Assignment 3

Deadline: Day 01/05/2017 @ 23:59

**[Total Mark for this Assignment is 50 (10 pts as bonus)]**

***Network Management***

***IT340***

Student Details:

|  |  |  |
| --- | --- | --- |
|  |  |  |
| **Name:** Munirah Alrushud  **CRN:** 21335 |  | **ID:** 140032004 |
|  |  |  |

**Instructions:**

* This Assignment must be submitted on Blackboard via the allocated folder.
* Email submission will not be accepted.
* You are advised to make your work clear and well-presented, marks may be reduced for poor presentation.
* You MUST show all your work.
* Late submission will result in ZERO marks being awarded.
* Identical copy from students or other resources will result in ZERO marks for all involved students.
* Convert this Assignment to PDF just before submission.

# Question One

***10 Marks***

*Learning Outcome(s):*

*Instructors: State the Learning Outcome(s) that match this question*

**Discuss about the SNMP Tools and describe the Command Tool in detail.**

**SNMP MIB Browser** with graphical interface, it’s easy to access from public software library. Some of it can also acquire private MIB objects. So first specify the IP address and then request information on specific MIB object.

**snmpsniff:** implemented in Linux/Free BSD tool. It stores the SNMP packets that across the segment for later analysis.

**SNMP command-line tools** those command tools are available in many operating systems UNIX, Linux, FreeBSD and Windows. SNMP command tools generate the SNMP messages:

**SNMPTest** helps to get values of several managed objects at one time.

**SNMPGet** it communicates with the network object by using get request messages.

**SNMPGetNext** like the snmpget command, the managed object responds to the expected get-response message on the object ID

**SNMPSet** sends the set-request message and receives the get-response command.

**SNMPTrap** generates a trap message, some implementation handles SNMPv1 traps and some of the implementations handle SNMP v1, v2, and v3.

**SNMPWalk** uses snmpgetnext to trace the MIB

**SNMPNetstat** displays the network status and the configuration of information from a network entity through the SNMP.

# Question Two

***10 Marks***

*Learning Outcome(s):*

*Instructors: State the Learning Outcome(s) that match this question*

**In order to ensure quality of service, what are the measured metrics employed in trunk test system and traffic measurement system**

**Trucks must measured by accessing every trunk in each switching office,**

**It must remove the failure track before it’s already fail. So, the trunk that fail to meet the criteria set for quality is removed from service. And the user must not notice any degradation of service.**

**Traffic measurement system measures the busy status of switch appear in each switch**

# Question Three

***10 Marks***

*Learning Outcome(s):*

*Instructors: State the Learning Outcome(s) that match this question*

**Dress a comparative table which compares: symmetric cryptography, asymmetric cryptography, message digest and digital signature.**

|  |  |  |  |
| --- | --- | --- | --- |
| symmetric cryptography | asymmetric cryptography | message digest | digital signature |
| Shared secret key between sender and receiver. Sender and receiver have the same key  The same key (private key) for encrypting and decrypting.  In the term of speed the symmetric is consider as fast. | Sender have private and public key.  Receiver has public and private key.  Sender encrypts the messages by receivers’ public key and the receiver decrypts the message by its private key.  In the term of speed the asymmetric is consider as slow. | There’s no key and no encryption.  In the term of speed the message digest is consider as fast. | Sender have private key and public key.  Receiver have private key and public key.  Sender encrypts the digest by its private key and the receiver decrypts the digest by the senders’ public key.  In the term of speed the digital signature is consider as fast. |

# Question Four

***10 Marks***

*Learning Outcome(s):*

*Instructors: State the Learning Outcome(s) that match this question*

**Discuss Ml, M2 and M4, M5 interface in ATM network management.**

**5 INTERFACES BETWEEN SYSTEM AND NETWORK:**

**M1 and M2 are the interface between private NMS and user or private network.**

**M3 allows private NMS to access to its network information in public NMS.**

**M4 is the interface between public NMS and public network.**

**M5 is the interface between NMS of two services providers. So, the traffic measurement system is depending on:**

**Packet Loss and errors and utilization metric, Delay metric, availability and Bandwidth.**

# Question Five (Bonus)

***10 Marks***

*Learning Outcome(s):*

*Instructors: State the Learning Outcome(s) that match this question*

**Compare Packet Filtering Firewall and application level gateway firewall**

**Firewalls is a specialized version of router that’s allow packets to pass from network to another network if the packet is coming from authorized source.**

**Packet filters:**

Is the ability to allow and filter a packet that will pass through firewalls. It’s done at OSI layer: data link layer, network layer, and transport layer. Packet filter check only the IP address for sender and receiver and the port number, but it wont check the data in the packets that’s why it’s less secure. And because of that it’s much faster. The packet filters are cheaper.

**Application level gateway:**

It's used to deal with some of the problems identified in packet filtering. The application gateway has proxy firewall that wont let the internet which computer is request for any file or webpage, that’s why it’s more secure, but it is slower than the packet filter because it’s also check the data in the packets. The application level gateway is higher cost than the packet filter.