Elektrotehnički fakultet u Beogradu
Katedra za računarsku tehniku i informatiku

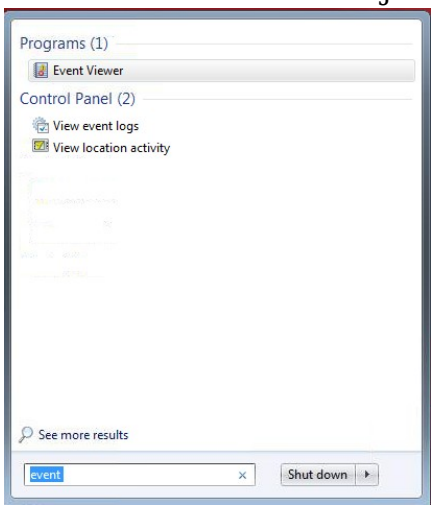
Zaštita računarskih sistema i mreža

- Deveta laboratorijska vežba -

9.1 Windows logovi[1]

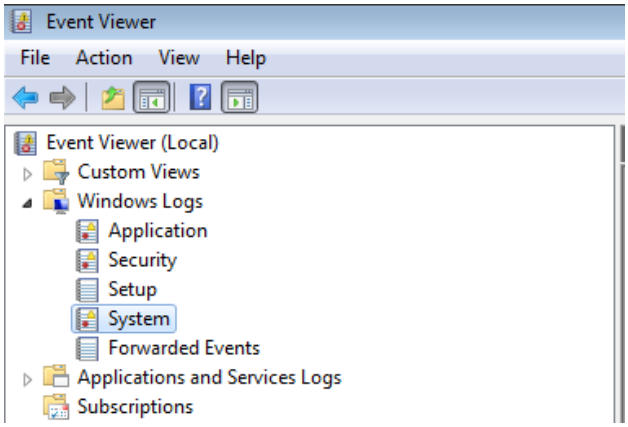
Kao i na svakom operativnom sistemu ili korisničkom programu i na Windows operativnom sistemu postoje logovi. Oni služe za praćenje rada sistema, očekivanih i neočekivanih događaja unutar sistema. Kod Windows operativnog sistema logove je moguće pratiti na lokalnoj mašini, ali je moguće i pratiti logove koji se šalju sa druge mašine.
Sledeći koraci predstavljaju demonstraciju generisanja i pregleda logova na Windows 7 operativnom sistemu.

1. Otvoriti EventViewer što je Microsoft-ov program za pregledanje logova.



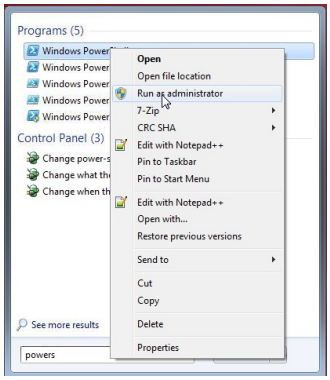
2. Sa leve strane programa moguće je biranje tipa logova koje korisnik želi da pregleda. Kartica Application predstavlja logove aplikacija, Security je vezan za logovanja u sistem i ostale logove vezane za bezbednost, System predstavlja logove vezane za sistem.

[1] Nastavnici na predmetu Zaštita računarskih sistema i mreža se zahvaljuju studentu Luki Mrdaku za pripremu scenarija ovu laboratorijsku vežbu

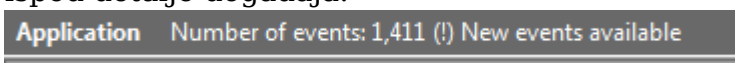


3. Unutar Application primetiti da tvnserver predstavlja vnc server, Defrag defragmentaciju diska. Pogledati i ostale logove i pregledati ostale događaje koji se loguju.

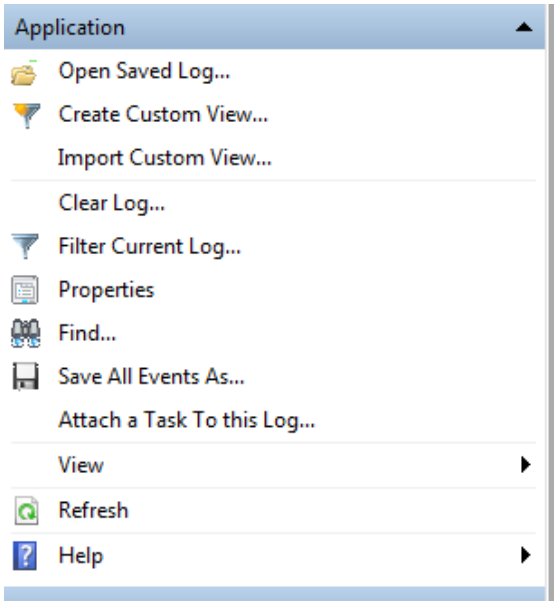
4. Odabrati karticu Application jer će tu biti biti prikazani logovi koji će biti izgenerisani u sledećim koracima.
5. Pokrenuti PowerShell kao administrator.



