CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

OSNOVE ANALIZE LOGOVA PRI RAČUNALNIM INCIDENTIMA

NCERT-PUBDOC-2014-02-341

Nacionalni CERT

foi CSS

Sadržaj

Ovaj dokument izradili su studenti Fakulteta organizacije i informatike u Varaždin u sklopu kolegija Sigurnost informacijskih sustava. Dokument je izrađen uz pomoć laboratorija za Otvorene sustave i sigurnost FOI OSS te je recenziran od strane Nacionalnog CERT-a. Rad u digitalnom obliku možete pogledati na http://security.foi.hr/wiki.

1. Uvod

Svako računalo je izloženo različitim vrstama rizika. Analiza logova može poslužiti kao preventivna mjera za sprječavanje mogućih incidenata, ali i kao forenzički alat prilikom otkrivanja uzroka incidenta. Cilj svakog administratora informacijskog sustava je smanjiti moguće rizike te učiti na greškama (ako do njih dođe).

Analiza logova razlikuje se ovisno o okruženju tj. operacijskom sustavu i programskoj podršci. Sama analiza može se provesti "ručno" bez dodatne programske podrške ili uz pomoć nekog od alata. Ovaj članak služi kao pregled osnova analize logova uz nekoliko primjera prikupljenih podataka s realnih sustava.

2. Analiza logova

Log datoteka je skup zapisa o svim događajima koji su se dogodili i koji se trenutno događaju na računalu. Jedan zapis predstavlja jedan događaj unutar sustava. Sukladno tome analiza logova predstavlja kontrolu računalnog sustava, odnosno kontrolu događaja u računalnom sustavu. Također, analiza logova pomaže u pronalasku događaja koji je prouzročio incident u informacijskom sustavu, ali može poslužiti i za prevenciju mogućih incidenata. Pojedini napredni napadi (incidenti) mogu izbrisati, zaobići ili izmijeniti zapise u logovima, ali čak i tada, uz pozorno praćenje analiza logova može dati mnogo informacija o samom incidentu.

2.1 Vrste log zapisa

Za razumijevanje zapisa unutar logova potrebno je razumjeti format zapisa u logovima. Svaki operacijski sustav ima vlastiti format zapisa. Također, programi i servisi vode vlastite logove te koriste i vlastite formate.

Postoji više različitih podjela logova prema vrstama, ali kao dvije glavne vrste logova mogu se uzeti **sistemski** (eng. System) i **aplikacijski** logovi (eng. Application). Primjeri sistemskih logova su **authentication** i **security** logovi, a primjer aplikacijskih logova su php i mysql logovi. **Error** i **access** su vrlo važni logovi, njihove zapise mogu generirati operacijski sustav i razne aplikacije na računalu.

U pojedinim slučajevima na računalu mogu postojati error logovi posvećeni samo sistemskim zapisima i error logovi posvećeni samo aplikacijskim zapisima. Zbog toga je teško svrstati error i access logove u jednu od vrsta. Pojedini stručnjaci ih često svrstavaju u sistemske logove. U ovom članku bit će prikazana oba slučaja.

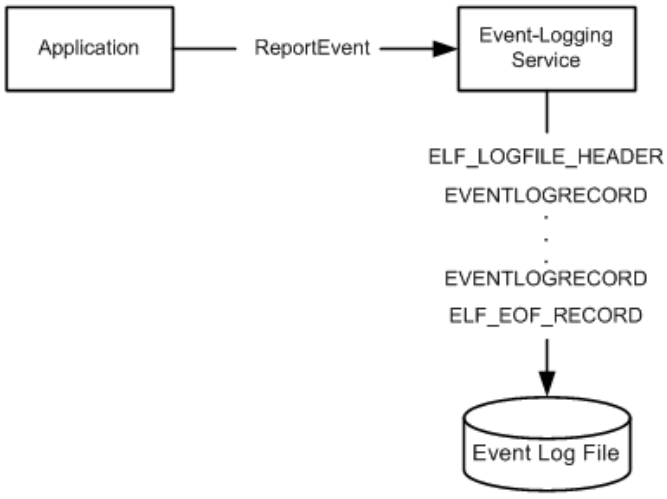
Iz te dvije glavne vrste logova granaju se druge podvrste. Također, logove je moguće podijeliti i na vremenske i statičke. Vremenski zapisi sadrže točno vrijeme događaja dok statički zapisi sadrže generalne podatke o konfiguraciji.

S obzirom na operacijski sustav računala razlikuju se nazivi logova, formati zapisa te njihova lokacija unutar sustava.

2.1.1 Sistemski zapisi u Windows operacijskim sustavima

Kod Windows operacijskih sustava podjela logova je nešto drugačija. Uz sistemske i aplikacijske logova postoje još i **sigurnosni** (eng. Security) logovi. U sigurnosnim logovima nalaze se zapisi o događajima vezanim uz prijavu i odjavu korisnika, kreiranje, uređivanje i brisanje datoteka, itd. Kako je većina sigurnosnih zapisa kreirana od strane operacijskog sustava moguće je sigurnosne logove svrstati u sistemske logove.

Kada aplikacija ili neki sistemski proces unutar Windows operacijskog sustava želi stvoriti vlastiti zapis, šalje se zahtjev s podacima „Event-Logging“ servisu koji zatim dobivene podatke formatira i dodaje u log datoteku.



Slika 1. Dijagram stvaranja aplikacijskog zapisa u logove,

izvor: http://msdn.microsoft.com/en-us/library/windows/desktop/bb309026%28v=vs.85%29.aspx

Događaji u logovima mogu se klasificirati prema razini važnosti. Razine važnosti događaja unutar sustava su:

1. Kritična (eng. Critical),
2. Pogreška (eng. Error),
3. Upozorenje (eng. Warning),
4. Informacija (eng. Information),
5. Opširan zapis (eng. Verbose).

Kod zapisa u Windows operacijskim sustavima svaki zapis se sastoji od zaglavlja koje sadrži sistemske podatke te „tijela“, odnosno podataka o specifičnom događaju koji se bilježi. Ovakvi logovi se najčešće spremaju o obliku XML datoteke, ali u nekim slučajevima postoje i zapisi u HTML obliku. Uz to aplikacijski logovi mogu imati sažeti oblik koji se najčešće sprema s .log ekstenzijom te nalikuje zapisima u Linux okruženju.

U ovom primjeru odabrano je osobno računalo s Windows 7 operacijskim sustavom. Logovima se pristupa putem "upravljačke ploče" (eng. Control panel), zatim se odaberu "administrativni alata" (eng. Administrative Tools) i na kraju odabere se "Event Viewer". Gotovo isti postupak pristupanja i analize logova vrijedi i za Windows servere. Postoje pojedine razlike među novijim i starijim verzijama servera i operacijskih sustava.

```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  <System>
    <Provider Name="Service Control Manager" Guid="{555908d1-a6d7-4695-
8e1e-26931d2012f4}" EventSourceName="Service Control Manager" />
    <EventID Qualifiers="49152">7031</EventID>
    <Version>0</Version>
    <Level>2</Level>
    <Task>0</Task>
    <Opcode>0</Opcode>
    <Keywords>0x8080000000000000</Keywords>
    <TimeCreated SystemTime="2014-02-08T12:53:50.186199300Z" />
    <EventRecordID>1327860</EventRecordID>
    <Correlation />
    <Execution ProcessID="556" ThreadID="692" />
    <Channel>System</Channel>
    <Computer>Laptop</Computer>
    <Security />
  </System>
  <EventData>
    <Data Name="param1">Mobile Connect Service</Data>
    <Data Name="param2">1</Data>
    <Data Name="param3">60000</Data>
    <Data Name="param4">1</Data>
    <Data Name="param5">Ponovno pokretanje servisa</Data>
  </EventData>
</Event>
```

Gornji primjer predstavlja zapis u sistemskom logu. Kao što je vidljivo sistemski podaci se nalaze unutar „System“ tagova, a podaci vezani uz sam događaj nalaze se unutar „EventData“ tagova. Riječ je o lokalnom usklađivanju vremena pomoću NTP-a (eng. Network Time Protocol) s pouzdanim Microsoft serverima.

Tablica 1. Značenje najvažnijih polja u sistemskom zapisu Windows OS-a

Polje	**Opis**
Provider	Izvor tj. proces koji je zatražio zapis događaja.
EventID	Broj koji identificira tip događaja (u ovom slučaju Event ID 35 predstavlja „Local Time Synchronization“ događaj).
Version	Može sadržavati podatke o verziji događaja.
Level	Numerička oznaka razine važnosti događaja (u ovom slučaju riječ je o Informacijskoj razini)
Task	Ovo polje ostavlja se na korištenje procesu koji poziva zapisivanje događaja,a može sadržavati podatke o pozivu.
Opcode	Numerička vrijednosti koja označava aktivnost koja se izvršavala u vrijeme kada je kreiran zahtjev za stvaranjem zapisa o događaju.
Keywords	Ključne riječi koje mogu pomoći pri pretraživanju srodnih zapisa.
TimeCreated	Sistemsko vrijeme kreiranja zapisa.
EventRecordID	Specifična oznaka tog zapisa, odnosno događaja.
Execution	Sadrži oznaku procesa i dretve koji su generirali događaj.
Channel	Log u koji se zapisuje događaj.
Computer	Ime računala na kojem se dogodio događaj.
Security	Sigurnosni podaci o aktivnom korisniku / računalu.
EventData	EventData tag predstavlja „tijelo“ zapisa unutar kojeg se nalaze podaci o samom događaju, a može sadržavati atribute kao što su ime.
Data	Podaci o samom događaju.

S obzirom da je riječ o Microsoftovom operacijskom sustavu, format zapisa je sličan novijim inačicama Windows Servera i Azure cloud servisu.

