Centro de Estudios de Postgrado
Máster Interuniversitario en Enseñanza Bilingüe y AICLE

UNIVERSIDAD DE JAÉN

UNIVERSIDAD DE CÓRDOBA

Master's Dissertation/
Trabajo Fin de Máster

FOSTERING ACADEMIC LANGUAGE IN CLIL; A PROPOSAL FOR A CYBERSECURITY COURSE.

Student: **Gaitán López, Francisco Javier**

Supervisor: Dr. Y.L. Teresa Ting
Department: Dept. of Chemistry and Chemical Technologies, The University of Calabria

February, 2020

MIEB

Content

1. Introduction

Contents studied in secondary education are new and potentially complex to students, just at the same time as students experiment the transition from concrete to formal operational stages (Piaget, 1936), when pupils develop their ability to think about abstract concepts, and logically test hypotheses. Indeed, at the compulsory secondary education level (CSE henceforth) students start learning about concepts such as the cell structure, electric current in circuits, mathematical functions, the atom structure, or probability. These complex, intangible concepts cannot be spontaneously discovered by students but must be explicitly taught. Consequently, learning-teaching practices should be *aware of content complexity*.

Sophisticated concepts involve abstract thinking, which is formulated by language. In order to both understand and verbalize concepts, it is necessary to master the language in which those concepts are expressed. At the same time, this language is not colloquial but *academic language*, which represents a foreign language for students, even in their mother tongue. Hence, learning-teaching practices should be *language-aware* so as not to alienate students from school.

This applies to learning through L1. Accordingly, it seems evident that a CLIL class cannot just consist of *doing the same, but in English*[1], as it would expose students to a double FL: academic language and English. In addition, students must acquire not only receptive but also productive skills in the foreign language, providing the globalized labour market they are to become part.

In the first part of this Master Dissertation, a literature review relating CLIL and the importance of academic language awareness in complex content instruction is written. In the second part of it, a proposal of a learning sequence on a specific content from a Vocational Education and Training (VET) Cybersecurity course is presented, taking into account the previous considerations.

[1] English will be considered the L2 henceforth.

2. Literature review: Academic Language

The following sections in this chapter analyse some considerations about learning complex concepts and their representation by language. While these reflections are valid for learning through L1, later during Chapter 4, the addition of a foreign language will be discussed.

2.1. The connection between complex concepts and language

The contents in the curriculum of CSE present a complexity level high enough to make learning difficulties appear. Students start learning about abstract, intangible concepts such as the elements in the periodic table, mathematical inequalities, sociologic consequences of complex worldwide events, or probability. Opportunely, it is the time when students experience the transition from childhood to adult life, when they not only grow their identity and construct their life socially and culturally but also develop cognitively (Piaget, 1936). Triggering this intellectual upgrade properly is of paramount importance in order to make students succeed at school, and more importantly, to learn complex concepts.

Constructivism is a widely accepted model of school learning today. Scaffolding in the zone of proximal development (Vygotsky, 1979) should be provided to learners so that *they* move forward in *their* learning progression. Consequently, the focus is on learning rather than teaching; specifically, there are relevant interactions that occur in the triangle between the teacher (as facilitator) – the student(s) – the disciplinary subject.

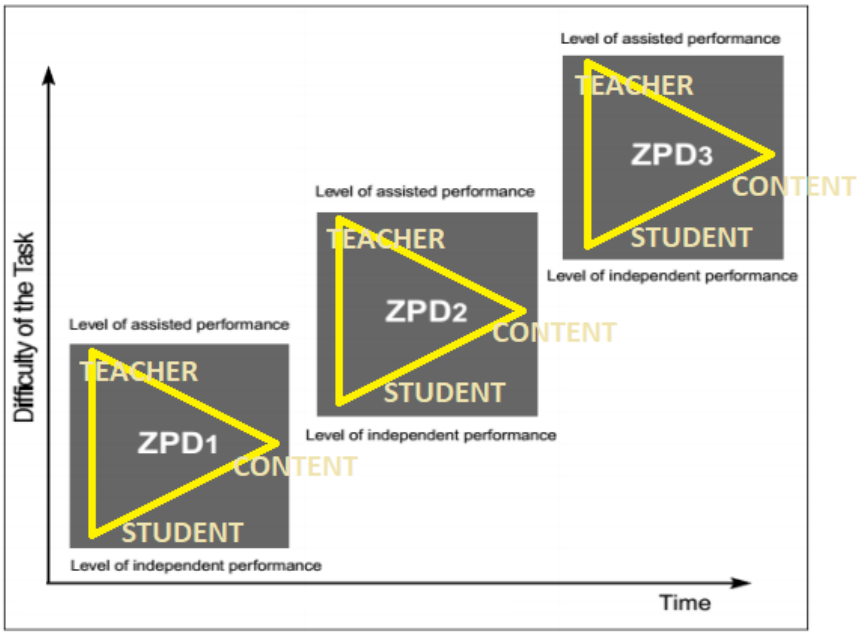


Figure 2-1. Changes in a students' ZPD over time. Adaptation from Leong (1998)

Onrubia (1993) proposes some guidelines to design those interactions and learning situations, related to how the new concepts are linked to the students' context, to previous knowledge, or *how the language is used*. Actually, he discusses the importance of regulating the language so that it is used "as clearly and explicitly as possible" and "to continually re-contextualize and re-conceptualize" learning experiences. In addition, he promotes cooperative learning techniques where students are encouraged to make explicit their insights through the language, and to compare them with the rest of the students' speech. In the same way, Mazur (1997) proposes what he calls "Peer Instruction", in order to shift instruction from traditional-delivered lessons to peer-discussed classes, where contents are negotiated through discussion, that is, through language.

