**Task 2 & 3 – Guide**

**2.1** Implement network taking screenshots. Document and explain this process.

**2.2 – 2.3 Testing the NOS Functionality**

Create a table like below. Include everything you have installed or configured on Windows Server. Include tests at the client end to check services and features have been set up correctly. Screenshot’s ideally should be used as evidence.

|  |  |  |  |
| --- | --- | --- | --- |
| **Test** | **Expected Result** | **Actual Result** | **Problems** |
| Installation of Windows 2012 | Successful installation of NOS | Successful but had issues creating a new partition. | List issues and how you overcame them. |
| Domain created/set up | Successful domain creation of ABCMarketing.net domain |  |  |

Screenshot any issues and how you fixed them

**Task 3 – Guide**

**3.1 - You need to establish and justify a performance baseline and monitor the performance of the network against this baseline. (U27 4.1, 4.2)**

Essentially testing your networks performance. Test initial boot up times, login time, network transfer speeds(Lan speed test), internet access download and upload speeds(speedtest.net), backup times, printing(Speed of transfer, ), virus and malware detection, disc space and usage speeds, firewall(Including internet filtering) etc. Then test average speeds when under heavy load over a period of time. A table such as above could be used. Use Kali Linux with OpenVas to check for security loop holes. Check security configurations. Log changes and improvements that you make.

**3.2 – Justify the performance optimisation and update to the NOS. (U27 4.3)**

Based on 3.1 explain the improvements you have made to the network, justifying any expense or changes with evidence when possible.

**3.3 – Manage the network security solution applied. (U46 4.1)**

Explain the security software or hardware you have installed (e.g. anti-virus, firewall, physical security.). How do you use them to manage the network? Create documentation which would show the network manager how to use the security features you have implemented. Include username, passwords, IP addresses and a user guide on configuring software and devices.

**3.4 – Analyse (U46 4.2)**

Think about the strengths and weakness of the network and its creation. Could be merged with 3.5 to include improvements.

**3.5 – Recommend potential changes that you could make to the security. (U46 4.3)**