

Making assessment and feedback fun: feedback before and after assessments

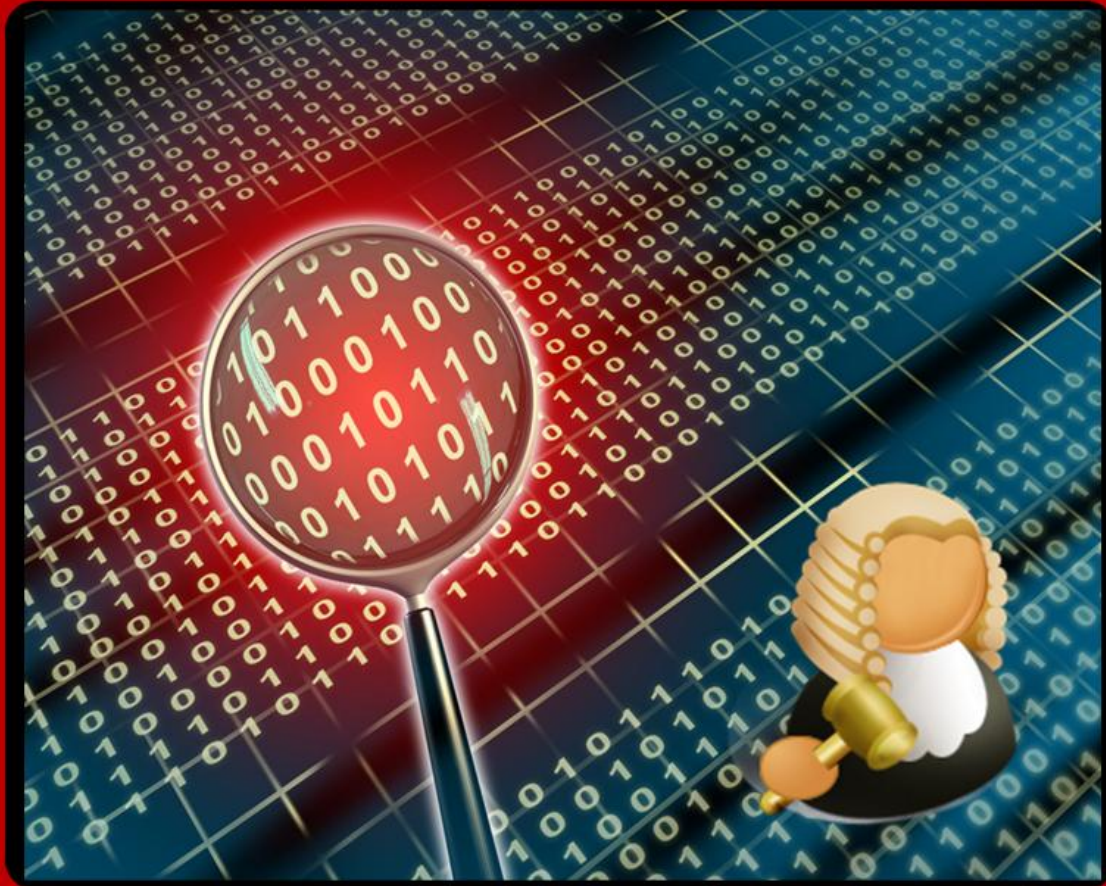
Motivation: To create a scientific approach to testing, that is designed with feedback in mind at every stage.

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

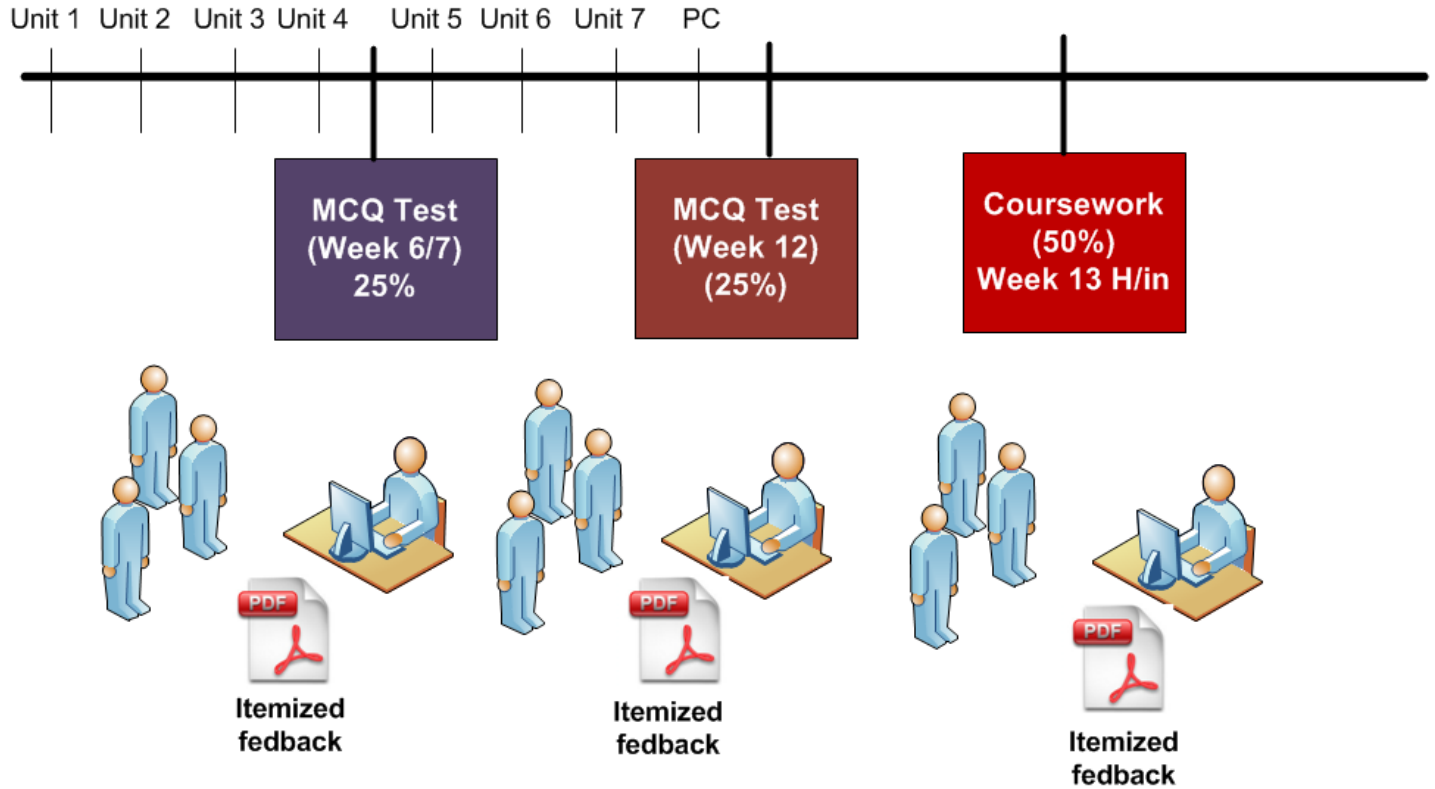
Prof Bill Buchanan, School of Computing



Feedback...



