5. Vulnerabilities and Assets

COMP6441 • KC Notes

5.1 Vulnerabilities

- **Vulnerability**: a potential flaw or weakness
- **Bugs**: Human errors that are in the code
    - **Memory corruption bug**: changing contents of memory that were not expected to be changed
    - **Buffer overflow**: when there is a variable amount of space available and you write outside the buffer area
        - You can sometimes overflow and modify pointers (e.g. where a function will return to or go after it is done)
    - If you can *dream* it happening, it is true
- **Exploits**: taking advantage of a vulnerability
    - **Shell code**: do something that will pop up a remote shell or terminal
    - C programs are self-regulatory and usually check if someone isn't meant to be somewhere
- How do you know where to return to, to run malicious code you have entered?
    - Memory or information leak in the program
    - Brute forcing pointer addresses
    - Internal documentation
    - **nop sleds (no operation)** – you can fill the buffer with 0x90's, and you have a larger range to point to. It will then **slide down to your malicious code**.
        - **Intrusion detection systems** can detect nop sleds, but in the end this becomes **a cat and mouse game**
- **National Vulnerability Database**: a database of common vulnerabilities and exposures. Each one is a year and a number.

5.2 Assets

- What assets are we actually protecting?
- How important is each asset relative to each other?

5.2.1 STRATEGIES FOR IDENTIFYING ASSETS

- Involve **a lot of people** – people will bring their own takes and experiences
    - Dominant or arrogant people will lock others out of their views and shape an audit to their own ways
- **Develop a sensible plan**
    - It is easy to overlook things or centre on specific points – it may be good to brainstorm beforehand
    - Criticise everybody's ideas
- **Revise** the set of assets frequently – what they are and whether they are being protected

5.2.2 EXAMPLES OF ASSETS

- **Team America** – are we protecting against the terrorists or are protecting the innocent?
- **Car doorbell**: Richard's friend rigged a car door to a doorbell in their apartment, so that when the door opens, the doorbell rings.
    - Prioritising **the car or yourself as an asset**: is the car worth more than getting hurt from a criminal gang?
- **Coke**/other companies: reputation and branding is a very big asset
    - Difficult to put a price into a company's reputation

5.2.3 TYPES OF ASSETS

- **Tangible**: easy to value
- **Intangible**: hard to value (difficult does not mean don't do!)
    - Employee morale and security
    - Consumer information
    - Company secrets
    - Availability of services
    - Psychological and emotional