Nompumelelo Mtshatsheni – BXMDLL7W9

ITSC311- Take Home Assessment

June 12, 2020

Section A

Question 1 – Scenario Questions: Kerberos

1.1

- The system protection and reliability within a network can be unmanageable (RedHat, 2020). It can dominate the time of numerous managers just to maintain trace of what services are being operated on a network and the approach in which these services are employed (RedHat, 2020)
- Additional, validating clients to network services can confirm to be unsafe when the procedure utilized by the protocol is essentially unprotected (RedHat, 2020), as demonstrated by the relocation of unencrypted passwords over a network employing a file transfer protocol and Telnet protocol
- It is a way to remove the need for protocols that permit treacherous procedures of validation (RedHat, 2020), thus improving the whole network security
- It is a network verification protocol
- It uses a symmetric-key cryptography (Whitman & Mattaord, 2016) to validate clients to network services, which implies passwords are certainly not in fact transmitted across the network
- Therefore, when clients validate to network services using Kerberos (RedHat, 2020), unapproved clients try to collect passwords by observing network traffic are essentially thwarted

1.2

- According to (Whitman & Mattaord, 2016), the authentication server (AS), is a Kerberos server that validates users as well as servers
- The key distribution center (Whitman & Mattaord, 2016), which creates along with concerns gathering secrets. To validate clients to a set of network customer services. Once a user confirms to the key distribution center (Whitman & Mattaord, 2016), the KDC transmits a tag unique to that session in return to the user's system, and any Kerberos-aware services (Whitman & Mattaord, 2016) look for the tag on the customer's system instead than calling for the client to verify using a password.
- The ticket granting service (TGS), which offers permits to users who ask for essential services (Whitman & Mattaord, 2016). In Kerberos, a permit is an id card for a specific user that authenticates to the server that the user is demanding services and that the user is a genuine representative of the Kerberos system and then approved to obtain services (Whitman & Mattaord, 2016). An identifier contains for the user's first name as well as system address, a permit authentication commencing along with closing time, along with the session key (Whitman & Mattaord, 2016) everything encoded within the confidential key of the server from which the user remains demanding essential services

1.3

- The key distribution center identifies (Whitman & Mattaord, 2016)the confidential keys of each users combined with servers across the system
- The key distribution center will firstly trade data with the user and server by the use these confidential keys (Whitman & Mattaord, 2016)
- Kerberos validates a user to a demanded essential services on a server through the ticket granting service (Whitman & Mattaord, 2016) in addition through distributing provisional session keys for telecommunications between the user and key distribution center, the server and key distribution center, as well as the user as well as server
- The communications will occur among (Whitman & Mattaord, 2016) the user as well as server utilizing short-term session keys

1.4

- It is very protected blocking numerous types of intervention attacks
- The supplier of data is supplied through trade of a confidential session key among a user and service. Once the key is used to encrypt data between the two parties, then either party knows that only a party in control of the session key could have supplied the data
- It happens to use permits that can be strongly produced by a user or a service (Olsen, G. 2012, 2020) on the user's behalf to a server to gain access for the local services
- It will license interoperability with other Kerberos territories such as Unix (Olsen, G. 2012, 2020) by allowing non-Windows users to validate to windows domains and obtain entry to resource
- It offers verification across the internet for web application

