JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Analyzing Secure Architectures

Security Architecture & Tool Sets

Analyzing Architectures

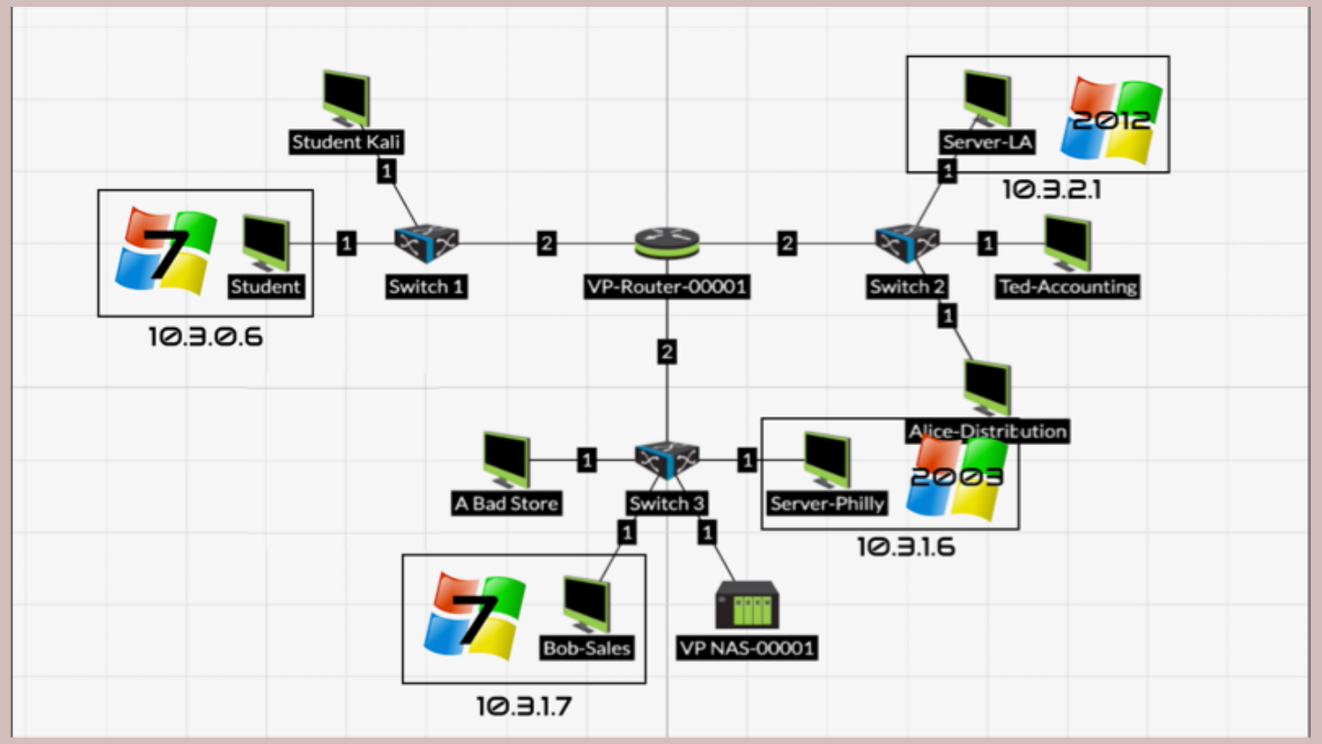
- Attackers always look for the flaw in the architecture's security controls
- Penetration testers act like an attacker to find these flaws, gaps, and single points of failure
- When analyzing security controls, determine if they meet the given requirement or stated goal

Reviewing Architectures

- Operational View
  - Focuses on how a function is performed or is supposed to accomplish
- Technical View
  - Focuses on technologies, configurations, and settings used in an architecture (system or service)
- Logical View
  - Focuses on the interconnections of systems with less technical details than the technical view

Common Issue: Single Points of Failure

- Singular part of the system that could cause the entire system to fail or the desired security level to fail is exploited



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Common Issue: Data Validation and Trust

- Data is commonly assumed to be valid and trustworthy in a system
- Can cause issues, such as trusting input provided to web application will be valid
- Can lead to SQL injections or other issues
- To prevent this, systems should be designed with validation and integrity checking

Common Issue: Users

- The largest cause of a security failure
- Mistakes and abuse can be at fault
- To prevent this:
  - Use automated monitoring to detect error
  - Constrain interfaces to only allow activities
  - Implement procedural checks and balances
  - Provide user awareness training

Common Issue: Authentication & Authorization

- User credentials, passwords, and permissions can cause security failure

- To prevent this:
  - Multifactor authentication
  - Centralized account management
  - Centralized privilege management
  - Monitor privileged account access
  - User awareness training

Architecture Reviews

- Step-by-step analysis of organization security needs
- Begin with the design requirements and then look at technical and logical diagrams
- Identify issues and report them per your organizational processes

Maintaining Secure Architectures

- Threats change over time and systems become outdated
- Conduct scheduled reviews
  - Systems, networks, and processes
- Continual Improvement
  - Incremental improvements over time
- Retirement of processes
  - Policies can become no longer relevant