Getting started with malware analysis

Judith van Stegeren

Definitions

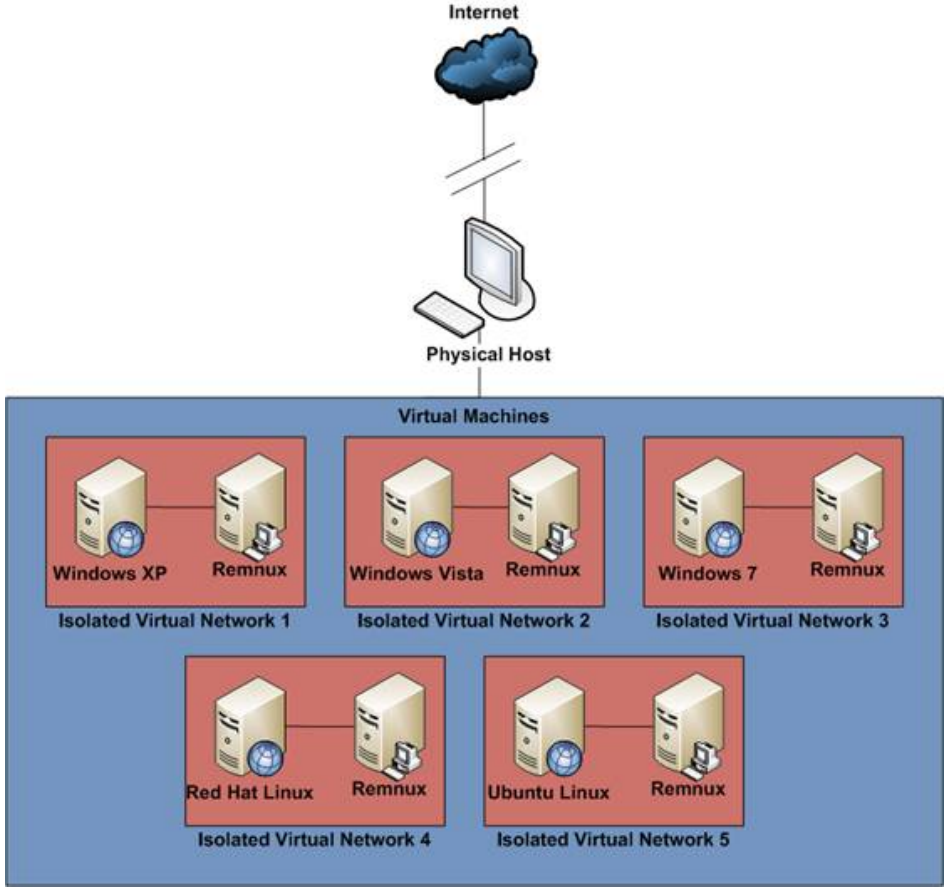
Malware: any software that does something that causes harm to a user, computer or network, including viruses, trojan horses, worms, rootkits, scareware and spyware.

Malware analysis: the art of dissecting malware to understand how it works, how to identify it and how to defeat or eliminate it.

Malware analysis: what, why, when, who

Building a malware lab

Building a malware lab: hardware and network

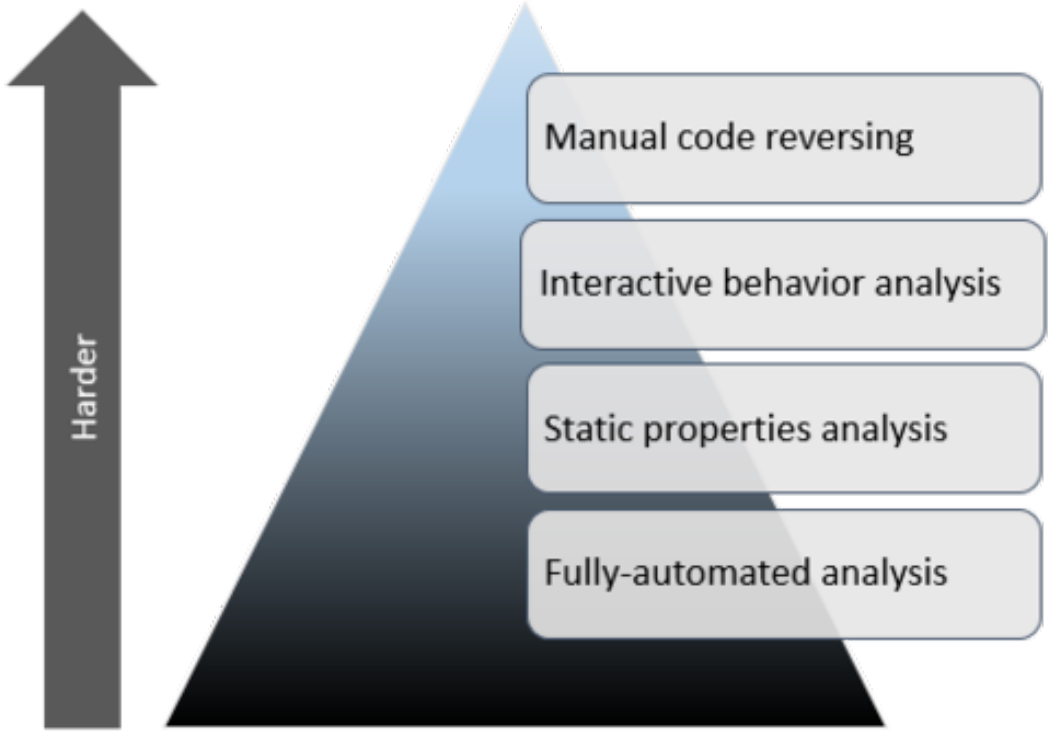


http://www.windowsecurity.com/articles-tutorials/viruses_trojans_malware/

Building-Malware-Analysis-Lab.html

Types of malware analysis

1. Static analysis aka code analysis
2. Dynamic analysis aka behavioral analysis



https://zeltser.com/mastering-4-stages-of-malware-analysis/

Demo

Want to know more?

- *Practical malware analysis*, Honig & Sikorski (also includes labs)
- A curated list of awesome malware analysis tools and resources: `https://github.com/rshipp/awesome-malware-analysis`
- Open Courseware: `http://github.com/RPISEC/Malware` (course on malware analysis based on the book 'Practical malware analysis')
- anything by Lenny Zeltser (webcasts, blog articles)
- Digital Forensics Blog, SANS: `https://digital-forensics.sans.org/blog/`
- `http://tuts4you.com` for tutorials on reverse engineering
- `http://crackmes.de` for crackme/reverseme executables to reverse :)

Questions?