2.1.1. Pedagogical implications of brain based learning

When concepts are complex, it is especially important for instruction to pay attention to the following implications on *how* the human brain learns. Cognitive load memory theory (Sweller, 1994) is focused on how the brain processes and stores information. In this framework, memory is divided into working memory, the system where the processing of new information takes place, and long-term memory, the system where large amounts of already learnt knowledge are stored. Learning new concepts involves a cognitive load in working memory, defined by Clark, Kirschner, & Sweller (2012) as "the **limited** mental space in which we think" [my bold]. Working memory is recognised to be able to manage a certain amount of information at once, depending on the individual. It is admitted that cognitive overload in working memory causes confusion and concepts not to be understood, and the impossibility to transfer new knowledge to the long term memory. This transferring occurs through *schema construction* and *automation*. For instance, trying to remember the combination of letters *n-g-i-e-l-r-n-a* requires our working memory to load eight items at once. In turn, trying to remember the letter combination *l-e-a-r-n-i-n-g* will make use of the schema from the long-term memory for the word 'learning'. As a result, working memory is required to remember only one item, so it can process more information.

Sweller (2010) proposes three different types of cognitive load: intrinsic, extraneous and germane load. Their characteristics are described in Table 2-1.

Load type	Source	Effect on learning	Example
Intrinsic load	The inherent complexity of the disciplinary concepts that must be learnt.	Necessary to learning, but problematic because it can cause cognitive overload. Since students must learn these complex concepts, it is the "lightening" of this intrinsic load that is at the heart of "good education".	Learning how to solve the mathematical equation a/b=c, solve for a. Learning this equation might have a high intrinsic load for a novice maths student, but would have a low intrinsic load for an expert mathematician
Extraneous load	Poorly designed instruction that does not facilitate schema construction and automation.	Harmful because it does not contribute to learning.	The student is required to figure out how to solve the equation themselves, with minimal guidance from the teacher. This imposes a high cognitive load, but does little to encourage schema construction because the student's attention is focused on solving the problem rather than on learning the technique.
Germane load	Well-designed instruction that directly facilitates schema construction and automation.	Helpful because it directly contributes to learning.	The student is explicitly taught how to solve the problem and given lots of worked examples demonstrating how to do it. This imposes a lower cognitive load on the student, enabling them to learn and remember how to solve the problem when faced with it again.

Table 2-1. Types of cognitive load. Adapted from (Centre for Education Statistics & Evaluation, 2017).

The restricted amount of information that working memory is able to hold at once, and the pertinence of using the germane type of cognitive load determine aspects that should be addressed while designing teaching materials or during instruction, like the suitability of explicit instruction:

> Decades of research clearly demonstrate that for novices (comprising virtually all students), direct, explicit instruction is more effective and more efficient than partial guidance. So, when teaching new content and skills to novices, teachers are more effective when they provide explicit guidance accompanied by practice and feedback, not when they require students to discover many aspects of what they must learn. (Clark et al., 2012)

In this same vein, and linked to the idea of explicit teaching, Hattie's work (2009) on *visible learning* states that instruction should be transparent: the objectives should be explicitly exposed to the students, the didactic proposals must be challenging, and the feedback should be provided throughout the process.

Despite these considerations on learning complex concepts through constructivism or following an explicit, yet student-centered, instruction model should not force teachers to advocate exclusively for one or the other. Depending on the subject and the complexity of the concepts, a discovering approach might be suitable. For instance, in elementary school, students might learn different fruit characteristics (color, texture, taste, etc.) manipulatively, with occasional teacher instruction. Contrarily, in secondary school, students cannot learn about nutrients, metabolic processes, carbohydrates or lipids *by discovery*.

In this sense, Geary (2008) models knowledge into *biologically primary knowledge* and *biologically secondary knowledge*. He proposes the former being "Humans' brain and cognitive systems that have evolved to attend to, process, and guide behavioural response to evolutionary significant information" and the "core domains of human cognition, and coalesce around folk psychology, folk biology, and folk physics" (p.180). Self-awareness, automatically processing of facial information on other individuals, or babies' communication forms with their caregiver are examples of biologically primary knowledge that we naturally develop without explicit instruction thanks to our evolved-for-survival brain.

In turn, biologically secondary knowledge comprehends the set of competencies and abilities not necessary for *immediate* survival and consequently not loaded *by default* in our brains during evolution processes. Geary attributes this aspect to the extremely rapid pace at which cultural knowledge and competencies have been developed in the last thousand years. Examples of biologically secondary knowledge are chemical reactions, mathematical algorithms, phonetics, or magnetic field equations.

Geary's framework might help teachers to realize that it seems unreasonable that students learn biologically secondary knowledge by discovery instead of direct instruction. In Sweller's (2008) words "Since Geary's formulation, it has become clear that theories like cognitive load theory apply solely to the biologically secondary knowledge for which schools and other educational institutions were invented" (p.215).

More interesting reflections on explicit instruction, motivation, and curriculum design after Geary and Sweller's theories are provided by Didau (2017) in his blogpost *Education isn't*

natural – that's why it's hard. The case of **language** is striking: while little children learn how to speak without explicit instruction, simply by immersion in a listening/speaking society, students need to be taught at school how to read and write. According to Geary's framework, the reason for this relies on the spoken language being more ancient than **literacy**, i.e. the ability to read and write, which is a more recent cultural development.

Indeed, literacy plays an important role when learning new concepts, even in non-linguistic subjects, and even in the mother tongue. Thinking is formulated by language, and so is its verbalization. In order to understand a concept, learners ought to understand first the language in which it is expressed – no matter what language it is. In the same way, the learning scaffolding process uses language to increase the student's level of independent performance. Note that with independence on *how* that scaffolding is presented (i.e. through graphics, manipulative demonstrations, worked examples, or multimedia products) concepts must be finally verbalized. Consequently, to effectively learn new content, it is necessary that students absorb both the concepts and the language that expresses those concepts in a precise, non-ambiguous manner, and with academic rigour, that is, the academic language.

