CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

# CECS 303: Networks and Network Security

## Penetration Testing (cont'd) and Defense in Depth

***Chris Samayoa***

Week 10 – 2nd Lecture
3/24/2022

# Course Information

CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

- CECS 303
  - Networks and Network Security – 3.0 units
- Class meeting schedule
  - TuTH 5:00PM to 7:15PM
  - Lecture Room: VEC 402
  - Lab Room: ECS 413
- Class communication
  - chris.samayoa@csulb.edu
  - Cell: 562-706-2196
- Office hours
  - Thursdays 4pm-5pm (VEC-404)
  - Other times by appointment only

# Objectives



- Penetration Testing Continued
  - Exploitation
  - Escalation
  - Analysis / Reporting
  - Remediation
- Defense in Depth

# Penetration Testing Stages



- Planning (scoping)
- Reconnaissance
- Gaining Access (exploitation) – Lateral Movement
- Maintaining Access / Escalation
- Analysis / Reporting
- Remediation

# Objectives



- Penetration Testing Continued
  - Exploitation
  - Escalation
  - Analysis / Reporting
  - Remediation
- Defense in Depth

# Exploitation



- Can begin while reconnaissance is still ongoing
  - More reconnaissance is needed after successful exploitation
  - Time constraints are always of concern
- Opportunistic approach
  - Chase whatever leads become available
  - Prioritize based on sensitivity and criticality
- Human-hacking
  - Use information gained from reconnaissance to guess passwords or used exposed ones
  - Use known personal information to fool an employee or one of their relations
- Find lateral avenues to continue testing

# Exploitation (cont'd)



- Evasion (avoiding detection)
  - Anti-Virus
    - Avoid known attack signatures and other known TTPs
  - Encoding
    - Obfuscate actual data/information by rearranging
  - Encrypting
    - Attempt to bypass security checks with encryption. Goal is to decrypt in memory after security mechanisms have performed their checks
  - Process Injection
    - Hide malicious activity within another, legitimate, process
  - Purely Memory Resident
    - Ability to detect when writing to disk is typically greater
    - Attacker can find a way to only live in running memory

# Exploitation (cont'd)



- Zero-Day Angle
  - Fuzzing
    - Automated process used to uncover software security bugs using crafted inputs into a program that analyzes the results; often looking for system crashes that can be exploited
    - Can be used with software, firmware, networks, and hardware
    - Can function with or without access to source code
  - Source Code Analysis

# Exploitation (cont'd)



- General Exploitation Techniques
  - Buffer Overflows
  - Physical Access
  - PC Access
  - WiFi Attacks
    - Rogue access points
    - Crack passcodes
    - Exploit protocol vulnerabilities

# Objectives



- Penetration Testing Continued
  - Exploitation
  - Escalation
  - Analysis / Reporting
  - Remediation
- Defense in Depth

# Escalation



- Privilege escalation
  - e.g. Dirty Pipe
  - Allows for additional lateral or local movement
- Continually search for new opportunities
  - Access to new devices or credentials offer potential pathways
  - Different VLANs, IP addresses, or devices have access to different network resources
- Establish persistent access
  - Reverse shells
  - VNC servers
  - Firewall rule changes
  - “Malicious” software

# Objectives



- Penetration Testing Continued
  - Exploitation
  - Escalation
  - Analysis / Reporting
  - Remediation
- Defense in Depth

# Reporting



- Full (private) Report
  - Includes the following:
    - Detailed summary of findings
    - Individual finding reports
    - Remediation checklist
  - No results should be held back from the penetration test
- Executive Report
  - Summary of findings with no details regarding found vulnerabilities
  - High-level of information (e.g. how many vulnerabilities were identified)
  - Can be used to inform budgeting decisions
- Public Facing Report
  - Suitable for distribution to the general public
  - Sanitized report that confirms scope of work and mitigation of vulnerabilities

# Objectives



- Penetration Testing Continued
  - Exploitation
  - Escalation
  - Analysis / Reporting
  - Remediation
- Defense in Depth

# Remediation



- Not performed by penetration testers
  - Local network/system administrators
  - Third party-contractors
- Retesting
  - Often when planning a penetration test, funding is secured in advance to re-run testing in order to document that remediations were successful
- Accepted Risk (if applicable)
  - If a remediation cannot be completed due to operation needs, then the vulnerability can be documented as an accepted risk by the organization