Slijedi jednostavan primjer error zapisa u sistemskom logu:

```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
```

```
  <System>
    <Provider Name="Service Control Manager" Guid="{555908d1-a6d7-4695-
8e1e-26931d2012f4}" EventSourceName="Service Control Manager" />
    <EventID Qualifiers="49152">7031</EventID>
    <Version>0</Version>
    <Level>2</Level>
    <Task>0</Task>
    <Opcode>0</Opcode>
    <Keywords>0x8080000000000000</Keywords>
    <TimeCreated SystemTime="2014-02-08T12:53:50.186199300Z" />
    <EventRecordID>1327860</EventRecordID>
    <Correlation />
    <Execution ProcessID="556" ThreadID="692" />
    <Channel>System</Channel>
    <Computer>Laptop</Computer>
    <Security />
  </System>
  <EventData>
    <Data Name="param1">Mobile Connect Service</Data>
    <Data Name="param2">1</Data>
    <Data Name="param3">60000</Data>
    <Data Name="param4">1</Data>
    <Data Name="param5">Ponovno pokretanje servisa</Data>
  </EventData>
</Event>
```

U gornjem primjeru nije se uspio pokrenuti servis za povezivanje s mobilnim Internetom putem USB sticka. S obzirom na to kako i error zapis spada u sistemske logove, vidljiva je gotovo ista struktura polja unutar zapisa. Razlika je što ovaj error zapis sadrži više podataka o samom događaju tj. unutar EventData tagova nalazi se više Data tagova s različitim atributima.

Za automatizirano i detaljnije nadgledanje (eng. Monitoring) prikupljenih logova najčešće se koriste dodatni alati koji će biti opisani u nastavku članka.

2.1.2 Sistemski zapisi u UNIX operacijskim sustavima

Dok u Windows operacijskim sustavima format zapisa definira Event-Logging servis tu dužnost kod UNIX operacijskih sustava obavlja *rsyslog*. Rsyslog je servis koji implementira syslog protokol na UNIX operacijskim sustavima. Syslog je zapravo de facto standard kojim se definiraju format i podaci koji će se bilježiti u svakom zapisu. Svaki syslog zapis trebao bi se sastojati od tri polja, a to su:

- PRI,
- Header,
- MSG.

PRI polje sastoji se od nekoliko ASCII znakova, a počinje znakom „<“ i završava znakom „>“. ASCII broj koji se nalazi unutar zagrada odnosi se na izvor događaja te razinu važnosti događaja. Slično kao i kod Windows operacijskih sustava, Header polje sadrži podatke o vremenu događaja i računalu na kojem se događaj dogodio. Posljednje, MSG polje, se sastoji od oznake programa ili procesa koji je generirao poruku te od samog sadržaja poruke. Konfiguracijske datoteke rsysloga moguće je prilagoditi prema vlastitim potrebama što povećava personalizaciju izvještaja i zapisa logova, ali utječe na manju standardiziranost logova.

Kod UNIX operacijskih sustava vrste logova dijele se na sistemske i aplikacijske. Događajima u UNIX operacijskim sustavima dodjeljuje se jedna od osam razina važnosti. Te razine su:

0. Izvanredno stanje (eng. Emergency),
1. Uzbuna (eng. Alert),
2. Kritična (eng. Critical),
3. Pogreška (eng. Error),
4. Upozorenje (eng. Warning),
5. Opomena (eng. Notice),
6. Informacija (eng. Informational),
7. Debug informacija (eng. Debug).

Za razliku od Windows logova, UNIX logovi se najčešće spremaju u linijskom zapisu, odnosno rijetko su strukturirani u obliku XML dokumenata. Sistemski logovi su izuzetak te mogu sadržavati više detalja kroz nekoliko redaka. Primjer sistemskog zapisa:

```
Dec 16 23:59:53 frappuccino sshd[5242]: pam_unix(sshd:session):
session opened for user dafilipaj by (uid=0)
```

Gornji primjer prikazuje autorizaciju prijave korisnika „dafilipaj“ na računalo „frappuccino“. S obzirom na to kako je pitanje o *SSH* spajanju na računalo može se zaključiti kako je riječ o udaljenoj sesiji, odnosno korisnik se spajao putem Interneta. Navedeni sistemski zapis sastoji se od polja navedenih u sljedećoj tablici.

Tablica 2. Značenje najvažnijih vrijednosti u primjeru sistemskog zapisa UNIX OS-a

Vrijednosti	Opis
Dec 16 23:59:53	Vrijeme događaja.
frappuccino	Računalo na kojem se dogodio događaj.
sshd[5242]	Process i njegov ID koji su pozvali zapis u log.
pam_unix(sshd:session)	Oznaka poruke unutar zapisa.
session opened for user dafilipaj by (uid=0)	Tekst poruke unutar zapisa.

Kao i osobna računala s Windows operacijskim sustavima razne distribucije Linuxa sadrže ugrađene i jednostavne programe za pregled logova. Za ovaj primjer odabrana je Ubuntu distribucija verzije 12.04. Unutar Ubuntua koristi se Log File Viewer, kojeg je moguće pokrenuti sa „dash home“ izbornika ili putem terminala. Log File Viewer pruža jednostavnu listu dostupnih logova te njihov pregled. Najvažniji logovi se nalaze u /var/log datoteci.

2.1.3 Apache server

Ovdje je riječ o aplikacijskim logovima unutar Apache 2 servera na Linux Ubuntu operacijskom sustavu. Prikazat će se primjeri zapisa u access i error logovima Apache 2 servera. Spomenuti logovi se odnose na zapise pristupa i grešaka unutar servera. Format zapisa u error logovima:

```
ErrorLogFormat "[%t] [%l] [pid %P] %F: %E: [client %a] %M"
```

Tablica 3. Značenje varijabli u formatu error log zapisa

Varijabla	Opis
%t	Trenutno vrijeme sustava
%l	Razina log zapisa
%P	ID trenutnog procesa
%F	Datoteka i linija koda koja je pozvala zapis u log
%E	Kod statusa aplikacije ili operacijskog sustava (npr. 500, 404…)
%a	IP adresa klijenta i port na koji je poslan zahtjev
%M	Poruka, tekstualni sadržaj

Logovi Apache servera se nalaze u /var/log datoteci ako je riječ o Linux operativnim sustavima, a u slučaju Windows operativnog sustava oni se nalaze unutar instalacijske datoteke Apache servera (npr. C:\Program Files\Apache Software Foundation\Apache2.2\log).

Najvažniji logovi koji se vode unutar Apache servera su *error* (najčešće imenovan "error_log.log" ili "error.log") i *access* logovi. S obzirom na to kako je ovdje riječ o zapisima koje poziva i generira Apache server riječ je o aplikacijskim logovima.

Error log bilježi sve pogreške koje se pojave tijekom rada servera. U slučaju računalnog incidenta ovo je najbolje mjesto za početak analize. Primjer zapisa unutar error loga na Unix operativnom sustavu:

```
[Sun Dec 15 14:51:16 2013] [error] [client 65.55.215.82] File does not exist: /var/www/robots.txt
```

Iz prethodnog primjera možemo saznati nekoliko podataka. Prvo je vidljivo vrijeme nastanka zapisa, a to je 15.12.2013. u 14:51:16 sati. Pogreška je nastala u trenutku kada je klijent s IP adresom 65.55.215.82 pokušao pristupiti nepostojećoj datoteci na adresi /var/www/robots.txt. Pomoću online servisa moguće je saznati više informacija o ovoj IP adresi. Moguće je saznati da je riječ o Microsoft automatiziranom botu koji "indeksira" web mjesta. Datoteka kojoj je pokušao pristupiti obično sadrži njemu namijenjene upute koje mu govore što smije, a što ne smije indeksirati.
Access log bilježi sve zaprimljene zahtjeve prema web poslužitelju. Format zapisa u access logu je sljedeći:

```
LogFormat "%h %l %u %t \"%r\" %>s %b"
```

Tablica 4. Značenje varijabli u formatu access log zapisa

Varijabla	Opis
%h	IP adresa udaljenog računala koje pristupa serveru.
%l	Razina log zapisa
%u	Korisničko ime u slučaju da je prihvaćena autorizacija.
%t	Trenutno vrijeme sustava
%r	Prva linija zahtjeva prema serveru.
%s	Status, odnosno kod statusa.
%b	Veličina odgovora u bajtovima.

Slijedi primjer zapisa u **Access** logu:

```
208.177.76.9 - - [16/Dec/2013:16:10:28 +0100] "GET /php/register.php HTTP/1.1" 200 5962 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
```

Kao i kod error loga zapis sadrži vrijeme i IP adresu klijenta. Također, vidljivo je koja je datoteka zatražena, status odgovora (status 200 znači OK) i veličina poslane datoteke (5962 bajta). Datoteka će biti poslana samo ako je zahtjev uspješan tj. ako je zatražena datoteka postoji i korisnik joj smije pristupiti. Uz to zapis sadrži više podataka o samom klijentu tj. programskoj podršci korisnika. Osim klijentskih zahtjeva, bilježe se i interni zahtjevi kao što je:

```
127.0.0.1 - - [15/Dec/2013:23:10:12 +0100] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.2.22 (Ubuntu) (internal dummy connection)
```

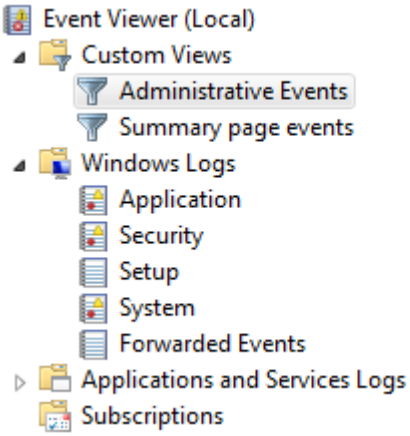
Osim gornjih, sistemskih logova bilježe se i aplikacijski logovi. Primjer takvih logova je zapis PHP errora koji se javio zbog pogreške u programskom kodu:

```
[Sun Dec 15 17:50:48 2013] [error] [client 91.207.7.13] PHP Notice: Undefined index: registration in /var/www/php/work_register.php on line 11, referer: http://studentresearchsymposium.com/php/register.php
```

Vidljivo je kako je ovaj zapis detaljniji te govori čak u kojoj datoteci i kojoj liniji koda se nalazi uzrok greške. Standardno, zapis sadrži točno vrijeme i IP adresu klijenta koji je zatražio datoteku s greškom. Ovo je dobar način otkivanja počinitelja napada na web sjedište. Za automatizirani i detaljniji "monitoring" prikupljenih logova najčešće se koriste dodatni alati koji će biti opisani u nastavku članka.