Question 2 - Scenario Questions

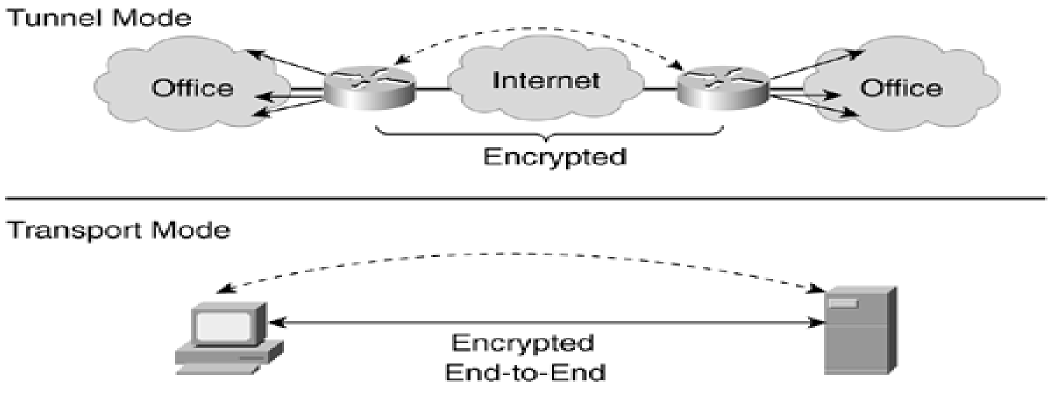
2.1

- A virtual private network stays accurate explanation for defending the network boundary at the same time as offering protected gain entry to a range of appliances alternating from the department processing tools (Whitman & Mattaord, 2016)
- The simplest explanation in all instances in which cost-effective, solitary, protected, personal network requires to be generated or retrieved across the internet
- It permits you to control current (OPENVPN, 2020) consolidated network protection structure to present an integrated protection next to dangers all over the corporation's networked appliances irrespective of the site
- It offers reliable entry to essential core essential services for the workers ever rising their production
- It decreases protection threat by permitting entry to network sources to just clients whom were permitted, translating information (OPENVPN, 2020), and thus safeguarding against unreliable Wi-Fi entry, and offering stability for consolidated cohesive danger managing

2.2

- According to (Whitman & Mattaord, 2016) the encapsulation for the usage of inbound plus outgoing information, in which the inherent protocol of the user is implanted inside the structure of a protocol that will be transmitted across the public network as well as can be compatible through the server network location
- The encryption for the inbound combined with outgoing information to maintain the information insides confidential whilst in transfer throughout the public network (Whitman & Mattaord, 2016), although functional with the user as well as the server workstations in addition to the area networks sitting on both ends to have a virtual private network relationship
- Authentication of the distant pc and possibly the remote users as well (Whitman & Mattaord, 2016). It is ensuing user approval to operate certain activities are founded upon correct as well as trustworthy recognition of the remote system as well as users

2.3



Tunnel mode and Transport mode VPN (eTutorials, 2020)

- Transport mode

    - Information within an internet protocol packet is programmed (Whitman & Mattaord, 2016), but the banner information is non
    - Allowing the client to create a protected connection precisely from a remote cloud encoding barely the information insides within a package
    - The drawback of this completion is that package observers know how to even locate the target method
    - It uses an end-to-end shipping of encoded information. The two end operators can connect promptly, encoding and decrypting their networks as required, according to (Whitman & Mattaord, 2016) all the machine perform as the end-node virtual private network
    - Secondly, a small entry employee links to the department network across the internet by linking to a virtual private network server on the boundary (Whitman & Mattaord, 2016)
    - Hence the virtual private network will act as an in-between point, translating traffic flow from the protected intranet and communicating (Whitman & Mattaord, 2016)

- Tunnel mode

    - It introduces double border tunnel servers to interpret all traffic flow that will power pass by across an insecure network (Whitman & Mattaord, 2016)
    - In this mode, the absolute user/client packet is encrypted and combined as the information segment of a packet referred from one tunneling server to an another
    - The obtaining server decrypts the packet and transmits it to the definitive address, this model is that an interrupted packet uncovers unknown regarding the true target system
    - It is supplied by ISA Server(Whitman & Mattaord, 2016)
    - Its execution, by having one the user end, a windows operator can create a virtual private network by constructing on their system to link up to a virtual private network server (Whitman & Mattaord, 2016)
    - The process is straightforward. It firstly, allows the user link up to the internet via a direct network connection. And lastly, the client verifies the connection with the remote access virtual private network server (OPENVPN, 2020)

