TEHNIČKA ŠKOLA
RUĐERA BOŠKOVIĆA
Zagreb, Getaldićeva 4

Nastavni predmet:	**SIGURNOST INFORMACIJSKIH SUSTAVA**
Vježba: 06	Dnevnički zapisi na Linux sustavima
Cilj vježbe:	Upoznati učenike s pregledavanjem i korištenjem dnevničkih zapisa na Linux sustavima

PRIPREMA ZA VJEŽBU

Proučiti osnovne pojmove vezane uz dnevničke zapise na Linux sustavima.

IZVOĐENJE VJEŽBE

Postupke, korištene naredbe i dobivene rezultate zadataka zapisivati u bilježnicu te odgovoriti na postavljena pitanja vezana uz vježbu.

Pokrenuti **Linux** operacijski sustav.

Unijeti zaporku: **osboxes.org**

Ulogirani smo kao korisnik **osboxes.org**.

Zadatak 1: Korisnički račun LOG

a) Stvoriti korisnički račun (**LOG**) korištenjem terminala.

Pokrenuti terminal.

Da bi privremeno dobili administratorske ovlasti treba u terminal upisati naredbu:

su

Nakon toga treba unijeti zaporku administratorskog računa: **osboxes.org**

b) U terminal upisati navedenu naredbu za stvaranje korisničkog računa **LOG**:

useradd –m –s /bin/bash LOG

Dodijeliti zaporku stvorenom korisničkom računu **LOG** korištenjem naredbe:

passwd LOG

Unijeti zaporku: **log**

Potvrditi zaporku.

c) Da bi ukinuli administratorske ovlasti upisati naredbu:

exit

d) Provjeriti da li je stvoren korisnički račun **LOG**. U terminal upisati naredbe:

pwd

cd /home

ls

Da li je stvoren željeni korisnički račun?

Zadatak 2: Vrste dnevničkih zapisa

Dnevnički zapisi u Linux operacijskom sustavu sadrže informacije i poruke o sustavu, uslugama, aplikacijama koje se koriste i sl.

Dnevnički zapisi se nalaze u direktoriju **/var/log i njegovim poddirektorijima**.

a) Pozicionirati se u direktorij **/var/log**:

cd /var/log

Pogledati sadržaj ovog direktorija:

ls

b) Pogledajte datoteke i direktorije i u bilježnicu zapišite koje datoteke ili direktoriji bi se mogli koristiti za:

Dnevničke zapise o podizanju sustava:

Dnevničke zapise o logiranju korisnika:

Dnevničke zapise o instaliranim i deinstaliranim aplikacijama:

Datoteke možete pogledati korištenjem naredbe **cat** npr.:

cat auth.log

cat messages

itd.

c) Gdje bi mogli biti dnevnički zapisi o stvorenom novom korisniku?

Pozvati nasatavnika i pokazati što ste zapisali!

Zadatak 3: Pohrana dnevničkih zapisa

a) Pozicionirati se u direktorij **/var/log**:

cd /var/log

Ispisati sadržaj direktorija:

ls

Pogledati sadržaj datoteke **syslog**:

cat syslog

Pogledati sadržaj datoteke **syslog.1**:

cat syslog.1

b) Da li su u ove dvije datoteke isti zapisi ili se razlikuju? Obratite pažnju na vrijeme koje je navedeno u pojedinom zapisu!

Što bi moglo biti pohranjeno u datoteci **syslog.1**?

c) Uočite da postoje i datoteke:
syslog.2.gz

syslog.3.gz

syslog.4.gz

itd.

Zašto datoteke imaju nastavak **.gz**, zašto su označene brojevima i što bi moglo biti pohranjeno u njima?

d) Postoji li u direktoriju **/var/log** još koja vrsta dnevničkih zapisa koja je zabilježena tj. pohranjena na ovaj način. Navesti barem **3 vrste takvih zapisa** u bilježnicu.

Pozvati nastavnika i pokazati odgovore na pitanja iz ovog zadatka!

Zadatak 4: Logrotate

Pozicionirati se u direktorij /etc:

cd /etc

Ispisati sadržaj direktorija:

ls

Uočite da se u ovom direktoriju nalazi datoteka **logrotate.conf** i direktorij **logrotate.d**.

Pogledati sadržaj datoteke **lograte.conf**:

cat logrotate.conf

Pročitati komentare u kojima su opcije za rotaciju dnevničkih zapisa.

Kao što piše u prvoj liniji komentara upišite u terminal:

man logrotate

Pročitati opis (Description) i u bilježnicu ukratko (rečenica ili dvije – ne više!) napisati čemu točno služi **logrotate**.

Pritisnuti **q** za izlaz.