2.1.4 Windows Server

Kao i kod osobnog računala, Microsoft je u svoju programsku podršku za polsužitelje ugradio *Event Viewer* koji sadrži detaljan pregled sistemskih i aplikacijskih logova. Uz to *Event Viewer* omogućava filtriranje, pretragu i spremanje pojedinih zapisa što do određene mjere omogućava detaljan nadzor (eng. Monitoring) logova, te poduzimanje zaštitnih mjera. Logovima se pristupa putem upravljačke ploče (eng. Control panel), zatim se odaberu administrativni alati (eng. Administrative Tools) i na kraju odabere se Event Viewer. Za razliku od Apache servera logovi su nešto drugačije strukturirani. Strukturu logova moguće je vidjeti na sljedećoj slici.



Slika 2. Struktura logova u Windows okruženju

Primjer zapisa u *error* logu servera:

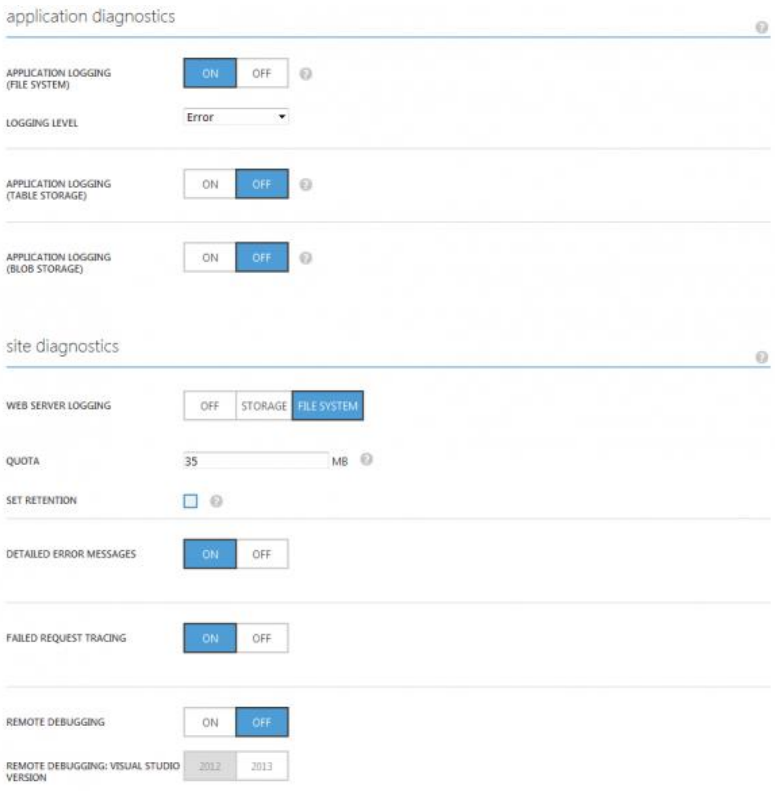
```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  <System>
    <Provider Name="Microsoft-Windows-WindowsUpdateClient" Guid="{945a8954-
c147-4acd-923f-40c45405a658}" />
    <EventID>20</EventID>
    <Version>0</Version>
    <Level>2</Level>
    <Task>1</Task>
    <Opcode>13</Opcode>
    <Keywords>0x8000000000000028</Keywords>
    <TimeCreated SystemTime="2014-01-07T15:16:19.713Z" />
    <EventRecordID>8327</EventRecordID>
    <Correlation />
    <Execution ProcessID="1072" ThreadID="2604" />
    <Channel>System</Channel>
    <Computer>WIN-TJJGQXHP53O</Computer>
    <Security UserID="S-1-5-18" />
  </System>
  <EventData>
    <Data Name="errorCode">0x80070643</Data>
```

```
    <Data Name="updateTitle">Update for Microsoft .NET Framework 4 on Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows Server 2008 x86 (KB2468871)</Data>
    <Data Name="updateGuid">{596ADB47-108D-482D-85BA-A513621434B7}</Data>
    <Data Name="updateRevisionNumber">100</Data>
  </EventData>
</Event>
```

Vidljiva je velika sličnost s formatom zapisa unutar osobnih računala s Windows operacijskim sustavom. Zapis se standardno sastoji od zaglavlja (eng. Header) i tijela zapisa (eng. Body). EventViewer omogućuje također poduzimanje određenih mjera kao što su na primjer pokretanje specifičnog programa, obavještavanje putem elektroničke pošte ili ispisivanje poruke u pop-up prozoru na ekranu.

2.1.5 Azure cloud

Danas su sve popularniji cloud servisi. Svaki cloud servis ima vlastiti pristup prikupljanju i dijeljenju logova. Kod Azure cloud servisa dio logova se prikuplja automatski, a dio je po potrebi moguće uključiti u postavkama servisa. Svim postavkama i dostupnim informacijama moguće je pristupiti putem online portala na http://www.windowsazure.com, a dio podataka dostupan je i putem FTP protokola.



Slika 3. Azure postavke za prikupljanje logova

Na trećoj slici vidljive su opcije dostupne korisnicima ovoga servisa na samome portalu. Azure nudi i dosta detaljan monitoring logova što smanjuje potrebu za korištenjem dodatnih programskih rješenja. Slika "Azure monitoring" pokazuje osnovne podatke o radu servera.
Kao i kod standardnih Windows servera Azure sadrži error log u detaljnijem, strukturiranom zapisu.
Primjer Error log zapisa na Azure cloud servisu:

```
HTTP Error 404.0 - Not Found
The resource you are looking for has been removed, had its name changed, or is
temporarily unavailable.
Most likely causes:

    The directory or file specified does not exist on the Web server.
    The URL contains a typographical error.
    A custom filter or module, such as URLScan, restricts access to the file.

Things you can try:

    Create the content on the Web server.
    Review the browser URL.
    Create a tracing rule to track failed requests for this HTTP status code and
see which module is calling SetStatus. For more information about creating a
    tracing rule for failed requests, click here.

Detailed Error Information:
Module    IIS Web Core
Notification    MapRequestHandler
Handler         StaticFile
Error Code      0x80070002
Requested URL         http://cquest:80/robots.txt
Physical Path
C:\DWASFiles\Sites\cquest\VirtualDirectory0\site\wwwroot\robots.txt
Logon Method    Anonymous
Logon User      Anonymous
More Information:
This error means that the file or directory does not exist on the server. Create
the file or directory and try the request again.
```

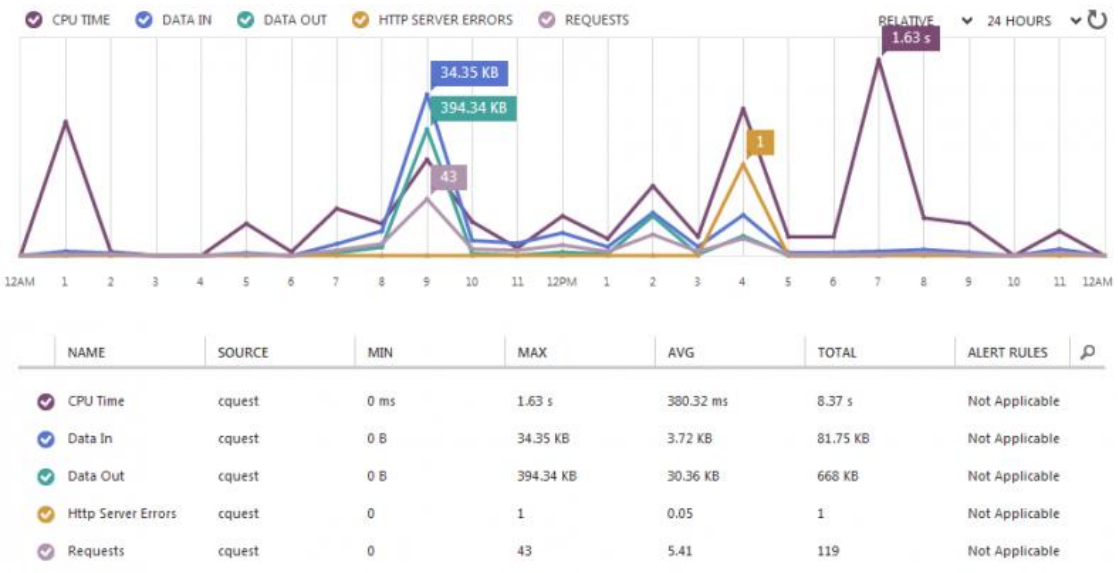
Iz gornjeg primjera jasno se može iščitati mjesto, vrijeme i razlog nastanka greške, a uz to ponuđeni su i neki od mogućih uzroka greške. Azure format zapisa sadrži puno više informacija te je prilagođen svim vrstama korisnika. Primjer http zapisa koji predstavlja Windows inačicu Apache access loga:

```
2014-01-03 20:03:03 CQUEST GET /robots.txt X-ARR-LOG-ID=7597f108-cc45-45b0-bac5-
85719661bc18                  80                  -                  66.249.76.101
Mozilla/5.0+(compatible;+Googlebot/2.1;++http://www.google.com/bot.html)    -    -
www.cquest.eu 404 0 2 431 616 31
```

Format zapisa je sljedeći, a nalikuje prethodno objašnjenim formatima unutar Windows operacijskih sustava:

```
#Fields: date time s-sitename cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) cs(Cookie) cs(Referer) cs-host sc-status sc-substatus sc-win32-status sc-bytes cs-bytes time-taken
```

Ovdje je ponovno riječ o botu koji je indeksirao web mjesto. Ovog puta riječ je o Google botu koji je zatražio robots.txt datoteku u naznačeno vrijeme (3.1.2013. u 20:03:03). IP adresa Google bota je 66.249.76.101. Vidljivo je kako je status 404 tj. tražena datoteka nije pronađena. Poslan je 431 byte, a primljeno 616 byteova.



