Week 10 Research

CIT 288

Chaz Davis

2020-03-28

---

1) From Ch - 11 –Define defensive programming.

Defensive programming is a form of defensive design intended to ensure the continuing function of a piece of software under unforeseen circumstances. Defensive programming practices are often used where high availability, safety, or security is needed.

2) Define input fuzzing. State where this technique should be used.

Fuzzing or fuzz testing is an automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program. The program is then monitored for exceptions such as crashes, failing built-in code assertions, or potential memory leaks.

3) List several software security concerns associated writing safe program code.

- **Correct Algorithm Implementation**
- **Interpretation of input** (wrong type, unauthorized filenames)
- **Injection attacks**
- **Cross-site scripting**
- **Race Conditions**
- **replacing legitimate dynamic libraries with malicious ones**
- **tampering with environmental variables**
- **"Hijacking" temporary files (also input to the program)**

4) Define the principle of least privilege.

Programs should execute with the least amount of privileges needed to complete their function.

5) Identify several issues associated with the correct creation and use of a temporary file in a shared directory.

The temporary file must not be accessed by another process. An attacker could guess the name of the temporary file and create it in between the time the

program checks if it exists and subsequently creating it. The program could be redirected and would overwrite the existing file. Thus the use of secure system calls is advised to avoid race conditions.

6) From Ch 12 – What are the basic steps needed in the process of securing a system?

- patch operating systems and applications using auto-update
- patch third party applications
- restrict admin privileges to users who need them
- white-list approved applications

7) What are the basic steps needed to secure the base operating system?

- install and patch the operating system
- harden and configure the operating system to adequately address the identified security needs on the system by:
  - removing unnecessary services, applications, and protocols
  - configuring users, groups, and permissions
- install and configure additional security controls such-as anti-virus, host-based firewalls, and intrusion detection systems
- test the security of the base operating system to ensure that the steps taken adequately address its security needs

8) What are the pros and cons of automated patching?

Because security patches can, on rare but significant occasions, introduce instability, You should stage and validate all patches on test systems before deploying them in production.

9) What is the point of removing unnecessary services, applications, and protocols?

So that a suitable level of functionality is provided.

10) What type of access control model do Unix and Linux systems implement?

Linux and Unix provide discretionary access controls to all file system resources.

11) What steps are used to maintain system security?

12) What is the main host firewall program used on Linux systems?

The main firewall program in Linux is perimeter firewall.

13) Where are two places user and group information may be stored on Windows systems?

They can be placed within the Security Account Manager, or centrally managed by Active Directory.

14) What are the major differences between the implementations of the discretionary access control models on Unix and Linux systems and those on Windows systems? Be thorough.

Linux and Unix implements discretionary access controls to all file system resources, not only files and directories, but memory, and even most system resources.

Windows applies DAC to files, shared memory, and name pipes and much of the configuration information is centralized in the Registry.

15) What is virtualization?

Virtualization is technology that provides an abstraction of the computing resources used to run in a simulated environment.

16) What are the main security concerns with virtualized systems?

- guest OS isolation, ensuring that programs executing within a guest OS may only use the resources allocated to it and not interact with programs or data either in other guest OS's or in the hypervisor.
- guest OS monitoring by the hypervisor, which has privileged access to the programs and data in each guest OS, and must be trusted as secure from subversion and compromised use of this access.
- virtualized environment security, particularly as regards to image and snapshot management, which attackers may attempt to view or modify.

17) What are the basic steps to secure virtualized systems?

- carefully plan the security of the vitualized system
- secure all elements of a full virtualization solution, including the hypervisor, guest os, and virtualized infrastructure, and maintain their security.

- ensure that the hypervisor is properly secured
- restrict and protect administrator access to the virtualization solution.

18) From Ch 13 – What is OpenStack?

The OpenStack OS consists of a number of independent modules, each of which has a project name and a functional name. The modular structure is easy to scale out and provides a commonly used set of core services. Typically, the components are configured together to provide a comprehensive IaaS capability. However, the modular design is such that the components are generally capable of being used independently.

19) Define the Internet of things.

The Internet of things (IoT) is a term that refers to the expanding interconnection of smart devices, ranging from appliances to tiny sensors. A dominant theme is the embedding of short-range mobile transceivers into a wide array of gadgets and everyday items, enabling new forms of communication between people and things, and between things themselves.

20) Define the patching vulnerability.

Patching vulnerabilities is the process of getting patches, usually from the vendors of the affected software or hardware, and applying them to all the affected areas in a timely way. This is sometimes an automated process, done with patch management tools.

21) What is MiniSec?

MiniSec is a secure network layer that obtains the best of both worlds: low energy consumption and high security. MiniSec has two operating modes, one tailored for single-source broadcast communication.

22) List and briefly define the principal components of an IoT-enabled thing.

- **sensor:** A sensor measures some parameter of a physical, chemical, or biological entity and delivers an electronic signal proportional to the observed characteristic, either in the form of an analog, voltage level or a digital signal. In both cases, the sensor output is typically input to a microcontroller or other management element.
- **microcontroller:** The "smart" in smart device is provided by deeply embedded microcontroller.
- **Actuator:** An actuator recieves an electronic signal from a controller and responds by interacting with its environment to produce an effect on some parameter of a physical, chemical, or biological entity.

- **Transceiver:** A transceiver contains the electronics needed to transmit and receive data. Most IoT devices contain a wireless transceiver, capable of communication using Wi-Fi, ZigBee, or some other wireless scheme.
- **Radio-Frequency Identification:** RFID technology, which uses radio waves to identify items, is increasingly becoming an enabling technology for IoT. The main elements of an RFID tags and readers. RFID tags are small programmable devices used for object, animal, and human tracking. They come in a variety of shapes, sizes, functionalities, and costs. RFID readers acquire and sometimes require information stored on RFID tags that come within operating range (a few inches up to several feet). Readers are usually connected to a computer system that records and formats the acquired information for further uses.

23) Define cloud computing.

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (eg. networks, servers, storage, applications, and services) that can be rapidly provisioned with minimal management effort or service provider interaction.

24) List and briefly define three cloud service models.

- **SaaS** Software as a Service, allows your business to quickly access cloud-based web applications without commiting to installing new infrastructure. The applications run on the vendor's cloud, which they, of course, control and maintain.
- **PaaS** Platform as a Service, a third-party vendor provides your business with a platform upon which your business can develop and run applications.
- **IaaS** Infrastructure as a Service, the most flexible of the cloud models, allows your business to have complete, scalable control over the management and customization of your infrastructure.

25) Describe some of the main cloud-specific security threats.

The potential threats posed to cloud computing include data breaches, human error, malicious insiders, account hijacking, and DDoS attacks.