The Requirement for F/B



Face-to-face

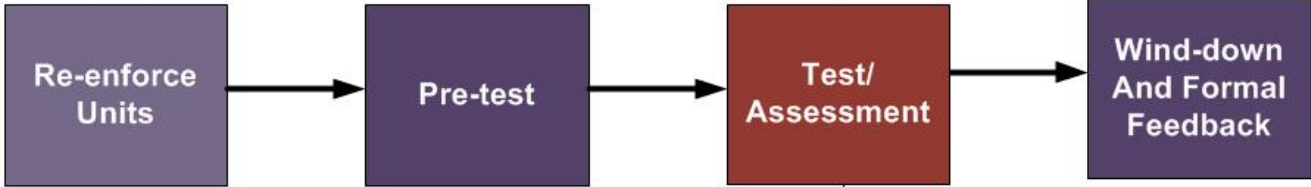
2x2
3x4

Blended

2x2
3x4

Remote student

Increasing requirement for feedback



Tests



iPhone/iPad

On-line lectures

Face-to-face

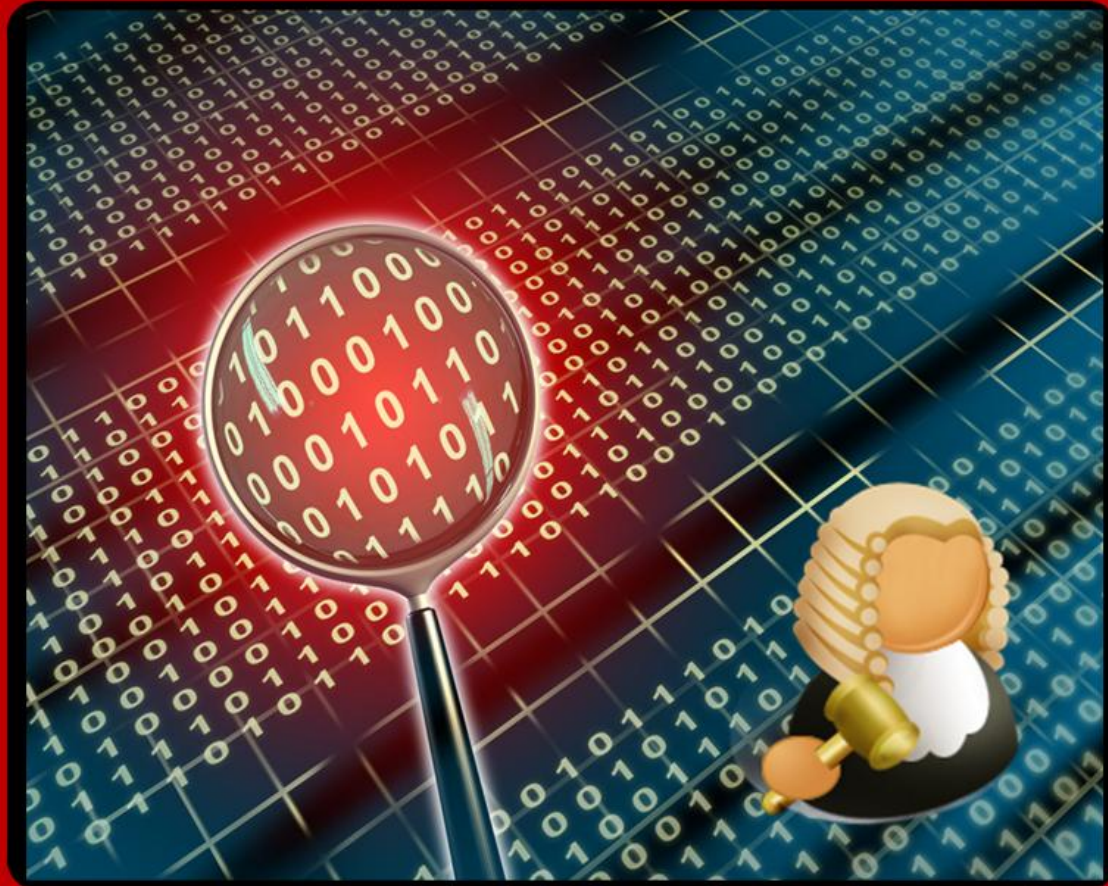
Blended

Remote student

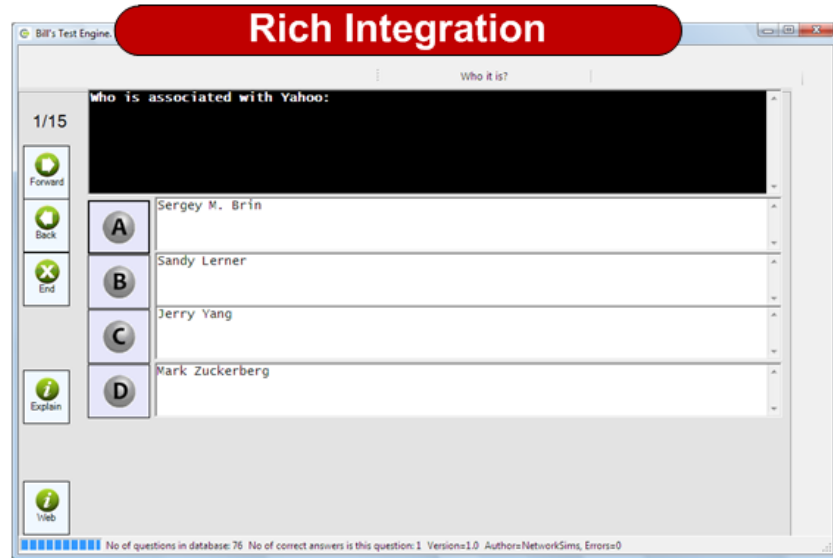
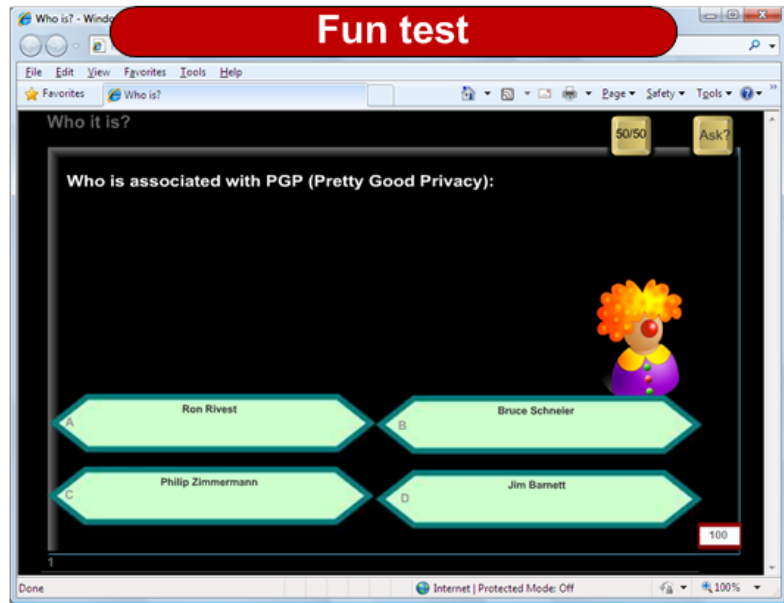
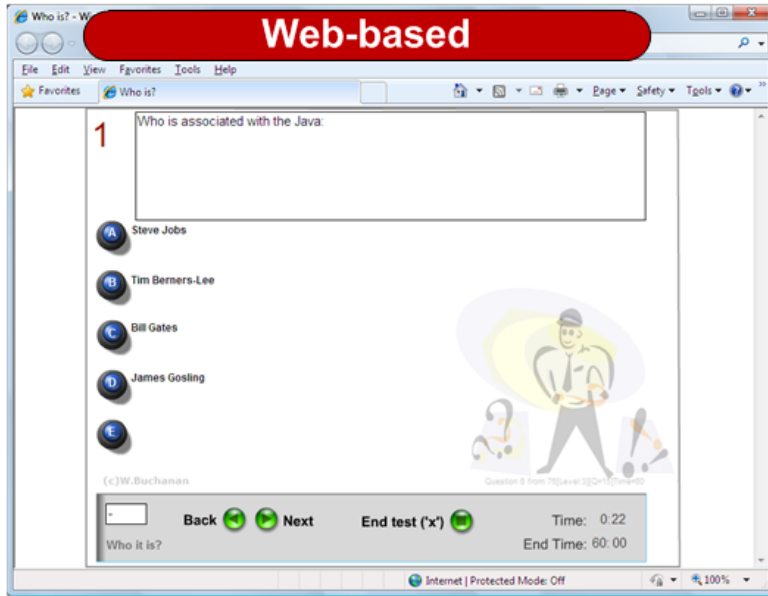
Time line requirements

Feedback...