Slika 4. Azure monitoring

3. Alati za analizu log zapisa

Standardni alati koji dolaze uz operacijske sustave nisu uvijek najbolji pri vizualizaciji podataka i za brze preglede nad njima. Stoga danas na tržištu postoje mnogi alati, komercijalni i besplatni, za analiziranje i vizualizaciju log zapisa. Ovisno o vrsti namjene alati mogu biti interaktivni gdje krajnji korisnik točno odabire koji podataka želi vidjeti. Alati za analizu logova mogu poslužiti kao prezentator log zapisa kroz vrijeme, te slanje obavijesti odgovornim osobama o pojedinim događajima u sustavu.

3.1.1 Goaccess

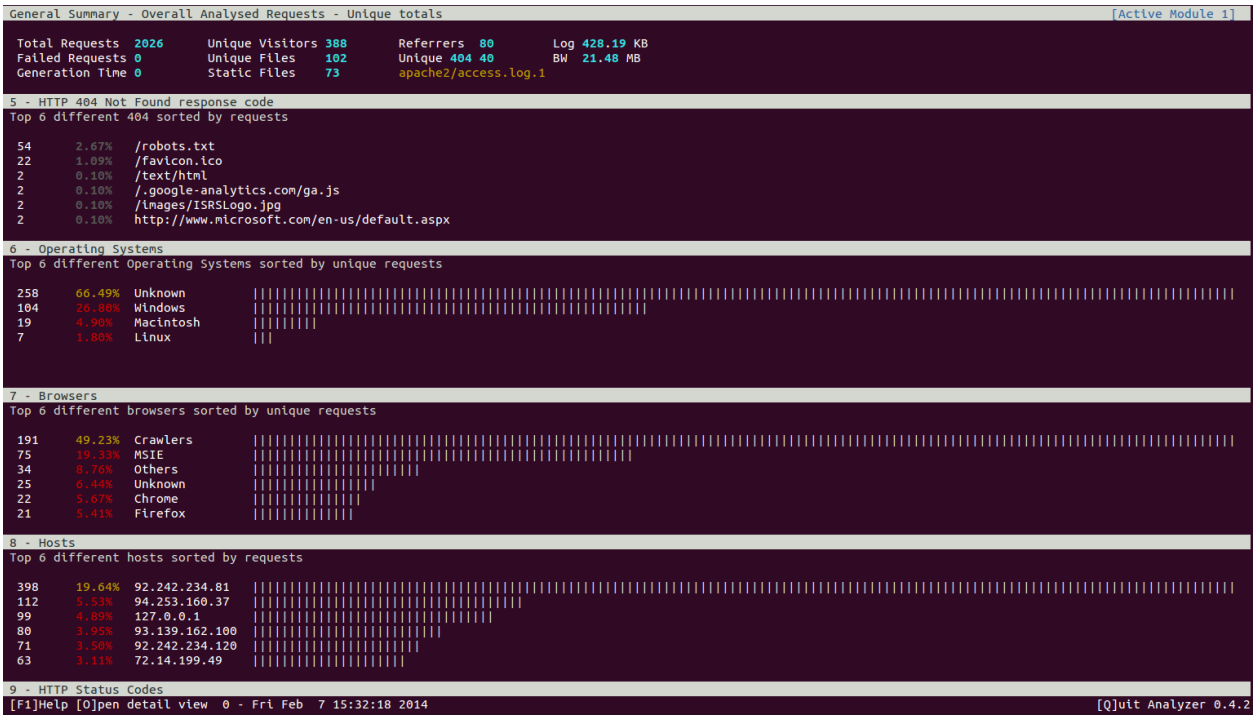
Goaccess je besplatni open source alat za analizu Apache access logova. Pokreće se unutar terminala. Analiza započinje pozivanjem Goaccess programa unutar terminala s nekoliko atributa. Kao atributi obavezna je putanja do željene log datoteke, a opcionalni argumenti

služe za ograničavanje HTTP statusnih kodova, lista user agenata, IP adresa koje će se isključiti iz obrade, itd. Primjer jednostavnog poziva:

```
goaccess –f  var/log/apache2/access.log
```

Ovakav poziv prikazuje unutar terminala rezultat analize. Rezultati analize su prikazani u obliku generalnog sažetka i jedanaest kategorija podataka. Unutar generalnog sažetka nalaze se podaci poput ukupnog broja zahtjeva, jedinstvenih posjetitelja, datoteka itd. U ovom slučaju postoji ukupno 2026 zahtjeva prema serveru, 388 jedinstvenih posjetitelja, 40 grešaka s 404 kodom itd. Spomenute kategorije podataka su:

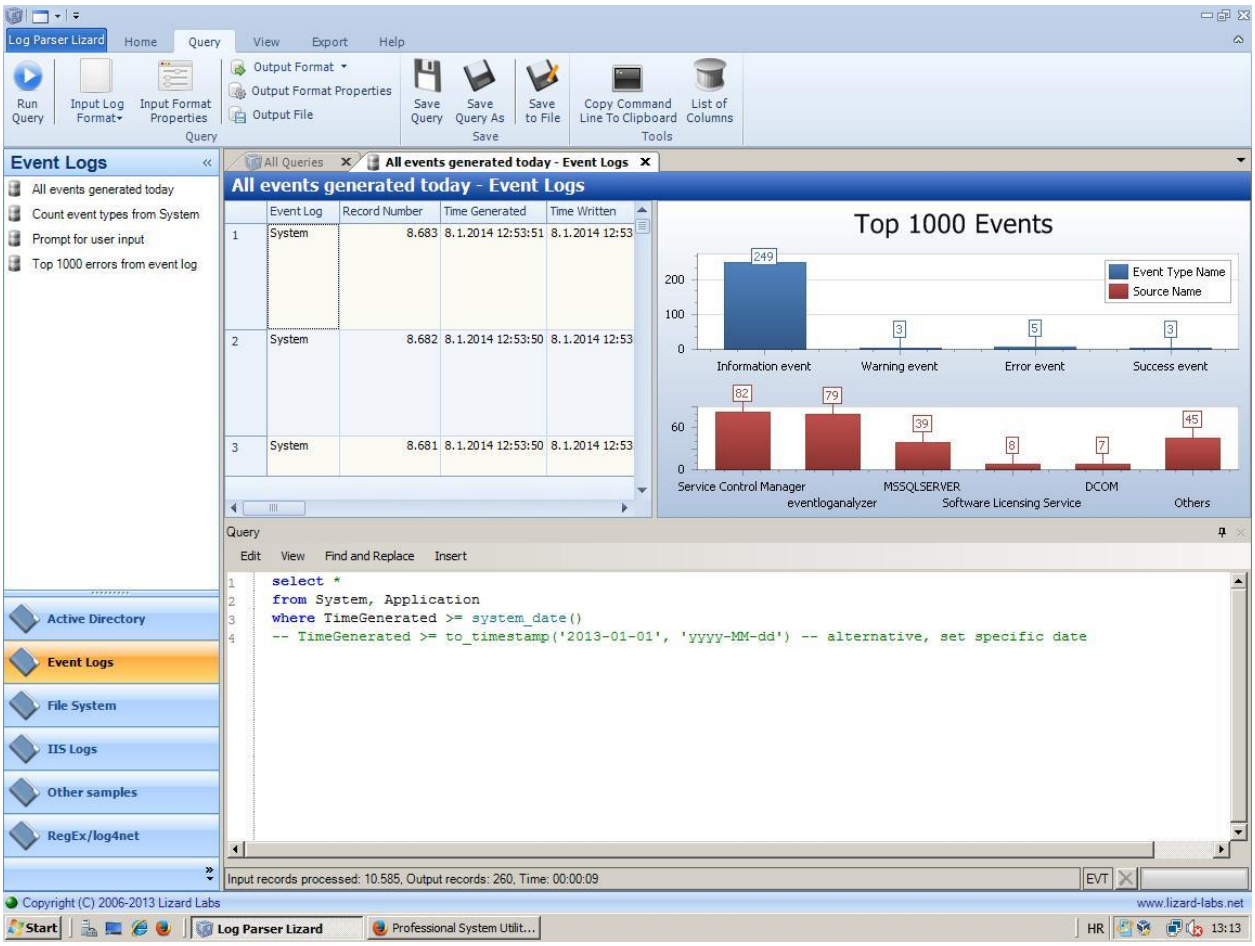
1. Kronološki prikaz ukupnog broja jedinstvenih posjetitelja,
2. Najtraženije datoteke (URL-ovi),
3. Najtraženije statične datoteke (CSS datoteke, JavaScript datoteke, slike itd.),
4. Web adrese koje usmjeravaju na promatrani server (poredane po broju proslijeđenih zahtjeva),
5. Datoteke (URL-ovi) koji su prouzročili najviše grešaka s kodom 404, odnosno datoteke koju su zatražene, ali nisu pronađene na serveru,
6. Najčešći operacijski sustavi posjetitelja,
7. Najčešći preglednici,
8. Najčešće IP adrese,
9. Najčešće vraćeni HTTP statusni kodovi,
10. Web mjesta koja su usmjerila najviše posjetitelja prema promatranom serveru,
11. Najčešće ključne riječi unutar Google pretraga koje su usmjerile posjetitelje na promatrani server.



Slika 5. Dio sučelja Goaccess alata

3.1.2 LogParser

Log Parser je Microsoftov besplatni komadni alat za analizu logova unutar sustava. Alat omogućuje univerzalni upitni pristup tekstualnim podacima kao što su log zapisi, XML zapisi, CSV zapisi, te naravno zapisi Windows operativnih sustava kao što su Eventlog, Registry, sistemski zapisi te drugi. Alat koristi SQL sintaksu za pregled i analizu podataka. Pomoću njega se radi upit nad određenim zapisom te se vizualno prezentira putem dijagrama. Krajnji korisnici ne vole previše raditi s alatima u komandnoj liniji. Zbog toga je razvijeno GUI sučelje, prikazano na slici 6, kojega je implementirala grupacija Lizard Labs.



