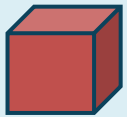
White Box Testing

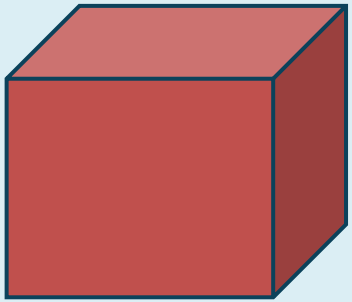
- Also called *transparent testing*
- Known to the tester
  - Implementation details
  - Documentation
- Illustrates the result of "inside help"

Black Box Testing



- Also called *behavioural testing*
- Subject details are unknown to the tester
  - Implementation details
  - Documentation
  - Security controls that may be in place
- Simulates an external attack
- Identifies vulnerabilities

Gray Box Testing



- Falls between white and black box testing
- Partial understanding of
  - Configuration details
  - Security controls that may be in place

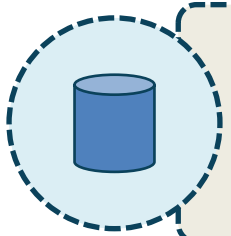
Vulnerability Scanning

- Identify weaknesses
  - Network
  - Host
  - Application
- Passive scanning
  - Identifies, but does not exploit weaknesses

The Vulnerability Scanning Process

Scan network

Scan network devices



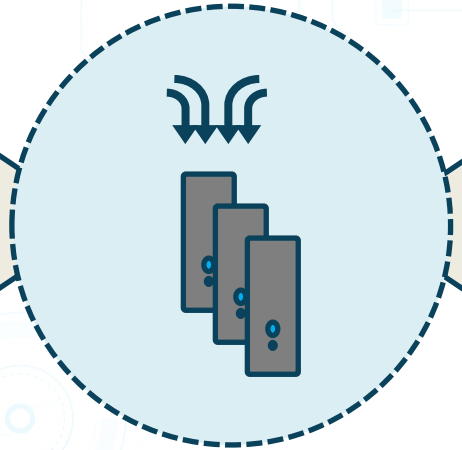
Use vulnerability database to check for weaknesses

Vulnerability Scanning Considerations

- Establish a baseline of a "normal" configuration
- Keep vulnerabilities database up to date
- Determine scan target(s)
- Credentialed vs. non-credentialed scans
- Reporting
  - Identification of changes

Penetration Testing

Active



Attempts to exploit vulnerabilities

Pen Testing - Rules of Engagement

- Scheduling
- Potential service disruption
- Non-disclosure agreement (NDA)

Penetration Testing

Red team

- Executes pen tests
  - Network
  - Devices
  - Applications
  - Databases
- Simulates real world attacks

Blue team

- Monitors for security events
- Prevents and stop attacks
- Educates IT staff on mitigation strategies and techniques

Honeypots

- Mimics production systems and data
- Can be configured to appear vulnerable

Honeypots

Pros

- Early incident detection
- Learn about
  - Attack patterns
  - Attack vectors
  - Attacker identities

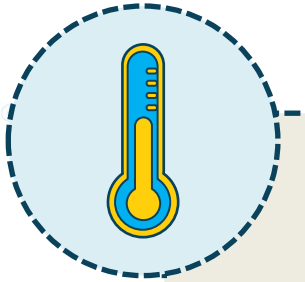
Cons

- Legal liability
  - Inadvertent data breach
  - Compromised system used for illegal activity

Honeypot Configurations

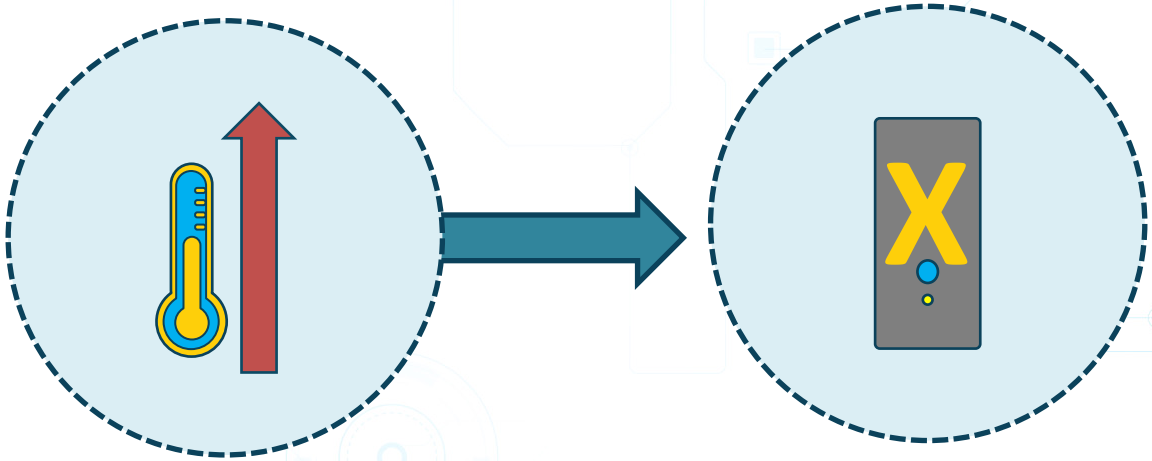
- Server operating system
- Specific service
- Individual file or folder
- HoneyDrive honeypot
  - Linux-based virtual appliance
  - SSH honeypot
  - Website honeypot
  - Monitoring and analytical tools

Heating, Ventilation, and Air Conditioning (HVAC)



