Free the tracepath screen show is shown below essay example

Business, Company

Question 1

Social engineering can be defined as the non-technical way in which intrusion to information systems can be broken into with the use of human interaction and tricks that are more of social than technical. Social engineering is a common means in which virus developers will try to break into a system. Social engineering will try to trick the computer user to give some information that will give a hint to the social engineer to break into the system.

The social engineer will try to play what is referred to as a con game which is a way in which they will gain the trust and confidence of the computer user. The social engineer will try to understand the routine that the computer user will be having. In this process of gaining the trust and confidence of the user, the social engineer will gain entry to the system by accessing the information from the user. The user will give the social engineer the confidential credential that will be used by the social engineer to get into the network.

Social engineering is a technique that is used by virus developers. They will use social engineering to convince the users to run a given malware program in pretence that they are running a genuine program. In this process, the attackers shall have gained the needed access to the system. This method is the development of the way the system is seen to be valuable to social engineers and social attackers.

Another tactic that is used by social engineers is through the use of the inability of people to follow some culture that has been developed to be used in information technologies. An example is that people will make use of

passwords that are meaningful to them. The social engineer will break to the system through the use of common words that are meaningful to the system users.

Question 2

One of the software firewall solutions is McAfee Firewall Enterprise. One advantage of McAfee Firewall Enterprise is that it has application control mechanism. This enables applications to have some form of security over the enterprise. With the advent of cloud computing, applications are now accessed by many users and enterprises on the cloud. The use of Firewall Enterprise is to ensure that the threats are understood within an organization. McAfee Firewall Enterprise solution is reliable as it has been adopted by many companies. Firewall Enterprise has a lot of the sources which are not trusted in the organization. McAfee is a reputable company as it is known to be used across many companies in the world. The virus protection programs have been popular with many organizations and individuals alike. This is where the company gained the popularity it has with the products it ha.

Another firewall solution is Barracuda Networks. This firewall solution is used for niche markets and is cost-effective when compared to other solutions. In terms of reputation, Barracuda Networks phion firewall solution is not as reputable as McAfee. It is considered to be a good option for companies that want one solution provider for their security instances. It is cheaper when compared to other firewall options.

The other firewall solution provider is that of Check Point Software Solutions.

Check Point Software Firewall has blade technology where the additional security will be added to the system with the use of blade technology. In terms of reputation, the software solution is found to be reputable. It also has reliable support for their products. Compared to McAfee and Barracuda Networks, it is considered to be expensive.

Question 3

Servers will need to have different configurations in terms of whether they should be installed as virtual, or they should be installed as physical to the organization. There are several issues that need to be considered. In the case provided, DNS server that is running on an old version of Windows Server should not be virtualized. It is not useful to virtualize the DNS and DHCP server because the DNS servers are one of the requirements that will be needed by the virtual server so that they function. If this is virtualized, it will make a virtual network be slow and will not work in some cases. For virtualization to be able to work efficiently, there is a need to have the DNS server which is used to manage the virtualization. If this will be virtualized, it will make a virtual network be slow. The DHCP will need to be operating from the normal physical servers because it will be required to manage the changing of the IP addresses in the organization. The network should be maintained so that it is fast.

The file, contact and email servers can be virtualized. The services and the transactions from these servers are not time-critical. The file servers will still be effective with virtualization. The speed of access to this server is not critical to the system. Leaving them in the physical servers will not affect the

criticality and the use of these servers. They will be accessed from the virtual locations. The contacts and email server will help in saving some space in the organization. It is important to understand the role that this will play in the organization.

Question 4

The difference between the two virtualization systems is the way they interface with the hardware of the server. VMware is installed and sits on top of the operating system which is used to host applications. On the other hand, ESX virtualization server is installed on the bare server hardware and does not have another operating system. In Windows virtualization terms, ESX virtualization server makes use of Hypervisor-1 while VMware makes use of Hypervisor-2. There is, therefore, better performance with the use of ESX server virtualization because of less overhead. They do not depend on any other software that has been installed on the hardware. They interface with the software directly. ESX manages the hardware resources on its own. On the other hand, VMware uses the resources of a powerful operating system that has been installed on the server and s the one that is managing the hardware resources.

There are more features that come with ESX than VMware. Some of the features include VMFS, VMotion, and DRS. VMware is a free product while ESX is a commercial product that needs to be purchased. VMware is an option that suits migration to a virtual environment slowly. In situations where one wants to learn the virtualization, VMware is the best option. It also offers the opportunity and chance to learn the virtualization.

In terms of performance, ESX server is seen to perform better than VMware. ESX has a higher throughput when another load is added. Even if there is the addition of single VMark which is able to handle 6 workloads VMware, the ESX server is still able to handle the new workload. There is also better scalability when another workload is added to the ESX server.

