Module Code	B9IS103
Module Name	Computer Systems Security
Date	29-April-2020
Student number	10387794
Student name	SRIKANTH SHILESH PASAM

By uploading this exam from my Moodle account SRIKANTH SHILESH PASAM *am confirming that this document is all my own work.*
I understand that DBS will carry out checks such as text-matching (via Urkund), bench-marking and viva voce exams in order to verify the authenticity of submissions.

Please input your answers below. You may answer the questions in any order but you must ensure they are clearly labelled.

Question 1

a. In relation to Encryption, explain the following terms: a. Plain Text b. Cipher Text

Plain text – This refers to the data which can be read or accessed directly. There is no encryption on this kind of data and hence is the least secured.
Cipher text – This refers to the data that is encrypted. The data can only be read or accessed after decrypting it. Hence this is very secure.

b. In relation to Firewalls, briefly explain what is meant by SPI.

A firewall is one of the critical lines of defence against attackers over the internet. SPI is a special kind of firewall. It stands for Stateful Packet Inspection or dynamic packet filtering. In this method the technology monitors the incoming packet data and checks if these corresponds to the connections active. Based on certain parameters it will decide whether to grant or deny access to them.
SPI determines the validity of each connection by observing the packets and determining certain set of rules for each of them. It does not inspect each packet like deep packet inspection so it is much faster.

c. In relation to Information Security, distinguish between a Virus and a Worm.

Virus – A virus is a computer program which can replicate and attach itself to another program or file. It can transmit from one device to another through email, memory cards or even through the network. When an unsuspecting user executes the file, it starts to spread in the system. Virus can cause a program to misbehave, delete files or corrupt them. Generally, virus needs a medium to be transferred from one device to another.
Worm – A worm is a kind of virus. It can duplicate and transfer itself from one device to another. Unlike a virus, a worm is a program on its own and doesn't need any kind of human intervention but can spread automatically through the network. A worm usually targets the

resources of a device like its memory, bandwidth or the processor. This tends to the device crashing.

d. Explain AAA and how it is used in a network environment.

AAA stands for Authentication, Authorization and Accounting. It is a security policy term used to reference the protocols and policies involved when it comes to usage of IT resources.
Authentication – It is a way of identifying an user. This is done through the use of login/email ID's and passwords. When the user provides his/her credentials, this is cross referenced with the existing ones on a database.
Authorization – This refers to whether an user has the authority to perform certain tasks. Authorization takes effect only after an user it authenticated first. Authorization enforces rules that applies to different kinds of users in the organization.
Accounting – This is a measure of the amount of resources an user is eligible to access. This could be network speed or bandwidth, storage or computing resources and such. It tracks this by monitoring the users session.

e. Briefly explain the term Confusion in relation to Encryption. Give an example of a Cipher type that adds confusion.

Confusion is a cryptographic term used to indicate the process of making the relationship between a cipher and its key as complicated as possible. This is done by assigning each digit of a plaintext to multiple digits of the cipher text. This means, even when a single digit in plaintext is changed, the entire cipher text changes. This helps ensure that no correlation between the cipher and the plain text is formed directly and thus enables high degree of encryption. Confusion techniques use substitution algorithm.
AES (Advanced Encryption Standard) is a technique which uses confusion.

f. Explain what an ACL is in relation to network security.

ACL stands for Access Control list. It is a network security layer that acts like a firewall. This controls the flow of traffic at the routers interface. It is similar to stateless firewall which restricts the flow only from certain addresses while allowing the rest. ACL's are best suited in routers that connect to the internet directly such as between the public internet and the DMZ. There are four types of ACL:

- Standard
- Dynamic
- Extended
- Reflexive

g. In relation to Cyber-Security, define the following terms: i. Vulnerability ii. Malware

Vulnerability – A vulnerability is a computer security weakness. An attacker can capitalize on this weakness and compromise the CIA (Confidentiality-Integrity-Availability) of the organization. Vulnerability management needs to be implemented in order to classify, remediate and mitigate any existing vulnerabilities.

Malware – Malware is malicious software that enters a device without the users consent and causes some kind of damage. There are different kinds of malware. The most commonly known ones are:

- Virus
- Worms
- Trojans
- Spyware
- Keyloggers

h. Explain what RADIUS is and how it is used in a network environment.

RADIUS stands for Remote Authentication Dial-in User Service. It is a client-server user protocol that runs in the application layer. RADIUS helps achieve AAA. It is used with 802.1X authentication.

RADIUS runs in the background as a service in Windows or UNIX systems. A RADIUS server checks the users authentication and once validated it returns one of the three responses:

- Access Reject – when access is denied for the client
- Access Challenge – when additional information or authentication is required by the client
- Access Accept – when the client is granted access

Post authentication and authorization RAIDUS moves to accounting protocols.

i. In relation to Encryption, explain what is meant by Symmetric Encryption and Asymmetric Encryption.

