

SİBER OLAY TESPİT (LOG ANALİZİ)

ENES ŞAHİN

19360859012

Log Nedir?

- Bilişim sistemlerinin ürettiği kayıt bilgilerine log denir. Loglama ise bu kayıtların ve dijital hareketlerin tutulma işlemidir.
- Meydana gelen olayları ve hareketleri kayıt altına alırlar.
- Yazılımlar, IoT cihazları, işletim sistemleri ve web sunucuları aktif olarak log kaydı tutarlar.
- *Örneğin bir web sunucusunun içerisinde yer alan log dosyaları incelenerek ziyaretçilerin nereden geldiği ve web sunucusuna hangi istekleri gönderdiği kolaylıkla anlaşılabilir.

Loglar Nereden Üretilir?

- Uygulamalar
- *Konteynerlar
- Veritabanları
- Güvenlik Duvarları
- Uç Noktalar
- IoT Cihazlar
- Ağlar

Loglar Nereden Üretilir?

- Ağ Hizmetleri
- Sunucular
- İşletim Sistemleri

Günlük Log Kaydı Örneği

- 127.0.0.1 user-identifier frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200 2326 (Wikipedia sunucu günlük kaydı örneği)
- user-identfier → Kullanıcı Tanımlayıcısı
- 127.0.0.1 → Uzak ana makine adı. DNS ana makine adı IP kullanılır.
- Frank → Sayfayı isteyen kişinin kullanıcı kimliği.
- [10/Oct/2000:13:55:36 -0700] → Eylemin tarihi.
- GET /apache_pb.gif HHTTP/1.0 → GET gerçekleştirilebilen iki komuttan biridir. apache_pb.gif HTTP erişilen URL'dir. HTTP sürümüdür.

Günlük Log Kaydı Örneği

- 127.0.0.1 user-identifier frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200 2326
- 200 →Döndürülen belgenin durum kodu.
- 2326 →Döndürülen belgenin bayt cinsinden boyutu.

Neden Log Kaydı Tutulur?

- Güvenlik Konusu : Saldırı olayları ve diğer izinsiz olayları araştırmak.
- Geliştirme ve Kalite Güvencesi : Bir program ya da uygulama oluşturmasında sorunlu bug'ların kontrol edilmesi için yapılandırılan programlamanın düzgün çalışıp çalışmadığını kontrol etmek için.
- Ağ Sorunlarını Giderme : Bir ağdaki yanıtlama ve sistem hatalarını düzeltme.
- Uyum Konuları : Kurumsal firma ya da devlet politikalarına yanıt olarak bilgi toplama.

Log Kayıtları Kimler Tarafından Kullanılır?

➤ DevOps:

- CI/CD'yi yönetme.
- Uygulama çalışma süresini koruma.
- Kritik uygulamaların hatalarını tespit etmek.
- Uygulamaların performansını optimize etmek için alan belirleme.

➤ DevSecOps:

- Uygulama geliştirme ve güvenliği.

Log Kayıtları Kimler Tarafından Kullanılır?

➤ DevSecOps:

- Dağıtımdan önce olası sorunları bularak zaman, para ve tekrarlama gibi sorunlardan kurtulmak için.

➤ SecOps:

- Bir saldırı hakkında 'kim, ne zaman, nerede' gibi ipuçları verir.
- Şüpheli etkinliği tanımlama.
- Engellenen/izin verilen trafikteki ani artışları görmek için.
- OODA döngüsü gibi metodolojilerinin uygulanması.

Log Kayıtları Kimler Tarafından Kullanılır?

- BT Analistleri:
 - Uyumluluk yönetimi ve raporlama.
 - OpEx ve CapEx.

