Making assessment and feedback fun: feedback before and after assessments

Motivation: To create a scientific approach to testing, that is designed with feedback in mind at every stage.

- Requirement for Feedback.
- Test Design and Creation
- Test Preparation and Analysis
- Feedback System
- Some Results
- Conclusions

Prof Bill Buchanan, School of Computing
Feedback...

The Requirement for F/B
Assessment flow

Unit 1 Unit 2 Unit 3 Unit 4 Unit 5 Unit 6 Unit 7 PC

MCQ Test (Week 6/7) 25%
MCQ Test (Week 12) (25%)
Coursework (50%) Week 13 H/in

Itemized feedback
Itemized feedback
Itemized feedback

Face-to-face
Blended
Remote student

Feedback...

Author: Prof Bill Buchanan
Increasing requirement for feedback

Re-enforce Units → Pre-test → Test/Assessment → Wind-down And Formal Feedback

Tests

iPhone/iPad

On-line lectures

Face-to-face

Blended

Remote student

The challenge...
Feedback...

Preparing for the test
Web-based

Fun test

Frogger-type

Rich Integration

Ways to engage
<quest id="000001">
  <title>Who is associated with Apple:</title>
  <q1>Steve Wozniak</q1>
  <q2>Tim Berners-Lee</q2>
  <q3>Bill Gates</q3>
  <q4>James Gosling</q4>
  <correct>q1</correct>
  <level>1</level>
  <explain>http://en.wikipedia.org/wiki/Steve_Wozniak</explain>
</quest>
My study guide

My study guide (Test 1)
This is an online study guide for Test 1 and may change at any time. Please check back. The test accounts for 27% of the module. It is a closed book test, and normal examination conditions apply. A correct answer scores +1, an incorrect answer scores -1, and a non-answer gets a score of 0. The score will be normalized and converted into an indicative grade (A, B, C, etc.).

Threats (Approx questions = 11)

1. Define and describe DDoS.
2. Understand the range of regulations involved in security.
3. Define the objectives of phishing testing.
4. Understand how 90 bars work.
5. Define the previous term used in phishing testing.
6. Outlines how ATP is used to detect phishing.
7. Define the key classifications for Botnet taxonomy.
8. Outlines how SQL injection operations (especially a focus on SQL injection attacks).

Student study

Students study with wide range of sample questions

Student study

Feedback...

MCQ Ratings
Feedback on theory

Certified Ethical Hacker

Challenge 1: Business Aspects of Pen Testing
- Match the presentation [A] (network, integrity, and availability)
- Define ethical hacking
- List the elements of security
- Differentiate ethical hackers and their duties. This includes physical and logical controls.
- Complete the activity of ethical hacking
- Know the laws related to computer crimes

Challenge 2: Technical Foundations of Hacking
- View the presentation [B] (sample web traffic, traffic steering)
- TCP/IP structure
- Topology
- IP addressing
- Ports

Challenge 3: Exploitation and Scanning
- View the presentation [C] (sample web traffic, traffic steering)
- Post exploit vulnerability scanner
- Network range
- Identify active hosts

Gained knowledge relative to computer crimes

CSEM Business Aspects of Pen Testing

What is an examination of services against a known vulnerability database using an automated tool?

A: Forensic readiness test
B: Penetration test
C: Vulnerability assessment
D: Security policy test

2/10

Pre-test feedback

Vulnerability assessment

From Wikipedia, the free encyclopedia

A vulnerability assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system. Examples of systems for which vulnerability assessments are performed include, but are not limited to, nuclear power plants, information technology systems, energy supply systems, water supply systems, transportation systems, and communication systems. Such assessments may be conducted on behalf of a range of different organizations, from small businesses up to large regional infrastructures. Vulnerability from the perspective of disaster management means assessing the threats from potential hazards to the population and to infrastructure, along with the political, social, economic, or environmental fields.

Vulnerability assessment has many things in common with risk assessment. Assessments are typically performed according to the following steps:

1. Cataloging assets and capabilities (resources) in a system
2. Assigning a quantifiable value (or at least rank) a value (or priority) and importance to those resources
3. Identifying the vulnerabilities or potential threats to each resource
4. Mitigating or eliminating the most serious vulnerabilities for the most valuable resources

Classical risk analysis is principally concerned with investigating the risks surrounding physical plant (or other object), its design and operation. Such analyses tend to focus on causes and the direct consequences for the studied object. Vulnerability analyses, on the other hand, focus on the

Author: Prof Bill Buchanan
Feedback on theory

Certified Ethical Hacker

Challenge 1: Business Aspects of Pen Testing
- Which is both an Unethical and an Ethical hacker:
  - Blue hat
  - White hat
  - Gray hat
  - Black hat

Challenge 2: Technical foundations of hacking
- Which helps with Confidentiality:
  - Mirrored servers
  - Passwords
  - Failover devices
  - Fast network speeds

