Linux Forensics

Dr. Phil Polstra

PhD, CISSP, CEH

@ppolstra

http://philpolstra.com

Certifications:
http://www.securitytube-training.com
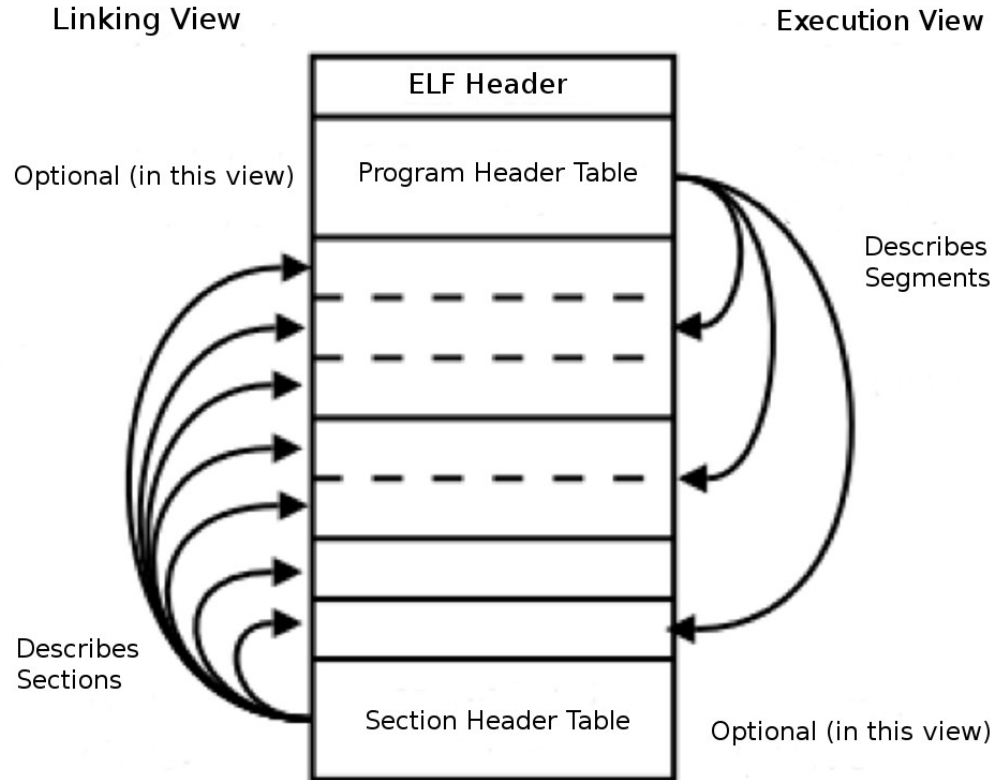
Pentester Academy: http://www.PentesterAcademy.com

ELF Files

Executable & Linkable Format

- The standard format for

  - Executables

  - Libraries

  - Object files

- Two views: Executing & Linking

- Executing

  - File broken into segments

- Linking

  - File broken into sections

  - Sections are normal parts of segments

ELF High Level View

Readelf Demo