Network Security Defence

Question 1

a) In your own words, explain how a firewall functions and how it can be used to implement a DMZ.

b) How does a firewall using packet filtering approach compare with a proxies approach?

c) What attacks can a firewall help mitigate?

Question 2

a) What type of VPN is most commonly used today?

b) Describe each of the three mechanisms used in the VPN identified in a) in particular noting what information security property they achieve

c) What type of attacks could a VPN mitigate?

Question 3

a) In your own words, explain how TLS works. In particular address digital certificates, the role of certificate authorities, and how secure communication is achieved.

b) What attacks does TLS help mitigate?

c) Why does TLS not help in mitigating a replay attack?

Scenario-based Question

Your friend Alex has decided to start an online business selling the digital art they produce. To do this Alex has purchased a machine which they have configured as a web server. The web server is stored in an office which he rents. In the office there is also a computer which is connected to the LAN and the internet.

Alex often works from home. At home, Alex uses a personal computer and a tablet which are connected to their local area network using a hub. Alex also has a router which allows them to

connect to the internet. Work Alex completes a PC is stored on the local hard drive and is uploaded to the webserver from the hard drive when necessary through the internet. From the office Alex can also upload any work to the webserver on the office LAN.

Q: Propose countermeasures which can be implemented to minimise the risk of attacks identified in the network vulnerabilities week which relate to this scenarios. If you need to make assumptions, document them in your answer.