Elf Dosyası Nedir?

Bir ELF çalıştırılabilir ve Linkable Formatında oluşturulan bir sistem dosyasıdır. Bu çalıştırılabilir programlar, hafıza dökümlerini ve paylaşımlı kütüphaneleri saklayabilirsiniz. ELF birçok Unix tabanlı sistemlerde kullanılan standart bir dosya biçimidir.

Elf Headers

Dosya formatlarının en önemli kısımlarından birisi başlık bölümüdür. Bu bölüm altında ilgili dosyanın ne tür bir biçime sahip olduğu,hangi mimari için derlendiği ve diğer kısımlar hakkında bilgiler yer alır. Mesela ilk 16 byte olarak ayrılmış kısımda ilk 4 byte'ı Magic kısım olarak geçer ve bu dosya ELF dosyasıdır demek için gereklidir. 5.byte'da yer alan bilgi dosyanın sınıfı tutar. Bu değerin 0 olması Geçersiz,1 olması 32 Bit nesne ve 2 olması 64 Bit nesne olduğunu gösterir.Geri kalan kısımlardan dosyanın hangi işletim sistemi tarafından kullanılacağı gibi bilgiler elde edilebilir.

File Komutu

Dosya uzantısında dosyanın hangi tür dosya olduğunu anlayamadığımız zaman "File" komutunu kullanabiliriz.
Unix sistemlerde belirli uzantılı dosyaların başı bilinen bir harf veya harf grubu ile başlar. File komutu dosyanın başındaki karakterleri kontrol eder ve bunları bir listeyle "(/etc/magic)" karşılaştırarak dosyanın ne tür olduğunu söyler.

Kullanımı :

```
file [Option] [File]
```

en basit haliyle dosya adını gösterir

```
$ file /etc
```

Çıktısı

```
/etc/group: ASCII text
```

Yanlızca dosya türü için

```
file -b /etc/group
```

Çıktısı

```
ASCII text
```

file komutu birden fazla dosya ile aynı anda çıktı verebilir

```
file /bin/bash /opt/card.zip
```

Örneğin bu kodun çıktısında her bir dosyanın türünü ayrı olarak yazacaktır

```
/bin/bash:     ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=42602c973215ba5b8ab5159c527e72f38e83ee52, stripped

/opt/card.zip: Zip archive data, at least v1.0 to extract
```

Readelf Komutu

Elf dosyaları hakkında bilgileri görüntüler

Taglar

-h / --file-header : Dosyanın başında ELF başlığında bulunan bilgileri görüntüler .

-l / --program-headers :Varsa, dosyanın segment başlıklarında bulunan bilgileri görüntüler.

-S / --sections : Varsa, dosyanın bölüm başlıklarında bulunan bilgileri görüntüler.

-g / --section-groups : Varsa, dosyanın bölüm gruplarında bulunan bilgileri görüntüler.

-t / --section-details :Ayrıntılı bölüm bilgisini görüntüler. İma -S .

-s / --symbols :Girdileri varsa, dosyanın tablo tablosu bölümünde görüntüler.

-e / --headers :Dosyadaki tüm başlıkları göster. -H -l -S'ye eşdeğerdir .

-n / --notes :Varsa, NOT bölümlerinin ve / veya bölümlerinin içeriğini görüntüler .

-r / --relocs :Eğer varsa, dosyanın taşınma bölümünün içeriğini görüntüler.

-u / --unwind :Eğer varsa, dosyanın çözme bölümünün içeriğini görüntüler. Şu anda sadece IA64 ELF dosyalarının çözme bölümleri desteklenmektedir.

-d / --dynamic :Varsa, dosyanın dinamik bölümünün içeriğini görüntüler.

-V / --version-info :Dosyadaki sürüm bölümlerinin içeriğini görüntüler.

-A / --arch-specific :Varsa, mimariye özgü bilgileri dosyada görüntüler.

-D / --use-dynamic :Sembolleri görüntülerken, bu seçenek el kitabının semboller bölümünde değil, dosyanın dinamik bölümünde bulunan sembol tablosunu kullanmasını sağlar.

-x <number or name> / --hex-dump=<number or name :Belirtilen bölümün içeriğini onaltılık bayt olarak görüntüler. Sayı, bölüm tablosundaki dizine göre belirli bir bölümü tanımlar; başka bir dize, nesne dosyasında bu ada sahip tüm bölümleri tanımlar.

-v / --version : sürüm numarasını görüntüler.

-H / --help :Okur tarafından anlaşılan komut satırı seçeneklerini

görüntüler.