CEH: Business Aspect of Pen Testing

What is the likelihood of the occurrence of something that could cause harm, loss or damage:

A. A Risk
B. A Threat
C. A Vulnerability
D. An asset

Author: Prof Bill Buchanan

Pre-test feedback
### 2011

<table>
<thead>
<tr>
<th>Question</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
<th>18</th>
</tr>
</thead>
<tbody>
<tr>
<td>Correct</td>
<td>50</td>
<td>55</td>
<td>46</td>
<td>57</td>
<td>45</td>
<td>38</td>
<td>41</td>
<td>45</td>
<td>10</td>
<td>16</td>
<td>18</td>
<td>30</td>
<td>56</td>
<td>14</td>
<td>26</td>
<td>23</td>
<td>55</td>
<td></td>
</tr>
<tr>
<td>Not ans</td>
<td>8</td>
<td>9</td>
<td>8</td>
<td>10</td>
<td>8</td>
<td>10</td>
<td>12</td>
<td>11</td>
<td>13</td>
<td>25</td>
<td>12</td>
<td>12</td>
<td>12</td>
<td>7</td>
<td>9</td>
<td>9</td>
<td>8</td>
<td>10</td>
</tr>
<tr>
<td>Incorrect</td>
<td>9</td>
<td>3</td>
<td>13</td>
<td>2</td>
<td>12</td>
<td>21</td>
<td>26</td>
<td>14</td>
<td>11</td>
<td>44</td>
<td>26</td>
<td>37</td>
<td>29</td>
<td>2</td>
<td>44</td>
<td>33</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

| Score    | 49.1| 54.7| 44.7| 66.8| 43.8| 35.9| 28.4| 39.6| 43.9| 5.6 | 13.4| 14.3| 27.1| 55.8| 9.6 | 22.7| 19.6| 54.6|

| Rating   | 2   | 1   | 2   | 1   | 3   | 3   | 4   | 3   | 3   | 4   | 3   | 4   | 2   | 5   | 4   | 4   | 5   | 1   |

### 2010

<table>
<thead>
<tr>
<th>Question</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
<th>18</th>
</tr>
</thead>
<tbody>
<tr>
<td>Correct</td>
<td>39</td>
<td>44</td>
<td>36</td>
<td>48</td>
<td>42</td>
<td>22</td>
<td>22</td>
<td>38</td>
<td>34</td>
<td>6</td>
<td>10</td>
<td>16</td>
<td>37</td>
<td>44</td>
<td>19</td>
<td>32</td>
<td>10</td>
<td>48</td>
</tr>
<tr>
<td>Not ans</td>
<td>13</td>
<td>15</td>
<td>14</td>
<td>14</td>
<td>13</td>
<td>17</td>
<td>16</td>
<td>19</td>
<td>27</td>
<td>24</td>
<td>38</td>
<td>24</td>
<td>13</td>
<td>16</td>
<td>15</td>
<td>14</td>
<td>17</td>
<td>16</td>
</tr>
<tr>
<td>Incorrect</td>
<td>17</td>
<td>10</td>
<td>19</td>
<td>7</td>
<td>14</td>
<td>30</td>
<td>31</td>
<td>12</td>
<td>8</td>
<td>39</td>
<td>21</td>
<td>29</td>
<td>19</td>
<td>9</td>
<td>35</td>
<td>23</td>
<td>42</td>
<td>5</td>
</tr>
</tbody>
</table>

| Score    | 44.8| 51.6| 40.9| 66.8| 48.7| 22.8| 22.7| 44.2| 39.8| 2.5 | 9.5 | 15.7| 42.1| 51.7| 18.6| 35.6| 7  | 57 |

| Rating   | 2   | 1   | 2   | 1   | 2   | 1   | 2   | 4   | 3   | 3   | 5   | 5   | 5   | 2   | 2   | 5   | 3   | 5   | 1   |

### Score vs. Rating

- Score: 5
  - Rating: Same rating
  - Match: 15
  - %: 79
- Score: 4
  - Rating: One level difference
  - Match: 16
- Score: 3
  - Rating: Two level difference
  - Match: 5
  - Penalty: -0.1

**Evaluation of test questions 2010/2011**

Author: Prof Bill Buchanan
Feedback System
Module Descriptor (with definition of learning outcomes) → Itemized definition of learning elements → Test created which matches the learning elements → Study guide given to students with definition of learning elements → Student practices on-line with a wide range of sample questions → Test analysed for correct and incorrect results.

External Examiner

Formal feedback using mechanised procedures

Good things:
- No students can have any grumbles on the test.
- Students get a quick wind-down.
- Builds up bond with the academic team.
- Little change of errors the evaluation of performance.
- External examiner see an integrated approach.

