Myfw

context

dit document beschijft de installatie van Myfw (My Forensic Workstation), een Linux server met bruikbare tools voor DFIR.

installatie

- installeer een Debian / Ubuntu
- werk het OS bij: `apt-get update && apt-get upgrade`
- installeer volgende rpm's: `apt-get install tcptraceroute nmap apt-file acl git python3-pip`
- configureer de samba_share
- installeer volgend werktuig (meestal omdat rpm's te oud zijn):
  - TrID
  - VirusTotal
  - Exiftool
  - EventlogExplorer
  - ClamAV
  - recon-ng
  - shodan

linxu, digital forensics