2.2. Academic language

A crucial challenge to students learning complex contents is the academic language in which those contents are presented. As Snow (2010) explains:

> Academic language is designed to be concise, precise, and authoritative. To achieve these goals, it uses sophisticated words and complex grammatical constructions that can disrupt reading comprehension and block learning. Students need help in learning academic vocabulary and how to process academic language if they are to become independent learners.

Interestingly, the connection between academic language command and learning independence is presented, focusing on the use of sophisticated words and complex grammatical constructions, such as nominalizations or subordinations. It is of paramount importance that teachers raise awareness about both the former and the later. Traditionally, content teachers might be tempted to focus just on specific-field sophisticated words, while academic-purpose words or grammatical structures are considered to have their place in linguistic subjects. Nevertheless, as "Academic Language is no one's mother tongue" (Bourdieu & Passeron, 1977, p.115), or in Ting's words (2011, p.2), "the language of science turns our mother tongue into a foreign language", it is necessary to explicitly and actively teach it, as it would be the case of any other foreign language. Consequently, while linguistic areas

address academic language development, even in L1, it is also part of content subjects to provide the required skills so that the students cultivate competence in deciphering complex content input written in the "foreign language" of *academic language*.

Sato & Curis (2008) define academic language as "the language needed by students to do the work in schools", including "discipline-specific vocabulary, grammar and punctuation, and applications of rhetorical conventions and devices that are typical for a content area (e.g., essays, lab reports, discussions of a controversial issue.)". Along with the definition, they highlight the importance of developing students' academic language abilities, advising that learning objectives should be focused not only on content but also on language. In addition, these authors discuss the convenience of language-based tasks, which will be illustrated in Chapter 3 of this thesis through the proposed materials.

Snow (2010) reflects on how science teachers often pay attention to key, scientific, bolded words in a text without recognizing those words just being a component of the "linguistic puzzle that science texts present. […] [scientific words] are defined with general-purpose academic words that students also do not know" (p. 452). Therefore, efforts to help students understand complex content cannot disregard their need to understand the words used to write and talk about those contents: the all-purpose academic words as well as the discipline-specific ones.

With regard to this idea, Beck, McKeown, & Kucan (2002) propose a three-tiered model of vocabulary development.

- Tier 1 consists of everyday, common words that do not require instruction, such as *apple*, *car*, *run*, *see*, or *happy*. Students learn these words before school.
- Tier 2 consists of general-purpose, multi-disciplinary words that appear in different types of school texts, often representing a subtle or precise manner to say relatively simple things (e.g. abundance, combine, react, supplies).
- Tier 3 consists of easily identifiable words related to domain-specific vocabulary (e.g. algorithm, ventricle, iteration, concurrence) which is usually carefully taught by subject specialists.

Although most content-teachers focus on Tier 3 words, it is Tier 2 words that also poses a challenge to the understanding of academic language for students. Consequently, words in Tier 2 should be taken into consideration when promoting academic language command.

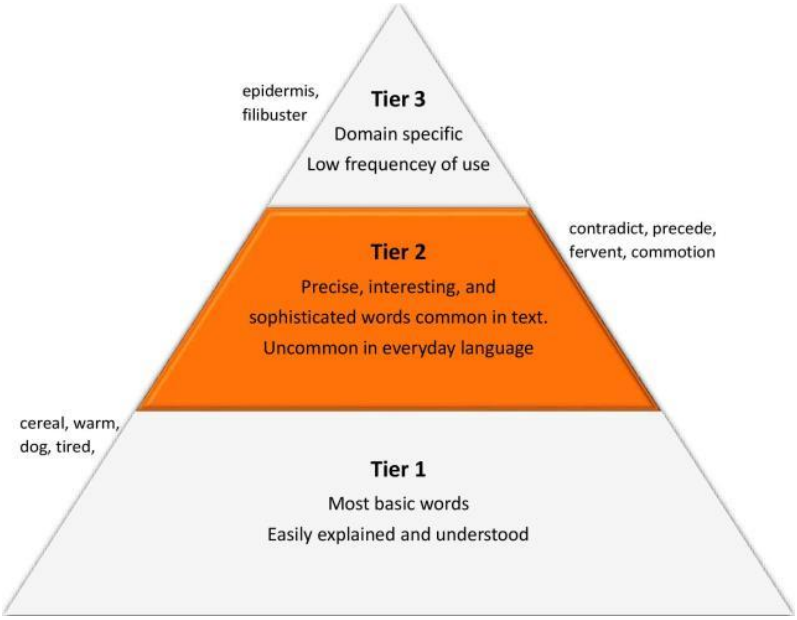


Figure 2-2 Three-tiered word model. Figure by Allison, Runeckles, Haynes, & Tharby (2017)

The proposed tier model can be used to analyse the complexity of texts, as well as their density in terms of academic vocabulary. As aforementioned, it is crucial that vocabulary in Tier 2 is addressed.

Similarly, Coxhead (2000) compiles a list of academic words that represents the "570 high-incidence and high-utility academic word families that are not in the most frequent 2000 words of English but which occur reasonably frequently over a very wide range of academic texts". Along with the 3-tiered model, Coxhead's set of words could be taken into consideration when fostering academic language through tasks (Beck, McKeown, & Kucan, 2019; Huynh, 2016).

The previous sections describe how academic language builds a discourse that is precise and effective to discuss academic topics. However, even in L1, it represents a foreign language for those users outside academic contexts or without sufficient academic proficiency, as is the case of learners. Halliday & Martin (1993) describe academic language as *alienating* and *centrifugal*. In fact, following Hattie & Yates' (2013) insights, seeing learning through the eyes of students, it is easy to understand that very frequently students face texts containing some words whose meaning might be known individually, but together form a *disciplinary discourse* which is not understandable.

