Správa používateľov a autentifikácia

- Zabezpečenie prístupu k počítaču
- Proces zavádzania operačného systému
- Spôsob prihlasovania
- Vytváranie a mazanie používateľov
- Zmena informácií
- Nastavovanie skupín
- Nastavovanie obmedzení
- Autentifikácia

Zabezpečenie prístupu (1)

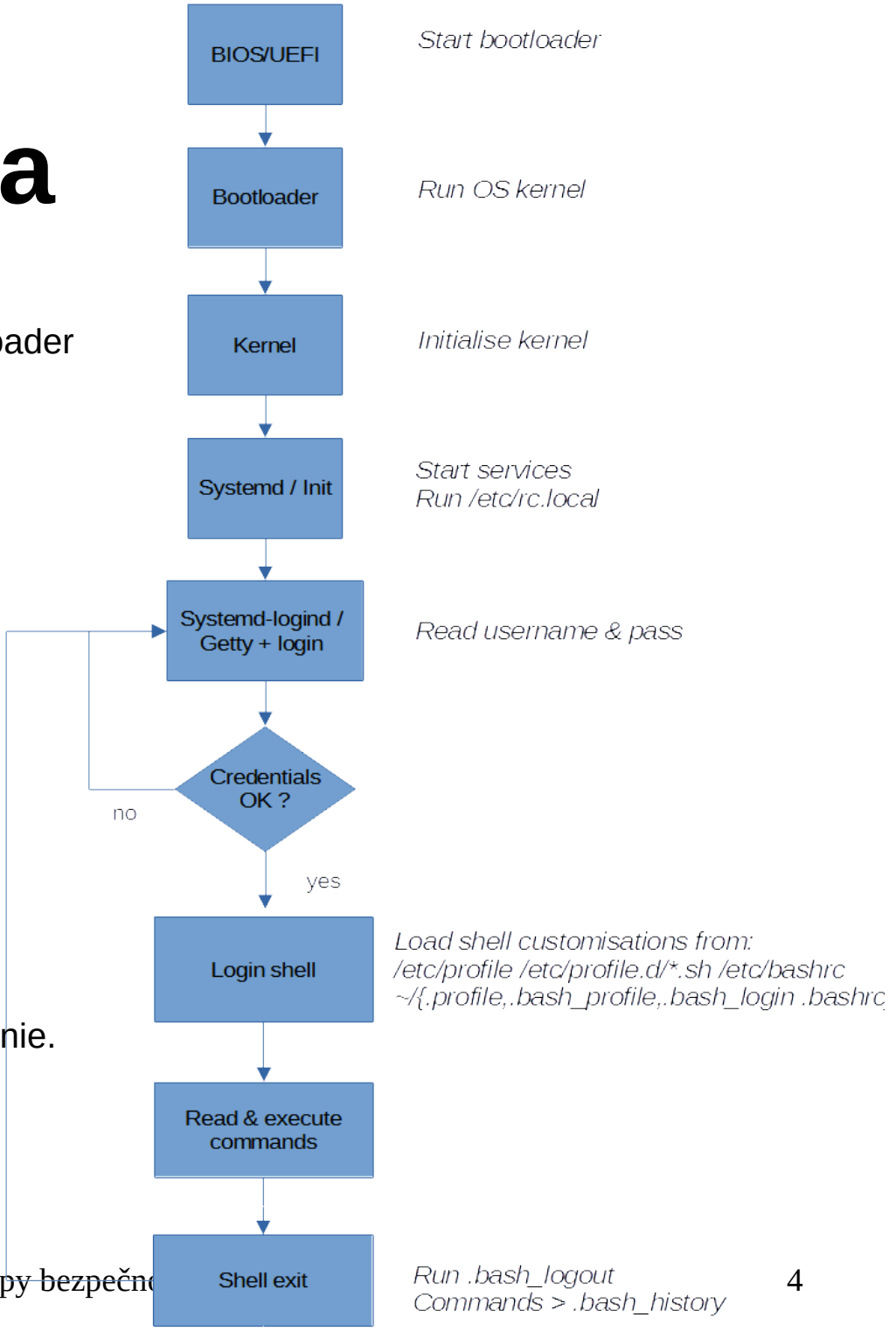
- Fyzická bezpečnosť
  - Kontrola fyzického prístupu k stroju (aj diskom a iným médiám).
- Bootovacie médium
  - Nastaviť heslo do BIOS-u / UEFI, zakázať bootovanie z vymeniteľných médií
  - V prípade nabootovania z média je možné získať prístup k súborovému systému (pokiaľ nie je šifrovaný),
    - Nastaviť heslo boot-loadera (/boot/grub/grub.conf: password),
    - Zmeniť heslo root-a.