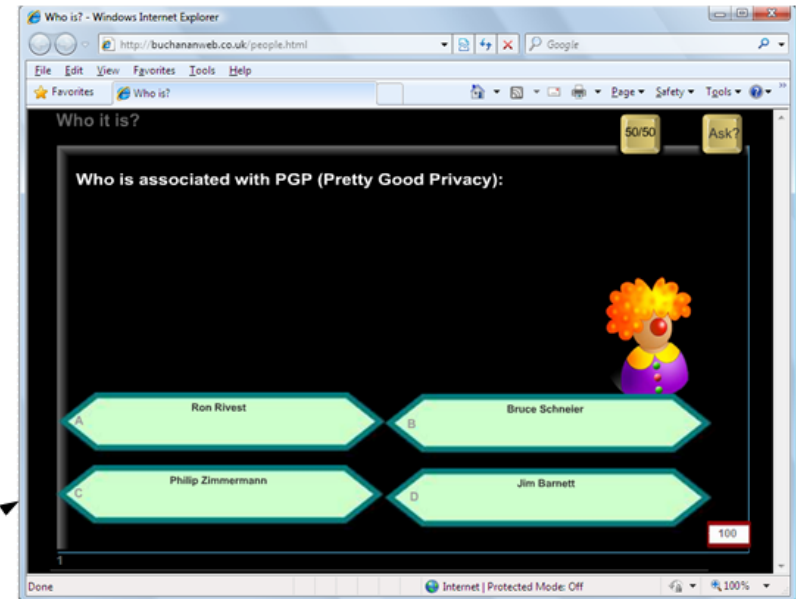
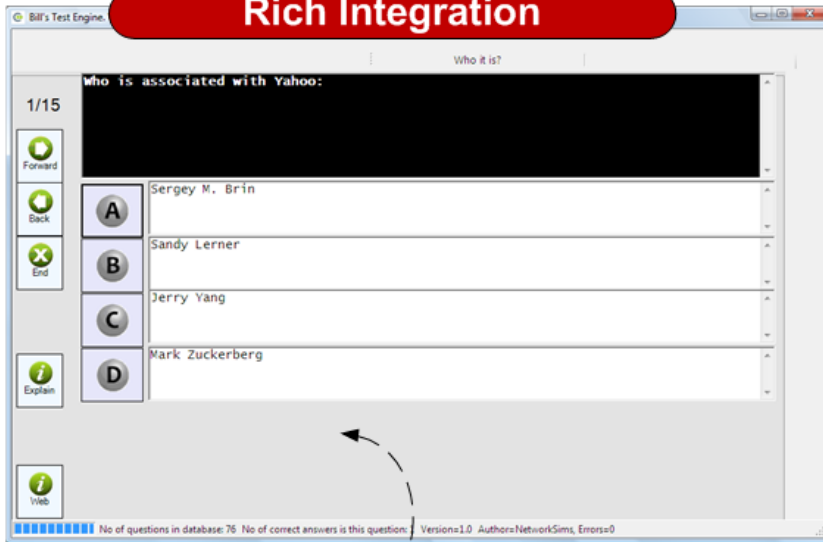
Feedback...



Preparing for the test



Rich Integration



Common data storage

```
<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>
```

Different interfaces

Feedback...

my_study_guide_asnf.pdf - Adobe Acrobat Pro

File Edit View Document Comments Forms Tools Advanced Window Help

Create Combine Collaborate Secure Sign Forms Multimedia Comment

1 / 3 54.4% Find

My study guide

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 -0.1, 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 polymorphism.	
10. Calculates inferred marks for running averages on a database.	

Matriculation No: 1



MCQ Ratings

Feedback...

Bill's Test Engine. Version: 1.11.0 (Build 140511)

Test 1

which is installed on a computer in order to understand a users behaviour:

8/10

Forward Back End Explain Web

- A Viruses
- B Bots
- C worms
- D Trojans
- E Logic bombs
- F Spyware

No of questions in database: 272. No of correct answers is this question: 1. Version: 1.0. Authors: NetworkSims, Errors: 0

Students study with wide range of sample questions

ProSIMs 6.201 (Build 300511)

Description

Home BK PWD Menu Cisco - Check - Juniper - Books - router rip

Test 1

50/50 Ask?

Which is the term used for testing with a partial knowledge of the target of interest:

A Yellowbox

B Blackbox

C Graybox

D Whitebox

100

Author: Prof Bill Buchanan

Student study

Feedback on theory

ProFSM 6.20.1 (Build 200511)

Networksims

Certified Ethical Hacker

[Home] The Certified Ethical Hacker (312-50) challenges include [Course brochure][Exam]:

- Challenge 1. Business Aspects of Pen Testing. [Fun test]
 - [Watch the presentation][PDF]
 - Understand the Security Triad: CIA (Confidentiality, Integrity and Availability).
 - Define ethical hacking.
 - List the elements of security.
 - Describe ethical hackers and their duties. This includes physical and logical controls.
 - Define the modes of ethical hacking.
 - Describe test deliverables.
 - Know the laws related to computer crimes.
- Challenge 2. Technical Foundations of Hacking. [Fun test]
 - [Watch the presentation][Sample Web page traffic][Sample ICMP traffic][PDF]
 - OSI
 - TCP/IP
 - TCP Packet Structure
 - TCP flags
 - UDP and TCP.
 - Ports
 - ICMP.
- Challenge 3. Footprinting and Scanning. [Fun test]
 - [Watch the presentation][PDF]
 - Seven-step information gathering.
 - Footprinting.
 - Network range.
 - Identify active machines.
 - [Watch the presentation][PDF]

Bill's Test Engine, Version: 1.110 (Build 140511)

CEH: Business Aspect of Pen Testing

2/10

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

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

No of questions in database: 108 No of correct answers in this question: 1 Version: 1.2 Authors: WB, Errors: 0

Content source: http://en.wikipedia.org/wiki/Vulnerability_assessment

Log in / create account

Article Discussion Read Edit View history Search

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 for 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 organisations, 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. It may be conducted in 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 quantifiable value (or at least rank order) 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 some other object), its design and operations. Such analyses tend to focus on causes and the direct consequences for the studied object. Vulnerability analyses, on the other hand, focus both on

Home Exit

business Aspect of Pen Testing What is an examination of services against a known vulnerability database using an automated tool powered by Google™

Cisco Wikipedia Web Image Book Video

CISSP, CEH, EC: 201 x 151
cam.videotrainer.com

NET Web Applica: 566 x 107
www.careeracademy.com

Penetration Test: 117 x 85
www.globalnetcc.com

penetration testit: 1275 x 1650
www.docstoc.com

Providing Feedback

Feedback...

Feedback on correct ans.

ProfSim 6.20.1 (Build 300511)

Home | Check | Juniper | Books | router rip

Certified Ethical Hacker

[Home] The Certified Ethical Hacker (312-50) challenges include [Course brochure][Exam]:

- Challenge 1. Business Aspects of Pen Testing. [Fun test]
 - [Watch the presentation][PDF]
 - Understand the Security Triad: CIA (Confidentiality, Integrity and Availability).
 - Define ethical hacking.
 - List the elements of security.
 - Describe ethical hackers and their duties. This includes physical and logical controls.
 - Define the modes of ethical hacking.
 - Describe test deliverables.
 - Know the laws related to computer crimes.
- Challenge 2. Technical Foundations of Hacking. [Fun test]
 - [Watch the presentation][Sample Web page traffic][Sample ICMP traffic][PDF]
 - OSI
 - TCP/IP
 - TCP Packet Structure
 - TCP flags
 - UDP and TCP.
 - Ports
 - ICMP.
- Challenge 3. Footprinting and Scanning. [Fun test]
 - [Watch the presentation][PDF]
 - Seven-step information gathering.
 - Footprinting.
 - Network range.
 - Identify active machines.
 - [View the active machine's configuration]

Bill's Test Engine, Version: 1.11.0 (Build 140511)

CEH: Business Aspect of Pen Testing

2/10

Forward

Back

End

Explain

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

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

Bill's Test Engine, Version: 1.11.0 (Build 140511)

CEH: Business Aspect of Pen Testing

2/10

Forward

Back

End

Explain

Web

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

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

No of questions in database: 108 No of correct answers in this question: 1 Version: 1.2 Author: WB, Errors=0

Bill's Test Engine, Version: 1.11.0 (Build 140511)

CEH: Business Aspect of Pen Testing

2/10

Forward

Back

End

Explain

Web

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

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

Turn review OFF

No of questions in database: 108 No of correct answers in this question: 1 Version: 1.2 Author: WB, Errors=0

Providing Feedback

Feedback...