# Objectives



- Penetration Testing Continued
  - Exploitation
  - Escalation
  - Analysis / Reporting
  - Remediation
- Defense in Depth

# Defense in Depth



- Refers to a layered approach to network security where defenses are placed at different locations in the environment to enhance an organizations overall security posture
  - Mechanisms may be redundant
  - Overall approach depends on what is being protected
- Major categories
  - Administrative (e.g. policies, procedures, and directives)
  - Physical (e.g. guns, guards, and gates)
  - Technical Controls

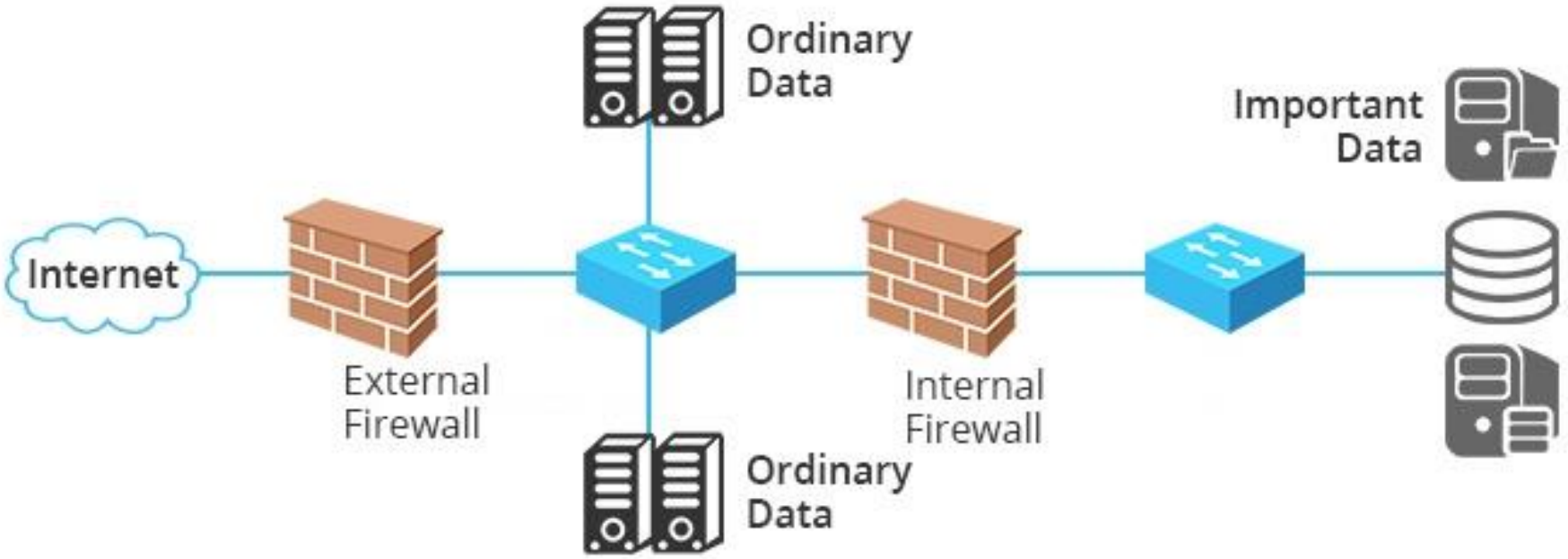
# Technical Controls



- Commonly used controls
  - Firewalls
    - DMZ
    - Segmentation
  - VPNs
  - Antivirus Software
  - Encryption / Hashing
  - Authentication / Multi-factor Authentication
  - Vulnerability Scanners
  - Sandboxing
  - Intrusion Detection System (IDS)
  - Packet Filters / Deep Packet Inspection (DPI)
  - Logging / Auditing