2.3. Disciplinary discourse

The term *communities of practice* was introduced by Lave & Wenger (1991) to designate the group of people who share a profession or interest in a particular domain. Accordingly, the *community discourse* is the specific *way of languaging* that a community of practice uses to share knowledge about their shared/common interest(s). Most people move within and between different discourse communities every day. For instance, the same person might express themselves using different discourse when discussing about the last published manga comic, at the reading club meetings, or during a runners' club training. In turn, disciplinary discourse is the language of academic disciplinary communities, such as mathematicians, psychologists, or biologists. Disciplinary discourse is used to communicate in an efficient, accurate way. For this reason, disciplinary discourse is the *language of schooling*, but at the same time, even in L1, represents a foreign language for those not belonging (yet) to the community, i.e., learners.

Example boxes 2.1 and 2.2 reproduce two fragments of verbalization of concepts, written in Spanish and English on purpose, to make explicit for the reader the fact that it is not sufficient to understand the language (tongue) in which they are written, but also the *discourse*.

Cantidad de movimiento

Véase también: transferencia de momento

La **cantidad de movimiento**, **momento lineal**, **ímpetu** o **momentum** es una magnitud física derivada de tipo vectorial que describe el movimiento de un cuerpo en cualquier teoría mecánica. En mecánica clásica, la cantidad de movimiento se define como el producto de la masa del cuerpo y su velocidad en un instante determinado. Históricamente, el concepto se remonta a Galileo Galilei. En su obra *Discursos y demostraciones matemáticas en torno a dos nuevas ciencias*, usa el término italiano *impeto*, mientras que Isaac Newton en *Principia Mathematica* usa el término latino *motus*[1] (movimiento) y *vis motrix* (fuerza motriz).

La definición concreta de cantidad de movimiento difiere de una formulación mecánica a otra: en mecánica newtoniana se define para una partícula simplemente como el producto de su masa por la velocidad, en la mecánica lagrangiana o hamiltoniana se admiten formas más complicadas en sistemas de coordenadas no cartesianas, en la teoría de la relatividad la definición es más compleja aun cuando se usan sistemas inerciales, y en mecánica cuántica su definición requiere el uso de operadores autoadjuntos definidos sobre un espacio vectorial de dimensión infinita.

Example 2.1 Spanish Wikipedia entry definition for 'Cantidad de movimiento'.

Unjust enrichment

In contract law, **unjust enrichment** occurs when one person is enriched at the expense of another in circumstances that the law sees as unjust.[1] Where an individual is unjustly enriched, the law imposes an obligation upon the recipient to make restitution, subject to defences such as change of position. Liability for an unjust (or unjustified) enrichment arises irrespective of wrongdoing on the part of the recipient. The concept of unjust enrichment can be traced to Roman law and the maxim that "no one should be benefited at another's expense": *nemo locupletari potest aliena iactura* or *nemo locupletari debet cum aliena iactura*.

The law of unjust enrichment is closely related to, but not co-extensive with, the law of restitution. The law of restitution is the law of gain-based recovery. It is wider than the law of unjust enrichment. Restitution for unjust enrichment is a subset of the law of restitution in the same way that compensation for breach of contract is a subset of the law relating to compensation.

Example 2.2 English Wikipedia entry for 'Unjust enrichment'.

Analyzing Example 2.2 English Wikipedia entry for 'Unjust enrichment'. using EAP Foundation (2020) webpage, which performs a search of academic words in a text, thirteen words from Coxhead's (2000) academic word list (AWL) were found (highlighted in the text in Example box 2.3). Tier-3 (T-3) words, law specific domain, are underlined.

In contract law, unjust enrichment occurs when one person is enriched at the expense of another in circumstances that the law sees as unjust. Where an individual is unjustly enriched, the law imposes an obligation upon the recipient to make restitution, subject to defences such as change of position. Liability for an unjust (or unjustified) enrichment arises irrespective of wrongdoing on the part of the recipient. The concept of unjust enrichment can be traced to Roman law and the maxim that "no one should be benefited at another's expense": *nemo locupletari potest aliena iactura* or *nemo locupletari debet cum aliena iactura*. The law of unjust enrichment is closely related to, but not co-extensive with, the law of restitution. The law of restitution is the law of gain-based recovery. It is wider than the law of unjust enrichment. Restitution for unjust enrichment is a subset of the law of restitution in the same way that compensation for breach of contract is a subset of the law relating to compensation.

Example 2.3 Coxhead (2000) AWL and T-3 words in English Wikipedia entry for 'Unjust enrichment'.

Even though the individual meaning of many emphasized words might be known, the disciplinary discourse of law sounds like a foreign language to a reader not belonging to the law community. This is due to the fact that disciplinary discourse is built upon not just the dictionary meaning of the words, but also the ways of knowing about the specific field. As Hyland (2009) claims, "the discourses of the disciplines […] work to interpret the world in particular ways, each drawing on different lexical, grammatical and rhetorical resources to create specialized knowledge" (p. 7). In the same work, two features of disciplinary discourse

are responsible for its difficulty: technicality and abstraction. Technicality establishes a range of discipline specific terms which are ordered to explain how things happen or exist, creating further technicality through defining, classifying and explaining. In addition, abstraction moves from instances to generalizations by gradually shifting away from particular contexts.

On account of these features, as Airey & Linder (2006) explain, simple exposure to disciplinary discourse is not enough for people outside the community to experience disciplinary ways of knowing. Thus, students need practice in using disciplinary discourse to construct meaning for themselves.

3. Personal learning experiences

In this chapter, two experiences related to the topic of this thesis are presented, from the perspective of a learner and as a neophyte teacher.

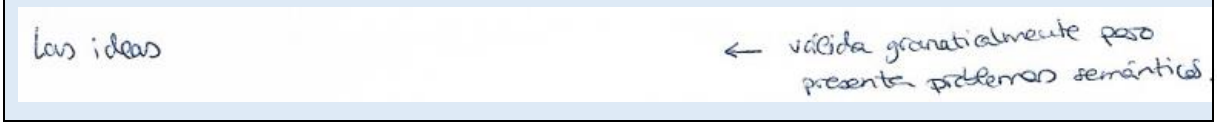
3.1. A linguistics course: personal experience as learner outside the community

Recently, I could experience as a student the fact that disciplinary discourse, even in the mother tongue, might represent a foreign language for individuals outside the community.