Feedback on theory

ProfSIMs 6.20.1 (Build 300511)

Home | Check | Junipe | Books | router rip

Certified Ethical Hacker

[Home] The Certified Ethical Hacker (312-50) challenges include [C]

- Challenge 1. Business Aspects of Pen Testing. [Fun test]
 - [Watch the presentation][PDF]
 - Understand the Security Triad: CIA (Confidentiality, Integrity, Availability)
 - Define ethical hacking.
 - List the elements of security.
 - Describe ethical hackers and their duties. This includes:
 - Define the modes of ethical hacking.
 - Describe test deliverables.
 - Know the laws related to computer crimes.
- Challenge 2. Technical Foundations of Hacking. [Fun test]
 - [Watch the presentation][Sample Web page traffic]
 - OSI
 - TCP/IP
 - TCP Packet Structure
 - TCP flags
 - UDP and TCP.
 - Ports
 - ICMP.
- Challenge 3. Footprinting and Scanning. [Fun test]
 - [Watch the presentation][PDF]
 - Seven-step information gathering.
 - Footprinting.
 - Network range.
 - Identify active machines.
 - Identify active machines.

CEH: Business Aspect of Pen Testing 50/50 Ask?

Which is both an Unethical and an Ethical hacker:

A Blue hat B White hat
C Grey hat D Black hat

CEH: Business Aspect of Pen Testing 50/50 Ask?

Which helps with Confidentiality:

Mirrored servers B Passwords
Failover devices D Fast network speeds

CEH: Business Aspect of Pen Testing 50/50 Ask?

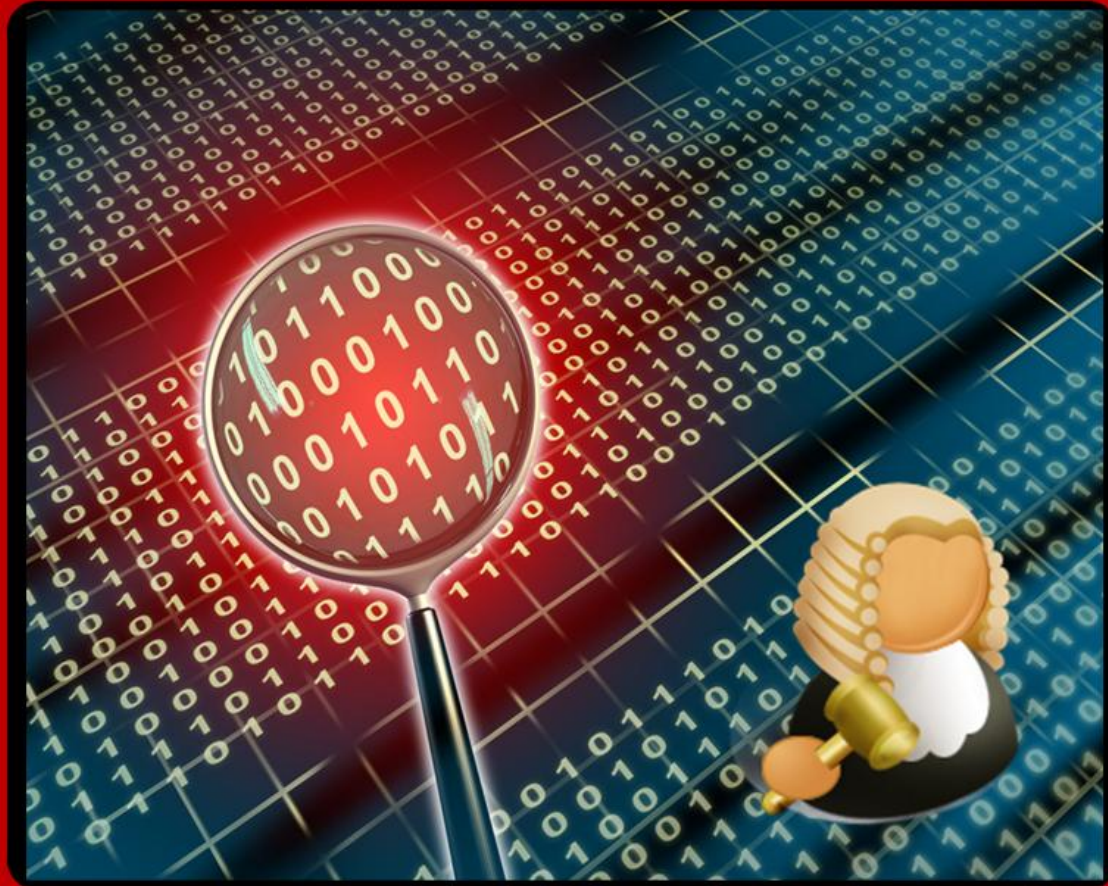
What is the likelihood of the occurrence of something that could cause harm, loss or damage:

A A risk B A vulnerability
C A threat D An asset

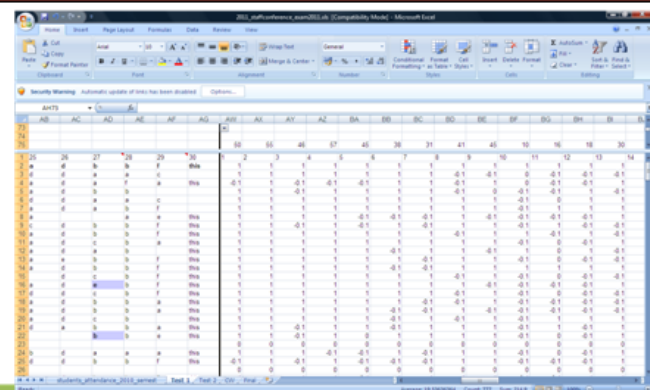
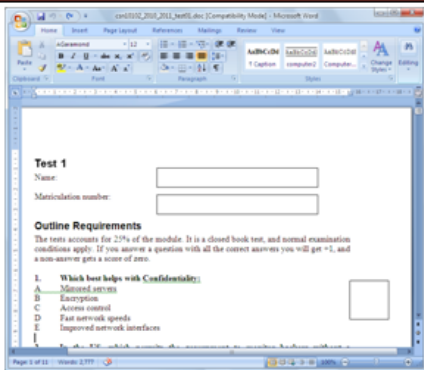
Providing Feedback

Feedback...

Feedback...



Test Preparation and Analysis



2011

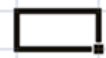
Question	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Correct	50	55	46	57	45	38	31	41	45	10	16	18	30	56	14	26	23	55
Not ans	8	9	8	8	10	8	10	12	11	13	25	12	8	9	9	8	10	8
Incorrect	9	3	13	2	12	21	26	14	11	44	26	37	29	2	44	33	34	4
Score	49.1	54.7	44.7	56.8	43.8	35.9	28.4	39.6	43.9	5.6	13.4	14.3	27.1	55.8	9.6	22.7	19.6	54.6
Rating	2	1	2	1	3	3	4	3	3	5	5	5	4	2	5	4	5	1

2010

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Correct	39	44	36	48	42	22	22	38	34	6	10	16	37	44	19	32	10	48
Not ans	13	15	14	14	13	17	16	19	27	24	38	24	13	16	15	14	17	16
Incorrect	17	10	19	7	14	30	31	12	8	39	21	29	19	9	35	23	42	5
Score	44.8	51.6	40.9	56.8	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	4	4	3	3	5	5	5	2	2	5	3	5	1

Score	Rating	Match	%
<20	5	Same rating	15 79
<30	4	One level difference	3 16
<40	3	Two level difference	1 5
<50	2		
<60	1		