# Firewall Placement

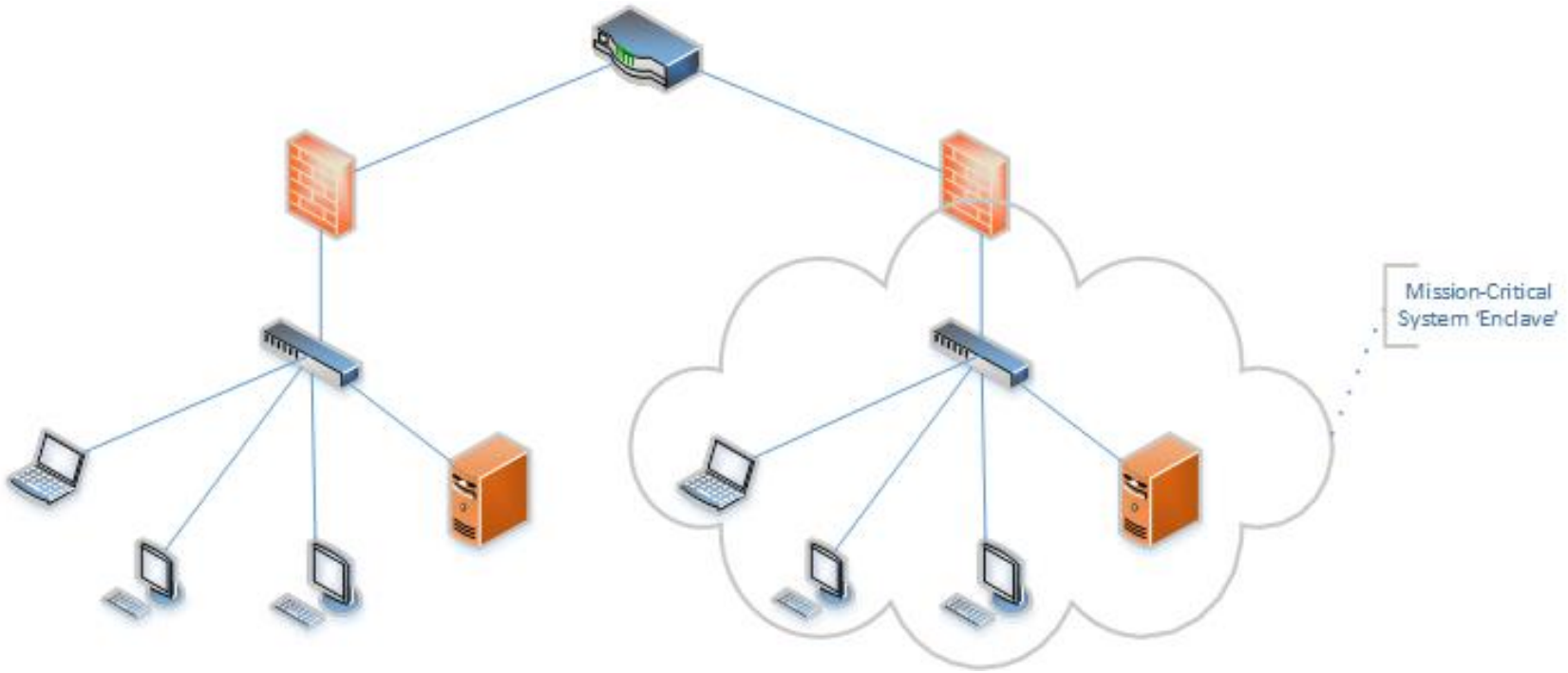
CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering




Source: https://community.fs.com/blog/network-switch-router-firewall-why-need-all-three.html

