10 : IT Infrastructure Auditing and Remediation

IT6406 - Network Security and Audit

Level III - Semester 6

Overview

10.1. Scope of an IT compliance audit

- 10.1.1. Compliance basics
- 10.1.2. Introduction to IT Infrastructure auditing
- 10.1.3. Maintaining IT compliance
- 10.1.4. Compliance within user domain
- 10.1.5. Compliance within workstation domain
- 10.1.6. Compliance within LAN domain
- 10.1.7. Compliance within LAN-to-WAN domain
- 10.1.8. Compliance within the WAN domain
- 10.1.9. Compliance within the remote access domain

10.2. Network Auditing and Assessment Tools

10.3. Network Security Issue Remediation and Infrastructure Hardening

10.1.1. Compliance basics

- Organizational policies provide general statements that address the operational goals of an organization.
- IT security policies concerned with protecting the confidentiality, integrity, and availability of information and information systems.

- COBIT is a popular and widely used control framework for IT in general.

Read More: Ref 2: Pg. (63-70)

10.1.2. Introduction to IT Infrastructure auditing

- Objectives of infrastructure auditing
  - Examine the existence of relevant and appropriate security policies and procedures.
  - Verify the existence of controls supporting the policies.
  - Verify the effective implementation and ongoing monitoring of the controls.

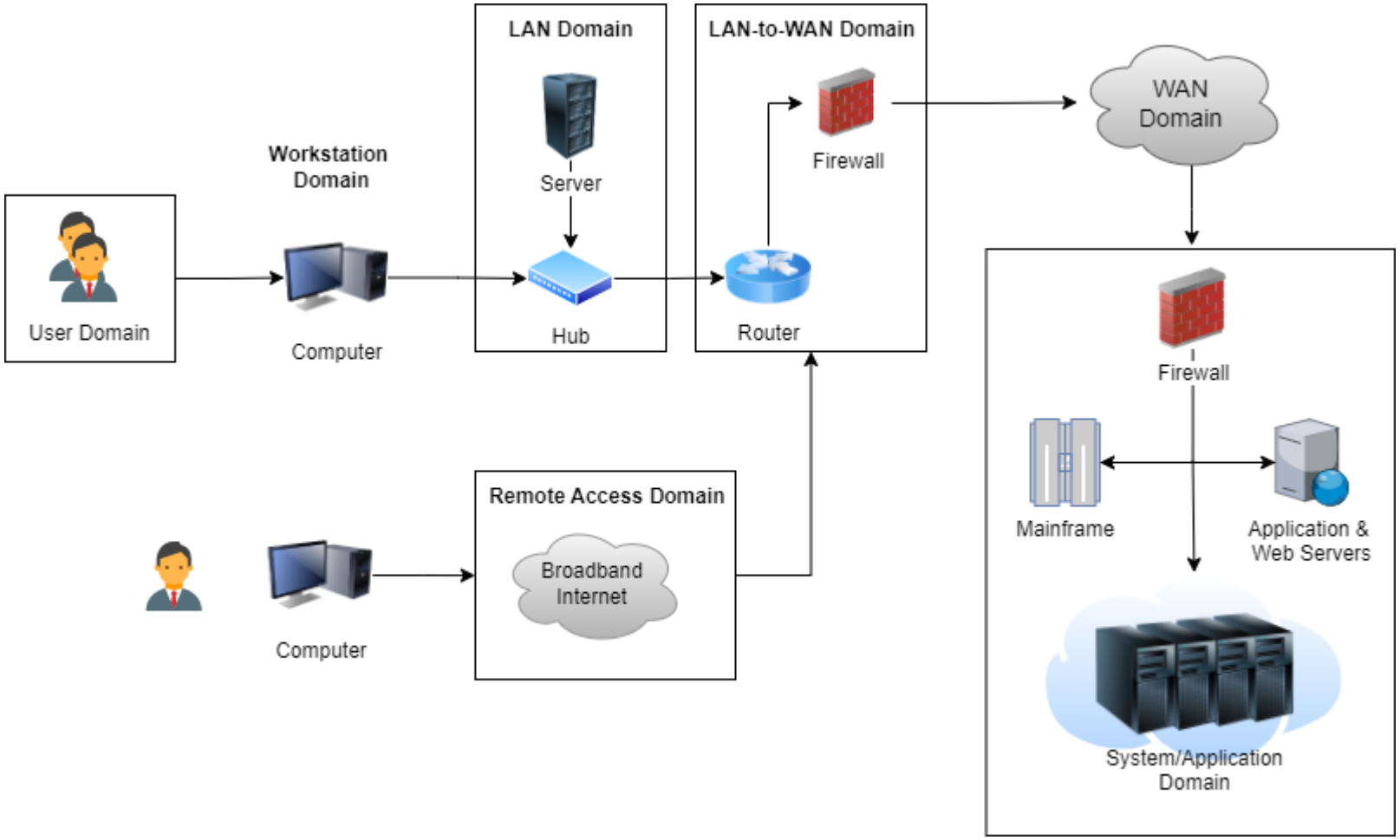
Read More: Ref 2: Pg. (70-75)