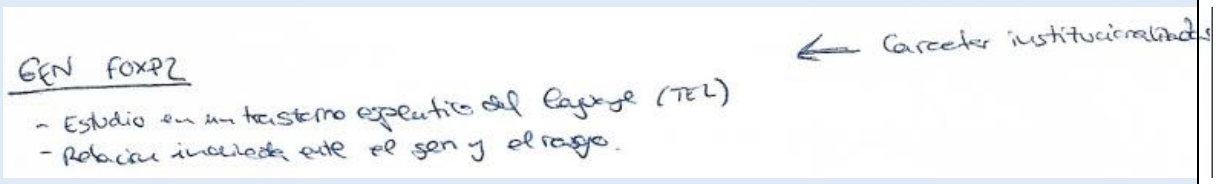
As a pre-service teacher learning CLIL, it seemed a good idea to attend a seminar course called "*Links between language and biology*". It looked to me as if it was a course about how the brain learns languages.

Soon during the first session, I realized that the course had very specific target students, as all the audience belonged to a linguistics Ph.D. program from the University.

All through four sessions, in which the orators were using Spanish, I struggled to understand every commentary being made. Even though I was very motivated to learn, I ended up very frustrated because I could not even take notes of something I was not understanding at all. The following is a fragment from my notes from sessions 1 and 2, where I was not even able to catch a complete sentence:



Other notes, although complete, do not represent any meaning to me now, some time after I took them:



I *do* know the meaning of these words individually but cannot understand the concept they are describing together. Similarly, they talked about "*Universal grammars*", described items as "*Chomskyans*" or distinguished between "*process models*" versus "*product models*". Although I know the individual meaning of the words in italics (universal, grammar, process, product, model, etc.), they represented concepts I did not know at the moment, so I had to try to follow the discourse in spite of the *gaps* I was experimenting in my mental input processing. At some point, the number of gaps was high enough to feel completely lost – cognitive overload in the working memory had just happened.

In turn, the rest of the students seemed to be *following the discourse.* This was a key aspect: speakers and audience belonged to the same academic community, and accordingly, they were using a common specific language.

By contrast, in sessions 3 and 4, the speakers were an ethologist and a physician, who, aware that they were outsiders from the audience community of Ph.D. linguistics students, *modulated their discourse* to make themselves understood. They did not talk about pure, theoretical linguistics but about communication forms in animals and nervous system function principles, respectively. In some occasions, the surgeon explicitly explained language aspects and showed their relationship to concepts in the nervous system e.g. prefixes in the words '*orto*simpático' and '*para*simpático' were related to the relative positions of the systems involved. Because of this modulation on language discourse, I could understand most of their speech.

Although I could not learn much about *Links between language and biology*, this course represented a personal learning experience for this Master Dissertation, providing me first-hand experience with the following insights:

- Disciplinary discourse is a foreign language for those outside the community of practice, even in their mother tongue.

- Although motivation plays an important role in student's performance, even highly motivated, students who are willing to learn (such as I was) can feel alienated and frustrated from direct instruction if it is not comprehensible.
- Discourse can, up to a certain point, be modulated so that individuals outside the community can understand it. i.e. attenuating the "extraneous load" of instruction.

3.2. Reflections on Academic Language during my first teaching position

Teaching complex contents in Spanish

In the month of March in the last academic course (AA 2018-2019), I had the opportunity to start working as a teacher in a Computer Science Vocational Education and Training (VET) programme. It was not CLIL, but it brought me the opportunity to increase my knowledge about teaching-learning practices, and how students learn. In addition, this experience made me realize that the learning of complex content is closely related to learning the academic discourse in which it is embedded.

Having been an enthusiastic teacher, I could not understand why students were performing poorly in the first assessment experience (May, 2019). Results showed that students were not able to solve the expected problems, and what is more important, they were not able to verbalize their doubts.

Following my Master Dissertation supervisor's advice, I started recording my reflections as a "personal correcting diary" which was not originally meant to be part of this dissertation, but work for myself, that would guide my frustrating reflections into insights on how to foster learning experiences. This is in line with the use of the very qualitative research methodology of "narrative inquiry" for professional development (Johnson & Golombek, 2003; Ting, 2005). For this reason, the diary was written in informal English. The interested reader can find the diary with raw data in Annex I.

Old-school teaching

Thanks to this initial practice as a teacher, I experienced that classroom implementation of the theories studied in teacher-training programs is not trivial nor as easy as they seemed. Learning processes take place in a context and in heterogeneous groups which add many variables to the teaching-learning situations.

For instance, student-centered methodologies and cooperative learning are widely studied in teacher-training programs, both general and CLIL. However, once in the classroom, it took some time to realize that I was just delivering lectures. In spite of all the previous readings, not until the exam correcting did I comprehend that what I was actually doing was frontal explanation, which does not convey knowledge to someone outside the discipline community.

In some cases, it was frustrating reformulating the input trying to make myself understood without success. Interestingly, there were some occasions where I could witness students finally understanding a concept after another student's clumsy explanation. This "talking to your neighbour" approach might be useful in the future, and so peer instruction (Crouch, Watkins, Fagen, & Mazur, 2007) will be taken into account as a form of cooperative learning.

Humbly, this indicates that I could have still "gone less accurate but understandable", trying to "see learning through the eyes of the student" (Hattie, 2009), and consequently, making sure that a proper didactic transposition (Chevallard, 1997) to students' level was carried out when presenting complex concepts to students.

Academic language awareness

Focusing on academic language, students struggled to understand the meaning of the following Tier-3 (T-3) words, in Spanish:

Algorithm, data structure, abstract, array, iteration, loop, Cartesian product, projection, selection, join, subquery, recursion

At the same time, only 2 out of 19 students managed to solve a typical programming problem consisting of three operations: reading a file, loading its content on memory, and populating

a *HashMap* structure (a data structure containing items of the form {key, value}) with data read from the file.