Section B

Question 4 – Scenario Questions: Encryption

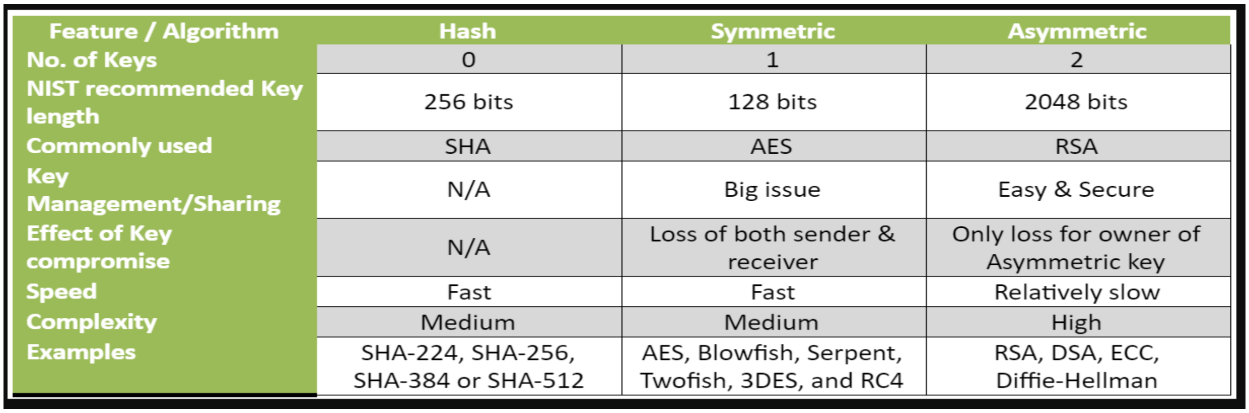
4.1

The main intention is to defend the confidentiality of digital information put in storage on the pc systems or transported across the internet or any other pc network. According to (SearchSecurity, 2020) the acceptance of encryption is frequently motivated by the need to join the agreement for guidelines. Several companies and standards bodies both propose or compel sensitive information to be encrypted to avoid unauthorized third parties or danger actors from the gain access to the information

4.2

Types	Explanation
Symmetric encryption	▪ It is referred to as shared key ▪ A key is employed for in cooperation to encrypt and decrypt traffic ▪ Commonly used procedures (Stretch, 2010, 2020) consist of DES, 3DES, AES, and AES ▪ Its procedures can be tremendously be fast, and quite minimal density make available for easy execution in the computer hardware ▪ The plaintext is coded utilizing a key, and the similar key is utilized at the collecting end to decrypt the obtained ciphertext (Stretch, 2010, 2020) ▪ Though, they need that all hosts partaking in the encryption have already been aligned with the confidential key via some external method
Asymmetric encryption	▪ It differs from symmetric encryption mainly in that two keys are managed: one for encryption and one for decryption. ▪ It is available to every user, although confidential key will not be revealed ▪ It used for day-to-day communication across the internet ▪ The use of digital certificates within the client/server prototypical know how to be employed to release confidential key ▪ The most popular algorithm is RSA, PKSC and DSA (CYWARE SOCIAL, 2020) ▪ It enforces a high pc weight and tend to be very much dimmer ▪ Therefore, it is not normally utilized to safeguard load information ▪ As an alternative, its main strength is its capacity to create a reliable (Stretch, 2010, 2020) channel over a nonsecure medium

	▪ The corresponding confidential key, which is certainly not distributed, it is usually utilized to decrypt information
Hashing	▪ They are known as the structure for modern-day cryptography ▪ It is employed to transfer huge unplanned size information to smaller permanent extent information ▪ It generates and authentication of digital signatures ▪ It compresses a memo into an irretrievable static-length worth ▪ It is employed only to confirm information; the initial memo cannot be recovered after a hash (Stretch, 2010, 2020) ▪ It is normally used to verify protected commutation ▪ It a typically end result of the initial message long with a confidential key ▪ Its algorithms (Stretch, 2010, 2020) are commonly castoff without a top-secret key for double examining errors ▪ It is commonly using md5sum and sha1sum services over a Linux for experimenting