# Firewall Segmentation

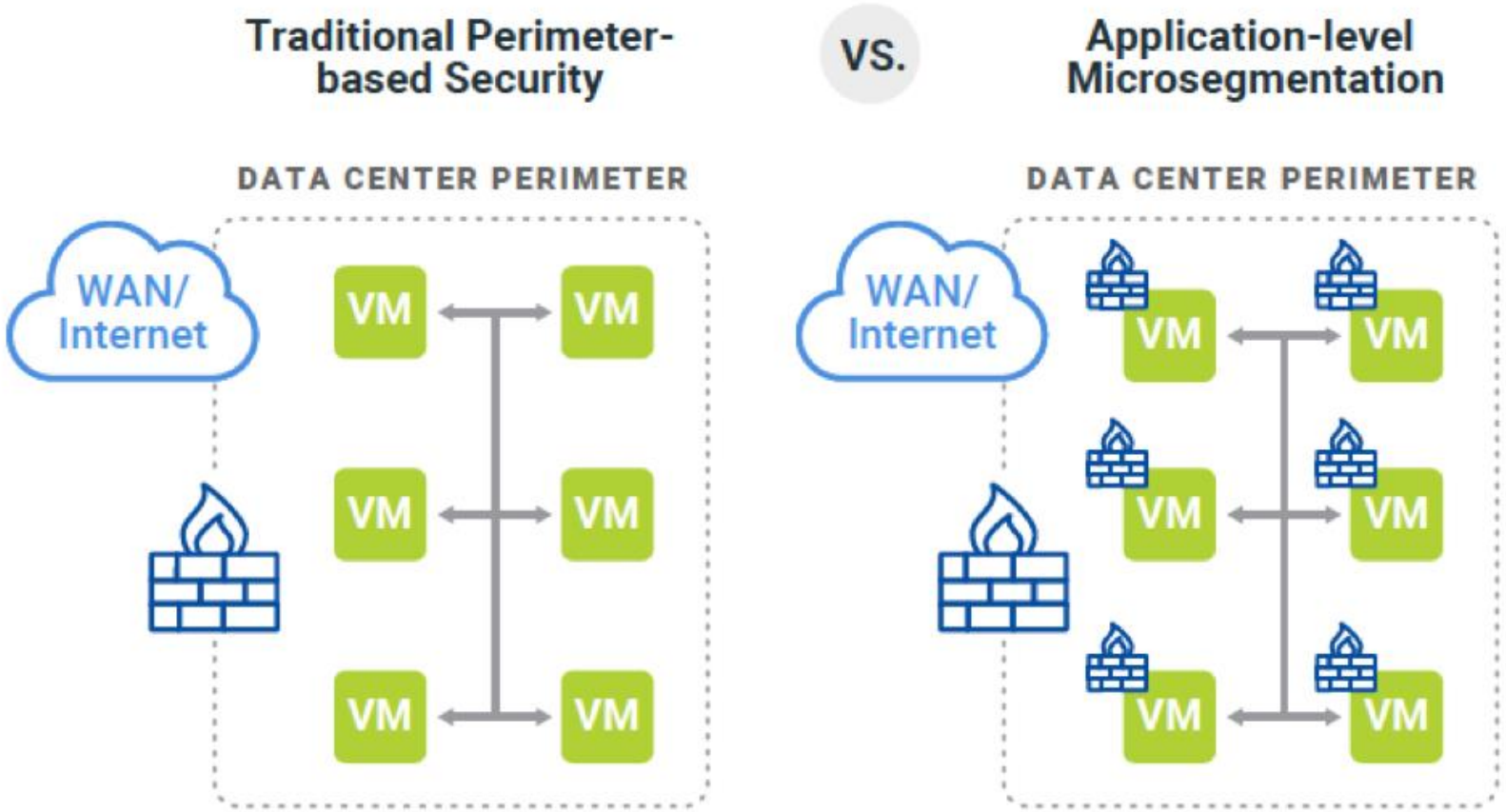
CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering




Source: https://insights.sei.cmu.edu/blog/network-segmentation-concepts-and-practices/

# Micro-Segmentation






Source: https://medium.com/@me_isbella/microsegmentation-for-a-better-iot-cdeb25e51941

# Sandboxing



- The practice of creating an isolated environment for observing behavior of potentially malicious code or threat actors
  - Important to keep separate from normal / production environments to avoid compromise
- Benefits
  - Mitigation of risk to network devices (e.g. host operating systems)
  - Evaluate potentially malicious software for threats
  - Quality assurance (QA) usage
    - Test before introducing code to production
  - Quarantine threats (including zero-day attacks)

# Sandboxing (cont'd)



- Implementation
  - Cloud-based
  - On-premise appliance
  - Software
  - Web browser extensions
- Potential Evasion
  - Malware can be programmed to terminate if sandbox environment is detected
  - Intrusion detection capabilities can be circumvented
    - Encrypted files
    - Large formats
    - Benign file extensions
  - Malware can be "context-aware" in order to wait for triggers that typically indicate end user activity

# Summary



- Exploitation of a system can use existing or zero-day attacks
- Privilege escalation is not necessary to extract data, but does open additional avenues of attack
- Ensure that your penetration test is scoped to deliver all reports needed for your organization
- Defense in Depth is the practice of using well-thought out, layered defense mechanisms to protect a given environment