Today, after all the readings about academic language, the connection between the two aforementioned facts seems obvious. When trying to solve the *HashMap* problem, students were provided with my instructions, full of computer science T-3 words, linked between them with T-2 academic, scientific words. That is to say, students heard a discourse full of gaps, in enough number to overload their working memory.

An example of an alienating activity, using the term *loop* would be as follows:

"A *loop* consists of a set of instructions that are executed repeatedly until a condition is met. Instructions are embedded between delimiters. The following piece of code is an example of a loop that prints 'Hello World' on the console indefinitely.

```
while (true){
      print("Hello World");
}
```

Now, modify this piece of code so that the loop executes two instructions each step: it should print *Hello World* and *Bye Bye World*".

A didactic transposition was accomplished, providing that there are many more characteristics to learn about loops but this might well be an initial set of aspects to be covered. However, even though this fragment might represent a more digestible piece of information - addressing only one of the concepts involved in the *HashMap* problem, note how the cognitive demand remains high. Language awareness still is crucial because in this brief excerpt five words from Coxhead's (2000) AWL were used (consists, instructions, code, indefinitely, and modify).

Future insights

In the future, a different approach will be addressing the learning of unknown words or features of language one at a time, in a low content cognitive demanding context, instead of during the high-cognitive problem-solving task. This approach might help the teacher to detect the moment in which learning difficulties appear, and to scaffold from that point.

Only after the student has effectively learnt necessary crucial concepts, will they be able to understand other task complex instructions like "*Your algorithm needs to iterate over the lines in the file to populate a data structure, like an array. Then, try to find duplicates through a projection, and finally construct the HashMap structure from the pairs <key, value> that you must have calculated*" that are completely incomprehensible to someone outside the discipline, like learners.

A summary from my diary, of other reflections not directly related to language but linked to instruction, assessment, or motivation, from the perspective of a novice teacher, can be found in the "final reflections" section in Annex I.

4. Learning through a Foreign Language with CLIL

CLIL (**C**ontent and **L**anguage **I**ntegrated **L**earning) reveals the necessity to address the learning of both the content and the language/discourse needed to talk about the content, in consonance with the considerations explained in the previous chapters, which were valid for learning thought the mother tongue. Similarly, learning through a foreign language requires the command of *that* language, apart from other aspects that will be explored in this section. The problem is that, as students are expected to learn more complex concepts, the language in which those new concepts are embedded becomes more sophisticated, increasing the risk of alienation.

The simple substitution of the vehicular language for English might result in EMI lessons (English as a Medium of Instruction), consisting of "academic subjects taught through English, one making no direct reference to the aim of improving students' English" (Dearden & Macaro, 2016), but not in a *Content and Language Integrated Learning* "a dual-focused educational approach […] a fusion of both subject content and language learning" (Coyle, Hood, & Marsh, 2010). More than that, students would be exposed to a double foreign language: academic language and English.

The recent publication of PISA 2018 results (OCDE, 2019), has revealed that only

> 8.7 % of students, on average across OECD countries, were top performers in reading, meaning that they attained Level 5 or 6 [out of 6] in the PISA reading test. At these levels, students are able to comprehend lengthy texts, deal with concepts that are abstract or counterintuitive, and establish distinctions between fact and opinion, based on implicit cues pertaining to the content or source of the information. (p. 86)

One reason for this lack of deep reading skills might be the extent to which digital technologies are transforming the world. For instance, the last PISA survey reveals a 5% increase in students who consider reading a "waste of time", just at the same time as exposure to digital screens has augmented in an hour during weekdays (OECD, 2020). In addition, Pertierra (2019) reflects on the incapacity of today's youth to focus on reading, since hypertext multiplies the sources and thus focusing times are drastically reduced. This is in line with Hattie & Yates' (2013) visible learning chapter '*Is the Internet turning us into shallow thinkers?*'. Whatever it may be the cause, it is of paramount importance that this issue is addressed from school, providing the globalized, volatile, post-truth world in which students live, consume, and will vote.

Being instructed through the years by academically proficient teachers, and tested in their mother tongue, PISA students still obtain the aforementioned modest results in deep reading. Consequently, regarding CLIL implementation, it seems clear that *just* delivering lessons in English will not improve the students' receptive literacy. In fact, it could cause the opposite effect, as students simply might not understand a word. Thus, a key aspect for promoting learning in the classroom is *how* language is used in order to make content comprehensible, rather than the teacher's mastery of the foreign language (Pérez Cañado, 2016).

According to Shanahan & Shanahan (2008), content-subject teachers usually do not pay enough attention to teaching the language of instruction, based on the misconception that it is a matter of the language subjects. What is more, usually, as content acquires more depth, less attention is paid to language, in favour of that complex content. It is crucial that content-subject teachers become involved in teaching their discipline-specific language, as experts in their fields. This applies both to education through the mother tongue and a foreign language.

In fact, Grandinetti, Langellotti, & Ting (2013) highlight how CLIL, *even in a sub-optimal bilingual context*, can serve as the catalyst to renovate education because of language awareness. Thanks to the foreign language, CLIL teachers usually become language-aware: they need to present content using comprehensible language as well as constantly evaluate whether that language is being understood. As a result, content is also presented in digestible chunks of information whose assimilation equally needs to be evaluated. Consequently,

any process that constantly evaluates both the comprehensibility of both language and content plus how well learning is taking place, focuses on the process of learning rather than the act of teaching. This alone makes for better education (p.372).

Such content and language awareness enables CLIL teachers to distinguish between CLIL (*content* and *language*) materials or just mere translations from the mother tongue originals. Figure 4-1 shows an example from a "Bilingual" Spanish Maths textbook which consists of a mere translation of the textbook written in Spanish, with occasional English vocabulary notes, like the one in the right margin stating that *dice is the plural of die, and the dots on a die are called pips*. As already discussed, just using this textbook might suppose learning through a double foreign language for a non-native student: English, and the academic language in which textbooks are written. In addition, the importance of learning that dots on a die are called "pips" is questionable.