Feature / Algorithm	Hash	Symmetric	Asymmetric
No. of Keys	0	1	2
NIST recommended Key length	256 bits	128 bits	2048 bits
Commonly used	SHA	AES	RSA
Key Management/Sharing	N/A	Big issue	Easy & Secure
Effect of Key compromise	N/A	Loss of both sender & receiver	Only loss for owner of Asymmetric key
Speed	Fast	Fast	Relatively slow
Complexity	Medium	Medium	High
Examples	SHA-224, SHA-256, SHA-384 or SHA-512	AES, Blowfish, Serpent, Twofish, 3DES, and RC4	RSA, DSA, ECC, Diffie-Hellman

Some characteristics of algorithms (Mehmood, A., 2017)

4.3

- Public key infrastructure is an integrated system of software (Whitman & Mattaord, 2016), it allows clients to communicate strongly across the utilization of digital certificate
- The digital signatures the encrypted message mechanisms that can be mathematically proven as dependable (Whitman & Mattaord, 2016)
- The digital certificates the public-key trunk documents that allow PKI system mechanisms and end-users to authenticate a community key and discover its possessor
- The hybrid cryptography systems enable the swapping of confidential keys (Whitman & Mattaord, 2016) by making use of public-key encryption
- The steganography is known as the information concealing technique that includes inserting data within other documents, such as digital photographs (Whitman & Mattaord, 2016)

Question 5 – Scenario Questions: SecSDLC

5.1

Phase	SecSDLC Steps
Investigation	▪ It occurs with a mandate from upper management, influencing the procedure, results, and objectives of the development (Whitman & Mattaord, 2016), as well as its financial plan and other restrictions. ▪ Often, this phase starts with the company's information security policy, which will define the execution of the security program within the organization. ▪ The team of responsible are usually organized ▪ All the difficulties are analyzed ▪ The scope, goals and objectives of the new project are defined and as well extra constraints for the program procedures ▪ Lastly, structural probability analysis is accomplished to define whether the company has the reserves and dedication obliged to execute (Whitman & Mattaord, 2016) an effective defense assessment and layout.
Analysis	▪ In this phase, the official papers from the inspection phase are examined ▪ The established group will organize an initial analysis of current protection strategies or even procedures, along with that of recorded existing threats and correlated regulations ▪ The risk management task too commences in this phase. o Risk management is the procedure of recognizing, evaluating, and estimating the heights of risk challenging the company (Whitman & Mattaord, 2016), particularly the warnings to the company's security and to the data gathered and processed by the company
Logical	▪ During this phase, it will explore and executes key procedures ▪ The group prepares the incident response proceedings ▪ It will plan for a company response to disaster ▪ Establishes the feasibility of ongoing and outsourcing the project (Whitman & Mattaord, 2016)

Physical	▪ Substitute solutions are formed in this phase ▪ The proposals for basic protection procedures to boost the recommended technical results are generated. ▪ Towards the end of this phase (Whitman & Mattaord, 2016), a probability study must establish the willingness of the company intended for the planned development. ▪ Although, all groups participating would have an opportunity to approve the design before execution of the project begins
Implementation	▪ It is like the old SDLC ▪ The security mixtures are obtained (could be created or purchased), verified, executed, and tested again to double checked for any faults ▪ The personnel concerns are assessed (Whitman & Mattaord, 2016), and specialized preparation and education programs will be performed ▪ Ultimately, the complete verified package is introduced for the top-level executive for the final approval of the project
Maintenance & change	▪ It is the extended and most costly phase ▪ It contains of the responsibilities essential towards sustain and alter the system for the rest of valuable life cycle ▪ Regularly, the system is checked for fulfillment, with company demands. ▪ All the upgrades, updates, and repairs are controlled ▪ Once the existing system be able to no longer provide for the company, the development is concluded (Whitman & Mattaord, 2016), and a brand-new development/project will be implemented.