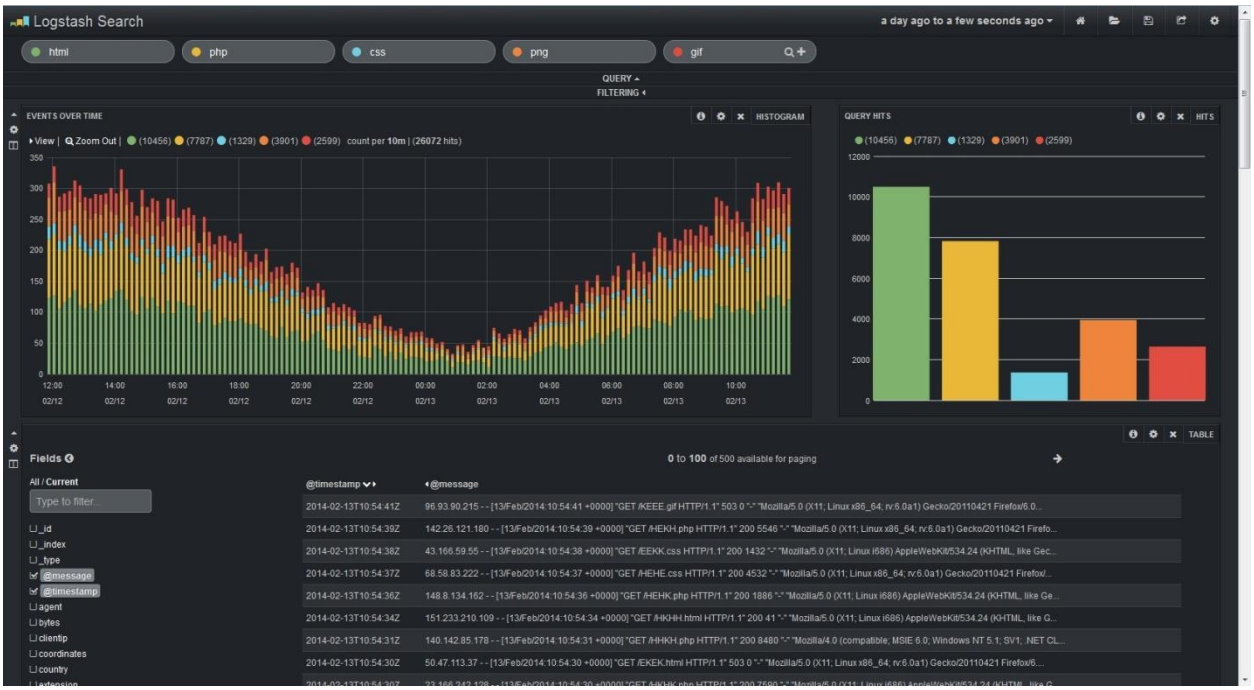
Slika 6. LogParser - LizardLabs GUI

3.1.3 Logstash

Još jedan besplatni alat za Unix bazirane operacijske sustave je Logstash. Logstash se ističe po vrlo velikim, naprednim mogućnostima filtriranja zapisa u logu no zahtjeva nešto više vremena za učenje. Napredni korisnici mogu kreirati do najmanjih detalja personalizirane, prilagođene analize.

Nakon preuzimanja alata i njegove instalacije, potrebno je kreirati konfiguracijsku datoteku u kojoj se specificira koje se sve logove želi uzeti za analizu te kako ih se želi prikazati. U ovoj konfiguracijskoj datoteci leže spomenute napredne mogućnosti filtriranja podataka i prilagođavanja analize.

Interaktivan pregled dobivenih rezultata analize moguće je dobiti u web pregledniku pomoću dodataka preuzetih s programom. Web sučelje je realizirano pomoću *Kibana* dodatka.



Slika 7. Logstash realiziran pomoću Kibana dodatka

3.1.4 Petit

Petit je besplatan program za analizu logova napisan za UNIX operacijske sustave. Glavna funkcionalnost ovog programa je analiza jedne datoteke, neovisno o broju zapisa u njoj. Kao najkorisnije funkcionalnosti ističu se poredak ključnih riječi po učestalosti ponavljanja, filtriranje zapisa od čestih, neopasnih sistemskih zapisa, generiranje jednostavnih grafova koji prikazuju raspodjelu zapisa prema datumu. Ovaj alat zapravo pomaže uočiti bitne stavke unutar velikih logova. Također, jednostavna statistika koju pruža govori na što je potrebno obratiti pažnju (npr. koje datoteke često uzrokuju greške u radu i slično).

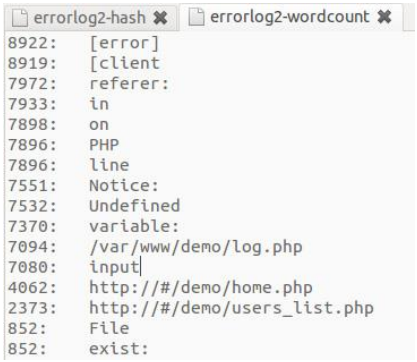
Program se pokreće i izvodi unutar terminala. Nakon preuzimanja, program je potrebno otpakirati i odmah je spreman za upotrebu. Lista dostupnih funkcija se ispisuje pomoću "petit -h" ili "petit --help" kao i kod mnogih drugih Linux programa.

Za sljedeće primjere koristit će se error log s velikim brojem zapisa koji uključuju i pokušaj napada na web stranicu. Koristit će se funkcije „wordcount“ i „hash“ unutar programa Petit. Uz naredbe wordcount i hash moguće je koristiti dodatne filtere za određene ključne riječi unutar logova pomoću naredbe „filter“ ili „fingerprinting“. Izvršavanje programa se izvodi pomoću sljedećih naredbi:

```
petite --wordcount error.log.2 > errorlog2-wordcount.txt
```

```
petite --hash error.log.2 > errorlog2-hash.txt
```

Naredba „wordcount“ vratiti će popis najučestalijih ključnih riječi poredanih po broju pojavljivanja. Sljedeća naredba, hash, će vratiti pročišćeni log bez sistemskih zapisa koji se često ponavljaju te se smatraju sigurnima i nepotrebnima u ovom slučaju. S obzirom da je riječ o velikoj datoteci s puno zapisa i izlazni podaci će sadržavati puno informacija. Kako bi se povratne informacije sačuvale za kasniju uporabu te bile preglednije preporučuje se spremanje rezultata u nove datoteke.



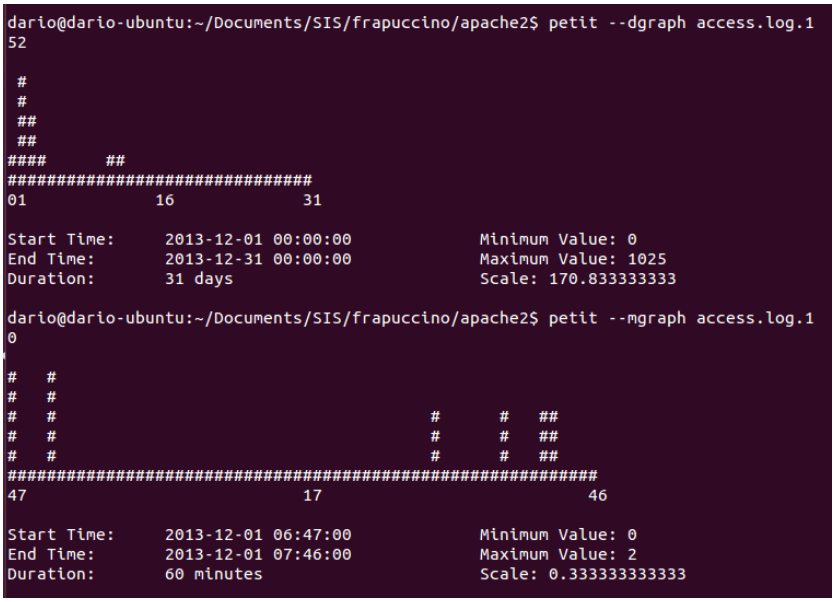
Slika 8. Rezultati naredbe wordcount

U povratnim rezultatima moguće je uočiti anomalije tj. ključne riječi koje odskaču od ostalih s obzirom na učestalost pojavljivanja. U error logu izbrojane su ukupno 8922 greške, a od toga je 7896 vezano uz PHP. Jako velik broj grešaka je vezan uz datoteke *log.php*, *home.php* i *users_list.php*.

Detaljnijim pregledom otkriva se ponavljajući uzorak neuspjelih pokušaja pristupanju navedenim stranicama. Ovdje je riječ o nečijem pokušaju pronalaženja sigurnosnog propusta s ciljem krađe informacija iz baze podataka ili dobivanja administrativnih ovlasti. Ovakve napade potrebno je prijaviti nadležnim institucijama ili osobama te pojačati sigurnost na mjestima koja su bila najizloženija.

Osim do sada navedenih funkcija Petit sadrži i funkcije za crtanje grafova. Grafovi pokazuju distribuciju zapisa kroz određeno vrijeme. Definirane su funkcije za crtanje grafova na temelju logova u posljednjih 60 sekundi, 60 minuta, 24 sata, 31 dan, 12 mjeseci ili 10 godina. Grafovi su u ovom slučaju efikasniji kod logova s manje zapisa jer oscilacije lakše dolaze do izražaja. Za crtanje grafova korištene su sljedeće naredbe:

```
petite –dgraph access.log.1
petite –mgraph access.log.1
```



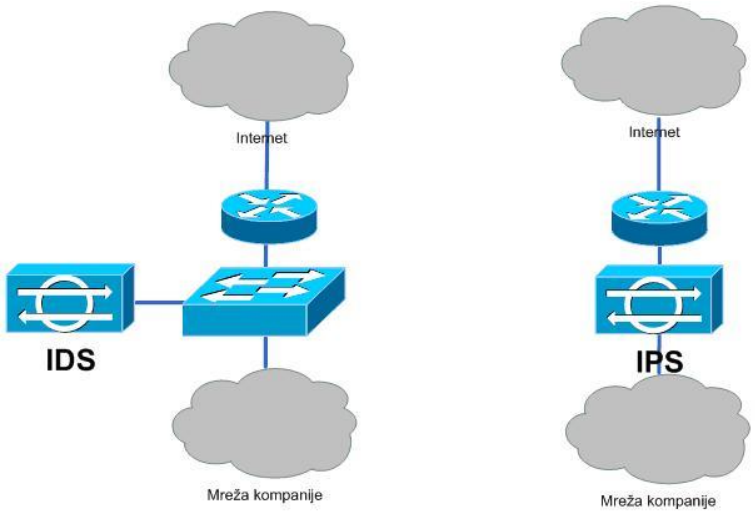
Slika 9. Iscrtani grafovi u programu Petit

3.1.5 Security onion

Security Onion je Linux distribucija namijenjena lakom podizanju različitih IDS (eng. Intrusion Detection Systems) sustava i mrežnog nadzora. Sadrži alate koji olakšavaju upravljanje log zapisima. Razvoj Security Onion distribucije počeo je 2008. godine, dok je 2009. izašla prva verzija s alatima Snort i Squil. Godine 2010. puštena je nova verzija temeljena na Ubuntu 10.04 s alatima *Suricata*, *Squert* i OSSEC. Kasnije su dodani alati *Argus*, *Bro*, *NetworkMiner* i *Snorby* te podrška za distribuirane senzore. Security Onion posjeduje alate koji omogućuju pregled različitih izlaznih formata koje generiraju sustavi poput *Broa*, *Suricate* ili *Snorta*. Distribucija sadrži mnoge alate za detaljan pregled i analizu zapisa, kao što su *Squert*, *Squil*, *ELSA* i mnogi drugi alati i skripte. Alat se svakodnevno razvija i poboljšava.

