Operating Systems

Objectives

- Discuss threats to operating systems
- Explain common methods to securing operating systems

Common Desktop Operating Systems

- Numbers are debatable
- Microsoft
  - Overall around 80-85% market share – NetShare
  - 400 million Windows 10 devices alone – 25% of Windows market - NetShare
  - Over 1 billion devices
- Apple
  - Overall around 7-10% market share – NetShare
  - 100 million devices as of April 2017
- Linux
  - Around 2% share

Common Mobile Operating Systems

- Worldwide
- Microsoft
    - <1% - NetShare
- Apple
    - 33% - NetShare
- Linux
    - 64% - NetShare

How operating systems work

- Kernel – Ring level 0
- User Level – Ring level 3
- Some operating systems have rings 1 and 2
- Most later operating systems have just 2 rings – 0,3
- 0 is most privileged

Vulnerabilities

- Most vulnerabilities are in applications
- Some vulnerabilities in the operating system
- Year over year Apple has had the most vulnerabilities (~60% desktop, 84% of mobile)
- Microsoft is #2
- Linux vulnerabilities are very small in comparison

Threats

- In order to look at threats, we need to look at market share
- Even though Apple has historically had more vulnerabilities, their threats are less due to market share
- It’s more lucrative to go after the market share
- Trojans
- Worms
- Viruses

Securing operating systems

- Use least privilege
- Remove unnecessary services, applications and protocols
- Use antivirus – it’s your last line of defense
- Use best practices
- Hardening guides – CIS, NIST, NSA