DAILY ASSESSMENT FORMAT

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | **20/07/2020** | **Name:** | **Nayanashree** |
| **Course:** | **Coursera** | **USN:** | **4AL16EC042** |
| **Topic:** | **Network security and vulnerabilities** | **Semester & Section:** | **8 A** |
| **Github Repository:** | **Nayana\_online** |  |  |

|  |
| --- |
| **FORENOON SESSION DETAILS** |
|  |
| **Report**  **Network security:**  A network vulnerability is a weakness or flaw in software, hardware, or organizational processes, which when compromised by a threat, can result in a security breach. Nonphysical network vulnerabilities typically involve software or data. Information security management system A set of policies concerned with information security management, the [information security management system](https://en.wikipedia.org/wiki/Information_security_management_system) (ISMS), has been developed to manage, according to [Risk management](https://en.wikipedia.org/wiki/Risk_management) principles, the [countermeasures](https://en.wikipedia.org/wiki/Countermeasure_(computer)) to ensure a security strategy is set up following the rules and regulations applicable to a given country. These countermeasures are also called [Security controls](https://en.wikipedia.org/wiki/Security_controls), but when applied to the transmission of information, they are called [security services](https://en.wikipedia.org/wiki/Security_service_(telecommunication)). Vulnerability consequences The impact of a security breach can be very high. The fact that IT managers, or upper management, can (easily) know that IT systems and applications have vulnerabilities and do not perform any action to manage the [IT risk](https://en.wikipedia.org/wiki/IT_risk) is seen as a misconduct in most legislations. [Privacy law](https://en.wikipedia.org/wiki/Privacy_law) forces managers to act to reduce the impact or likelihood of that security risk. [Information technology security audit](https://en.wikipedia.org/wiki/Information_technology_security_audit) is a way to let other independent people certify that the IT environment is managed properly and lessen the responsibilities, at least having demonstrated the good faith. [Penetration test](https://en.wikipedia.org/wiki/Penetration_test) is a form of verification of the weakness and countermeasures adopted by an organization: a [White hat](https://en.wikipedia.org/wiki/White_hat_(computer_security)) hacker tries to attack an organization's information technology assets, to find out how easy or difficult it is to compromise the IT security. [[26]](https://en.wikipedia.org/wiki/Vulnerability_(computing)#cite_note-Vacca22-26) The proper way to professionally manage the IT risk is to adopt an [Information Security Management System](https://en.wikipedia.org/w/index.php?title=Information_Security_Management_System&action=edit&redlink=1), such as [ISO/IEC 27002](https://en.wikipedia.org/wiki/ISO/IEC_27002) or [Risk IT](https://en.wikipedia.org/wiki/Risk_IT) and follow them, according to the security strategy set forth by the upper management. [[16]](https://en.wikipedia.org/wiki/Vulnerability_(computing)#cite_note-Vacca-16)  One of the key concept of information security is the principle of [defence in depth](https://en.wikipedia.org/wiki/Defence_in_depth" \o "Defence in depth): i.e. to set up a multilayer defence system that can:   * prevent the exploit * detect and intercept the attack * find out the threat agents and prosecute them   [Intrusion detection system](https://en.wikipedia.org/wiki/Intrusion_detection_system) is an example of a class of systems used to detect [attacks](https://en.wikipedia.org/wiki/Attack_(computing)).  [Physical security](https://en.wikipedia.org/wiki/Physical_security) is a set of measures to protect physically the information asset: if somebody can get physical access to the information asset, it is quite easy to make resources unavailable to its legitimate users. Examples of vulnerabilities Vulnerabilities are related to:   * physical environment of the system * the personnel * management * administration procedures and security measures within the organization * business operation and service delivery * hardware * software * communication equipment and facilities * peripheral devices [[32]](https://en.wikipedia.org/wiki/Vulnerability_(computing)#cite_note-32) [[33]](https://en.wikipedia.org/wiki/Vulnerability_(computing)#cite_note-33) * and their combinations.   It is evident that a pure technical approach cannot even protect physical assets: one should have administrative procedure to let maintenance personnel to enter the facilities and people with adequate knowledge of the procedures, motivated to follow it with proper care. See [Social engineering (security)](https://en.wikipedia.org/wiki/Social_engineering_(security)).  Four examples of vulnerability exploits:   * an attacker finds and uses an overflow weakness to install malware to export sensitive data; * an attacker convinces a user to open an email message with attached malware; * an insider copies a hardened, encrypted program onto a thumb drive and cracks it at home; * a flood damages one's computer systems installed at ground floor.   **The Difference between IDS and IPS Systems**  The main difference between them is that IDS is a monitoring system, while IPS is a control system. IDS doesn't alter the network packets in any way, whereas IPS prevents the packet from delivery based on the contents of the packet, much like how a firewall prevents traffic by IP address.  **Network Address Translation**  Network address translation (NAT) is a method of remapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.  **Basics of Routing and Switching, Network Packets and Structures**  **Routing** is the process of selecting a path for traffic in a [network](https://en.wikipedia.org/wiki/Network_theory) or between or across multiple networks. Broadly, routing is performed in many types of networks, including [circuit-switched networks](https://en.wikipedia.org/wiki/Circuit_switching), such as the [public switched telephone network](https://en.wikipedia.org/wiki/Public_switched_telephone_network) (PSTN), and [computer networks](https://en.wikipedia.org/wiki/Computer_network), such as the [Internet](https://en.wikipedia.org/wiki/Internet).  