Sustavi za detekciju upada (IDS, eng. Intrusion Detection Systems) su sustavi koji nadgledaju rad nekog sustava i otkrivaju pokušaje napada. Funkcije IDS – a su da pripomažu i ublažavaju štetu koja može nastati neovlaštenim pristupom sustavu koji se nadzire te tijekom nadziranja automatski obavještavaju nadležnu osobu o anomalijama, odnosno administratora sustava. Izvedbe IDS sustava mogu biti izvedeni na fizičkoj ili na programskoj razini. Postoji više različitih tipova IDS sustava. Jedan od tipova je sustav detekcije upada temeljen na mrežnom prometu (NIDS, eng Network Intrusion Detection Systems). To je sustav koji neovisan o glavnom sustavu. Njegova je zadaća identificirati napade, upade i ostalo provjerom mrežnog

prometa. Za razliku od vatrozida (eng. Firewall), NIDS ne utječe na mrežni promet jer prisluškuje (snifa, eng. sniff) te pregledava sadržaj paketa. Razlikujemo dva različita načina izvedbe NIDS–a. To su sustavi za detekciju (IDS, eng. Intrusion Detection Systems) i sustavi za prevenciju upada (IPS, eng. Intrusion Prevention Systems). Alati koji koriste ove načine su Snort, Bro i Suricata.



Slika 10. NIDS, dva načina provedbe

Snort je alat otvorenog koda (eng. open source) za detekciju i prevenciju upada (IDS / IPS). Snort vrši analizu nad mrežnim prometom u stvarnom vremenu. Prevencija se temelji na pravilima koje korisnik može sam definirati u postavkama alata. Snort nema nikakvo grafičko sučelje i izvršava se putem komandne linije. Danas to nije sasvim praktično te se uz njega koriste drugi alati, odnosno njihovo grafičko sučelje, za pregled prikupljenih zapisa kao što su Snorby i Squert. Alat je orijentiran na sam podatkovni promet, odnosno na pakete.

Za razliku od Snorta, Bro je također alat otvorenog koda za detekciju i prevenciju upada te za mrežni nadzor (NSM, eng. Network Security Monitoring), koji analizira mrežne konekcije.

Oba dva alata vrlo su popularna i u zajedničkoj integraciji pružaju vrlo dobar oslonac za detekciju i prevenciju upada u sustav. Kako Snort, tako i Bro omogućuje definiranje pravila pomoću kojih će se pratiti mrežni promet. Prikaz zapisa moguće je prikazati preko grafičkog sučelja ELSA.

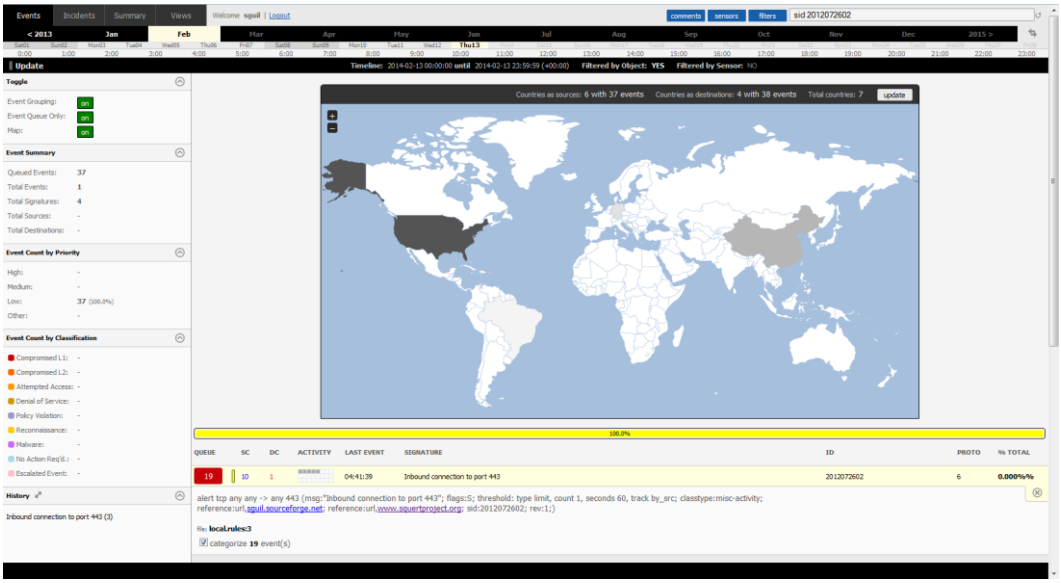
Suricata je alat otvorenog koda koji služi za detekciju i prevenciju upada temeljen na mrežnom prometu (NIDS). Razvijen je da zamjeni već postojeće alate. Prednost ovog alata je visoka skalabilnost jer omogućuje višedretvenost, odnosno dodjeljivanje jednog procesora

(jedne jezgre) točno jednom senzoru, iz tog razloga može obraditi veću količinu mrežnog prometa. Također, prednost alata je prepoznavanje najčešće korištenih protokola. Višedretvenost omogućuje protok velike količine podataka što je dovoljno za više gigabitne mreže, za razliku od Broa koji omogućuje protok oko jednog gigabita Snort obrađuje puno manje količine podataka. Također je omogućeno pisanje pravila, ali na višoj razini od dosadašnjih alata.

Snorby je Web 2.0 alat za prikaz informacija baziran na NIDS porukama. Snorby je potrebno upariti s nekom od baza podataka koju će puniti alati kao Snorta, Suricate, Broa ili slični. Alat je namijenjen za vizualan prikaz i analizu zapisa, postavljanje određenih upita, pretraživanje među zapisima i drugo. Kao početna stranica otvara nam se radna površina (eng. Dashboard) koja prikazuje brzi pregled zapisa mrežnog prometa. Na radnoj površini možemo odabrati vremenski period koji nas interesira. S desne strane vidljiv je popis senzora, popis pet najaktivnijih korisnika, jedinstvenih događaja te događaji klasificirani prema pojedinim kriterijima. Alat nudi mogućnosti pretraživanja događaja klikom na karticu Search u gornjem izborniku. Snorby također ima mogućnost obavještavanja korisnika putem email poruka ili pokretanjem nekog programa.

Slika 11. Snorby - Dashboard[1]

Squert je kao i Snorby grafičko sučelje za alate poput Snort, Squil i drugih koji nudi dodatne opcije za prikaz zapisa. Snorby prikazuje metapodatke, vremenske sljedove i ostalo. Squert omogućuje prikaz podataka putem grafova, te prikaz podataka korisnika na karti svijeta. Squert također omogućuje detektiranje lokalnih zapisa, odnosno zapisa samog operacijskog sustava te zbog toga ga svrstavamo pod lokalni sustav za detekciju i prevenciju upada. (HIDS, eng. Host – based Intrusion Detection Systems).

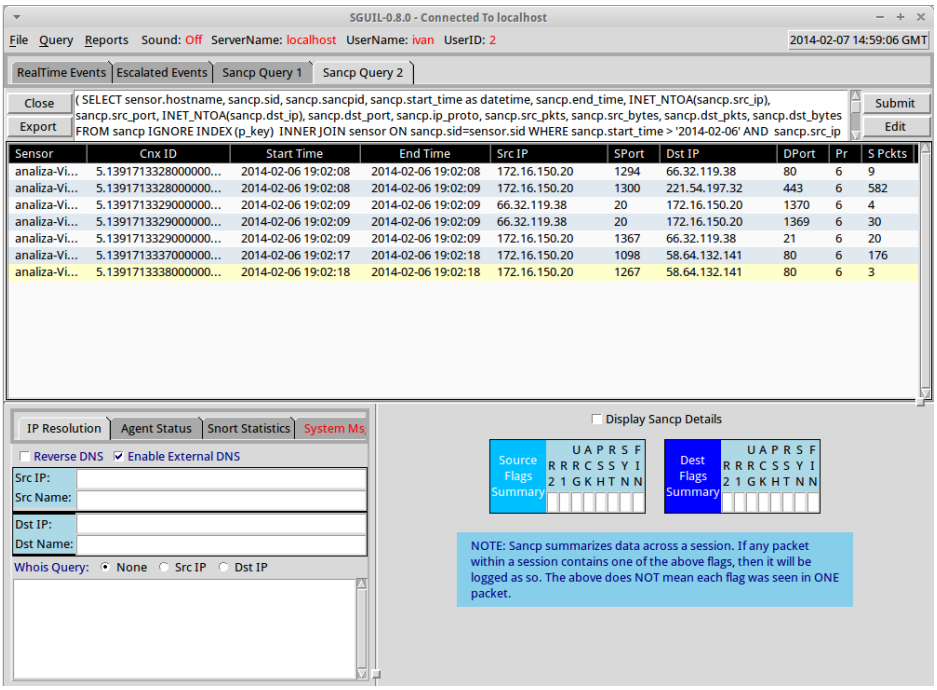


Slika 12. *Squert* – Prikaz zapisa na mapi[2]

Squil je alat za detekciju i prevenciju upada u sustav, koji radi na mrežnoj razini i omogućuje pregled sadržaja paketa. Squil ima upiti jeziki sličan SQL koji omogućuje zadavanje upita nad zapisima.

