Network Vulnerabilities Questions

Question 1

a) Port scanning is the process of identifying which ports are open on a network. Which port in particular might be useful for adding malware to a system? Is there anything else you may need to do this?

b) Imagine you are the network administrator for a company and you view the logs to see a large number of connection requests to a sequential range of ports from a single host. What type of scan might this indicate and why?

c) If the attacker in part b wanted to be a bit less obvious, what steps could they take?

Question 2

a) In your own words describe the different approaches to DoS attacks from the module, providing an example from each category.

b) Packet sniffing is monitoring information in packets when sent across a network. What conditions need to be satisfied for such an attack to be successful?

c) How does a man in the middle attack differ to a packet sniffing attack?

d) Explain why a Man in the Middle attack using ARP spoofing would not work on the internet

e) What type of spoofing would be required for a Man in the Middle attack to work on the internet?

f) Explain why hashing a password with a salt won't (on its own) protect against 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, i.e. a computer which is able to deliver web content such as html pages to end users. 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 from home on his 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: Analyse the potential threats to security Alex currently faces based on the material presented in the module.