|  |  |
| --- | --- |
| **Network Security**  Diploma in CSF  Year 3 Apr 2021 Semester 5 | Week 1 |
| Tutorial |
| Fundamentals of Network Security | |

**OBJECTIVES**

* List the 7 domains of a typical IT infrastructure
* Discuss how these domains can be targets of hackers
* Discuss how network security components help to mitigate threats
* Network security case study

**Section A**

1. Draw a diagram to illustrate the 7 domains of a typical IT infrastructure which are favourite targets of hackers.

|  |
| --- |
|  |

1. Explain how the following network security components can be used to mitigate security threats:
2. Hosts and Nodes
3. Switches and Routers
4. Proxy Servers

|  |
| --- |
| 1) Hosts and Nodes  - Both nodes and hosts can be harmed by physical attacks and DoS attacks. A host can be harmed by malicious code, authentication attacks, and even be remotely controlled by hackers  - - Node protection – physical access control along with basic network filtering against flooding  - Host protection – hardended OS, removing unnecessary software, installing updates and impose secure configuration settings  2) Switches and Routers  - Switches provides network segmentation through hardware  - Switches can be monitored to detect errors and malicious traffic (by watching the construction and modification of the switch’s mapping table).  - Intelligent and multilayer switches can perform security monitoring function  - Routers support security by guiding traffic down preferred routes rather than routes that might not be as logically or physical secure  3) Proxy Servers  - Application proxy servers filters traffic, but also acts as a middleman between the internal client and the external server  - A proxy server hides the identity of the original requester from the server through a process know as network address translation (NAT)  - Proxy server also can do content filtering where it can block employee’s access to Internet resources that are not relevant or beneficial to company’s businesses. Hence malicious code, hacker tools and excessive bandwidth consumption may be prevented. |

1. Explain how Ingress filtering and Egress filtering on a firewall are able to mitigate network attacks such as spoofing.

(4 marks)

|  |
| --- |
| Ingress filtering – When an internal LAN address appears as a source address in a packet on its way into a network from outside – this is a spoofed address  Egress filtering – If a packet with a source address from the outside such as an Internet address is received by a firewall from an interface inside the private LAN – then this is a spoofed address |

**Section B (Reflection)**

1. Work in a team, research and discuss with your teammates to give examples of potential network security problems in our daily life. Also suggest your action plans on how to mitigate these network security concerns.

|  |
| --- |
|  |