Zabezpečenie prístupu (2)

- Bootloader
  - umožňuje odovzdávať parametre jadru, napríklad aj “runlevel”,
  - umožňuje teda získať administrátorský (root) prístup cez “single-user mode” / zmenu bootovania,
  - Nastaviť heslo bootloader-a
- Heslo root-a
  - Má v systéme všetky práva.
- Šifrovanie diskov
- Zabezpečiť sieť, administrátorské rozhrania (ILO…)
- Aktualizácie,...

Proces bootovania

- Po štarte počítača BIOS / UEFI načíta a spustí bootloader
  - BIOS: načítanie z boot sektoru
  - UEFI: načítanie z EFI System Partition (ESP)
    - UEFI Secure Boot
- Bootloader zavedie do pamäte a spustí jadro OS (prípadne ďalšie časti, napr. obraz initramfs)
- Bootloader odovzdá jadru parametre.
  - napr. umiestnenie súborového systému / (root),
  - Parametre je možné zmeniť pri bootovaní (s potrebnými právami)
- Jadro načíta potrebné moduly a načíta root súborový systém (read-only).
- Jadro po inicializácii spustí init službu (daemon-a)
  - V Linux-e typicky SysV init (/sbin/init) alebo systemd.
- Init služba inicializuje služby, používateľské nástroje, pripojí súborové systémy a zobrazí výzvu na prihlásenie.
- Po úspešnom prihlásení sa inicializuje používateľské prostredie.



Runlevel-y

- Režim práce operačného systému.
- Je ich 7, definované v */etc/inittab* a RC skriptami (*/etc/rc[0-6].d*)
  - 0: Halt
  - 1: single-user mode
  - 2 - 4: multi-user mode, textový so sieťou
  - 5: multi-user mode, grafický so sieťou
  - 6: reboot
- Prepínanie “runlevel-ov” - *runlevel, telinit*
- Systemd používa namiesto “runlevel-ov” tzv. *Systemd targets.*
  - napr. *multi-user.target* – aktivuje systém v textovom multi-user režime.
  - funkcionalita “runelvel-ov” kvôli spätnej kompatibilite.

Single-user mode

- Poskytuje len jednu textovú konzolu pre administrátora (root).
- Nie sú spustené služby (daemony).
- Neumožňuje prihlásenie bežných používateľov.
- Len pre údržbu, opravu, konfiguráciu.
- Umožňuje získať výlučný prístup k systému (bez root hesla), za rýchto predpokladov:
  - Prístup ku konzole stroja po reštarte,
  - Možnosť pridať bootovací parameter jadra, napr. “single” (poznať heslo do bootloader-a).

Používateľ v Linux-e

- Používateľ je niekto, kto má oprávnenie používať daný systém.
- Má priradené svoje meno - **username**.
- Je identifikovaný jednoznačným **UID.**
- Patrí do skupiny s jednoznačným **GID**.
- Autentifikácia **menom** a **heslom** (typicky).
- Po prihlásení sa spustí shell (interpret príkazov, napr. */bin/bash*).

Databáza používateľov */etc/passwd*

- Polia oddelené dvojbodkou
- **Používateľské meno –** 1 – 32 znakov
- **Heslo** – ak obsahuje “x”, heslo je uložené zahashované v */etc/shadow*
- **UID –** user ID, jedinečný identifikátor
  - 0 – root,
  - 1-99 – preddefinovaní používatelia,
  - 100 – 999 – systémové kontá (služby),
- **GID –** group ID, používateľova primárna skupina
- **Informácie o používateľovi –** doplňujúce informácie
- **Domovský adresár (home) –** absolútna cesta k adresáru, do ktorého sa používateľ dostane po prihlásení. Ak adresár neexistuje, domovský adresár = /.
- **Shell –** absolútna cesta k príkazu alebo interpretu príkazov, ktorý sa spustí po prihlásení (typicky */bin/bash*).

