- Dynamic Attachment Analysis & sandboxing

Sandbox -> Mimic host system.

For dynamic analysis

- Process Activity
- Registry changes
- Network connection
- File Activity.

Tools for Sandboxing

-> HybridAnalysis.com

-> JoeSandbox.com

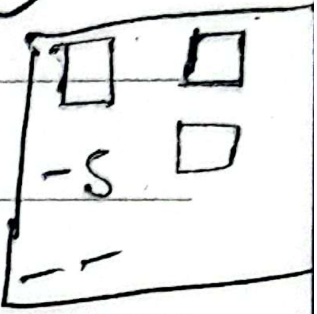
-> Any Run

- CVE # -> Common Vulnerabilities & Exposure
  - -> Tells info about Behaviour of file

Tells as

- IOC
- Network Interactions
- Domain Involved

Static Malware Doc Analysis



· Analysis of Mal-docs files

· Macro (sequence of automated action)

→ Malicious Macro → embedded into file

VBA
↓

OLE id developed by microsoft. for embedding macro.

Tools

ole dump.py (object linking & embedding)

↳ -S --vba decompress corrupt

Static PDF Analysis

virus-total

- Most used doc in pdf

— Pdf evade email filters

↳ Most pdf doesn't have embedding but link in them

Steps

Same process as attachment analysis

↳ If no data found, use pdfparser.py (-s for grep like stuff)

↳ Analyze embedded object

- For Embedded pdf

↳ Tools : pdfid.py

↳ shows embeed actions towards browsser like /JS other IOC

- /Launch
- / Embedder file

↳ then use pdf-parser.py which shows embedded file and can be used

D

Auto-mated Email Analysis with phishtool

Phishtool → Web-Base phishing analysis tools

Phishtool can also integrate virustotal through API Key

This is doing mostly what we did previously/manually and gives us the insight