- Often overlooked as a vulnerability
- Required, but can also negatively impact
  - Personnel
  - Equipment

HVAC



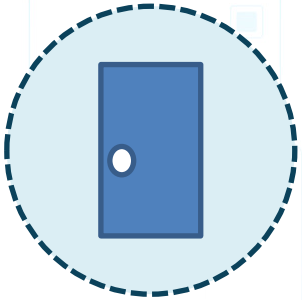
Too much heat

System slowdown or crash

HVAC IoT Devices

- Change default settings
- Apply updates
- Place devices on isolated restricted networks accessible through only a VPN

Physical Security



Physical Security

- Physical devices must be inventoried
- Device details and location must be known
- Preventative measures
  - Laptop lock-down cables
  - Locked server room doors
  - Locked server room racks

Physical Security

- Relationship to digital
  - Require client device PKI certificates for physical network access
  - Encryption of data at rest in case storage device is stolen
  - Air-gapped networks

Drones and Proximity Security

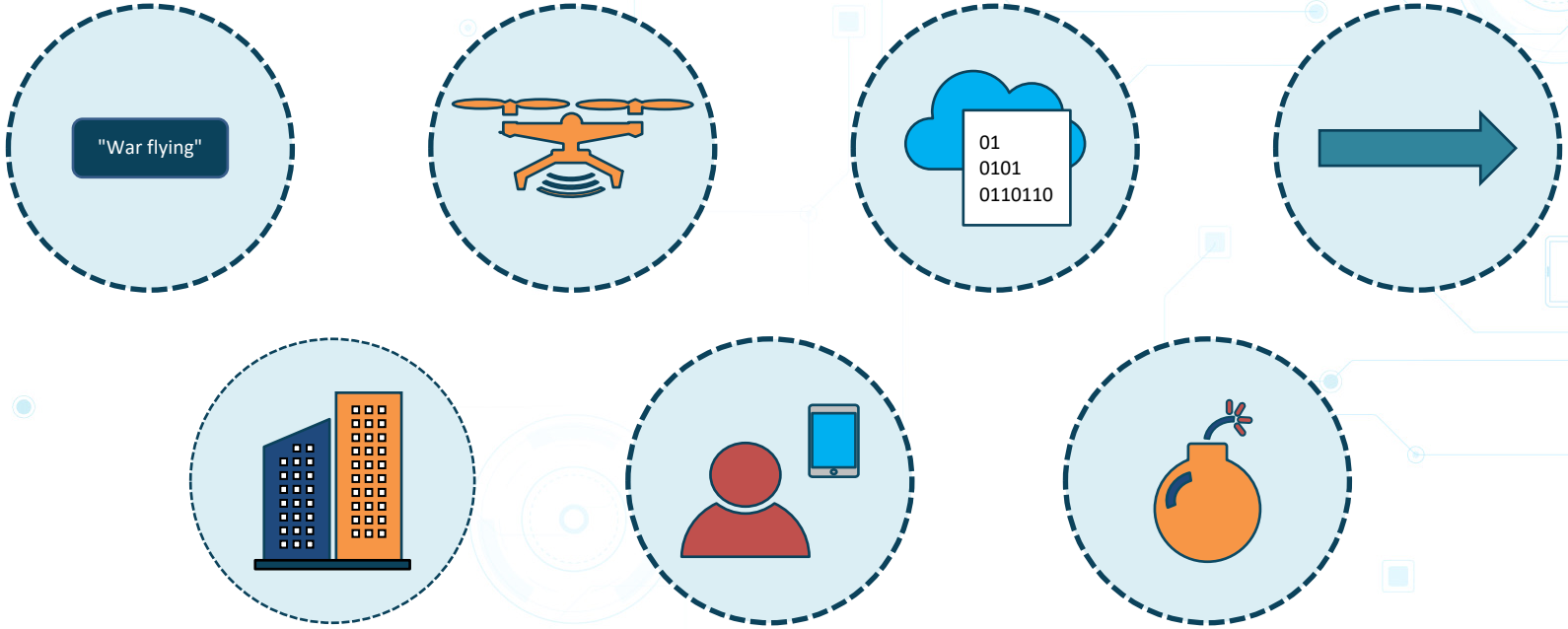
Mobile airborne device

Reconnaissance

Drones and Proximity Security

- Regulations
  - Drones are considered to be aircraft
  - Drone pilot certificate
  - Drone registration
  - Below 122 meters (400 feet)
  - Away from airports and other aircraft
  - Privacy and voyeurism

Drones and Proximity Security



Drones and Proximity Security

- Geo-fencing
  - Drone firmware honors drone no-fly zones such as airports
  - Based on GPS
  - Attackers could somehow disable GPS

Fire Suppression Systems

- Legal and regulatory compliance
- Data center and server room construction
- Fire detection systems
- Fire extinguishers

Fire Risks

- Harm to personnel
- Equipment damage
- Data loss
- Customer service disruption
- Expensive post-fire cleanup

Fire Suppression Systems

- Equipment is not as valuable as
  - Personnel
  - Data
- U.S. National Fire Protection Association Standard (NFPA 75)
  - IT equipment protection against fires

In this exercise, you will

- Differentiate between vulnerability and penetration testing
- Describe the purpose of a jump box
- List three examples of physical security
- Perform a non-credentialed vulnerability scan

Security Testing

- Vulnerability testing
  - Identify vulnerabilities
- Penetration
  - Exploit vulnerabilities

Jump Box

- Administrative connectivity point
- Accessible from external network
- Provides access to internal hosts

Physical Security

- Geo-fencing
- Security guards
- Door locks