5.2

Information Security Project Team	Role
Senior management	(CIO) is the accountable for (Whitman & Mattaord, 2016): the evaluation, managing and execution of data security within the organization
Champion	Endorses the development by ensuring its support, together business-wise & managerially
Team Leader	Knows project and personnel management and therefore, understands the information security technological constraints
Security policy designers	The individuals who comprehend the managerial ethnicity, along with current procedures
Risk assessment specialists	The individuals who comprehend the commercial risk evaluation procedures and the amount of the organization resources as well as the protection techniques that will be utilized
Security experts	They usually qualified and well-educated experts within features of data protection from equally a technological and non-technical standpoint
System managers	Controlling the systems that store the data operated by the corporation
End-users	▪ Accountable for the security and the use of a certain established of data (Whitman & Mattaord, 2016). They work with subordinate supervisors or managers to supervise the day-to-day management of information ▪ Accountable for the storing, upkeep, and safety of the data and overseeing information storage and backups ▪ Work with the data to perform their day-to-day tasks helping the objective of the company ▪ Each person is accountable for the organization and responsible for the security of information (Whitman & Mattaord, 2016)

(Whitman & Mattaord, 2016)

Bibliography

CYWARE SOCIAL. (2020, June 10). *Computer, Internet Security - Exploring the Differences Between Symmetric and Asymmetric Encryption*. Retrieved from https://cyware.com/news/exploring-the-differences-between-symmetric-and-asymmetric-encryption-8de86e8a

eTutorials. (2020, June 10). *eTutorials - IPsec Overwiew*. Retrieved from eTutorials: http://etutorials.org/Networking/MPLS+VPN+security/Part+III+Practical+Guidelines+to+MPLS+VPN+Security/Chapter+6.+How+IPsec+Complements+MPLS/IPsec+Overview/

Mehmood, A. (2017, October 27). *CRYPTOMATHIC - Differences between Hash functions, Symmetric & Asymmetric Algorithms*. Retrieved from https://www.cryptomathic.com/news-events/blog/differences-between-hash-functions-symmetric-asymmetric-algorithms

Olsen, G. 2012. (2020, June 10). *Resmond - Kerberos Authentication 101: Understanding the Essentials of the Kerberos Security Protocol*. Retrieved from https://redmondmag.com/articles/2012/02/01/understanding-the-essentials-of-the-kerberos-protocol.aspx

OPENVPN. (2020, June 10). *OPENVPN - Securing Remote Access Using VPN*. Retrieved from https://openvpn.net/whitepaper/

RedHat. (2020, June 10). *Red Hat Documentation - Kerboros*. Retrieved from https://web.mit.edu/rhel-doc/5/RHEL-5-manual/Deployment_Guide-en-US/ch-kerberos.html

SearchSecurity. (2020, June 10). *Data Security Guide: Everything You Need To Know - Encryption*. Retrieved from https://searchsecurity.techtarget.com/definition/encryption#:~:text=The%20primary%20purpose%20of%20encryption,or%20any%20other%20computer%20network.

Stretch, 2010. (2020, June 10). *PacketLife.net - Symmetric Encryption, Asymmetric Encryption, and Hashing*. Retrieved from PacketLife.net: https://packetlife.net/blog/2010/nov/23/symmetric-asymmetric-encryption-hashing/#:~:text=Asymmetric%20encryption%20differs%20from%20symmetric,tends%20to%20be%20much%20slower.

Whitman, M., & Mattaord, H. (2016). *Principles of Information Security. Fifth Edition* . Boston: Cengage Learning.