Symmetric encryption – In this type of encryption there is only one secret key to the cipher text. The secret key is usually a bunch of random letters or numbers. In order to decipher the text, both the sender and receiver must know the secret key. AES, DES are examples of symmetric encryption.

Asymmetric encryption – This is a newer mode of encryption technique. It is also called as a public key encryption. This method uses two different keys to encrypt data. It involves a public and a private key. Data encrypted by the public key can be decrypted by the private key and vice versa. RSA, DSA are examples of asymmetric encryption.

j. In relation to configuring network equipment, briefly explain why i. You should never use the default username and password. ii. You should use SSH over TELNET for device management

i. The default passwords of networking devices are common information. This is known by everyone. If an attacker is in range of the signal of the said networking device then they can easily access the network and hijack it. Traffic flow in the network can also be monitored. All this is very risky and so when configuring the networking device, its default user name and password must be changed.

ii. SSH is Secured Shell. It is a protocol which allows communication between remote devices securely. The communication between the devices is encrypted. This is done with the help of a public and private key. TELENET on the other hand works without any encryption. This means communication over this medium is susceptible to unauthorized access.

Question 3

a. It is generally agreed that network security commences with the design and topology of the network. Briefly discuss the previous statement by indicating security decisions commonly made during the network design process.

When planning the security protocols of a network, we start off with the network design and topology.

b. Explain what is meant by the term Defence in Depth. Illustrate your answer with a number of examples.

Defence in Depth refers to a cybersecurity feature where there are multiple layers of security to prevent an attacker from accessing information. This architecture protects the physical, technical and administrative controls. Defence in Depth has multiple elements in it which include antivirus, network security, data and behavioural analysis. On a broad spectrum they include protocols like:

- Access controls
- Antivirus
- Encryption
- Firewalls
- Network logging
- Auditing

c. In relation to network security, describe the following terms: a. IEEE 802.1X b. SSH c. IPSec d. DHCP Snooping

IEEE 802.1X – This is an IEEE standard for Port Based Network Access. This provides authentication for accessing the network securely. The users authentication is checked with

the help of username and password. This is confirmed by the RADIUS server. This protocol is commonly known as WiFi.

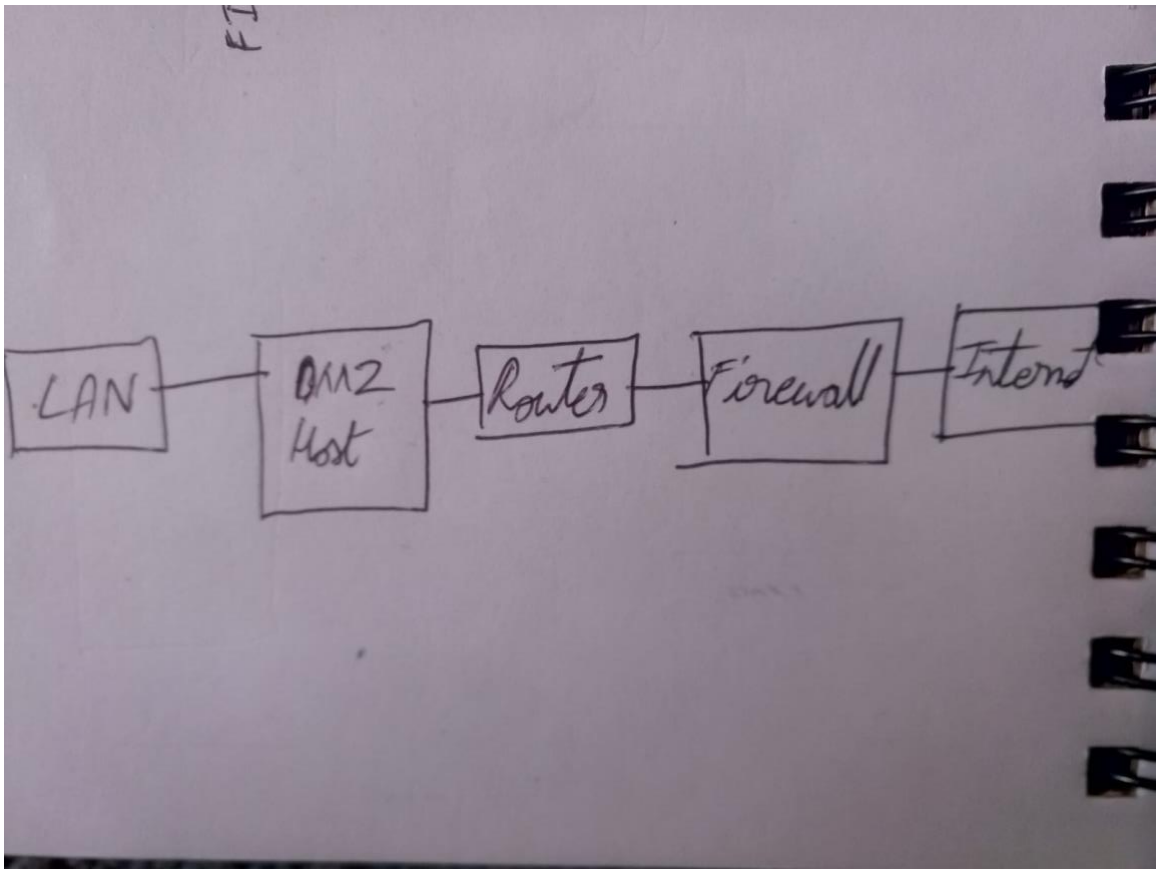
SSH – It stands for Secure Shell. It is a remote communication protocol between devices. It uses encryption for communication between devices. The encryption is done with the help of a public and private key. Linux users can use the SSH command while windows users can use clients like Putty for serving this purpose.

