­ELF

Elf “Yürütülebilir ve Bağlanabilir Dosya Biçimi”

Anladığım kadarıyla ELF formatı esnek, genişletilebilir ve çapraz platform olması neticesinde bir çok sistemde ve mimaride bir çok veri türlerini sorunsuzca ve kaliteli bir şekilde yönetebildiğinden ve yürütülebilir olduğundan ve başka programlarla da bağlanılabilirlik özelliği sayesnide rahatça kullanılabilir olduğundan dolayı bir çok platform ve farklı işletim sistemi tarafından da araştırmalarım sonucu benimsenmiş bir yapıya sahip olduğunu öğrendim.

FILE

İçinde bilgi veri veri barındıran verinin türlerine göre biçimi değişebilen bilgisayardaki veri depoları diyebiliriz.

File (komut) unix’te bir dosyada yer alan verilerin türünü belirlemek adına kullanılabilen bir kod parçacığıdır.

READELF

Readelf bahsedilen veri ve nesne dosyaları hakkında ‘objdump’gibi unix vb. Sistemlerde çeşitli bilgileri görüntülemek için kısaca dosya biçimi ve verileri görüntülemek adına kullanılan bir programdır. (kod parçacığı’da sayılabilir.)

ELF DOSYA FORMATI

Elf çalıştırabilir ve bağlanılabilir formatında bir sistem dosyasıdır.Çalıştırılan programlar hafıza dökümlerini ve kütüphaneleri saklayabilir.Elf,unix tabanlı sistemlerde standart bir dosya biçimidir.

READELF KOMUTU

Readelf, bir veya daha fazla ELF formatındaki dosyanın bilgilerini görüntüler.

Elffile incelenecek nesne dosyalırıdır.32 bit ve 64 bit Elf dosyaları,Elf dosyalarını içeren arşivler gibidir.

-a

--all

Equivalent to specifying --file-header, --program-headers, --sections, --symbols, --relocs, --dynamic, --notes, --version-info, --arch-specific, --unwind, --section-groups and --histogram.

-h

--file-header

Elf başlığında bulunan bilgileri görüntüler.

-l

--program-headers

--segments

Segment başlıklı bulunan dosyanın bilgilerini görüntüler.

-S

--sections

--section-headers

Dosyanın bölüm başlıklarında yer alan bilgileri görüntüler.

-g

--section-groups

Dosyanın bölüm gruplarında bulunan bilgileri görüntüler

-t

--section-details

Ayrıntılı bölüm bilgisini görüntüler -S anlamına gelir.

-s

--symbols

--syms

girdileri varsa dosyanın tablo bölümünde görüntüler

-e

--headers

Dosyadaki tüm başlıkları gösterir

-n

--notes

NOT bölümlerinin ve/veya bölümlerinin içerğini gösterir.

-r

--relocs

Dosyanın taşınma bölümünün içeriğini gösterir.

-u

--unwind

Dosyanın çözme bölümünün içeriğini görüntüler.

-d

--dynamic

Dosyanın dinamik bölümünün içeriğini görüntüler.

-V

--version-info

Dosyadaki sürüm bölümlerinin içeriğini görüntüler.

-A

--arch-specific

Mimariye özgü bilgileri dosyada görüntüler.

-D

--use-dynamic

Sembolleri görüntülediğinde,readelf de 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.

-R <number or name>

--relocated-dump=<number or name>

-p <number or name>

--string-dump=<number or name>

Belirtilen bölümün içeriğini dizeler olarak görüntüler.başka bir nesne dosyasında bu ad sahip tüm bölümleri getirir

-c

--archive-index

ikili arşivlerin başlık kısmında bulunan dosyalarının dizi bilgisini gösterir.Ar komutuyla aynı işlevi yerine getirir ancak BFD kütüphanesini kullanmadan yerine getirir.

-w[lLiaprmfFsoR]

--debug-dump[=rawline,=decodedline,=info,=abbrev,=pubnames,=aranges,=macro,=frames,=frames-interp,=str,=loc,=Ranges]

Dosyadaki hata ayıklama bölümlerinin içeriğini görüntüler.İsteğe bağlı harflerden veya kelimelerden biri düğmeyi takip ederse,yalnızca bu bölümlerde bulunan veriler silinir.

Not:= decodline seçeneği, bir debug\_line bölümünü yorumlanmış içerğini gösterirken, =rawline seçeneği içeriği ham biçiminde sarar

-I

--histogram

-v

--version

Readelf hangi sürümü olduğunu görüntüler.

-W

--wide

Daha geniş okunabilmesini sağlar

Readelf

Elf dosyalarını incelemek için kullanılır.

Debug tool’dur.

Paremetreler:

-> -a , --all

İçerisinde bulunan tüm modulleri kullanarask analiz eder ve çıktıları ekrana basar.

-> -h , --file-header

ELF dosyasını başlığındaki bilgileri bize gösterir.

-> -l , --program-headers , --segments

Eğer varsa dosyanın dosyanın segment başlıklarında bulunan bilgileri gösterir.

-> -g –section-groups

Eğer varsa dosyanın alt bölüm gruplarında bulunan bilgileri görüntüler.

Not: Olan bi tane bulamadım :(

-> -S , --section-details

Blüm bilgilerini daha ayrıntılı bir şekilde görüntüler.

-> -e , --headers

Dosyadaki tüm başlıkları gösterir. -H -l -S ile aynı işi görür.

-> -n , --notes

Varsa NOT bölümlerini gösterir.

-> -d , --dynamic

Varsa dosyanın dinamik bölümülerini ve içeriklerini gösterir.

-> -V , --version-info

Dosyanın içeriğindeki version bilgilerini gösterir.

-> -A , --arch-specific

Varsa mimariye özel bilgileri gösterir.

Not: Olan dosya bulamadım :(

-> -t , --section-details

->-s , --syms , --symbols

-> -r , --relocs

-> -u , --unwind

-> -D , --use-dynamic

-> -x <numara veya isim> , --hex-dump=<numara veya isim>

-> -w[liaprmfFsoR]

->--debug-dump[=rawline,=decodedline,=info,=abbrev,=pubnames,=aranges,=macro,=frames,=frames-interp,=str,=loc,=Ranges,=pubtypes,=trace\_info,=trace\_abbrev,=trace\_aranges,=gdb\_index]]

-> -I , --histogram

-> -v , --version

-> -W , --wide

-> -H , --help

file

dosyalar hakkında bilgi görüntülemek için kullanılır.