Question 5

A wiring schematic document is a document that is used to show how the electrical wiring has been undertaken. Any building has a wiring schematic document that is used to represent how the various electrical components have been connected in the building. A physical network diagram is a representation of how the various network elements have been laid out in an organization. Logical network diagrams are used to show how the IP addressing has been undertaken. Logical diagrams also show the protocols that have been included in the network. A policy is a document that shows the rules and procedures that should be observed in order to be allowed to use a resource in an organization. The policy document is a documentation that has the policies that are to be used in a network. A procedure is the steps that should be followed in order to manage to achieve a solution to the problem. Acceptable use policy is a policy that is to be accepted to be followed by a user in order to be allowed to make use of the internet and other network resources. A configuration is the way the components have been set up in a network or information system. This is a collection of items that are available in an entity and how they have been set up. A regulation is a rule that is set up by an authority that needs to be followed. In information

systems, security policy is a rule that is set up by administrators in order to have safe use of network resources. A security policy is a plan of how an entity intends to provide security to the assets that they have.

Question 6

After the window is open, the user will then open the save log file which will be achieved by Clicking Action and then clicking Open Save Log. This is the case for Windows 7, Windows 8, and Widows Vista. This is achieved in Windows 2000/XP/2003 by clicking Action then clicking Open Log File When the user is using Windows XP, there is a need to have some specification made on the type of log file that the user wants. The user can either want Application, System or Security log files. For zipped log files, there will be a need to extract the files first.

In Linux, log files are viewed with the use of commands in the command line. One command that will be used to view the log files in the shell is tail command. This is used to read the last lines of a given file. Example is tail –n 100 /var/log/mail. log. There is also the use of grep command which is used to search for a specific item in the log file. In order to view the whole content of the file in the shell, one has to use the cat command.

In Mac OS X, the log files will be found by opening the Console which can be opened by Applications> Utilities. In this folder, there are many log files. Some important log files include system. log, mail. log, and CrashReporter logs.

Question 7

One of the configurations is Enable/Disable which is used to enable or disable the functions of the wireless access points. There is also the SSID which is the Service Set Identifier. This configuration is used to set the network identification procedures. Another configuration is to enable the broadcast feature that is available for the wireless access point. This is allowing the SSID to broadcast its identity to the neighboring hosts. With this option, there will be a possibility to have the association of the access points with the other elements of the network.

There is also the use of channel for the configuration. This is the choice of the channel in which broadcasting will be done. With the choice of the channel, the other wireless access points in the network will depend on the configuration that is made in the device.

For configuring VLANs to wireless networks, the basic element is to add a wireless access point to the VLAN. This is achieved by configuring the SSID of the wireless access point to recognize the required VLAN ID. If the VLAN ID is recognized by the SSID of the WAP, there will be the establishment of a connection.

Question 8

The black hole problem is a problem that happens when there is the sending of large packets by the PMDU when there is a need to discover the path. This problem will occur when the packet that has been sent has Don’t Fragment (DF) flag which will not be fragmented. Some routers will not send the ICMP message to the host to send a smaller packet. This will cause the destination

router not to get the message and at the same time the host router will not get the acknowledgement about the message that has been sent.

The setting of DF flags on packets will prevent the routers from forwarding the packet to the next router on the network. This causes delay, and there will be problems that will be encountered in the packet. The problem is that there is the delay in the whole process of sending the packets.

The diagnosis can be done with the use of tracepath or mturoute tool which is used in Windows only. This will be achieved by first of all turning off the ICMP message sending for the router. One real world example is for two hosts (192. 168. 0. 0/24 and 192. 168. 1. 0/24) which have been connected via a router whose interfaces are F0/0 and F0/1 respectively. The host, 192. 168. 0. 0/24 . 2 is sending a 1400 bytes to destination 192. 168. 1. 0/24 . 2. The router does not support 1500 bytes and will not forward the packet to the destination. There is a need to ensure that there is better and efficient management of the path and the packets that are being sent.

In order to turn off the ICMP messages blocks, the following code will be applied:

Question 9

It is a not a good idea to undertake the three hot fixes and at the same time have swap the network card of the server. The network card will lose the configurations that had been intended to be applied on the server. The hot fixes will change the network configurations on the server. It is not right and in order to undertake the hot fixes while changing some hardware. The hardware should be changed after the hot fixes have failed. The hot fixes

have been designed so that they include the configurations for the hardware. The two processes will not be aligned because the drivers, and the firmware that the hot fixes have on the server will have changed. This is an issue that should be assessed and evaluated with the hot fixes. The hot fixes should be given the time to register the network card and see if that would solve the issue that is found in the server. This is an important step that should be assessed and analyzed. This will ensure that the hot fixes will have propagated with the hardware that is already there in the server. The swapping of the network card of the server will cause other problems on the network which might make the current problem bigger and hard to solve. It is important to have the problem solved with the hot fixes first then get the hardware solutions after this.

It is not a good idea to solve eth problems that are associated with the server using two different approaches at the same time. It will be hard to track the solution process, and the diagnosis will be hard to understand.