (2026/10/26 14:31)
  analyst@unixshadow: ~/cve-count/2026.log analyst@unixshadow:~# curl -s “https://services.nvd.nist.gov/rest/json/cves/2.0?pubStartDate=2026-10-01T00:00:00.000Z&pubEndDate=2026-10-26T00:00:00.000Z&resultsPerPage=1” # totalResults: 13934 The CVE Flood: Why 2026 Brokethe Vulnerability Count October 2026 published […]
- Panic on Boot? Rebuilding the initramfs on RHEL 6 Through 10, Running or in Rescue Mode (2026/10/26 13:53)
  root@rescue: ~/initramfs/rebuild.log root@rescue:~# dracut -f /boot/initramfs-$(uname -r).img $(uname -r) # panic on boot, rebuild it right Panic on Boot? Rebuilding […]
- Cairn & Storm-0940: Two Campaigns That Let AI Agents Do the Hacking [Under the Hood] (2026/10/25 18:54)
  analyst@unixshadow: ~/cairn-storm0940/analysis.log analyst@unixshadow:~$ explain cairn storm-0940 # two campaigns, one inflection: the human gives a goal, the agents do the […]
- Growing and Shrinking LVM Volumes on Linux: XFS, ext4, and parted Under VMware (2026/10/25 18:43)
  analyst@unixshadow: ~/lvm-resize/guide.log analyst@unixshadow:~$ lvm-resize –xfs –ext4 –vmware # growing works for both, shrinking only for ext4 Growing and Shrinking LVM […]
- PHP2Shell: Two Bugs That Turned Requests Into Shells [Under the Hood] (2026/10/25 18:43)
  analyst@unixshadow: ~/php2shell/analysis.log analyst@unixshadow:~$ explain php2shell # two bugs, no patch for most of the internet, shells for anyone who asks […]

From:
https://wiki.tromjaro.alexio.tf/ - **TROMjaro wiki**

Permanent link:
https://wiki.tromjaro.alexio.tf/doku.php?id=news:toplinuxmoon:unixshadow

Last update: **2021/10/30 11:41**