10.1.2. Introduction to IT Infrastructure auditing…(2)

- Seven domains of a typical IT infrastructure
  - User Domain
  - Workstation Domain
  - LAN Domain
  - LAN-to-WAN Domain
  - WAN Domain
  - Remote Access Domain
  - System/Application Domain

Read More: Ref 2: Pg. (70-75)

10.1.2. Introduction to IT Infrastructure auditing...(3)



Read More: Ref 2: Pg. (70-75)

10.1.3. Maintaining IT compliance

- Compliance is an ongoing process, therefore, it need to be maintained.
- Maintaining requires a well defined programmatic approach that involves processes and technology.
  - Regular assessment of selected security controls
  - Configuration and control management processes
  - Change management processes
  - Annual audit of the security environment

Read More: Ref 2: Pg. (75-79)

10.1.4. Compliance within user domain

- Items found in user domain
  - Employees - most trusted, fully access
  - Contractors - some trust is necessary, partial access
  - Guests/third parties - least trusted, limited access

- Types of documentation in the User Domain that affect compliance:
  - Human resources (HR) manuals
  - IT asset AUPs
  - Internet AUPs
  - E-mail AUPs

Read More: Ref 2: Pg. (168-184)

10.1.4. Compliance within user domain…(2)

- Separation of duties
- Privilege levels
- Confidentiality agreements
- Employee background checks
- Acknowledgment of responsibilities and accountabilities
  - RACI matrix - R (Responsible), A (Accountable), C (Consulted), I (Informed)
- Security awareness and training for new employees
- Information systems security accountability
- Adherence to documented IT security policies, standards, procedures, and guidelines
- Best practices for user domain compliance

Read More: Ref 2: Pg. (168-184)

10.1.5. Compliance within workstation domain

- Devices commonly found in workstation domain
  - Uninterruptible power supply (UPS)
  - Desktop Computers
  - Laptops/Tablets/Smartphones
  - Local Printers
  - Modems and Wireless Access Points
  - Fixed Hard Disk Drives
  - Removable Storage Devices

Read More: Ref 2: Pg. (187-205)

10.1.5. Compliance within workstation domain…(2)

- Maximizing C-I-A
  - Access rights and access controls in the workstation domain (C-I-A)
    - Confidentiality—Assurance that the information cannot be accessed or viewed by unauthorized users
    - Integrity—Assurance that the information cannot be changed by unauthorized users
    - Availability—Assurance that the information is available to authorized users in an acceptable time frame when the information is requested
- Workstation vulnerability management

Read More: Ref 2: Pg. (187-205)

10.1.6. Compliance within LAN domain

- Components in LAN domain
  - Connection media
  - Networking devices
  - Server computers and services devices
  - Networking services software
- LAN traffic and performance monitoring and analysis
  - Monitoring LAN performance
  - Changing configuration settings to optimize performance
  - Changing configuration settings to support new requirements
  - Adding necessary controls to address security issues
- Access Rights and Access Controls in the LAN Domain
- Maximize C-I-A

Read More: Ref 2: Pg. (208-225)

10.1.7. Compliance within LAN-to-WAN domain

- Components found in LAN-to-WAN domain
  - Routers
  - Firewalls
  - Proxy Servers
  - Demilitarized Zones
  - Honeypots
  - Internet Service Provider Connections and Backup Connections
  - Intrusion Detection Systems/Intrusion Prevention Systems
  - Data Loss/Leak Security Appliances
  - Web Content Filtering Devices
  - Traffic-Monitoring Devices

Read More: Ref 2: Pg. (228-251)

10.1.7. Compliance within LAN-to-WAN domain…(2)

- LAN-to-WAN traffic and performance monitoring and analysis
- FCAPS
  - Fault management
  - Configuration management
  - Accounting management
  - Performance management
  - Security management
- Network-Management Tools
- Maximize C-I-A

Read More: Ref 2: Pg. (228-251)

10.1.8. Compliance within the WAN domain

- Devices and components in WAN domain
  - WAN Service Providers
  - Dedicated Lines/Circuits
  - MPLS/VPN WAN or Metro Ethernet
  - WAN Layer 2/Layer 3 Switches
  - WAN Backup and Redundant Links