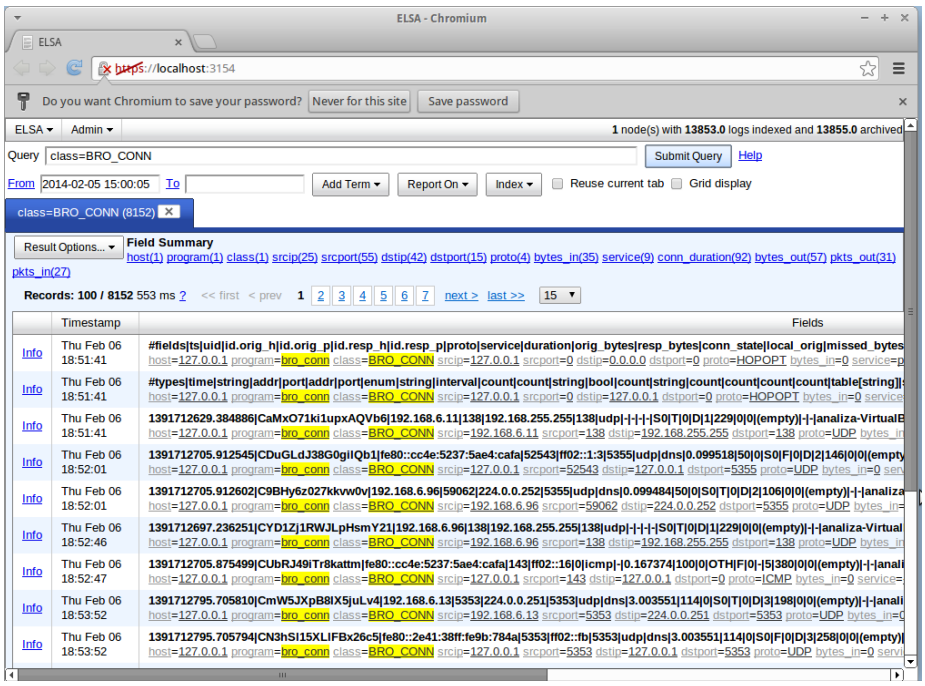
[1] Preuzeto sa: http://demo.snorby.org/dashboard - online demo verzija

[2] Preuzeto sa: https://demo.sguil.net/squert/ - online demo verzija



Slika 13. Squil

ELSA je centraliziran alat koji se bazira na syslog okviru (eng. framework), sadrži web sučelje za sistemske logove koje omogućuje pregled zapisa i njihovo pretraživanje. Uključuje alate za pregled logova, obavijesti putem emaila, postavljenje i planiranje upita te grafički prikaz. Ovaj alat može indeksirati veliki broja zapisa (30k log/sec), posjeduje LDAP autentikaciju i mnoge druge mogućnosti.



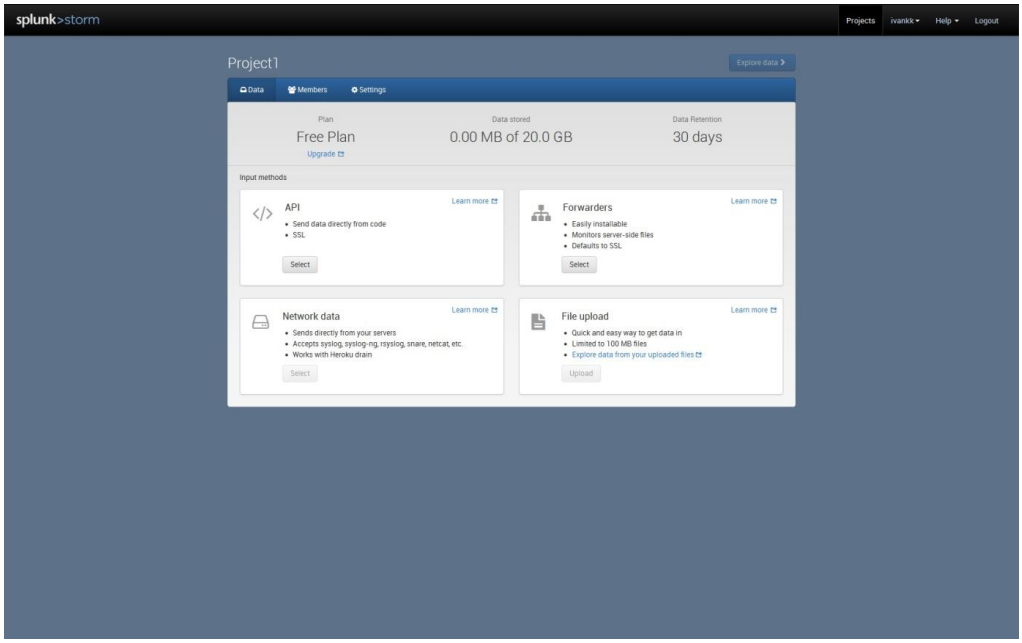
Slika 14. ELSA

3.1.6 Splunk Storm

Splunk je međunarodno poduzeće sa sjedištem u San Franciscu koje je započelo s radom 2003. godine. Sama tvrtka razvija alat za pretraživanje, nadziranje i analizu podataka putem web sučelja. Najpoznatiji alat je Splunk Enterprise.

Splunk je dostupan svim korisnicima, za osobnu upotrebu je besplatan je uz ograničenje u obradi prometa. Za komercijalnu uporabu potrebno je posjedovati licencu radi skidanja ograničenja mogućeg dnevnog limita obrade podataka, obrada je ograničena na 500 MB. Ovaj alat omogućuje pretraživanje, odnosno prikupljanje različitih zapisa u realnom vremenu, ali istovremeno nudi i pregled zapisa kroz povijest. Moguće je prikupljati podatke lokalno, s udaljenih računala, servera, mobitela.

Trenutna verzija *Splunk Enterprisea* 6 nudi neka poboljšanja naspram prijašnjih verzija. Jedno od najvećih je integrirana mapa omogućuje prikaz geografskih podataka. Također, postoji cloud servis Splunk Storm koji omogućuje pohranu do 20GB podataka.



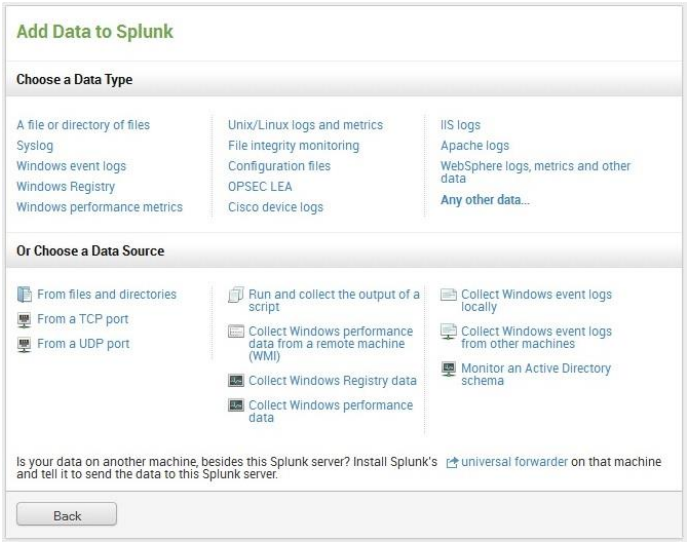
Slika 15. Splunk storm

Splunk Enterprise je samostalan alat koji se posebno instalira na neki od operacijskih sustava Windows, Linux, Unix ili OSx.

Za korištenje podataka potrebno je prvo dodati izbor podataka odnosno log zapise za analizu. Alat prihvaća različite formate podataka, kao što su na primjer event logovi, web logovi, mrežni zapisi te omogućuje čitanje specijaliziranih formata. Zapisi mogu biti pohranjeni

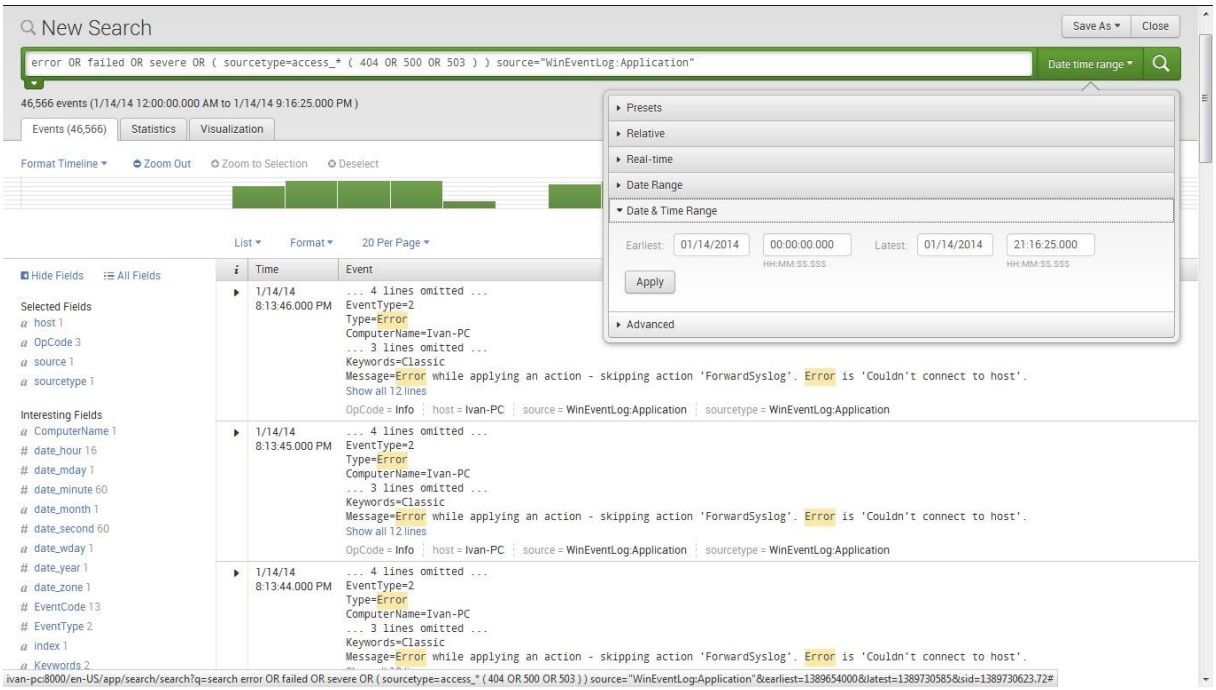
lokalno u sustavu ili mogu biti pohranjeni na udaljenom uređaju. Alat omogućuje spajanje na mrežna sučelja, udaljena računala i ostalu opremu.

