Defensive Linux Security Tools

@hackinarticles

https://github.com/Ignitetechnologies

https://in.linkedin.com/company/hackingarticles

Firewalls
- iptables
- Firewalld
- ufw
- Guarddog
- Vuurmuur
- Gufw
- Shorewall

Security Audit
- openSCAP
- openVAS
- Nmap
- Nikto
- Lynis
- SpiderFoot

IPS
- Snort
- Suricata
- Zeek
- OSSEC
- AIDE
- Security Onion
- OSSIM
- CrowdSec

Sandboxing
- Bubblewrap
- Firejail
- Flatpak
- Snappy
- Chroot Jail

Access Control
- SELinux
- AppArmor
- Smack
- Grsecurity
- Yama

Malware Detection
- wazuh
- chkrootkit
- rkhunter
- Tiger
- LMD

File Integrity Monitoring
- Tripwire
- Auditd
- Samhain
- OSSEC
- Wazuh
- Osquery
- Atomic OSSEC

Antivirus
- CrowdStrike
- ClamAV
- Rspamd

Log Monitoring
- Logwatch
- ELK Stack
- Graylog
- Sagan
- Fluentd
- OpenObserve
- Dynatrace

Filesystem Encryption
- dm-crypt
- fscrypt
- EncFS
- Veracrypt
- Gocryptfs
- eCryptfs
- SecureFS

WAFs
- ModSecurity
- NAXSI
- BunkerWeb
- Coraza
- open-appsec

Patch Manager
- Spacewalk
- Katello
- RH Satellite
- Landscape
- NinjaOne

VPN
- strongSwan
- OpenVPN
- WireGuard
- Libreswan
- SoftEther

Password Sec
- John the Ripper
- Hashcat
- KeePassXC
- pwgen
- GoPass

Secure Shell
- SSHGuard
- DenyHosts
- Knockd
- Fail2ban

Container Sec
- Docker Bench
- Calico
- Clair
- gVisor
- Grafeas
- Falco
- Dagda
- Cilium
- Dockle