IY5512: Coursework 7b

If feedback is required, coursework solutions must be submitted electronically via the course Moodle page. The deadline for receipt of submissions is 23:59 UK time on Friday 11/12/15. Coursework submissions should normally be in the form of a single pdf file. If you use Word, a free add-on to enable you to save a document in pdf format can be obtained from the Microsoft web site. Take care to ensure that you include your full name on the first page of your submission, the course number (IY5512), and the coursework number.

These questions are designed to test and extend your understanding of Part 7b of the course material.

1. It is often said that Unix is inherently less subject to attack than Windows as a result of flaws in software. Is this true, and if so why? Does this mean that Unix is completely secure, regardless of how well written it is?

2. In Windows, why do SIDs need to be unique within a domain forest?

3. Describe a vulnerability in the Kerberos authentication protocol.

4. Give an example of a Windows security principal, and describe the relationship between a Security Identifier (SID) and a security principal.

5. In Windows, a securable object possesses a security descriptor. Give two examples of securable objects. Briefly describe one of the functional components of a security descriptor.

6. Describe the main steps that occur in a Windows interactive login procedure when a user is logging in to a domain account. In your description cover the roles of Kerberos, the Winlogon process, the LSA, Active Directory, the SAS, a credential provider, and the creation of an access token.

7. Outline at a high level the pieces of information used by Windows in making an access control decision when a subject wishes to access an object.