Log Çeşitleri

➤ Event Log :

- Windows sistemlerde log kayıtlarının tutulduğu yerdir.
- Yönetici hesabı ile işlemler yapılabilir.
- Sistem üzerinde gerçekleşen bütün işlemler kayıt olarak tutulur.
- Hesap kitlemeleri, oturum açma işlemi, uygulama hataları gibi güvenlik için farklı türde olayları kaydeder.
- Event Log Kayıt Değerleri : 4624→ Başarılı Login, 4625→ Başarısız Login, 44672→ Admin Hesabı Logini, 5140→ Ağ Paylaşımı Planlandı, 5025→ Firewall Durduruldu.

Log Çeşitleri

➤ Syslog :

- Sistem günlüğü anlamına gelir. Mesaj loglama standartıdır.
- Unix ve Linux tabanlı sistemler için kullanılır.
- Güvenlik duvarları, yönlendiriciler ve yazıcılar gibi çeşitli cihazlar syslog standartını kullanır.
- Sistem yöneticileri için önemlidir.
- Sistem hataları, sisteme saldırılar veya sistem üzerinde oluşan sorunlar kayıt altında tutulur.
- Syslog sistemleri farklı bir sisteme devredilebilir. Bu sayede uzaktan log kayıtlarına ulaşım yönetim sağlanabilir.

Log Çeşitleri

- Server Log : Belirli bir zaman diliminde belirli bir sunucuyla ilgili etkinliklerin kaydını içerir.
- Transaction Log (SQL Server) : Temel olarak veri tabanındaki değişikliklerin kaydını tutar.
 - Örneğin bir kullanıcı veritabanına tablo ekler veya silerse transaction loga kaydedilir.
 - Eğer veritabanında bir arıza olursa veritabanının geri yüklenmesini ve verilerin kaybolmasını önler.

Log Dosya Türleri

- Access Log : Erişim günlükleri, sunucunuzdan hangi html dosyalarının istendiği bilgilerini kaydeder.
- Agent Log : Sunucunuzda hangi web istemcilerinin istekte bulunduğu ilişkin bilgileri kaydeder.
- Referrer Log : Web sayfanıza geçmeden önce ziyaretçinin bulunduğu URL hakkındaki bilgileri kaydeder.
- Error Log : Hata günlüğü, sunucunun başarısız isteklerini kaydeder. Birisi sunucunuzda var olmayan bir dosyaya erişmeye çalıştığında otomatik olarak hata mesajı oluşturur.

Log Yasası – 5651 Sayılı Kanun

- İnternet sağlayıcılarında paylaşılan ağ trafiklerinin izlenmesi ve bağlantı kuran aygıtlarının mac, ip, ziyaret adresi, oturum süresi, bağlantı istekleri raporlarının kaydedilmesini zorunlu kılan yasa.
- Amaç siber ortamda işlenen suç eylemlerinin yeri, zamanı ve failinin tespiti.
- Kayıtlar 6 ay ile 2 yıl arasında saklanmalı.
- Alınan kayıtların doğru, tutarlı ve sonradan değiştirilemez olması için zaman damgası (HASH) ile muhafaza edilir.

SIEM Nedir?

- Security Information and Event Management .
- Log yönetimidir.
- *Gerçek zamanlı çözümleyicidir.
- Bütün logları alıp toplar.
- Raporlama yapılır.
- *Tüm sistem hareketleri merkezi bir yerden analiz edilir. Gerekirse belirli politikalar belirleyip sisteme reaksiyon aldırılır.
- McAfee, Splunk, IBM QRadar yabancı, Cryptosim ve Logsign yerli SIEM ürünleridir.

Apache Web Server

- Apache açık kaynak kodlu, güçlü, sağlam ve esnek bir http (web) sunucusudur.
- Apache Software Foundation (ASF) tarafından geliştirilir.
- Açık kaynak kodlu olduğu için lisansı ücretsizdir.
- İnternetteki web sitelerinin %60'ı Apache üzerinde çalışmaktadır. Apache en yakın rakibi Microsoft'un web sunucularının 3 katı Pazar payına sahiptir.