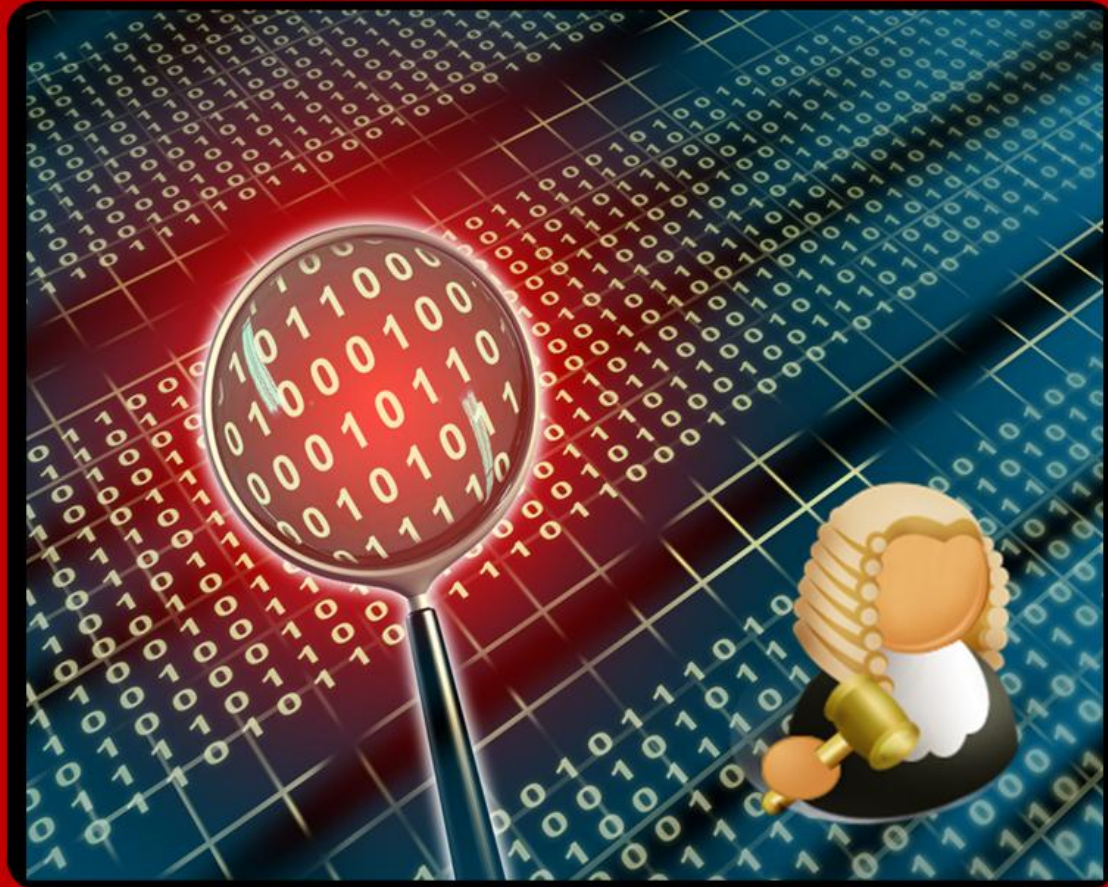
Penalty -0.1



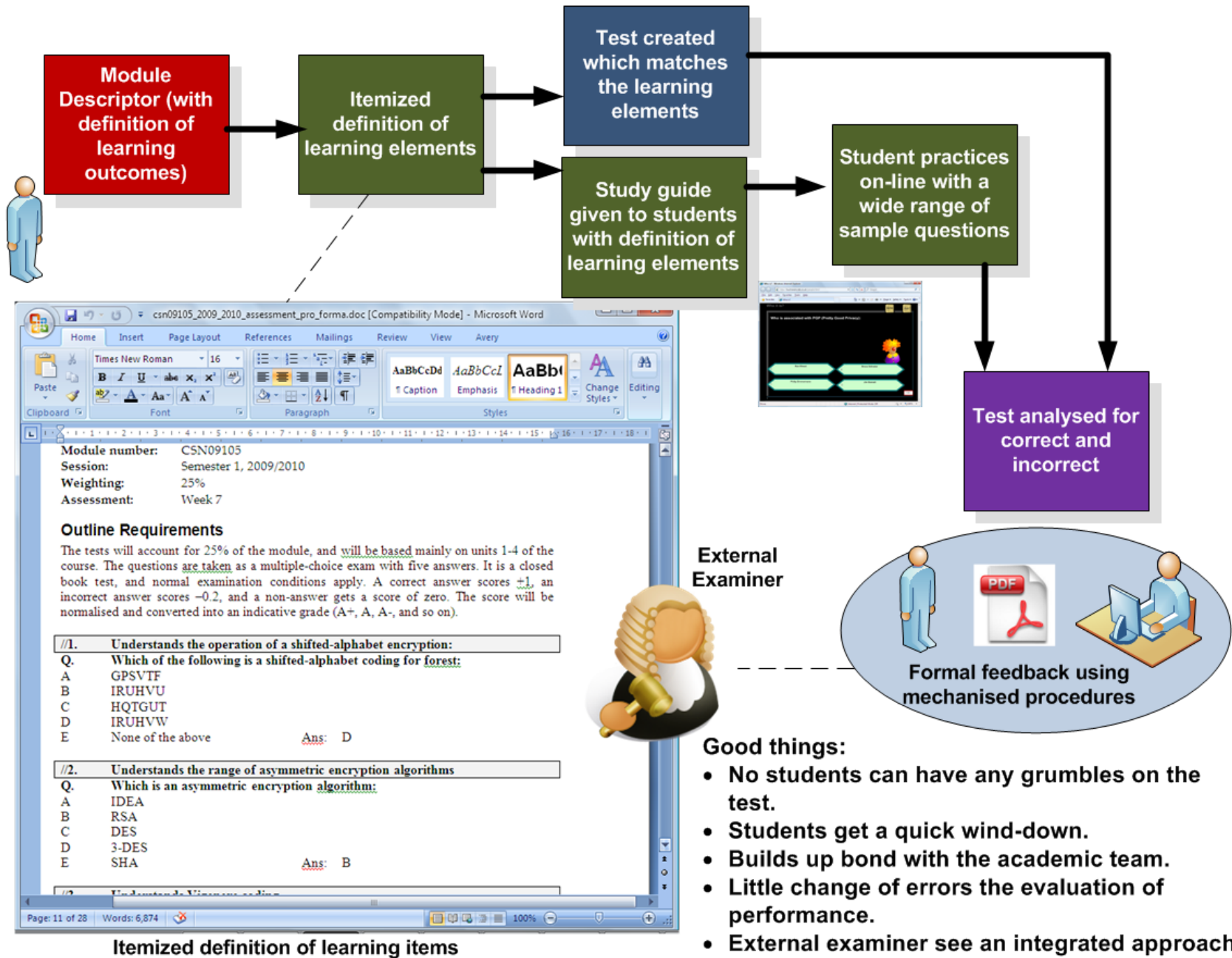
MCQ Ratings

Feedback...

Feedback...



Feedback System



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.



Student takes test

Test 1
Name:
Matriculation number:

Outline Requirements
The tests account for 25% of the module. It is a closed book test, and normal examination conditions apply. If you answer a question with all the correct answers you will get +1, and a wrong answer gets a score of zero.

1. Which tool helps with Confidentiality?
A. Meterpreter
B. Ettercap
C. Armitage
D. Flux network speeds
E. Improved net-usb interface

2. In the US, which permits the government to monitor hackers without a warrant?
A. Title 18: Crimes and Criminal Procedure - Sections 1029
B. Title 18: Crimes and Criminal Procedure - Sections 1030
C. Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT)
D. Security and Freedom through Encryption (SAFE)
E. Privacy Act of 1974

Excel Analysis



One-to-one Feedback session

Question	Rating	Learning Outcome
1	1	2 Classifies a method of confidentiality, such as that passwords keep a secret
2	2	1 Defines the key US laws related to computer security
3	3	2 Defines the key stages of a pen test
4	4	1 Understands the format of NMAP, especially around the main scans
5	5	3 Defines the key stages of a pen test within black box testing
6	6	3 Able to analyse a port scan and how it is used
7	7	4 Defines the characteristics of Botnet taxonomy, and classifies different methods
8	8	3 Understands a sample SQL injection attack using a SQL request to read from a database
9	9	2 Understands a sample SQL injection attack using a SQL request to update data on a data
10	10	5 Does a calculation on average marks and is able to infer the gradings for individual marks
11	11	5 Calculates the number of bits used for a certain entropy value
12	12	5 Analyses the ARP request and response, for data that has been modified
13	13	4 Analyses a network trace for the key parameters for Ethernet, IP and TCP
14	14	2 Understands how TCP is identified in an IP packet
15	15	5 Analyses a network trace for the TCP segment flow, and the key parameters
16	16	4 Understands the format of UDP parameters, and can determine changes in them
17	17	5 Analyses a network capture from a port scan from an intruder, and shows the packet sent

