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 clients and servers.
- The key distribution center (KDC) (Whitman & Mattaord, 2016), which creates and concerns gathering keys. 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 particular to that session back to the client's machine, and any Kerberos-aware services (Whitman & Mattaord, 2016) look for the tag on the client's machine 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). The identifier contains of the user's name and network address, a permit authentication commencing and ending time, and the session key (Whitman & Mattaord, 2016)all encoded in the private key of the server from which the user is demanding essential services

1.3

- The key distribution center identifies (Whitman & Mattaord, 2016)the confidential keys of all users and servers across the network
- 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) and by distributing provisional session keys for telecommunications between the user and key distribution center, the server and key distribution center, as well as the user and server
- The communications will occur among (Whitman & Mattaord, 2016) the user and server using these 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

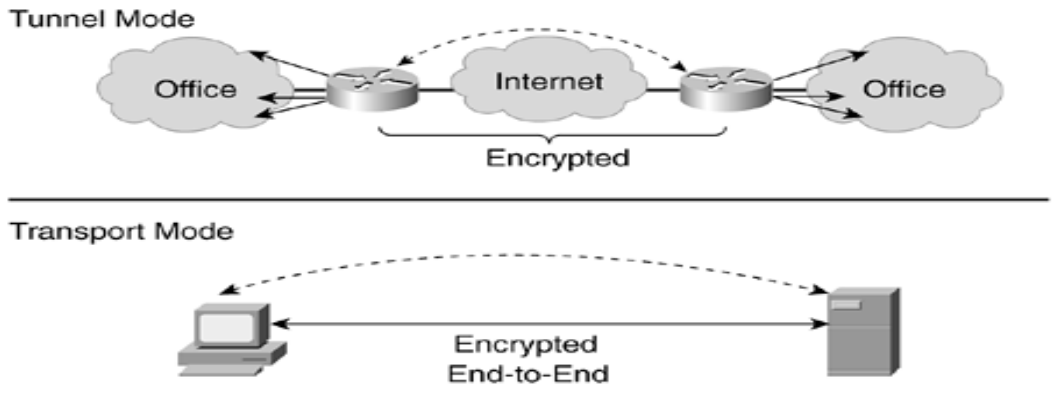
2.1

- A virtual private network is the accurate solution for defending the network boundary while offering protected gain access to a range of devices alternating from the office processing devices (Whitman & Mattaord, 2016)
- The simplest solution in all cases wherein an economical, isolated, secure, private network needs to be created or accessed over the internet
- It allows you to leverage current (OPENVPN, 2020) consolidated network security structure to offer a unified defense against threats throughout the corporation's networked appliances irrespective of the location
- It provides secure entry to needed core services for the workforce ever-increasing their productivity
- It decreases security risk by permitting access to network resources to only users who are permitted, encrypting information (OPENVPN, 2020), and thus safeguarding against unreliable Wi-Fi access, and offering continuity of consolidated unified threat management.

2.2

- According to (Whitman & Mattaord, 2016) the encapsulation for the usage of incoming and outgoing information, in which the inherent protocol of the client is implanted within the structure of a protocol that will be routed across the public network and can be compatible by the server network location
- The encryption for the incoming and outgoing information to keep the information contents private while in transfer throughout the public network (Whitman & Mattaord, 2016), but functional by the user and server workstations and the area networks on both ends to have the virtual private network connection
- Authentication of the remote computer and possibly the remote users as well (Whitman & Mattaord, 2016). It is ensuing user approval to operate certain actions are predicated on correct and trustworthy recognition of the remote system and users

2.3



Tunnel mode and Transport mode VPN (eTutorials, 2020)

Transport mode	Tunnel mode
In transport mode, the information within an IP packet is encoded (Whitman & Mattaord, 2016), but the banner information is not	It launches two border tunnel servers to interpret all traffic that will pass by through an insecure network (Whitman & Mattaord, 2016)
Allowing the user to establish a secure link directly with the remote host, encoding only the information contents of the packet	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 downside of this completion is that packet observers can still find the target system	The obtaining server decrypts the packet and transmits it to the definitive address, this model is that an interrupted packet uncovers nothing about the true target system
Transport mode virtual private network the end-to-end transport of encoded information. Two end users 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 server and client.	Tunnel mode virtual private network is supplied by ISA Server, when using the ISA Server, an association can create a gateway-to-gateway tunnel, compressing information within the tunnel (Whitman & Mattaord, 2016) ISA can use the point-to-point tunneling protocol
In the second, a remote access worker connects to an office network over the internet by connecting to a virtual private network server on the boundary (Whitman & Mattaord, 2016), allowing the freelancer's system to work as if it were part of the local area network.	Its execution, by having one the client end, a windows user can establish a virtual private network by constructing on their system to connect to a virtual private network server (Whitman & Mattaord, 2016)
Hence the virtual private network will act as an in-between node, encrypting traffic from the protected intranet and communicating (Whitman & Mattaord, 2016) it to the remote client, as well as decrypting traffic.	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 purpose of encryption is to defend the confidentiality of digital information put in storage on the computer systems or transferred 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 both to encrypt and decrypt traffic ▪ Commonly used algorithms (Stretch, 2010, 2020) include DES, 3DES, AES, and AES ▪ Its algorithms can be tremendously be fast, and quite low complexity make available for easy execution in the 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	▪ Well known as public-key cryptography ▪ 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 computational weight and tend to be very much dimmer ▪ Therefore, it is not normally utilized to safeguard payload information ▪ As an alternative, its main strength is its capacity to create a reliable (Stretch, 2010, 2020) channel over a nonsecure medium ▪ This is achieved by the trade of public keys, which can only be utilized to encrypt information

	▪ The corresponding private key, which is certainly not shared, it is usually utilized to decrypt information
Hashing	▪ They are known as the building blocks for modern cryptography ▪ It is employed to transfer large random size information to smaller fixed size information ▪ It generates and authentication of digital signatures ▪ It compresses a message into an irretrievable fixed-length value ▪ It is used only to verify information; the initial message cannot be recovered from a hash (Stretch, 2010, 2020) ▪ It is normally used to verify protected commutation ▪ It a typically result of the original message long with a secret key\ ▪ Its algorithms (Stretch, 2010, 2020) are commonly castoff without a secret key for double checking 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 directive from upper management, influencing the procedure, results, and objectives of the project (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, organizational feasibility analysis is accomplished to define whether the company has the resources and dedication required to perform (Whitman & Mattaord, 2016) an effective security analysis and design.
Analysis	▪ In this phase, the official papers from the investigation phase are examined ▪ The established team will organize a preliminary analysis of current security strategies or even programs, 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 designs for physical security procedures to boost the recommended technical solutions are generated. ▪ Towards the end of this phase (Whitman & Mattaord, 2016), a feasibility study must establish the willingness of the company for the planned project. ▪ 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 necessary to sustain and alter the system for the rest of its 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 can no longer support the company, the project 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 assessment, managing and execution of information security within the organization
Champion	Endorses the project and ensures its support, both business-wise & administratively
Team Leader	Knows project and personnel management and therefore, understands the information security technological constraints
Security policy developers	People who comprehend the organizational ethnicity, along with current procedures
Risk assessment specialists	People who comprehend the financial risk assessment procedures and the value of the organization assets as well as the security techniques to be utilized
Security Professionals	They usually trained and well-educated specialists in all features of information security from equally a technical and non-technical standpoint
System Administrators	Controlling the systems that store the information used by the company
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.