Windows Log

Olay Görüntüleyicisi

Dosya Eylem Görünüm Yardım

Olay Görüntüleyicisi (Yerel)

- Özel Görünümler
- Windows Günlükleri
 - Uygulama
 - Güvenlik
 - Kur
 - Sistem
 - İletilen Olaylar
- Uygulama ve Hizmet Günlükleri
- Abonelikler

Güvenlik Olay sayısı: 31.821

Düzy	Tarih ve...	Kaynak	Olay ...	Görev Kategorisi
Bilgi	28.03.20...	Microsoft Wi...	4672	Special Logon
Bilgi	28.03.20...	Microsoft Wi...	4624	Logon
Bilgi	28.03.20...	Microsoft Wi...	5379	User Account ...
Bilgi	28.03.20...	Microsoft Wi...	5379	User Account ...
Bilgi	28.03.20...	Microsoft Wi...	5379	User Account ...
Bilgi	28.03.20...	Microsoft Wi...	5379	User Account ...
Bilgi	28.03.20...	Microsoft Wi...	5379	User Account ...
Bilgi	28.03.20...	Microsoft Wi...	5379	User Account ...

Olay 5379, Microsoft Windows security auditing.

Genel Ayrıntılar

Kimlik Bilgileri Yöneticisi kimlik bilgileri okunmuş.

Konu:

Güvenlik Kimliği:	LAPTOP-8JLNON8Q\ENES
Hesap Adı:	ENES
Hesap Etki Alanı:	LAPTOP-8JLNON8Q
Oturum Açma Kimliği:	0x2ABFB

Okuma İşlemi: Kimlik Bilgilerini Listelendir

Bu olay, bir kullanıcı Kimlik Bilgileri Yöneticisi'nde depolanan kimlik bilgilerinde okuma işlemi gerçekleştirdiğinde oluşur.

Günlük Adı: Güvenlik

Kaynak: Microsoft Windows security auditi

Olay Kimliği: 5379

Düzy: Bilgi

Kullanıcı: Yok

İşlem kodu: Bilgi

Ek Bilgi: [Olay Günlüğü Çevrimiçi Yardımı](#)