Ući u direktorij **logrotate.d**

cd logrotate.d

Ispisati sadržaj direktorija:

ls

Pogledati sadržaj datoteke rsyslog:

cat rsyslog

Možete li odrediti na koje dnevničke zapise se odnose ove postavke?

U bilježnicu odgovoriti imaju li podaci u **rsyslog** datoteci neke veze s **Zadatkom 3**?

Zadatak 5: Dnevnički zapisi o logiranju korisnika

Dnevnički zapisi o logiranju korisnika mogu se pogledati unutar direktorija **/var/log** u datoteci **auth.log** (i ostalim datotekama **auth.log.1** itd.).

Za potrebe ovog zadatka koristiti će se datoteka **auth.log**.

a) Pozicionirati se u direktorij **/var/log**:

cd /var/log

Ispisati sadržaj direktorija:

ls

Pogledati sadržaj datoteke **auth.log**:

cat auth.log

U bilježnicu zapisati postoji li već zapis o logiranju korisnika?

Ako postoji o kojem je korisniku riječ?

b) Pokušati se ulogirati kao korisnik **LOG**, ali namjerno **2 puta za redom** unesite **KRIVU** lozinku.

U terminal upisatislijedeće:

whoami

Ulogirati se kao korisnik **LOG** koristeći naredbu su:

su LOG

Prvi put unesite krivu lozinku!

Pogledati da li je nastao zapis o tome u datoteci **auth.log**.

cat auth.log

Ponovno se pokušajte ulogirati kao korisnik **LOG**:

su LOG

Drugi put unesite krivu lozinku!

Pogledati da li je nastao zapis o tome u datoteci **auth.log**.

cat auth.log

Da li su nastali dnevnički zapisi o neuspješnom logiranju?

c) Ulogirati se kao korisnik **LOG** – s **ISPRAVNOM** lozinkom!

U terminal upisati:

su LOG

Unijeti **ISPRAVNU** lozinku: **log**

Provjerite da li ste ulogirani kao korisnik **LOG**:

whoami

Pogledati dnevničke zapise o uspješnom logiranju:

ls

cat auth.log

Što se dogodilo?

U bilježnicu zapisati zašto se ne mogu pogledati zapisi o logiranju korisnika.

Ponovo se ulogirati kao korisnik **osboxes**:

su osboxes

Unijeti ispravnu lozinku: **osboxes.org**

Provjerite da li ste ulogirani kao korisnik **osboxes**:

whoami

Sada pogledati dnevničke zapise o uspješnom logiranju:

ls

cat auth.log

Da li su stvoreni dnevnički zapisi o uspješnom logiranju? Koji su sve korisnici navedeni?

Zadatak 6: Dnevnički zapis u stvarnom vremenu

Bilo koji dnevnički zapis može se gledati u stvarnom vremenu, a za to se koristi naredba **tail** na slijedeći način.

a) U terminal upisati:

ls

tail /var/log/auth.log -f

Ovom naredbom je pokrenuto praćenje dnevničkih zapisa u datoteci **auth.log** u stvarnom vremenu.

Uočite da smo naveli **put** do datoteke **auth.log** i opciju **-f**.

Što se ispisalo u terminalu?

b) Maksimizirajte prozor terminala:

Kliknuti na oznaku **+** u gornjem desnom kutu prozora od terminala.

c) Pokrenuti **NOVI** terminal.

U novom terminalu provjeriti da li ste ulogirani kao korisnik **osboxes**.

whoami

d) Pokušati se ulogirati kao **„root“** korisnik, ali **unijeti krivu lozinku**!

U terminal upisati:

su

Unesite krivu lozinku!

Da li se nešto zapisalo u terminalu za praćenje dnevničkih zapisa?

e) Ulogirati se kao **„root“** korisnik s **ISPRAVNOM** lozinkom (**osboxes.org**).

U terminal upisati:

su

Unijeti ispravnu lozinku: **osboxes.org**

Da li se opet nešto zapisalo u terminalu za praćenje dnevničkih zapisa?

f) Da bi ukinuli administratorske ovlasti odlogirati se kao **„root“** korisnik.

U terminal upisati:

exit

Da li je zabilježen i zapis o odlogiranju?

g) Ugasite trenutno korišteni terminal:

exit

h) U terminalu koji je korišten za praćenje dnevničkih zapisa pritisnuti slijedeću kombinaciju tipki:

Ctrl-C

Time je prekinuto praćenje dnevničkih zapisa.

Zadatak 7: Više dnevničkih zapisa u stvarnom vremenu

Korištenjem naredbe **tail** i njenih opcija moguće je gledati više dnevničkih zapisa u stvarnom vremenu.

Potrebno je kao korisnik **osboxes** instalirati aplikaciju **htop** koja služi za gledanje i upravljanje procesima.

U stvarnom vremenu treba gledati dnevničke zapise vezane za instalaciju i deinstalaciju aplikacije!

