

School of Information Technology

Diploma in Information Technology

ITP311 Application Security & Project | 2020S2

Tutorial 1

1. Your team has been issued a new server (host) to host your web application. Other than a web server and a web application server, you discover that the server is still running an email server, a database server and a File Transfer Protocol server (FTP). For your purposes, you do not require the email server and FTP server. You require the database server but do not expect any need for external connections to the database server.

What steps should you take to take to secure the host? Perform the necessary research to determine specific protocols and ports.

Have patches and updates secure yourself against new vulnerabilities. Secure files and directories with restricted NTFS permissions or encryption followed by using port 443 to support HTTPS. Have auditing and logging to record attempted intrusions and have protocols to reduce the attack surface area by disabling port 21, 25, 143, 110 as we are not using them. Restrict the number of accounts accessible to the necessary set of service and user accounts and mandate strong passwords. Reduce the attack surface area even more by disabling unnecessary and unused services. Remove all unnecessary file shares and secure remaining shares with restricted NTFS permissions.

**~ End ~**

Page 1 of 1