6. Kreirati novi EventLog koji će biti u grupi logova Application, a čiji je izvor MyApp komandom
   New-EventLog -LogName Application -Source MyApp . Celokupna dokumentacija za ovu komandu može se pronaći na sledećem linku.
7. Kreirati jedan događaj u tom logu komadom
   Write-EventLog -LogName "Application" -Source "MyApp" -EventID 3001 -EntryType Information -Message "MyApp je izgenerisala događaj koji će se videti u logu" -Category 1 -RawData 10,20 . Celokupna dokumentacija za ovu komandu može se pronaći na sledećem linku.
8. Primetiti da se unutar EventViewer-a pojavio novi događaj. Kliknuti na **refresh** sa desne strane i primetiti da se događaj pojavio na vrhu. Kliknuti na taj događaj i videti ispod detalje događaja.



9. Pokušati dodavanje novog događaja sa flag-om **-EntryType Error**. Primetiti razlike između dva izgenerisana događaja.
10. Primetiti da postoje opcije za filtriranje logova, nalaženje ključnih reči u logovima i snimanje događaja. Pokušajte filtriranje logova samo za neku aplikaciju ili u nekom periodu.



11. Klikom na **Clear Log...** sa desne strane obrisati logove. Brisanjem logova mogu se sakriti tragovi nekih akcija na nekom računaru. Na primer, aplikacija MyApp je mogao biti neki neželjeni program i tragove njegovih akcija na računaru možemo obrisati ovom komandom

10.2 Logovi na Linuksu

Svaka aplikacija koja se danas koristi u nekoj formi koristi logove za lakše debagovanje i utvrđivanje problema. Prilikom logovanja na neki sistem i izvršavanja komandi na tom sistemu ostaje trag u vidu logova. Sledeći koraci objašnjavaju na koji se način na linuks mašini vrši pregledanje logova i utvrđivanje da li neko drugi pokušava da se uloguje na posmatrani računar, a takođe i kako je moguće sakriti tragove pristupanja nekoj mašini. Dokumentacija za korišćenje bash komandi koje se pominju u nastavku može se videti tako što se otkucaju sledeće komande u terminalu **komanda --help** ili **man komanda**.

1. Otvoriti ssh sesiju ka virtuelnij mašini VM3.
2. Otkucati komandu **cd /var/logs** kojom se prelazi na podrazumevanu lokaciju za logove na linuksu. Ukoliko se ovde otkuca komanda **ls** izlistaće se spisak svih fajlova i direktorijuma u tekućem direktorijumu. Za otvaranje ovih fajlova su potrebne administratorske privilegije, a one se dobijaju komandom **sudo su** koja predstavlja promenu korisnika u administratora sistema.

```
student@IbLab-198-bafer:/var/log$ ls
alternatives.log  dist-upgrade  lastlog              vmware-network.log
apport.log        dmesg         lxd                  vmware-vmsvc.1.log
apport.log.1      dpkg.log      syslog               vmware-vmsvc.2.log
apt               faillog       syslog.1             vmware-vmsvc.log
auth.log          fsck          syslog.2.gz          wtmp
auth.log.1        installer     unattended-upgrades
bootstrap.log     kern.log      vmware-network.1.log
btmp              kern.log.1    vmware-network.2.log
```

   Alternatives predstavlja alat koji omogućava postojanje više verzija istog programa koje se mogu menjati po potrebi (npr. više verzija Jave), apt predstavlja menadžer paketa koji govori koji su programi instalirani i tako dalje. Fajlovi koji imaju broj na kraju predstavljaju prekopiran sadržaj fajla bez broja zbog preglednosti i lakše podele, a fajlovi koji na kraju imaju .gz predstavljaju fajlove na koje je primenjen gzip algoritam da bi zauzimali manje prostora na disku. Komandom **cat ime_fajla** možemo pregledati sadržaj nekih od ovih fajlova, a komandom **nano ime_fajla** taj sadržaj otvaramo u editoru.
3. Otkucati komandu **sudo gunzip syslog.2.gz** (ili neki drugi broj ako je tako na virtuelnoj mašini) kojom će se fajl raspakovati da bi mogao da se pregleda njegov sadržaj.
4. Nakon ovoga otkucati komandu **ls** i primetiti otpakovan fajl.

```
student@IbLab-198-bafer:/var/log$ ls
alternatives.log  dist-upgrade  lastlog              vmware-network.log
apport.log        dmesg         lxd                  vmware-vmsvc.1.log
apport.log.1      dpkg.log      syslog               vmware-vmsvc.2.log
apt               faillog       syslog.1             vmware-vmsvc.log
auth.log          fsck          syslog.2             wtmp
auth.log.1        installer     unattended-upgrades
bootstrap.log     kern.log      vmware-network.1.log
btmp              kern.log.1    vmware-network.2.log
```

