

## 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, an incorrect answer scores -0.2, 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.	
Provides a deep understanding of a Kerberos system (Section 4.8).	
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 basic objectives for Phase 1 and 2 in IKE, and the settings that are defined in each phase.	
Defines the creation of an ACL to block/allow access.	

## Forensic Computing (Approx. Questions=12)

Area	Notes
Understands multi-factor authentication (Section 7.5).	
Defines the usage of timing and storage covert channels.	
Understands covert channel hiding in IP/TCP packets.	
Understands binary to text conversion format (Base-64/Hex).	
Understands how data can be hidden in images.	
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)	
Understands the operation of DNS, and how it can be used for covert channels and how it might be used to attack external systems.	

## CCSP (Approximate Questions = 9)

Area	Notes
Understands the CLI setup for an IP address, security level and name on a PIX interface for PIX 7.x.	
Defines the operation and tests used for PIX failover.	
Understands the CLI setup of static routes on a PIX.	
Understands the defaults flows between domains for a stateful firewall (inside/outside/DMZ).	
Understands the CLI setup of NAT and PAT on a PIX.	
Understands how to view the ASDM setup of NAT and PAT on a PIX.	

### Notes:

- 26 academic questions, and 9 PIX/ASA questions.
- Questions in total = 35.
- Test times: 9-9:55am or 10-10:55am, Tuesday 1 December 2009, B.2.

### Contact:

- Prof Bill Buchanan Email: [w.buchanan@napier.ac.uk](mailto:w.buchanan@napier.ac.uk)
- Richard Macfarlane Email: [R.Macfarlane@napier.ac.uk](mailto:R.Macfarlane@napier.ac.uk)

Matriculation No: