Linux 2 - Inlämning PDF - Team LED

Jarl - Karl - Timmy

Installation:

- OS - Ubuntu 22.04.3 LTS
- 2 Hårddiskar 500 Gig/each
- Raid1 av dom 2 hårddiskarna
- Skapar 4 logiska volymer på 100 Gig och använder som /mnt/
- Nginx, MySQL, WordPress, Fail2Ban installeras manuellt

Konfiguration:

- Fail2Ban:
  [nginx-wordpress-auth]
  enabled = true
  filter   = nginx-wordpress-auth
  action   = iptables-multiport[name=nginx-wordpress, port="http,https", protocol=tcp]
  logpath = /var/log/nginx/access.log
  maxretry = 3
  bantime = 1800 # 30 minutes
  findtime = 600   # 10 minutes

- MySQL:
  Skapar en root användare, och en användare som bara kan läsa.
  Användaren som bara kan läsa är den som kommer användas för att ge tillbaka svar vid förfrågningar.

- Ports:
  Begränsar portar till:
  443 HTTPS (om vi lyckas fixa SSL certifikat)
  80 HTTP
  9090: Byter SSH till 9090 istället för 22 för säkerhet
  3306 MySQL
  25 SMTP
  22 SCP
  53 DNS (Eventuellt)

- Default Nginx

- Default WordPress

Cronjobs:

- Autostart:
  Nginx
  MySQL
  Fail2Ban

- Loggar
  /var/log/nginx/access.log /var
  /var/log/nginx/error.log
  /var/log/syslog
  /var/log/messages
  /var/log/mysql/error.log
  /var/log/auth.log
  cat journaldctl > journald.log (kanske inte säkert att ha med)

  Alla loggar kopieras via ett skrip till /var/log/serverlogs/.
  /var/log/serverlogs/ “tar:ar” allt i sin folder med ett script och döpts till logs-timestamp och sedan skickas vidare till backup med scp.

- Scripts:
  Loggning
  Backups
  Uppdateringar

- Uppdateringar
  WordPress - Latest
  Nginx - Latest
  Fail2Ban - Latest
  MySQL - Latest
  Linux säkerhetsuppdateringar endast

- Backups
  MySQL:
  mysqldump -u username -p password --databases wp_* >
  /var/log/serverbakp/wp_bak.sql
  mysqldump -u username -p password --no-data --databases wp_* >
  wp_schema_bak.sql

  WordPress:
  tar -czvf wp_bak.tar.gz /var/www/html > /var/log/serverbackup/
  (Är det bättre att bara ta themes/plugins/config eller ta hela + themes/plugins/config)

  Nginx:
  tar -czvf nginx_configs_backup.tar.gz /etc/nginx > /var/log/serverbackup/

  Serverscripts tar vi också backup på och skickar vidare

Säkerhet:

- Brandvägg - Fail2Ban
- Säkra Lösenord
- SSH Nyckel
- Onsite har tillgång till root

- SSH begränsas
- Usercontrol
    1 Användare som bara kan läsa (backup användare)
    1 Sysadmin konto full access inte sudo
    daemons (kontrollera vilka daemons vi kommer ha så att inga andra skapas)