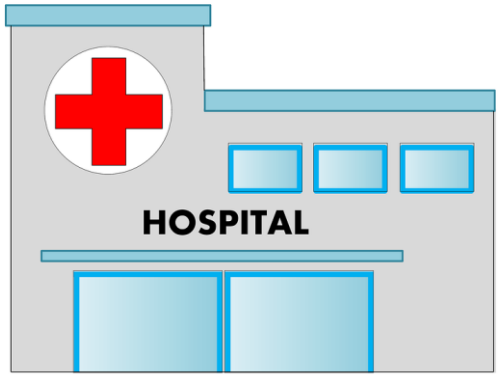
Metropolis General



2017 Gen Cyber Camp, Day 1, Morning

The Scenario: Overview

- Each of you is a new employee in the Metropolis General Hospital cyber-security department
- At the end of last week, the hospital was attacked by a hacker or group of hackers that referred to themselves as Fancy Bear.
    - Stole data
    - Created malicious users
    - Locked administrators out of computers/servers
    - Used hacked hospital servers to attack other hospital equipment

- Metropolis General has decided it needs to perform penetration testing.

Introductions: Metropolis General Staff

- Rob Olson
  - Chief Security Officer of Metropolis General Hospital
  - Speciality: Offensive Security and Ethical Hacking
- Joe Graham
  - Security Team Lead of Metropolis General Hospital
  - Specialty: Security Administration and Infrastructure
- Paul Meyerhofer
  - Chief Training Officer of Metropolis General Hospital
  - Specialty: Training and Employee Management

The Scenario: Hospital Infrastructure

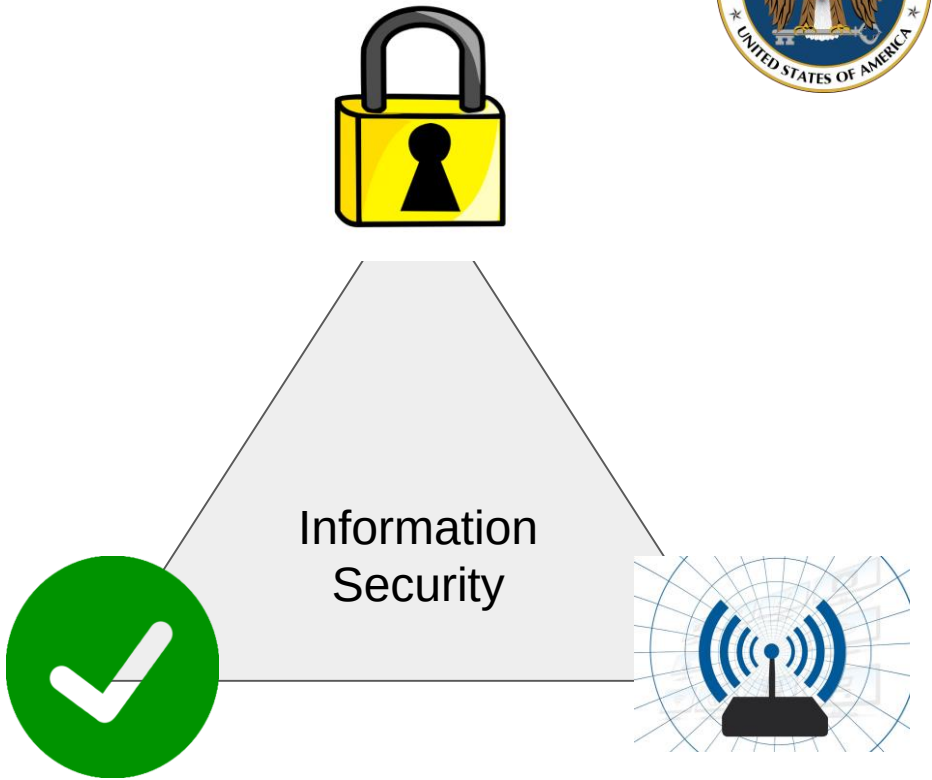
Web Server	Floor 1	Nurse Station	Nurse Station	Mgmt Desktop	Billing Desktop	New Windows Server	OSSIM
Email Server	Floor 2	Nurse Station	Nurse Station	Mgmt Desktop	Billing Desktop	New Windows Server	OSSIM
DNS Server	Floor 3	Nurse Station	Nurse Station	Mgmt Desktop	Billing Desktop	New Windows Server	OSSIM
File Server	. . .						
Heartbeat Server	Floor 12	Nurse Station	Nurse Station	Mgmt Desktop	Billing Desktop	New Windows Server	OSSIM