Author: Prof Bill Buchanan
<table>
<thead>
<tr>
<th>Question</th>
<th>Rating</th>
<th>Learning Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>Classifies a method of confidentiality, such as that passwords keep a secret</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>Defines the key US laws related to computer security</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>Defines the key stages of a pen test</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>Defines the key stages of a pen test within black box testing</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>Able to analyse a port scan and how it is used</td>
</tr>
<tr>
<td>7</td>
<td>2</td>
<td>Defines the characteristics of Botnet taxonomy, and classifies different methods</td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>Understands a sample SQL injection attack using a SQL request to read from a database</td>
</tr>
<tr>
<td>9</td>
<td>2</td>
<td>Understands a sample SQL injection attack using a SQL request to update data on a database</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
<td>Does a calculation on average marks and is able to infer the grading for individual marks</td>
</tr>
<tr>
<td>11</td>
<td>2</td>
<td>Calculates the number of bits used for a certain entropy value</td>
</tr>
<tr>
<td>12</td>
<td>2</td>
<td>Analyses the ARP request and response, for data that has been modified</td>
</tr>
<tr>
<td>13</td>
<td>2</td>
<td>Analyses a network trace for the key parameters for Ethernet, IP and TCP</td>
</tr>
<tr>
<td>14</td>
<td>2</td>
<td>Understands how TCP is identified in an IP packet</td>
</tr>
<tr>
<td>15</td>
<td>2</td>
<td>Analyses a network trace for the TCP segment flow, and the key parameters</td>
</tr>
<tr>
<td>16</td>
<td>2</td>
<td>Understands the format of UDP parameters, and can determine changes in them</td>
</tr>
<tr>
<td>17</td>
<td>2</td>
<td>Analyses a network trace from a port scan from an intruder, and shows the packet sent</td>
</tr>
</tbody>
</table>

### Feedback

**2011**

<table>
<thead>
<tr>
<th>Question</th>
<th>Correct</th>
<th>Not ans</th>
<th>Incorrect</th>
<th>Score</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>50</td>
<td>8</td>
<td>2</td>
<td>49.1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>55</td>
<td>9</td>
<td>3</td>
<td>64.7</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>46</td>
<td>10</td>
<td>12</td>
<td>44.7</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>57</td>
<td>8</td>
<td>21</td>
<td>56.8</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>45</td>
<td>10</td>
<td>12</td>
<td>43.8</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>38</td>
<td>8</td>
<td>21</td>
<td>35.9</td>
<td>3</td>
</tr>
<tr>
<td>7</td>
<td>31</td>
<td>8</td>
<td>21</td>
<td>28.4</td>
<td>2</td>
</tr>
<tr>
<td>8</td>
<td>41</td>
<td>10</td>
<td>12</td>
<td>39.6</td>
<td>3</td>
</tr>
<tr>
<td>9</td>
<td>45</td>
<td>8</td>
<td>21</td>
<td>43.9</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>10</td>
<td>12</td>
<td>5.6</td>
<td>5</td>
</tr>
<tr>
<td>11</td>
<td>16</td>
<td>8</td>
<td>21</td>
<td>13.4</td>
<td>4</td>
</tr>
<tr>
<td>12</td>
<td>18</td>
<td>8</td>
<td>21</td>
<td>14.3</td>
<td>4</td>
</tr>
<tr>
<td>13</td>
<td>30</td>
<td>8</td>
<td>21</td>
<td>27.1</td>
<td>4</td>
</tr>
<tr>
<td>14</td>
<td>56</td>
<td>8</td>
<td>21</td>
<td>56.8</td>
<td>4</td>
</tr>
<tr>
<td>15</td>
<td>14</td>
<td>8</td>
<td>21</td>
<td>19.6</td>
<td>4</td>
</tr>
<tr>
<td>16</td>
<td>26</td>
<td>8</td>
<td>21</td>
<td>22.7</td>
<td>4</td>
</tr>
<tr>
<td>17</td>
<td>23</td>
<td>8</td>
<td>21</td>
<td>19.6</td>
<td>4</td>
</tr>
<tr>
<td>18</td>
<td>55</td>
<td>8</td>
<td>21</td>
<td>54.6</td>
<td>4</td>
</tr>
</tbody>
</table>
Face-to-face feedback or over MSN Messenger or Skype text within one day of the test. Sometime by email.

- Emailed to us on the day of the assessment. Awesome.
- Bill gives very fast feedback.
- Yes. Same day results.
- Indeed, concise, and well presented.
- Excellent feedback on the tests, very fast and accurate.
- And so on.
Re-enforcing...

Some results
21. Which is the most useful for exam study (/accesses before exam)
23. With on-line tests which should be true:
Conclusions

Motivation: To create a scientific approach to testing, that is designed with feedback in mind at every stage.

- Integrated process which integrates students and external examiners.
- Scientific approach, with accurate assessment of performance.
- Students understand what they must study, and have a wide range of test questions.
- Face-to-face creates a bond between the student and academic.
- Itemized learning elements make it easier to analyse overall performance.

Prof Bill Buchanan, School of Computing