NAME	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18
CSAW161 Security and Forensics	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ALEY SEOHATI 07015101	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ANDERSON CLAR 06004330	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AZAREZ ZOKAR 06037904	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
BALAZS GABRIEL 06019163	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
BALLOCH HALL 06054405	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
BAPTE JOOE 06015113	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SARAS GARCARDO 06015059	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
BARTHOLOMEW 06011088	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
BE GIRE DAVID 06009122	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
BERTHELE CLEMENT 06014006	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
BRADLEY CHRISTOP 06004351	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
SKA ANTHONY 06012112	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
BRADY PASCAL 06014028	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CLERIC GUILHEM 06009119	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
COSTA HENRI 06014281	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
COVIE KAREN 06008042	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CROSSAN GRANT 07014051	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
CROWE SEAN 06001247	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DOHERTY JOSEPH 07019130	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
QUOCHI JEREMY 06015026	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
BAKERY BASTIEN 06021217	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

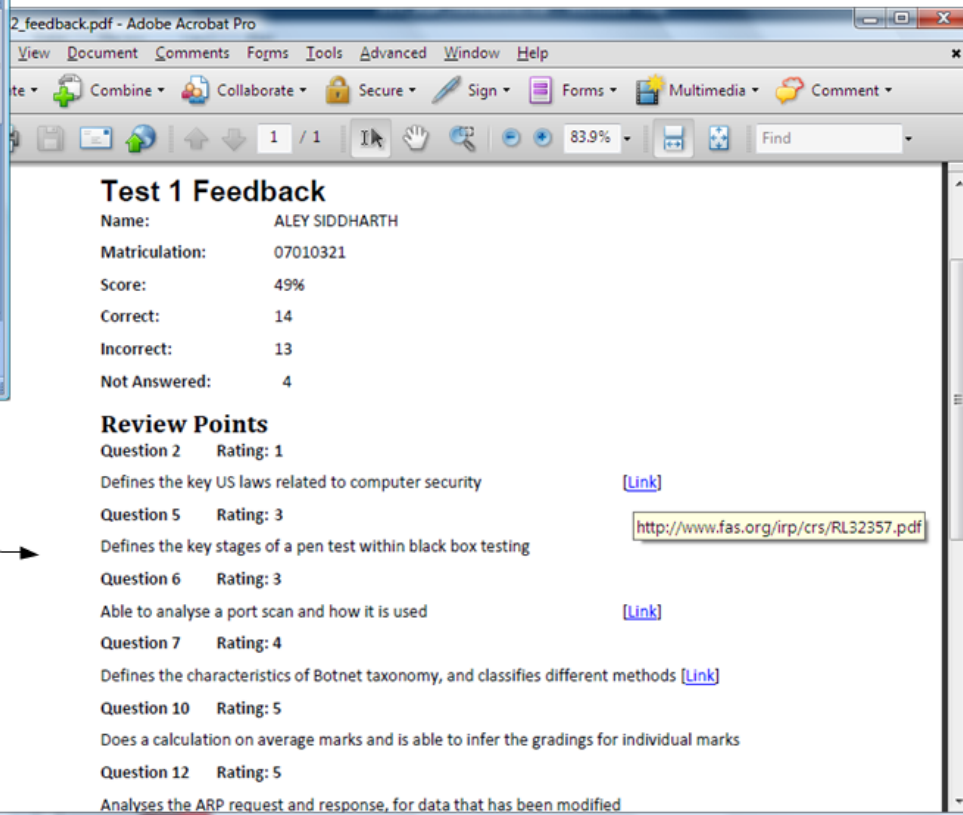
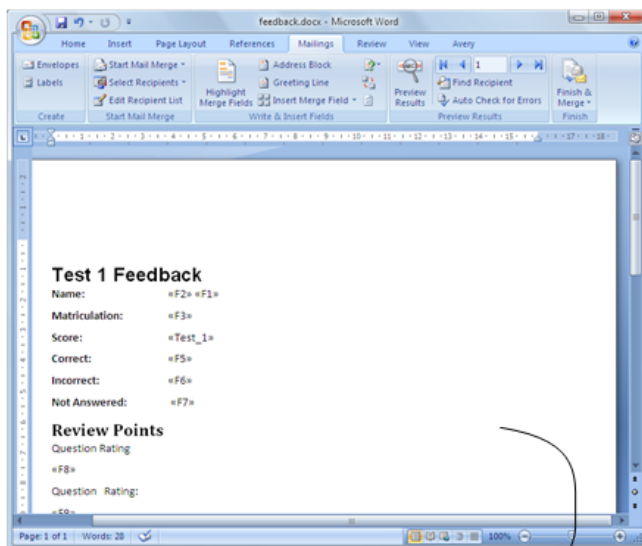
Feedback elements

Feedback...

	2011																	
Question	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Correct	50	55	46	57	45	38	31	41	45	10	16	18	30	56	14	26	23	55
Not ans	8	9	8	8	10	8	10	12	11	13	25	12	8	9	9	8	10	8
Incorrect	9	3	13	2	12	21	26	14	11	44	26	37	29	2	44	33	34	4
Score	49.1	54.7	44.7	56.8	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	5	5	5	4	2	5	4	5	1

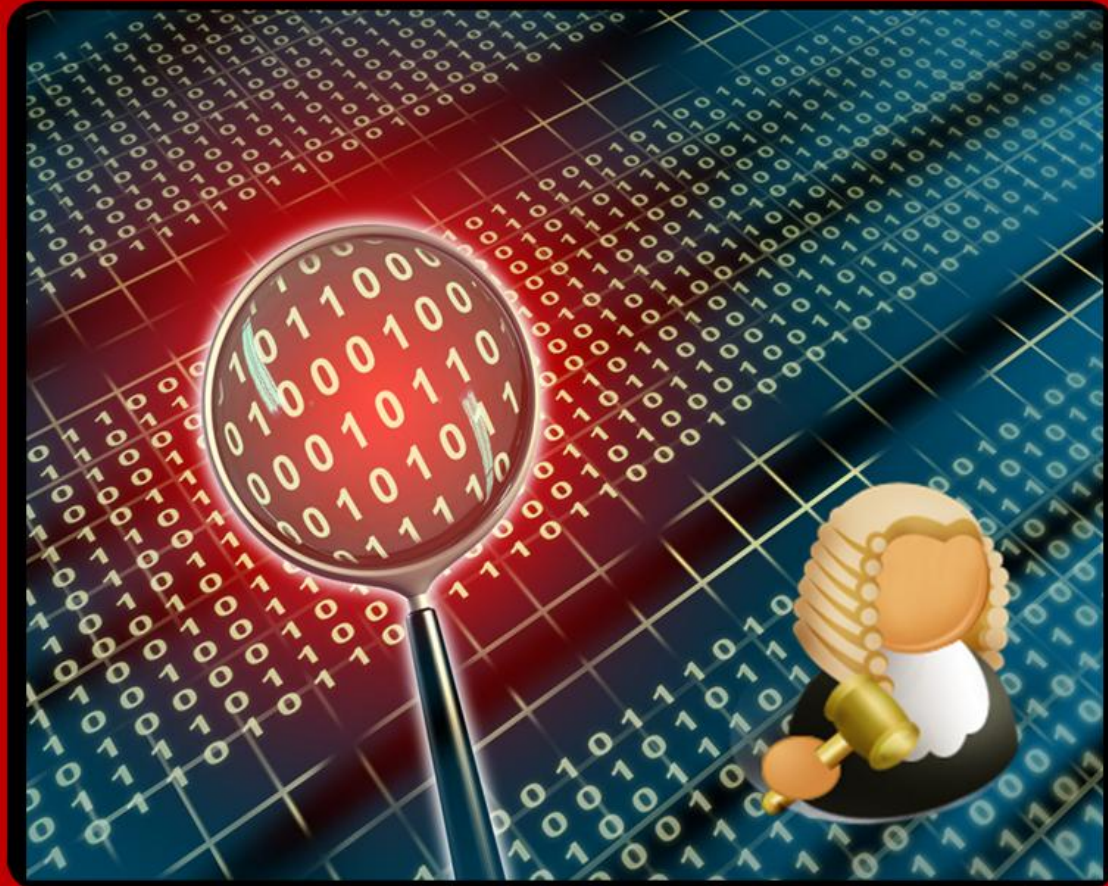


Face-to-face feedback or
over MSN Messenger or
Skype text within one
day of the test.
Sometime by email.