IPSec – This is the IETF (Internet Engineering Task Force) protocol for communication between two devices over the internet protocol. This provides features like authentication and integrity. IPSec encrypts the application layer data. It also protects the network data by IPSec tunnelling feature.

DHCP Snooping – Dynamic Host Configuration Protocol is used to dynamically assign IP addresses to all the devices connected on the network. DHCP snooping is a protocol that acts like a firewall between untrusted hosts and trusted DHCP servers. This protocol validates the DHCP messages and rejects any invalid ones. Through this, only allowed devices can access the network. This provides protection against ARP spoofing attacks.

d. Explain the role of a DMZ in a network environment. In your answer, refer to common DMZ topologies and how external and internal traffic accesses the DMZ. Use diagrams where appropriate.

DMZ stands for Data Management Zones. This is a kind of secure server which acts as a median between a secure network and the internet. Since this server has access to unsecure network, there are multiple security features implemented here like restricting unnecessary services and user accounts, limiting running services to only the required levels. In this way even if the DMZ is compromised, the LAN stays safe.



Question 4

a. Briefly outline the role of a VPN in a business environment. Your answer should include reference to the basic operation of VPN.

VPN stands for Virtual Private Networks. This protocol provides security and privacy when connecting to the internet. This is done by creating a secure path for communication between the two devices. VPN's usually use end to end encryption. This means users can access their office network remotely form anywhere without having to worry about the safety of the connection they are on. A business can also use VPN for access control. This means, the business can provide VPN access to clients based on their levels and revoke it when not required.

b. In relation to VPN, discuss: i. Key Exchange between VPN peers ii. Perfect Forward Secrecy

i. When two devices are connected through a VPN, they can encrypt or decrypt data based on their unique keys. This is done in two phases. It uses IKE (Internet Key Exchange) crypto profile and IPSec crypto profile. A SA (Security Association) is generated through this process. This SA acts as the key for the devices.

ii. This is a part of specific key agreement protocol. This is done by generating a unique session key for every session the user is active on. In this way even if one key is compromised, the other sessions are still safe.

c. Briefly discuss the following protocols in relation to VPN: i. PPTP ii. L2TP over IPSec

i. It stands for Point-to-Point Tunnelling Protocol. This is a networking protocol used in VPN's. This is done by connecting one point of a client to another point of the server. This connection between the devices is encrypted and encapsulated with another protocol and hence the word tunnelling. The other protocol is usually TCP/IP.

ii. It stands for Layer 2 Tunnelling Protocol. This protocol allows communication between a remote client using a public IP to a corporate network over a VPN. This is based on a client-server model. This particular protocol allows communication between the two devices over any internet. It does not require any kind of dedicated connection medium between the two.

d. Compare and contrast, a Site-to-Site VPN with a Remote-Access VPN. In your answer, distinguish between their different uses, the technology used in each type of VPN and the advantages and disadvantages of each type of VPN.

Site-to-Site VPN uses a public network to expand an offices network over the internet across multiple geographic locations. This is usually intranet or extranet based. Intranet based combines the network of multiple offices into one single WAN. Extranet based is used to connect an office network with that of any external network. Through site-to-site VPN, the VPN gateway of one network communicates with the gateway of the remote VPN. Site-to-site is achieved through two methods:

- Internet based VPN – This is a combination of the companies network with the external network. A VPN gateway manages this communication. This VPN typically uses IPSec thus enhancing the security.
- MPLS based VPN – In this method, the connection is created in the cloud. This means, the VPN provider provides the necessary infrastructure for enabling the VPN connection to establish. This type of VPN is more expensive than Internet based VPN.

Remote-Access VPN is the commonly used VPN by the general public. This provides a medium for a client to connect to a remote server over a secure encrypted channel. The remote device is responsible for encrypting and decrypting the data. This protocol usually requires a NAS (Network Access Server) or a VPN gateway. This means, the remote device needs to be installed with the corresponding software. The data is sent to the remote access VPN. From this it is forwarded to the VPN gateway that decrypts the data. This is then sent to the client.