Günlüğe kaydedilen: 28.03.2022 01:17:00

Görev Kategorisi: User Account Management

Anahtar Sözcükler: Denetleme Başarısı

Bilgisayar: LAPTOP-8JLNON8Q

Linux Logları

```
root@kali: /var/log
Dosya Eylemler Düzen Görünüm Yardım

(root@kali)-[~]
# cd /var/log

(root@kali)-[/var/log]
# ls
alternatives.log      auth.log.4.gz      btmap              debug.2.gz         inetsi
alternatives.log.1    boot.log           btmap.1           debug.3.gz         instal
alternatives.log.2.gz boot.log.1         daemon.log        debug.4.gz         journa
apache2              boot.log.2         daemon.log.1      dpkg.log           kern.l
apt                 boot.log.3         daemon.log.2.gz   dpkg.log.1        kern.l
auth.log            boot.log.4         daemon.log.3.gz   dpkg.log.2.gz     kern.l
auth.log.1          boot.log.5         daemon.log.4.gz   elasticsearch      kern.l
auth.log.2.gz       boot.log.6         debug             faillog            kern.l
auth.log.3.gz       boot.log.7         debug.1          fontconfig.log     kibana

(root@kali)-[/var/log]
#
```

```
(root@kali)-[/var/log]
# cat * kern.log3.gz
```

```
root@kali: /var/log
Dosya Eylemler Düzen Görünüm Yardım

Mar 26 21:56:57 kali dockerd[804]: time="2022-03-26T21:56:57.028355394+03:00"
Mar 26 21:56:57 kali dockerd[804]: time="2022-03-26T21:56:57.028831299+03:00"
Mar 26 21:56:57 kali dockerd[804]: time="2022-03-26T21:56:57.028949401+03:00"
Mar 26 21:56:57 kali dockerd[804]: time="2022-03-26T21:56:57.031448615+03:00"
Mar 26 21:56:57 kali dockerd[804]: time="2022-03-26T21:56:57.031566448+03:00"
Mar 26 21:56:57 kali dockerd[804]: time="2022-03-26T21:56:57.031599564+03:00"
Mar 26 21:56:57 kali dockerd[804]: time="2022-03-26T21:56:57.032328398+03:00"
Mar 26 21:56:57 kali dockerd[804]: time="2022-03-26T21:56:57.032467439+03:00"
Mar 26 21:56:57 kali dockerd[804]: time="2022-03-26T21:56:57.032526757+03:00"
Mar 26 21:56:57 kali dockerd[804]: time="2022-03-26T21:56:57.032548805+03:00"
Mar 26 21:56:57 kali systemd[1]: Starting RealtimeKit Scheduling Policy Servi
Mar 26 21:56:57 kali dbus-daemon[486]: [system] Successfully activated servic
Mar 26 21:56:57 kali systemd[1]: Started RealtimeKit Scheduling Policy Servic
Mar 26 21:56:57 kali rtkit-daemon[843]: Successfully called chroot.
Mar 26 21:56:57 kali rtkit-daemon[843]: Successfully dropped privileges.
Mar 26 21:56:57 kali rtkit-daemon[843]: Successfully limited resources.
Mar 26 21:56:57 kali rtkit-daemon[843]: Canary thread running.
Mar 26 21:56:57 kali rtkit-daemon[843]: Watchdog thread running.
Mar 26 21:56:57 kali rtkit-daemon[843]: Running.
Mar 26 21:56:57 kali rtkit-daemon[843]: Successfully made thread 836 of proce
Mar 26 21:56:57 kali rtkit-daemon[843]: Supervising 1 threads of 1 processes
Mar 26 21:56:57 kali rtkit-daemon[843]: Successfully made thread 837 of proce
Mar 26 21:56:57 kali rtkit-daemon[843]: Supervising 2 threads of 2 processes
Mar 26 21:56:57 kali rtkit-daemon[843]: Successfully made thread 838 of proce
Mar 26 21:56:57 kali rtkit-daemon[843]: Supervising 3 threads of 3 processes
Mar 26 21:56:57 kali rtkit-daemon[843]: Supervising 3 threads of 3 processes
Mar 26 21:56:57 kali rtkit-daemon[843]: Supervising 3 threads of 3 processes
```