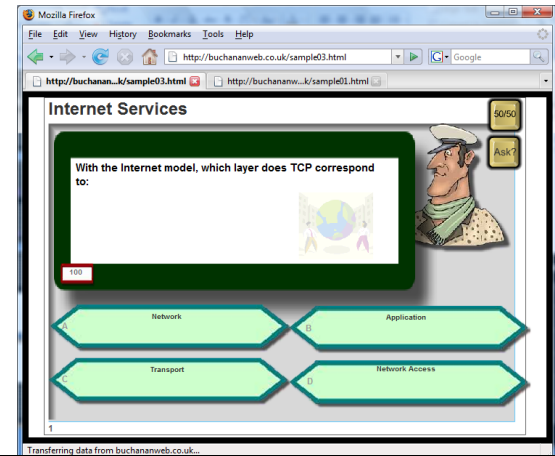
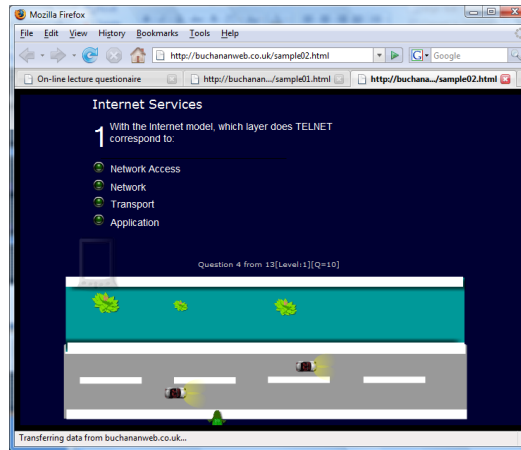
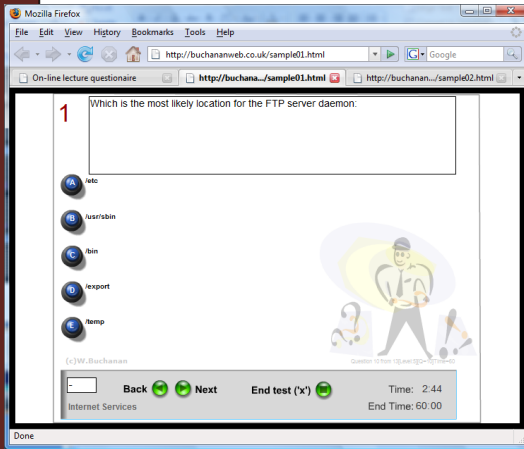


- Emailed to us on the day of the assessment. Awesome.
- Bill gives very fast feedback.
- Yes. Same day results.
- Indeed, concise, and well presented.
- Excellent feedback on the tests, very fast and accurate.
- And so on.

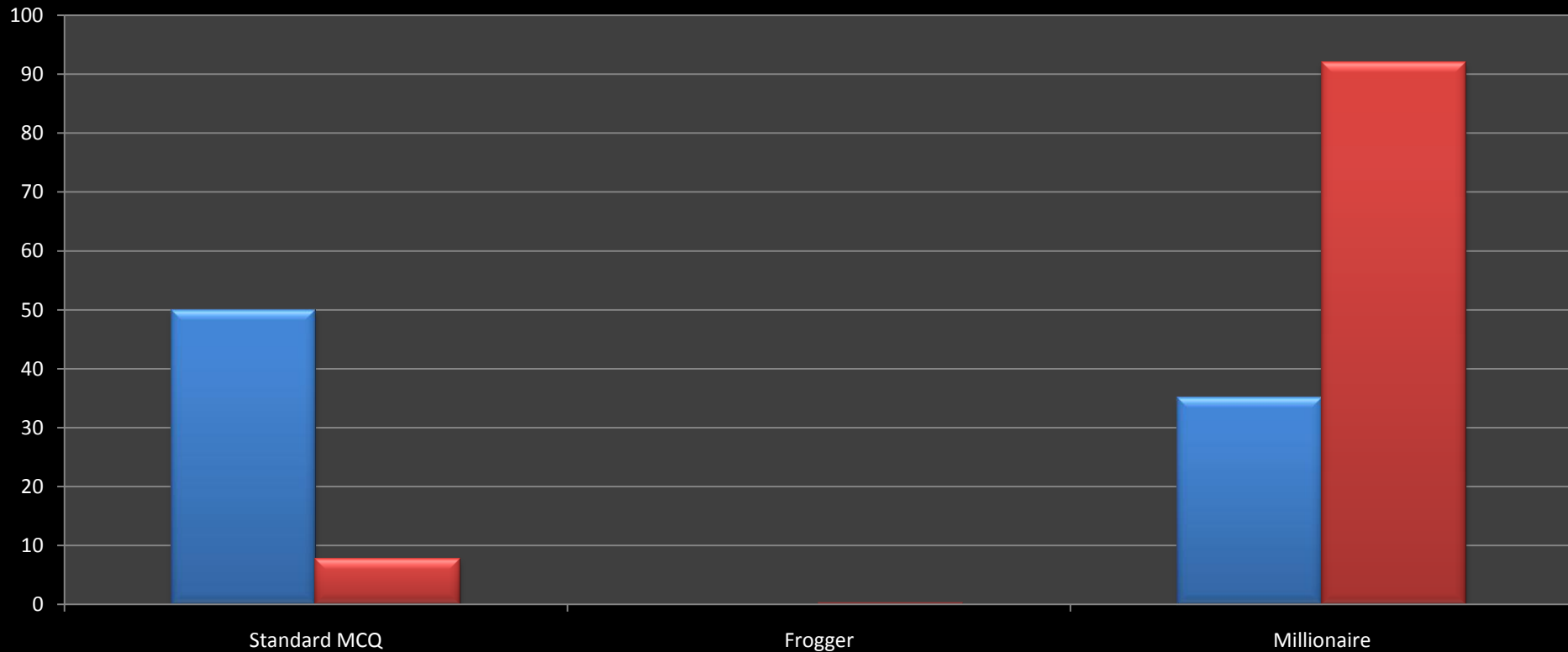
Re-enforcing...