First Principles
&
Core Concepts

CIA Triad

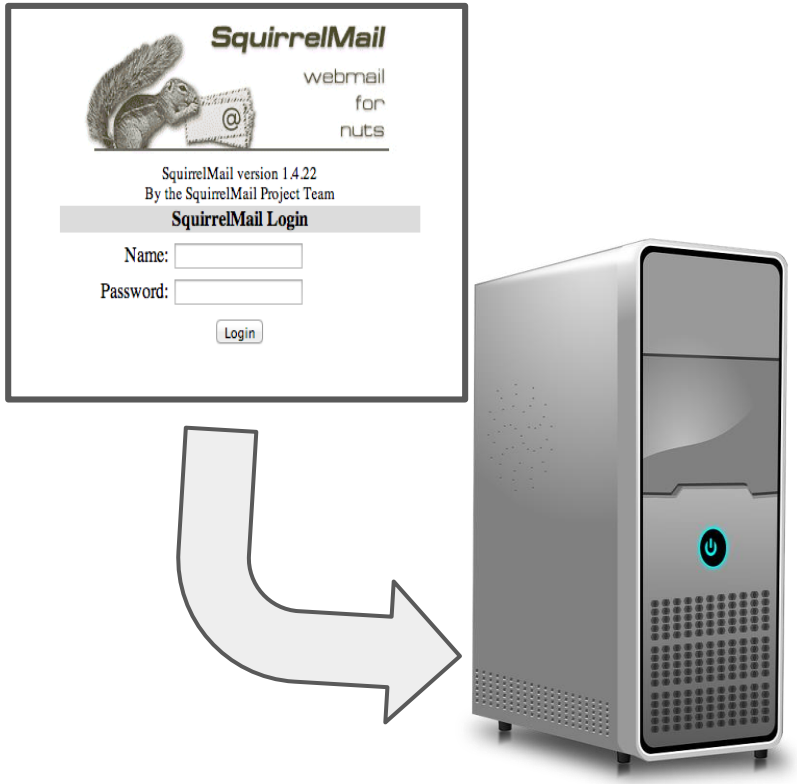
Primary Goals of Information Security

- Confidentiality
  - Keeping private data private
- Integrity
  - Making sure that data is accurate
- Availability
  - Making sure that data is available



CIA Triad: Email Server Example

- Confidentiality Attack
  - Attacker gains access to emails and makes them public
- Integrity Attack
  - Attacker spoofs (fakes) an email to employees pretending to be CEO.
- Availability Attack
  - Attacker conducts a denial of service attack against



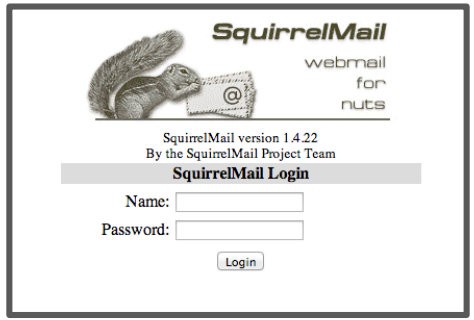
Basic Definitions

- Vulnerability
  - A flaw in the system that permits the CIA triad to be attacked
  - Any of the three parts of the triad could have a problem
- Exploit
  - A way to make use of a vulnerability to attack the system's confidentiality, integrity, or accessibility.
- Threat Actor
  - A person or group that might exploit a vulnerability to attack a system.
- Threat
  - Something bad a threat actor could do after a successful attack.

Definitions

Hacktivists (**a group of threat actors**) write a program that inserts a command into the configuration file (**exploit**) that the system will run.