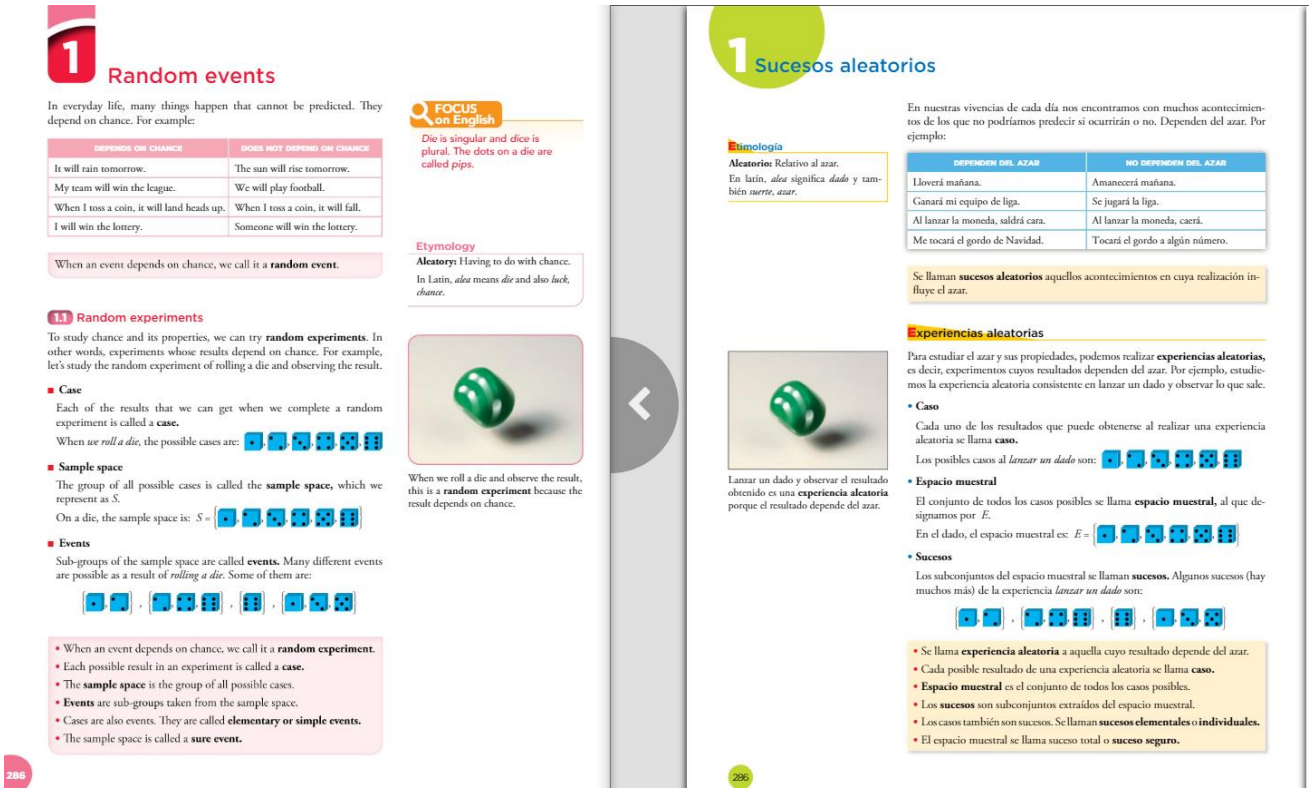


Figure 4-1. Equivalent pages from Spanish and "bilingual" math textbooks (Colera, 2015, 2016)

Figure 4-2 shows a worksheet from a secondary school "bilingual" book on the topic of the heart. Again, the schema is very similar to a Natural Science book in L1: unfamiliar topic information is first presented in a text form, embedded in disciplinary discourse, but in this case also in a foreign language. In addition, the picture accompanying the text is confusing for learning, as it is difficult to follow the blood flow in and out of the heart because of the

perspective drawing of arteries and veins. Schemata should be simplified for learning reasons, since an enhanced drawing of the heart structure is far from representing the organ, but can on the contrary blur learning. Moreover, tasks 1 and 2 involve low order thinking skills (Bloom, 1979); As the sentences needing to be completed are written exactly like in the text, a student could perfectly *school though* these two tasks, filling in the gaps correctly, but without having learnt a single new concept about the heart.

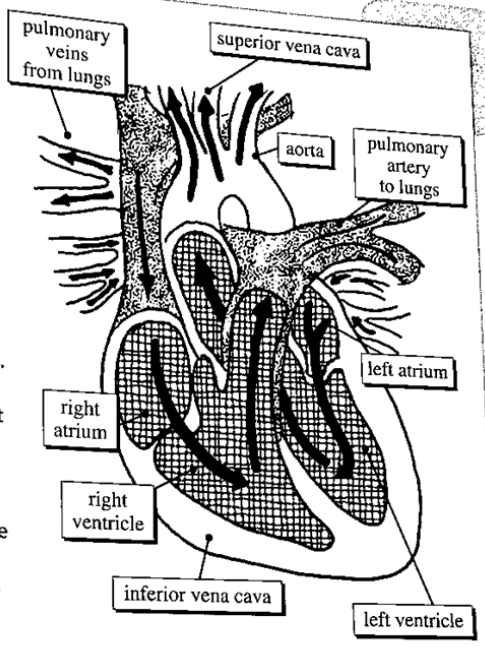
Natural science

THE HEART

The heart is a muscle about the size of your fist. The heart pumps blood around the body. Blood provides the body with the oxygen and nutrients it needs. The heart beats between 70 to 80 times every minute. When we exercise or when we are scared or excited, it beats faster.