5. Otkucati komandu **less syslog.7** i u editoru pregledati sadržaj fajla (fajl može da se skroluje gore-dole). Izlaz iz pregleda se dobija tasterom q.
6. Otkucati komandu **less auth.log**. Ovom komandom vrši se pregledanje sadržaja ovog fajla u trenutku kada je pritisnut enter nakon te komande, ali ovom komadnom ne može se pregledati sadržaj fajla "uživo". Za te potrebe se koristi komanda **tail -f auth.log** . Ova komanda pokazuje 10 poslednjih linija loga za autentikaciju, kao i sve nove događaje.

7. Da bi se izgenerisali neki događaji u ovom logu potrebno je otvoriti još jednu ssh sesiju ka VM3. Pre toga pokrenuti **tail -f auth.log.**

8. Probati otvaranje ssh sesije koristeći ime korisnika **pera** (koji ne postoji na sistemu). Da li se pojavila informacija o ovakvom pokušaju? Probati nakon toga otvaranje sesije sa regularnim parametrima za povezivanje. Šta se desilo?

9. Pokušati još nekoliko logovanja sa pogrešnim imenima i lozinkama. Primetiti da se svi neuspešni pokušaji ispisuju u konzoli.

10. Kliknuti na terminal u kom je otkucana komanda tail. Kombinacija tastera za zaustavljanje trenutno aktivnog programa u konzoli je **Ctrl+Z**. Za potpuno gašenje programa otkucati komandu **disown %1** .

11. Primetiti da sa vremenom veličina ovih fajlova postaje velika, a najčešći pristup linux sistemima jeste preko konzole. Jedan od čestih zahteva jeste filtriranje samo neuspešnih pokušaja logovanja u sistem. Komanda za postizanje tog rezultata je **cat auth.log | grep failure** ili **cat auth.log | grep "invalid user"**, gde se posle grep upisuje reč, string ili regularni izraz koji pretražujemo.

12. Komanda za brisanje svih fajlova i logova iz foldera /var/logs je **rm -rf /var/logs (Pažljivo sa direktorijumom koji se zadaje ovoj komandi – pokretanje u nekim folderima može da obriše ključne fajlove potrebne za rad virtuelne mašine)**, ali tada ako bi neko gledao logove posle izvršavnja ove komande primetio bi da nema logova i da je neko nešto radio sa ovim računarom. Elegantnije rešenje bi bilo pisanje skripte koja čisti logove, ali ostavlja fajlove.

13. Otkucati komandu **cd /opt** za prelazak u direktorijum gde biti kreirana skripa za brisanje logova. Otkucati komandu **nano delete_logs.sh** i time se otvara edirot u kome se kuca skripta. Tekst koji bi skripta trebalo da ima je sledeći (Paste u terminalu je desni klik):

```
#!/bin/bash
for CLEAN in $(find /var/log/ -type f)
do
    cp /dev/null  $CLEAN
done
```

Kombinacija tastera za zatvaranje programa je **Ctrl+X**, otkucati y za potvrdu snimanja i pritisnuti enter za potvrdu imena skripte. Fajlovi se u linux operativnom sistemu kreiraju podrazumevano bez prava na izvršavanje. Dodati to pravo kreiranoj skripti komandom **chmod +x delete_logs.sh**

Skriptu pokrenuti komandom **./delete_logs.sh** ili **sh /opt/delete_logs.sh**.

Opis onoga što izvršava ova skripta je da u sve fajlove koji se nalaze u folderu /var/log upisuje prazan tok podataka. Ponoviti korak tri i pogledati sadržaj log fajlova. Primetiti da su prazni ili da imaju veoma malo sadržaja.

Za pregledanje svih arhiva koje se nalaze u tom folderu može se iskoristiti komada **find /var/log -type f -regex ".*\.gz$"** . Za brisanje tih arhiva sve što je potrebno uraditi jeste dodavanja opcije **-delete** na kraj komande.

14. Pregledati istoriju otkucanih komandi pomoću komande: **history**
    Obrisati istoriju otkucanih komandi pomoću: **history –c**
    Ponoviti komandu **history**. Šta se desilo?