Podaci se mogu razvrstati u četiri kategorije: datoteke i direktoriji, mrežni događaji, OS zapisi te ostali izvori. Alat raspoznaje podatke prilikom definiranja izvora podataka, izborom predefiniranih formata zapisa te također direktnim konfiguriranjem inputs.conf datoteke. Slika 16 prikazuje web sučelje za definiranje unosa podataka, odabira udaljenih uređaja i ostalo.



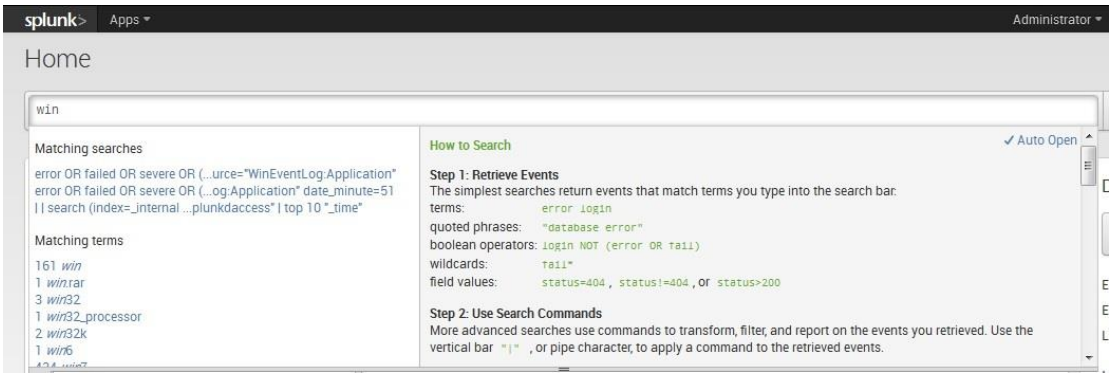
Slika 16. Add Data

Alat omogućuje pretragu indeksiranih zapisa u realnom vremenu. Posjeduje pregledno grafičko sučelje koje omogućava brzu, jednostavnu i laganu pretragu nad složenim upitima te pregled zapisa po određenim kriterijima. Na slici 17 vidimo primjer složenog upita nad tražilicom unutar alata. Vidljiv je i grafički prikaz zatraženih podataka kroz vrijeme. Rezultati pretrage nadalje se mogu obrađivati prema korisničkim zahtjevima te kreirati izvještaji s interaktivnim grafovima, tablicama i drugo. Ako ne znamo u potpunosti ono što tražimo, alat će nam ponuditi pomoć oko izbora mogućih upita i nadopuna riječi kao što je vidljivo na slici 18.

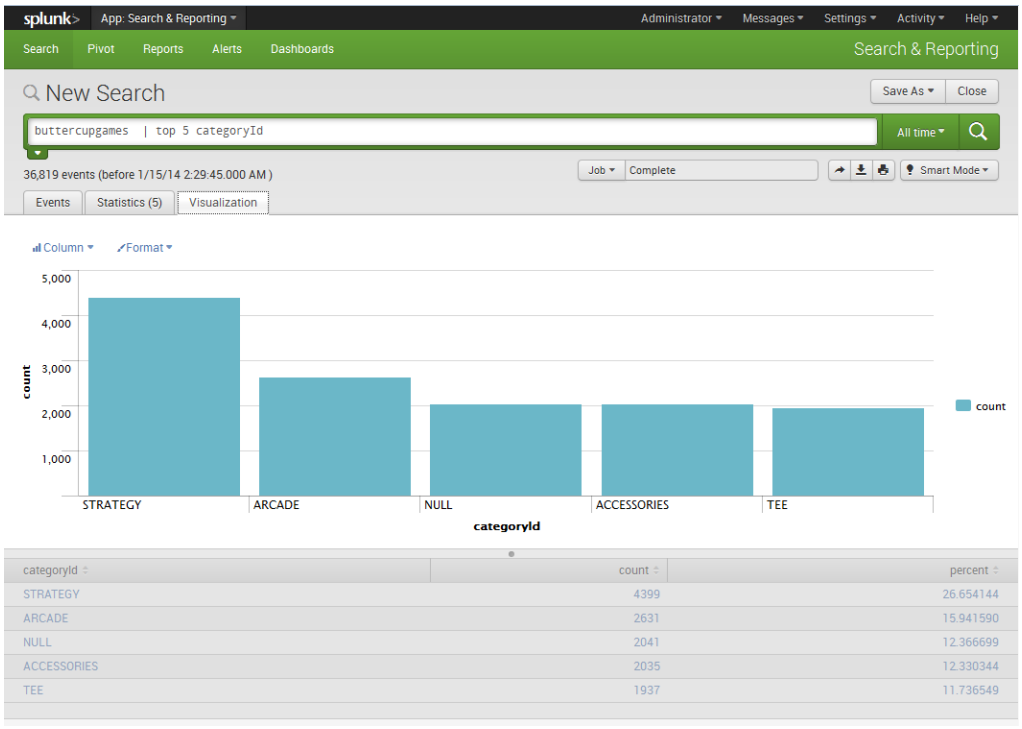


Slika 17. Primjer prikaza upita unutar Splunk alata

Alat omogućuje automatsko generiranje izvještaja i slanje obavijesti, na primjer putem emaila. Također, alat je moguće podesiti da reagira u realnom vremenu, odnosno da automatski pošalje obavijest odgovornoj osobi, odnosno administratoru o nekom događaju na sustavu koji se nadzire.



Slika 18. Pretraga zapisa



Slika 19. Top 5 categoryId prikazan vizualno

Nakon pretraživanja zapisa pretragu možemo spremiti u obliku izvještaja, panel ploče, kao upozorenje ili kao vrstu događaja unutar sustava. Izvještaj možemo spremiti u PDF format.

4. Zaključak

Pohrana i analiza log zapisa, događaja i ostaloga vezanog za pojedini sustav u današnje vrijeme omogućuje nadzor sustava i kontrolu nad njima. Kako su danas računalni incidenti česta pojava, a težnja informacijskog poslovanja je davanje besprijekorne usluge, takvi zapisi nam mogu pomoći u unaprjeđenju zaštite od računalnih incidenata. Pomoću njih vidimo što se događalo u prošlosti, te na temelju njih možemo obaviti neku analizu ili donijeti odluku. Danas također postoje alati koji u realnom vremenu prate tok podataka i događaje s više sustava te time osiguravaju pravovremenu informaciju o incidentu i pomažu prilikom zaštite informacijskih sustava.

5. Literatura

1. Apache HTTP Server 2.4 Documentation, dostupno na https://httpd.apache.org/docs/2.4/logs.html
2. Windows 2000 Server, Event Logging and Viewing, dostupno na http://technet.microsoft.com/en-us/library/bb726966.aspx
3. Analiza logova u računalnoj forenzici, Dr.Sc.E.E. Damir Delija, dostpuno na http://www.slideshare.net/DamirDelijadamirdeli/analiza-logova-u-digitalnoj-forenzici
4. Učinkovito nadgledanje i upravljanje logovima u Linux operacijskim sustavima, Branimir Radić, dostpuno na http://sistemac.srce.unizg.hr/fileadmin/user_root/seminari/Srce-Sys-Seminari-Logovi-Linux.pdf
5. Uncommon Event Log Analysis for Incident Response and Forensic Investigations, Technical Blog, dostupno na http://www.cylance.com/techblog/Uncommon-Event-Log-Analysis-for-Incident-Response-and-Forensic-Investigations.shtml
6. Using logs for forensics after a data breach, Gorka Sadowski, dostpuno na http://www.networkworld.com/news/tech/2010/110810-data-breach-logs-forensics.html?page=1
7. LogParser 2.2, dostpuno na http://technet.microsoft.com/en-us/scriptcenter/dd919274.aspx
8. Petit, dostpuno na http://crunchtools.com/software/petit/
9. Splunk Storm, dostpuno na https://www.splunkstorm.com/
10. Goaccess, dostpuno na http://goaccess.prosoftcorp.com/
11. Suricata, dostupno na http://suricata-ids.org/
12. EDPACS, Understanding intrusion detection systems, dostupno na: http://trygstad.rice.iit.edu:8000/Articles/UnderstandingIDS-EDPAC.pdf
13. IDS, dostupno na http://netsecurity.about.com/cs/hackertools/a/aa030504.htm
14. Snort, dostupno na https://www.usenix.org/legacy/publications/library/proceedings/lisa99/full_papers/roesch/roesch.pdf
15. IDS i IPS, dostupno na http://sistemac.srce.unizg.hr/index.php?id=35&no_cache=1&tx_ttnews[tt_news]=339
16. Security Onion, dosutpno na http://blog.securityonion.net/p/securityonion.html
17. Squert, dostupno na http://www.squertproject.org/
18. Snorby, dostupno na https://snorby.org/
19. Bro, dostupno na http://www.bro.org/index.html
20. A brief study and comparison of Snort and Bro, dostupno na http://www.ijarcce.com/upload/august/4-A%20brief%20study%20and%20comparison%20of.pdf
21. Snort, dostupno na http://snort.org/
22. ELSA, dostupno na http://code.google.com/p/enterprise-log-search-and-archive/