Apache Log

```
root@kali: /var/log
Dosya Eylemler Düzen Görünüm Yardım

(root@kali)-[/var/log]
# ls
alternatives.log      auth.log.4.gz      btmp                debug.2.gz          inetsi
alternatives.log.1    boot.log           btmp.1             debug.3.gz          instal
alternatives.log.2.gz boot.log.1         daemon.log         debug.4.gz          journa
apache2               boot.log.2         daemon.log.1       dpkg.log            kern.l
apt                  boot.log.3         daemon.log.2.gz    dpkg.log.1         kern.l
auth.log             boot.log.4         daemon.log.3.gz    dpkg.log.2.gz      kern.l
auth.log.1           boot.log.5         daemon.log.4.gz    elasticsearch       kern.l
auth.log.2.gz        boot.log.6         debug              faillog             kern.l
auth.log.3.gz        boot.log.7         debug.1            fontconfig.log      kibana

(root@kali)-[/var/log]
# cat * apache2
update-alternatives 2022-03-21 19:07:16: run with --install /usr/bin/www-browser
update-alternatives 2022-03-21 19:07:16: link group www-browser updated to po
n8a[s~Bp~k~s~h}~jW?~e~;~n ~NuW~Hbi}t
-~`~h~Z~/~S\?~ q~qM~qV~a~cU~m~.<~
4~2~P~8{A~2?~ R~[*~_1/~~t~6~u
^o~y~4~ X~j~ <i~h~8~b~9~|X=~n~q~Jh[~
e~!B~#~48~!S~)`6~ r~aC~k~0~8~(~~Fs~I
~.46

more you are able to hear"
```

```
root@kali: /var/log
Dosya Eylemler Düzen Görünüm Yardım

Mar 27 00:34:29 kali runuser: pam_unix(runuser:session): session opened for u
Mar 27 00:35:01 kali CRON[3474]: pam_unix(cron:session): session opened for u
Mar 27 00:35:01 kali CRON[3474]: pam_unix(cron:session): session closed for u
Mar 27 00:39:01 kali CRON[3505]: pam_unix(cron:session): session opened for u
Mar 27 00:39:01 kali CRON[3505]: pam_unix(cron:session): session closed for u
Mar 27 00:39:54 kali runuser: pam_unix(runuser:session): session closed for u
Mar 27 00:40:04 kali sudo: pam_unix(sudo:auth): authentication failure; logna
Mar 27 00:40:11 kali sudo: enessahin450 : TTY=pts/1 ; PWD=/root ; USER=root ;
Mar 27 00:40:11 kali sudo: pam_unix(sudo:session): session opened for user ro
Mar 27 00:40:11 kali su: (to root) root on pts/1
Mar 27 00:40:11 kali su: pam_unix(su:session): session opened for user root(u
Mar 27 00:42:05 kali su: pam_unix(su:session): session closed for user root
Mar 27 00:42:05 kali sudo: pam_unix(sudo:session): session closed for user ro
Mar 27 00:42:05 kali su: pam_unix(su:session): session closed for user enessa
Mar 27 00:47:41 kali systemd-logind[518]: New seat seat0.
Mar 27 00:47:41 kali systemd-logind[518]: Watching system buttons on /dev/inp
Mar 27 00:47:41 kali systemd-logind[518]: Watching system buttons on /dev/inp
Mar 27 00:47:42 kali lightdm: pam_unix(lightdm-greeter:session): session open
Mar 27 00:47:42 kali systemd-logind[518]: New session c1 of user lightdm.
Mar 27 00:47:43 kali systemd: pam_unix(systemd-user:session): session opened
Mar 27 00:47:51 kali lightdm: pam_unix(lightdm:auth): check pass; user unknow
Mar 27 00:47:51 kali lightdm: pam_unix(lightdm:auth): authentication failure;
Mar 27 00:47:56 kali lightdm: pam_unix(lightdm:auth): check pass; user unknow
Mar 27 00:47:56 kali lightdm: pam_unix(lightdm:auth): authentication failure;
Mar 27 00:48:04 kali lightdm: gkr-pam: unable to locate daemon control file
Mar 27 00:48:04 kali lightdm: gkr-pam: stashed password to try later in open
Mar 27 00:48:04 kali lightdm: pam_unix(lightdm-greeter:session): session clos

more you are able to hear"
```

ELK Nedir?