In packet switching networks, routing is the higher-level decision making that directs [network packets](https://en.wikipedia.org/wiki/Network_packet) from their source toward their destination through intermediate [network nodes](https://en.wikipedia.org/wiki/Node_(networking)) by specific packet forwarding mechanisms. [Packet forwarding](https://en.wikipedia.org/wiki/Packet_forwarding) is the transit of network packets from one [network interface](https://en.wikipedia.org/wiki/Network_interface) to another. Intermediate nodes are typically [network hardware](https://en.wikipedia.org/wiki/Network_hardware) devices such as [routers](https://en.wikipedia.org/wiki/Router_(computing)), [gateways](https://en.wikipedia.org/wiki/Gateway_(telecommunications)), [firewalls](https://en.wikipedia.org/wiki/Firewall_(computing)), or [switches](https://en.wikipedia.org/wiki/Network_switch). General-purpose [computers](https://en.wikipedia.org/wiki/Computer) also forward packets and perform routing, although they have no specially optimized hardware for the task.  The routing process usually directs forwarding on the basis of [routing tables](https://en.wikipedia.org/wiki/Routing_table). Routing tables maintain a record of the routes to various network destinations. Routing tables may be specified by an administrator, learned by observing network traffic or built with the assistance of [routing protocols](https://en.wikipedia.org/wiki/Routing_protocol).  Routing, in a narrower sense of the term, often refers to [IP routing](https://en.wikipedia.org/wiki/IP_routing) and is contrasted with [bridging](https://en.wikipedia.org/wiki/Bridging_(networking)). IP routing assumes that [network addresses](https://en.wikipedia.org/wiki/Network_address) are structured and that similar addresses imply proximity within the network. Structured addresses allow a single routing table entry to represent the route to a group of devices. In large networks, structured addressing (routing, in the narrow sense) outperforms unstructured addressing (bridging). Routing has become the dominant form of addressing on the Internet. Bridging is still widely used within [local area networks](https://en.wikipedia.org/wiki/Local_area_network). |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date:** | **17/7/2020** | **Name:** | **Nayanashree** | |
| **Course:** | **Salesforce** | **USN:** | **4al16ec042** | |
| **Topic:** | **Salesforce platform basics** | **Semester & Section:** | **8 A** | |
| **AFTERNOON SESSION DETAILS** | | | |
| **Report** Learning Objectives After completing this unit, you’ll be able to:   * Explain why voice matters. * Name the core components that make Alexa work. * Describe the capabilities of Alexa and Alexa-enabled devices.  The Power of Voice To help set the stage for this module—let’s start by talking about the power of voice. At Amazon, **we believe voice represents the next major disruption in computing**.Voice interfaces are the next progression in a series of ever-adapting user interfaces that we use every day. In the early days of computing, there was the venerable punch card, which was a limited character interface. The next step up was to text-only graphical user interfaces (GUI). Following the introduction of the mouse, we then had a progression of GUI that used more and more advanced layouts with modern operating systems. In the 90s, the explosion of the Internet and web pages drove web design as the new frontier. Enter the smartphone in the early 2000s with a new touch-based interface. And now, with advancements in neural nets, natural language processing, and speech recognition, we have [voice user interfaces (VUI)](https://developer.amazon.com/alexa-skills-kit/vui).  VUI have also evolved over time. The days of “Press 1 for the front desk, press 2 for housekeeping, press 3 for reservations” are slowly shifting to a more conversational flow that is more natural for users and allows them to be more succinct and accurate in their request. This evolution is referred to as **conversational user interface.** User Makes a Request When you say the **wake word** (in this case we are using **Alexa** ), the light ring around the Echo begins to glow blue to indicate Alexa is now listening and streaming that data to the cloud. The captured audio is called an **utterance** . **Note** : You can also change the wake word to a couple of other words: Echo, Computer, and Amazon. Amazon Alexa Cloud Once the utterance has been received in the cloud, a series of speech models are applied to it using automatic speech recognition (ASR) and natural language understanding (NLU) to figure out what you wanted and where to route that. In the previous example, Alexa figured out that this was an **intent** to check the weather. Intents are registered by a **skill** that can handle the intents, and the skill provides a number of sample utterances to help Alexa map out where requests go. Using Voice Interfaces Let’s examine a common interaction with Alexa. If you don’t know who Alexa is:  Alexa is the brain behind the Amazon Echo family of devices and other Alexa-enabled devices. Using Alexa is as simple as asking a question—just ask, and Alexa responds instantly. Alexa lives in the cloud and is always getting smarter.  Getting back to that conversation, it can look something like this:  **A typical user** : “Alexa, do I need an umbrella today?”  **Alexa** : “It might rain in Seattle today. There’s a 55% chance. You can expect about 0.14 inches.”  A simple question, but many different things needed to happen to get that response. And yes, it does rain frequently in Seattle. Your Service/Skill Handling Skills are built utilizing the Alexa Skills Kit, a collection of self-service APIs, tools, documentation, and code samples that makes it fast and easy for anyone to build for voice. In this case, let’s assume there is an AWS Lambda function that calls a service to check on the weather forecast when an incoming intent from Alexa is received.  Skills can be built using many different options such as AWS Lambda, Heroku, and custom web services communicated over HTTPS. As long as the skill is built to handle the incoming Alexa request in a secure manner, it doesn’t matter where it is hosted or what language it is written in. | | | |