My study guide (Test 1)

This is an outline study guide for Test 1 (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 a negative mark, 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).

Threats (Approx questions = 11)

Area	Notes
1. Defines and classifies CIA.	
2. Understands a range of regulations involved in security.	
3. Define the objectives of the phases of pen testing.	
4. Understands how OS Scans work.	
5. Defines the range of tools used in pen testing.	
6. Outlines how Snort is used to detect scanning.	
7. Defines the key classifications for Botnet taxonomy.	
8. Outlines how SQL injection operations (especially a focus on SQL injection). See Toolkit [SQL] and observe different commands.	
9. Defines usage of polyinstantiation.	
10. Calculates inferred marks for running averages on a database.	

11. Calculates key entropy.	

Network Forensics (Approx questions = 10)

Area	Notes
1. Understands the key parts of ARP.	
2. Understands the key parts of Ethernet.	
3. Understands the key parts of IP.	
4. Understands the key parts of TCP/UDP.	
5. Understands the key parts of DNS.	
6. **Understands the footprints of Port Scans**. Observe the pattern of SYNs caused by the scanner, and how the server responds to open and closed ports.	
7. **Understands the key parts of HTTP communications**. Gives a foundation of requests and replies. See Toolkit [Network->HTTP] and observe different replies.	
8. **Understands the key parts of FTP communications**.	

Data Hiding (Approx questions = 11)

Area	Notes
1. Classifies encryption methods (public key, private key and hashing) and encoding.	
2. Identifiers MD5 and SHA-1 hash signatures, and their format.	
3. Use a XOR key for data hiding.	
4. Understands some of the methods used to decrypt maliciously encrypted text.	
5. Converts an XOR conversion into a range of formats (Base-64, ASCII, hex).	
6. Does frequency analysis to determine possible coding.	
7. Defines opportunities for data hiding in IP and TCP.	
8. Defines basic signatures of OSs for ID field.	
9. Defines the basic signatures for key file formats.	

Notes:

- Questions in total = 32.

Contact:

- Prof Bill Buchanan Email: w.buchanan@napier.ac.uk
- Richard Macfarlane Email: R.Macfarlane@napier.ac.uk