- Elasticsearch : Dış uygulamalar üzerinden toplanan verilerin analizi ve içerik gibi işlemleri yapmamızı sağlayan bir arama motorudur.
- Logstash : Log toplayan, ihtiyaca göre onları işleyen ve Elasticsearch'e bu logları indekslenmek üzere gönderen sistemdir.
- Kibana : Toplanıp anlamlı hale getirilen verinin, analizini yaptıktan sonraki görselleştirme işlemini yapar. Grafik yapılar ile analiz.

```
root@kali: /usr/share/logstash

Dosya Eylemler Düzen Görünüm Yardım

(root@kali)~# sudo service logstash status
● logstash.service - logstash
   Loaded: loaded (/etc/systemd/system/logstash.service; disabled; vendor
   Active: active (running) since Mon 2022-03-28 10:39:25 +03; 12s ago
   Main PID: 1783 (java)
   Tasks: 18 (limit: 2257)
   Memory: 508.5M
   CPU: 32.377s
   CGroup: /system.slice/logstash.service
           └─1783 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseC

Mar 28 10:39:25 kali systemd[1]: Started logstash.
Mar 28 10:39:25 kali logstash[1783]: Using bundled JDK: /usr/share/logstash/
Mar 28 10:39:26 kali logstash[1783]: OpenJDK 64-Bit Server VM warning: Optio>

(root@kali)~# cd /usr/share/logstash

(root@kali)/usr/share/logstash# ls
bin          Gemfile      LICENSE.txt  logstash-core-plugin-api  tools
CONTRIBUTORS Gemfile.lock lib          modules                  vendor
data         jdk          logstash-core NOTICE.TXT              x-pack

(root@kali)/usr/share/logstash#
```

```
(root@kali)-[/usr/share/logstash]
# sudo service elasticsearch start

(root@kali)-[/usr/share/logstash]
# sudo service elasticsearch status
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/lib/systemd/system/elasticsearch.service; disabled; ve
   Active: active (running) since Mon 2022-03-28 10:52:25 +03; 31s ago
   Docs: https://www.elastic.co
   Main PID: 3355 (java)
   Tasks: 81 (limit: 2257)
   Memory: 988.2M
   CPU: 1min 24.250s
   CGroup: /system.slice/elasticsearch.service
           └─3355 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.

3 x
```



```
(root@kali)-[/usr/share/logstash]
# sudo bin/logstash -f /etc/logstash/conf.d/logstash.conf
Using bundled JDK: /usr/share/logstash/jdk
OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in
version 9.0 and will likely be removed in a future release.
[FATAL] 2022-03-28 11:04:58.691 [main] Logstash - Logstash stopped processing
because of an error: (NameError) missing class name ('org.apache.http.impl.c
lient.StandardHttpRequestRetryHandler')
org.jruby.exceptions.NameError: (NameError) missing class name ('org.apache.h
ttp.impl.client.StandardHttpRequestRetryHandler')
    at org.jruby.javasupport.JavaPackage.const_missing(org/jruby/javasupp
ort/JavaPackage.java:124) ~[jruby-complete-9.2.20.1.jar:~]
    at RUBY.<module:Manticore>(/usr/share/logstash/vendor/bundle/jruby/2.
5.0/gems/manticore-0.8.0-java/lib/manticore/client.rb:729) ~[?:~]
    at RUBY.<main>(/usr/share/logstash/vendor/bundle/jruby/2.5.0/gems/man
ticore-0.8.0-java/lib/manticore/client.rb:6) ~[?:~]
    at org.jruby.RubyKernel.require(org/jruby/RubyKernel.java:974) ~[jrub
y-complete-9.2.20.1.jar:~]
    at org.jruby.RubyKernel.require_relative(org/jruby/RubyKernel.java:10
02) ~[jruby-complete-9.2.20.1.jar:~]
    at RUBY.<module:Manticore>(/usr/share/logstash/vendor/bundle/jruby/2.
5.0/gems/manticore-0.8.0-java/lib/manticore.rb:70) ~[?:~]
    at RUBY.<main>(/usr/share/logstash/vendor/bundle/jruby/2.5.0/gems/man
ticore-0.8.0-java/lib/manticore.rb:18) ~[?:~]
```

```
(root@kali)-[/usr/share/logstash]
# curl -XGET 127.0.0.1:9200/_cat/indices?v
health status index          uuid          pri rep
docs.count docs.deleted store.size pri.store.size
green open   .geoip_databases  yKS_VCuIRv-SmWNDVkJMobg  1  0
      44         60      44.7mb      44.7mb
green open   .apm-custom-link  _Hc6_7kHQtaMGcgW5UtQcg  1  0
      0          0        226b        226b
green open   .apm-agent-configuration  Ha7IM17uQVG0E_2nCNilWQ  1  0
      0          0        226b        226b
green open   .kibana_task_manager_7.17.1_001 t27F_tinSk-E7L9eweqDwQ  1  0
      17         0       73.2kb       73.2kb
green open   .kibana_7.17.1_001 k5V5To74Tg-vBu3Yw03i7g  1  0
      11         0        2.3mb        2.3mb

(root@kali)-[/usr/share/logstash]
#
```