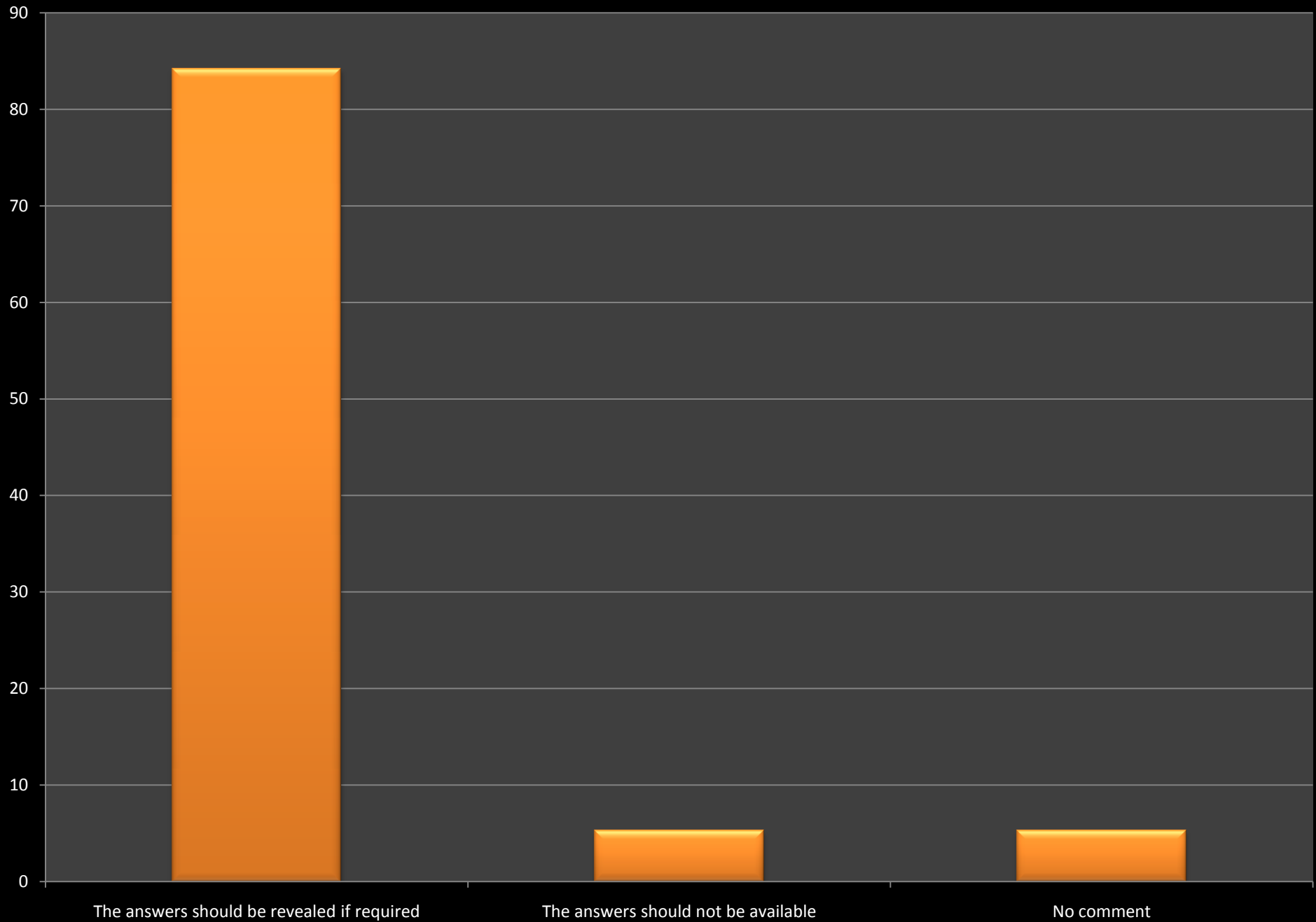
Some results

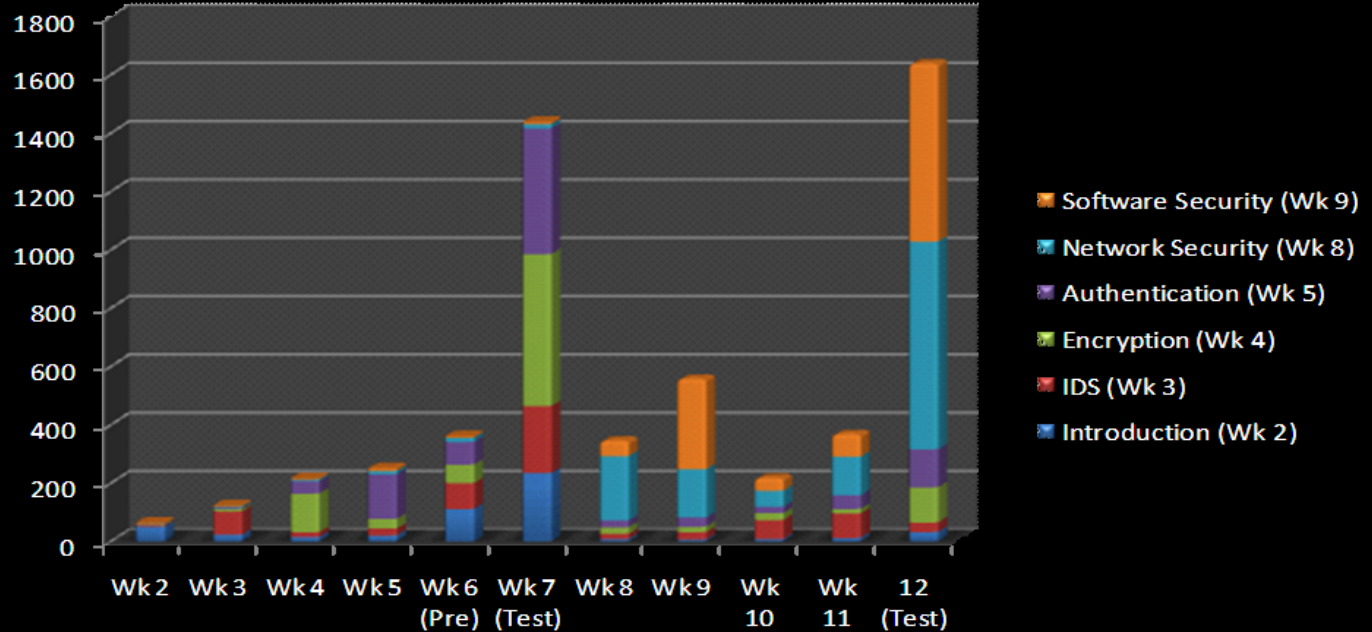
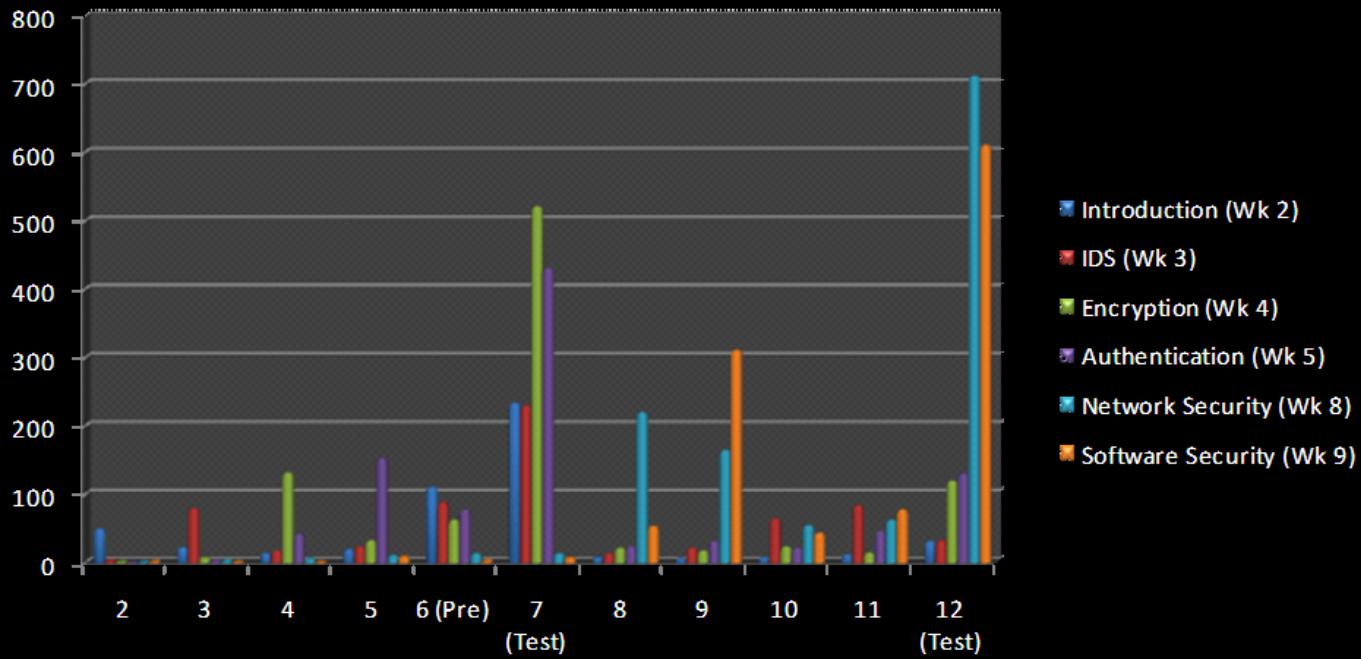


21. Which is the most useful for exam study (/accesses before exam)



23. With on-line tests which should be true:





Online lecture usage

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