Read More: Ref 2: Pg. (255-271)

10.1.8. Compliance within the WAN domain…(2)

- WAN traffic and performance monitoring and analysis
- WAN configuration and change management
- WAN management tools and systems
- Access rights and access controls in the WAN domain
- Maximizing C-I-A

Read More: Ref 2: Pg. (255-271)

10.1.9. Compliance within the remote access domain

- Devices and components in remote access domain
  - Remote Users
  - Remote Workstations or Laptops
  - Remote Access Controls and Tools
  - Authentication Servers
  - Internet Service Provider WAN Connections
  - Broadband Internet Service Provider WAN Connections

Read More: Ref 2: Pg. (274-291)

10.1.9. Compliance within the remote access domain…(2)

- Remote access and VPN tunnel monitoring
- Remote access traffic and performance monitoring and analysis
- Remote access configuration and change management
- Remote access management, tools, and systems
- Access rights and access controls in the remote access domain
- Best practices for remote access domain compliance
  - Preventive
  - Detective
  - Corrective

Read More: Ref 2: Pg. (274-291)

10.2. Network Auditing and Assessment Tools

- Nmap [https://nmap.org/docs.html]
  - Nmap - Network Mapper
  - Used for network exploration and security auditing
- Wireshark [https://www.wireshark.org/docs/]
  - Network packet analyzer
  - Used to
    - Troubleshoot network problems
    - Examine security problems
    - Verify network applications
    - Debug protocol implementations

10.3. Network Security Issue Remediation and Infrastructure Hardening

- Asset
  - An asset is any data, device, or other component of the environment that supports information related activities that should be protected from anyone besides the people that are allowed to view or manipulate the data/information.
- Vulnerability
  - Vulnerability is defined as a flaw or a weakness inside the asset that could be used to gain unauthorized access to it. The successful compromise of a vulnerability may result in data manipulation, privilege elevation, etc.

Reference: Baloch (2014)

10.3. Network Security Issue Remediation and Infrastructure Hardening

- Threat
  - A threat represents a possible danger to the computer system. It represents something that an organization doesn't want to happen. A successful exploitation of vulnerability is a threat. A threat may be a malicious hacker who is trying to gain unauthorized access to an asset.
- Exploit
  - An exploit is something that takes advantage of vulnerability in an asset to cause unintended or unanticipated behavior in a target system, which would allow an attacker to gain access to data or information.

Reference: Baloch (2014)

10.3. Network Security Issue Remediation and Infrastructure Hardening

- Infrastructure
  - Network devices, Network services, and Servers (web, email, application servers, etc.).

10.3. Network Security Issue Remediation and Infrastructure Hardening

- What is Vulnerability Assessment (VA)?
  - Vulnerability assessment is the process of scanning an information system to find out the weaknesses and document them accordingly.

10.3. Network Security Issue Remediation and Infrastructure Hardening

- Motivation to conduct VAs
  - Legal and regulatory constraints.
    - Financial institutions require to have regular VAs as part of their compliance
  - Risks to the business - reputation, financial, etc.
    - Information theft resulted due to a weakness of the system
  - Continuity of service as exploitation of a vulnerability would result in service interruptions

10.3. Network Security Issue Remediation and Infrastructure Hardening

- Testing Approaches
  - Black box testing
  - White box testing
  - Grey box testing

10.3. Network Security Issue Remediation and Infrastructure Hardening

- VA Techniques
  - Static analysis
    - analyse the code structure, design and contents of the system
    - does not exploit, thus no bad effect on system
    - very slow
    - Tools: Veracode, Semmle, etc.

10.3. Network Security Issue Remediation and Infrastructure Hardening

- VA Techniques
  - Manual Testing
    - Tester use his knowledge and experience to find out the vulnerabilities in the system
    - low budget
    - very slow
    - at most cases, does not use professional tools