Dnevnički zapisi vezani uz instalaciju i deinstalaciju aplikacija nalaze se u direktoriju **/var/log/apt** u datotekama:

history.log

i

term.log

a) Pozicionirati se u direktorij **/var/log/apt**:

cd /var/log/apt

Ispisati sadržaj diraktorija:

ls

U bilježnicu zapisati koje se datoteke nalaze u tom direktoriju!

Pogledati sadržaj datoteka **history.log i term.log**:

cat history.log

cat term.log

Da li je nešto zapisano u ovim datotekama?

b) Pokrenuti praćenje dnevničkih zapisa u stvarnom vremenu u datotekama **history.log** i **term.log**, ali dodati i praćenje zapisa o logiranju korisnika (**/var/log/auth.log**).

U terminal upisati:

ls

tail -f /var/log/apt/history.log -f /var/log/apt/term.log -f /var/log/auth.log

Uočite da smo naveli **puteve** do **3** datoteke u kojima bi trebali nastati željeni dnevnički zapisi.

Što se ispisalo u terminalu?

Da li već postoje neki zapisi od prije?

c) Maksimizirajte prozor terminala:

Kliknuti na oznaku **+** u gornjem desnom kutu prozora od terminala.

d) Pokrenuti **NOVI** terminal.

U novom terminalu provjeriti da li ste ulogirani kao korisnik **osboxes**.

whoami

e) Krenuti s instalacijom aplikacije **htop**.

Prije same instalacije nadograditi tj. ažurirati pakete u repozitoriju:

sudo apt-get update

Unijeti lozinku administratorskog računa: **osboxes.org**

Da li su nastali kakvi dnevnički zapisi nakon izvođenja ove naredbe i gdje?

f) Instalirati aplikaciju **htop**:

sudo apt-get install htop

Da li su nastali kakvi dnevnički zapisi nakon izvođenja ove naredbe?

g) Pokrenuti instaliranu aplikaciju. U terminal upisati:

htop

Izaći iz aplikacije pritiskom na tipku:

q

h) Deinstalirati aplikaciju **htop** korišetnjem naredbe:

sudo apt-get remove htop

Na pitanje „Do you want to conitnue?“ odabrati: **y**

Da li su nastali kakvi dnevnički zapisi nakon izvođenja ove naredbe i gdje?

i) Ugasite trenutno korišteni terminal:

exit

j) Prekinuti praćenje dnevničkih zapisa.

U terminalu koji je korišten za praćenje dnevničkih zapisa pritisnuti slijedeću kombinaciju tipki:

Ctrl-C

Zadatak 8: NTP server

a) Instalirati **NTP** iz repozitorija.

U terminal upisati:

sudo apt-get install ntp

Na pitanje „**Do you want to conitnue**?“ odabrati: **y**

b) Nakon instalacije u terminal upisati:

service ntp status

Koja se poruka pojavila?

c) Pogledati poslužitelje koji sudjeluju u sinkronizaciji vremena:

Upisati naredbu:

ntpq –p

d) Detaljnije postavke mogu se pogledati u datoteci **ntp.conf** koja se nalazi u direktoriju **/etc**.

Pozicionirati se u direktorij **/etc**:

cd /etc

ls

Pogledati sadržaj datoteke **ntp.conf**:

cat ntp.conf

Može li se dobiti kvalitetnija sinkronizacija vremena promjenom nekih postavki? Ako da, koje bi postavke trebalo izmijeniti?

Zadatak 9: Zadatak za ocjenu

Korištenjem **apt-get** naredbe instalirati naredbu **multitail**.

Pokrenuti praćenje dnevničkih zapisa vezanih za instalaciju aplikacije i logiranje korisnika u stvarnom vremenu.

Kod zapisa za instalaciju aplikacije ispisati samo **7** zadnjih linija, a ne standardnih **10** zadnjih linija.

Prikazati i zapise vezane za logiranje korisnika, ali samo zadnje **3** linije zapisa!

Pozvati nastavnika prije same instalacije! Tek tada pokrenuti instalaciju i pokazati nastale dnevničke zapise.

Provjera znanja:

1) Gdje se pohranjuju dnevnički zapisi na Linux sustavima? (1 bod)
2) Zašto su neki dnevnički zapisi komprimirani? (1 bod)
3) Na što se odnosi logrotate ako govorimo o dnevničkim zapisima? (1 bod)
4) Gdje se mogu pogledati dnevnički zapisi o logiranju korisnika? (1 bod)
5) Kako se mogu gledati dnevnički zapisi u stvarnom vremenu? (1 bod)
6) Kako se može gledati više dnevničkih zapisa u stvarnom vremenu? (1 bod)

Ocjene: 6 bodova = 5 ; 5 bodova = 4 ; 4 boda = 3 ; 3 boda = 2 ; <3 boda = 1