My study guide (Test 2)

This is an outline study guide for Test 2 (and may change, so please check back). The test accounts for 25% of the module. It is a closed book test, and normal examination conditions apply. A correct answer scores +1, with a negative penalty for an incorrect answer, and a non-answer gets a score of zero. The score will be normalised and converted into an indicative grade (A+, A, A-, and so on).

Software Security (Approx questions = 8)

Area	Notes
Understands the usage of the Global Assembly Cache in .NET.	
Understands security settings for ASP.NET Web (Web.Config).	
Defines the usage of the strong name used for in .NET assemblies.	
Understand the problems caused by "DLL Hell", and how it can be overcome with .NET.	
Understands the trends from port-based security with thick clients to Web-based thin-clients.	
Understands the methods used to obfuscate a .NET assembly.	
Understands how Cardspace is used within an IP/RP infrastructure.	
Defines best-practice for software security (see Software lecture).	
Outlines the usage of role-based security in .NET.	

Network Security (Approx questions = 6)

Area	Notes
Outlines the usage of NAT/PAT. This includes the advantages of using NAT/PAT	
Outlines the usage of proxies, such as for the trace left from external access	
Defines the creation of an ACL to block/allow access.	

Forensic Computing (Approx. Questions=12)

Area	Notes
Understands multi-factor authentication (Section 7.5).	
Understands binary to text conversion format (Base-64/Hex).	
Defines the usage and the operation of the OTP (One-Time Password) (Section 7.6)	
Performs an analysis of a network trace for forensic purposes (see Forensic Computing Lecture 2)	
Creates a Winpcap filter to capture certain types of data. (see Forensic Computing Lecture 2)	
Understand the main stages of a digital forensics investigation.	
Define the time stamp format for Windows (two questions).	
Define how an investigation uses the Registry (two questions).	
Define the usage of Web browser history usage in forensic investigations (two questions).	