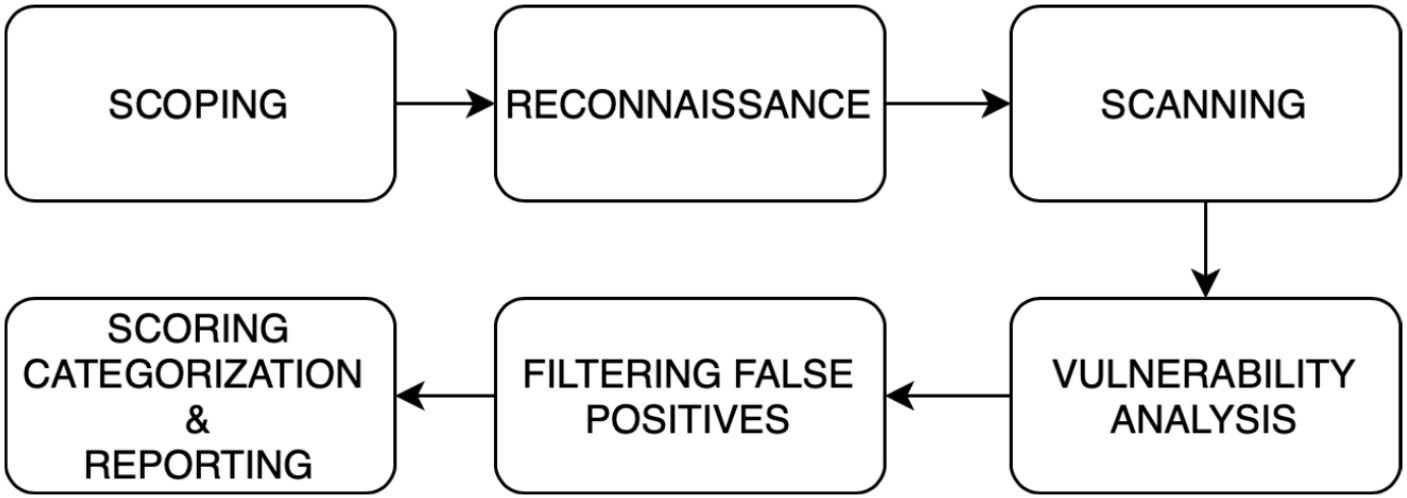
10.3. Network Security Issue Remediation and Infrastructure Hardening

- VA Techniques
  - Automated testing
    - Tester use automated tools specifically build for the particular application - e.g. web, network, database, etc.
    - tools are very expensive
    - very quick
    - Tools: e.g. Nessus, Rapid7, Acunetix, CoreImpact, Open source tools, etc.
    - Cloud solutions are available. e.g. Qualys
    - Minimum false positives
    - Penetration testing is also available to certain extent

10.3. Network Security Issue Remediation and Infrastructure Hardening

- VA Techniques
  - Fuzz testing
    - Test the robustness of the system by inputing invalid or random data
    - Automated tools available

10.3. Network Security Issue Remediation and Infrastructure Hardening



10.3. Network Security Issue Remediation and Infrastructure Hardening

- Scoping the VA
  - Time
  - Resourcing and Budget
  - Number of services, hosts, etc.
  - Information exposure (Black, Gray, White)

10.3. Network Security Issue Remediation and Infrastructure Hardening

- Reconnaissance
  - To gain much information as possible in a very less intrusive way
    - social engineering
    - Internet searching and google hacking
    - passive network scanning and sniffing
    - dumpster diving, etc.

10.3. Network Security Issue Remediation and Infrastructure Hardening

- Scanning and VA Tools
  - Nmap - open ports, open services, network device discovery, etc.
  - ZAP - web application vulnerability assessment
  - Metasploit - vulnerability assessment and penetration testing
    - Ref: https://www.offensive-security.com/metasploit-unleashed/
    - Ref: http://webbhatt.com/databas/metasploit.pdf

10.3. Network Security Issue Remediation and Infrastructure Hardening

- Vulnerability Scoring and Reporting
  - Common Vulnerability Scoring System
  - Ref: https://www.first.org/cvss/calculator/3.1

10.3. Network Security Issue Remediation and Infrastructure Hardening

- Vulnerability/Security Issue Remediation
  - Security Patches/updates
  - System hardening
  - Configuring using security best practices of the industry

10.3. Network Security Issue Remediation and Infrastructure Hardening

- Hardening the system
  - Hardening a system is the process of making the system robust for intruder attacks as much as possible
  - Could be both infrastructure (firewall, network) and deployment platform (web application server)
  - It could be:
    - Strengthening permissions and access control
    - Using secure cryptographic algorithms
    - Removing unnecessary data/apps from the system
    - Removing unwanted modules/components
    - Stop unused services
    - Removing unused libraries
    - Removing software building/compiling utilities
    - Enabling firewall
  - CIS guides are commonly used for the purpose; a good starting point (Ref: https://www.cisecurity.org/cis-benchmarks/)
  - Refer CIS guide for Apache Tomcat server harden a fresh installation of Apache Tomcat as an activity

Reference

- Ref 2. Auditing It Infrastructures for Compliance, 2nd Edition, Martin Weiss; Michael G. Solomon