security_cloud_cisce nje_odrzavanje

Sadržaj

##linux brisanje i čišćenje

#folder and system sh sudo rm -r -f /home/koordinacijahumanitaraca/homes/baza/ du -hx --max-depth 1 /home

#clean swap echo 1 > /proc/sys/vm/drop_caches free -w -h

#clamav scan systemctl | grep clam ps -ef | grep freshclam clamscan --infected --remove --recursive /home/user

#maldet scan sudo nano /usr/local/maldetect/conf.maldet email_alert=1 email_addr=EMAIL email_subj="Malware alerts for $HOSTNAME - $(date +%Y-%m-%d)" quarantine_hits=1 quarantine_clean=1 quarantine_susp=1 scan_clamscan="1" sudo maldet -a /home/?

#custom malware scan find . -type f -exec egrep -Hn 'mail(' {} ; If there are too many, you can lead the output into a file like this. I recommend naming the logfile after your search. find . -type f -exec egrep -Hn 'mail(' {} >maillog.txt ; find . -type f -exec egrep -Hn '*eval(base64_decode($_POST*' {} ; >base64log.txt find . -type f -exec egrep -Hn '*eval(base64_decode($_POST*' {} ; -delete find . -type f -exec egrep -Hn '<?php echo "!@#$%^&";' {} ; -delete

#Lynis - scan sudo ./lynis audit system --quick --auditor "Marijan Kopčić"