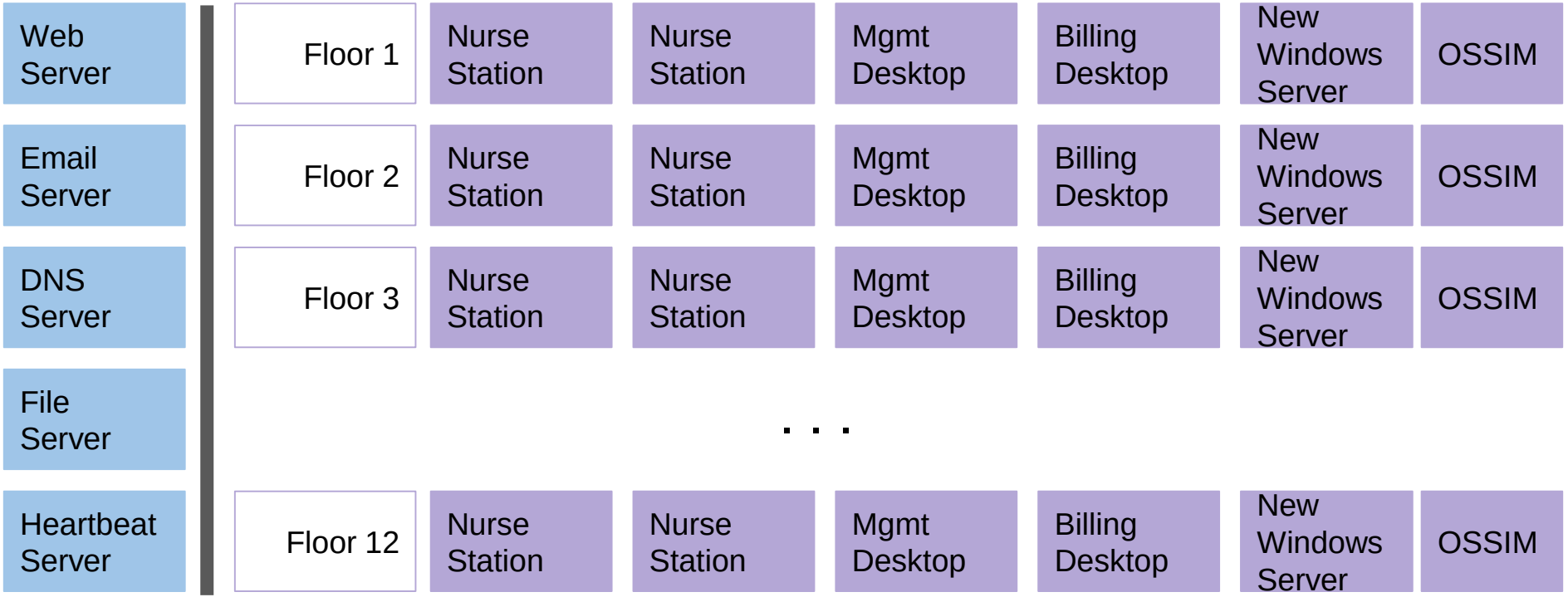
SquirrelMail has a known **vulnerability** that allows users to write to configuration files.



Administrators are concerned about the **threat** of email leaks.

First Principles of Cybersecurity

1. Domain Separation
    - Ensure that systems have a specific, dedicated role.
2. Process Isolation
    - Control and limit how programs can interact
3. Resource Encapsulation
    - Limit access to system resources
4. Least Privilege
    - Give individuals the fewest permissions possible
5. Modularity
    - Design systems so parts can easily be changed out when broken
6. Layering
    - Do not assume one level of protection is sufficient
7. Abstraction
    - Conceal information from users that isn't important to them
8. Data Hiding
    - Restrict access to data whenever possible
9. Simplicity
    - Avoid complex system designs
10. Minimization
    - Make sure as little as accessible to outsiders as possible.



1. Domain Separation
2. Process Isolation
3. Resource Encapsulation
4. Least Privilege
5. Modularity
6. Layering
7. Abstraction
8. Data Hiding
9. Simplicity
10. Minimization