Pridanie používateľa do systému

- Pridanie používateľa s preddefinovanými nastaveniami
  - *useradd -m student* (“-m” – vytvor domovský adresár)
- Vypísanie preddefinovaných nastavení
  - *useradd -D*
- Zmena preddefinovanej skupiny
  - *useradd -D -g 4321*
- Otestovanie prihlásenia
  - *su - student*

Zmazanie používateľa zo systému

- Zmazanie používateľského konta
  - *userdel student*
- Zmazanie konta vrátane súborov v home
  - *userdel -r student*
- Vyhľadanie všetkých súborov patriacich používateľovi
  - *find / -user student*
- Pred vymazaním je potrebné ukončiť používateľove procesy!

Pridanie / zmazanie skupiny

- Vytvorenie skupiny
  - *groupadd studenti*
  - *-g gid – špecifikovanie GID*
  - *-r – vytvorenie systémovej skupiny*
- Zmazanie skupiny
  - *groupdel studenti*

Pridanie / zmazanie ručne

- Treba si dať pozor na syntax!
- Používatelia
  - *vipw, vipw -s*
- Skupiny
  - *vigr, vigr -s*
- Domovský adresár
  - *cp -r /etc/skel/* /home/user/*
- Verifikovanie integrity súborov
  - *pwck, grpck*

Zmeny používateľského konta

- Zmena konta: *usermod student* (man usermod)
- Zmena informácii: *chfn student*
- Zmena prihlasovacieho shellu: *chsh student*
- Zmena hesla: *passwd* (inému použ. iba root)
- Zmena platnosti konta: *chage student*
- Zablokovanie konta: *passwd -l student*

Obmedzenie prihlasovania

- Zabránenie prihlásenia používateľov iných ako root
  - */etc/nologin* – ak súbor existuje a je čitateľný
- Nastavenie shellu na nepovolený
  - */bin/false*
  - */sbin/nologin*
  - */usr/sbin/nologin*
- Zoznam povolených shellov: */etc/shells*

Obmedzenia pre používateľov (1)

- */etc/security/limits.conf*
- Syntax: <*domain*> <*type*> <*item*> <*value*>
- Doména môže byť username, groupname, * (predvolené nastavenia)
- Typy limitov:
  - *soft* – používateľ môže zmeniť
  - *hard* – pevné limity, používateľ nemôže meniť ani prekročiť
- Zistenie limitov:
  - *ulimit -a*

Obmedzenia pre používateľov (2)

- *core* – nastavuje veľkosť core súboru (KB),
- *fsize* – maximálna veľkosť súboru (KB),
- *memlock* – maximum alokovanej pamäte (KB),
- *nofile* – maximálny počet otvorených súborov (KB),
- *cpu* – maximálny pridelený čas CPU (KB),
- *nproc* – maximálny počet procesov (KB).

Linux PAM

- Pluggable Authentification Modules – súbor knižníc umožňujúci administrátorovi nastaviť, akým spôsobom budú jednotlivé aplikácie autentizovať používateľov.
- Jednotlivé moduly sa nachádzajú v */libs/security*
- Konfiguračné súbory pre aplikácie: */etc/pam.d/**
  - napríklad pre sshd: */etc/pam.d/sshd*
- Syntax: <*control*> <*module*> <*arguments*>
- *Na moderných distribúciách sú k dispozícii pomocné nástroje.*
  - *authconfig, authselect*

Príklad PAM

- Autentifikácia do systému pomocou hesiel - */etc/pam.d/system-auth*
- Systém “kreditov” (za použitie špeciálneho znaku môže používateľ získať kredit a použiť tak kratšie heslo).
  password requisite pam_pwquality.so try_first_pass local_users_only retry=3 minlen=14 dcredit=1 ocredit=2 difok=3 authtok_type=
- Pre vyžadovanie minimálneho počtu daných znakov možno použiť záporný kredit.
- Pozor na syntax!

su vs. sudo

- su – “switch user”
  - primárne na prepnutie na iného používateľa
  - vyžiada heslo používateľa, na ktorého sa chceme prepnúť
  - *su – user2*
  - konfigurácia pomocou PAM
- sudo – “switch user and do”
  - primárne na vykonanie príkazu pod iným používateľom
  - vyžiada heslo používateľa, ktorý spúšťa sudo
  - *sudo -u user2 id*
  - konfigurácia v súbore */etc/sudoers*

Literatúra a zdroje

- Manuálové stránky
  - man príkaz
  - https://linux.die.net/man/
- Bootovací proces
  - https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/installation_guide/ch-boot-init-shutdown
- Init daemon-y a spúšťanie služieb
  - https://www.digitalocean.com/community/tutorials/how-to-configure-a-linux-service-to-start-automatically-after-a-crash-or-reboot-part-1-practical-examples