The heart has four main parts: the left and right atria at the top and the left and right ventricles at the bottom. A thick wall of muscle called the septum separates the left and right sides of the heart. The right side of the heart receives blood from the body and pumps it to the lungs. The left side of the heart does the opposite – it receives blood from the lungs and pumps it out to the body.

When the heart relaxes, blood returns to the heart from the lungs through the pulmonary veins, and from the rest of the body through the venas cavas. When the heart contracts, blood leaves through the pulmonary artery. This takes it to the lungs and to the aorta, which then takes it to the rest of the body.



1 **Complete the sentences.**

1. The heart beats between ..... to ..... times every ..... .
2. The heart has four main parts: the left and right ..... and the left and right ..... .
3. The left and right atria and ventricles are separated by the ..... .
4. When the heart relaxes, blood returns to the heart through the ..... and ..... .
5. When the heart contracts, blood leaves it through the ..... .

2 **Match A to B.**

A

1. Arteries take the blood
2. Veins take the blood

B

..... a. from the body back to the heart.
..... b. from the heart to other parts of the body.

Let's Investigate

Use an encyclopedia or the Internet.
How much blood have we got in our body?
What does it consist of?

.....
.....
.....
.....

35

Figure 4-2. “The heart” page on a Natural Science “bilingual” book for secondary school.

4.1. Catering to diversity

Traditionally, students belonging to a high socio-economic environment could carry a higher cultural capital of literacy (Bourdieu & Passeron, 1977), also in terms of foreign language command, since their families could afford extra lessons outside school. The irruption of CLIL in public schools democratically addresses this issue, as there is grounded evidence of the contribution of CLIL programmes to students' content and language learning, with independence of their socio-economic status (Pérez Cañado, 2018a, 2018b, 2019).

CLIL trained content-teachers are more alert to the need for *explicitly* teaching the "language to language about contents" in the classroom, following a visible pedagogy which clearly states the content to be learned, the criteria for success, and the language involved (Schleppegrell, 2004). It is crucial that teachers understand that the opposite, implicit pedagogy, does not cater for diversity, as it "puts at risk all but those students whose socialization has prepared them to […] engage in the kind of discussion that prepares them for tasks in school" (p.156).

In addition, the shift that CLIL yields from traditional lecturing to task-based learning helps teachers to address different learning paces in mixed ability groups. Instead of receiving the same input, now students are provided with different levels tasks, adapted to their progression point in content and language acquisition.

4.2. Importance of academic productive skills

Expecting productive academic literacy should be part of education, even though the mother tongue. After teaching students Chemistry in Spanish, they should be able to use Spanish to write about Chemical Reactions academically. Similarly, CLIL implementation seeks complete academic language literacy in L2, involving receptive and productive skills.

Indeed, CLIL application across Europe is motivated, among other reasons, by the European strategy to establish the need for EU citizens to be proficient in three European languages: the mother tongue and two foreign languages (European Commission, 1995). It seems reasonable than not only receptive but also productive literacy should be cultivated so that Europeans can use language to communicate effectively. A reflection about CLIL objectives is made by Ting (2014) as follows:

> If the main motivation to learn English is to get a good job, then the motivation to learn physics, maths, economics or history, etc. through English would be to get a better job. If science and philosophy are already difficult or boring in our mother tongue, why should we try to learn these

> through a foreign language if, in the end, our learners are not able to then use English to speak and write about that knowledge, and do so quite well? Otherwise, why should we bother? An Italian engineer will get a job in an International construction firm in Thailand only if, after he says, "my name is Francesco", he is able to write decent reports in English. Productive literacy is therefore a primary learning objective of CLIL (p. 108).

Consequently, content subjects must explicitly foster academic literacy through their specific-field language, as academic language is a complex construction that needs to be learnt and trained through systematic instruction at school (Wellington & Osborne, 2001).

4.3. Fostering academic language in content-subjects

The problem with productive academic literacy is that it is difficult and slow to develop. The reason for this difficulty relies on the fact that it is constructed on academic language, which, as aforementioned, represents a foreign language for students, even in their mother tongue. Because of its difficulty, teachers have to modulate the disciplinary discourse from textbooks so that students are able to comprehend complex concepts, but at the same time this enlighten prevents them to learn disciplinary discourse. This is related to what Ting (2017) calls "the education dilemma".

Schleppegrell (2004) discusses non-native students' difficulties to deal with academic language:

> For those students with academic language experience in their first languages, it can be very frustrating to be unable to express themselves in English with the complex syntax and lexis that they can draw on in their first language. An even greater challenge faces the many immigrant children in today's schools who have not had the opportunity to develop academic registers in their first languages. Even when they have achieved a good level of fluency in spoken English, they may have difficulty with academic language tasks. (p. 81)

Even though this last finding refers to immigrant students with no L1-CALP development, which is not exactly the case of CLIL students, similarities arise since, as already discussed, students often feel alienated from academic language, even in L1. Thus, the CLIL addition of the foreign language raises the necessity to be aware of possible learning difficulties in students that apparently master the language: while a student might be able to keep a class conversation or follow instructions, they might not necessarily be able to handle the content language of the textbook.

In this same vein, Cummins' (1979) BICS and CALP distinction in his research about immigrant students to Canada helps CLIL teachers to raise awareness about processes that foster academic language.

BICS (Basic interpersonal communicative skills) are considered as the required abilities to effectively communicate on every day situations, that is, conversational fluency. It is cognitively undemanding and relies on the context. With sufficient exposure to the foreign language, learners can master BICS in 1-3 years. In turn, cognitive academic language proficiency (CALP) refers to the ability to use language in a sophisticated manner in academic contexts, to deal with academic demands.

BICS/CALP distinction is usually schematized as a four-quadrant diagram whose axes represent degree of cognitive load and degree of dependence to context. In Figure 4-3, a face-to-face conversation task is situated as a cognitively undemanding, context embedded activity involving BICS, while writing a standardized test might represent a difficult task which involves CALP, being a cognitively demanding and context reduced activity.

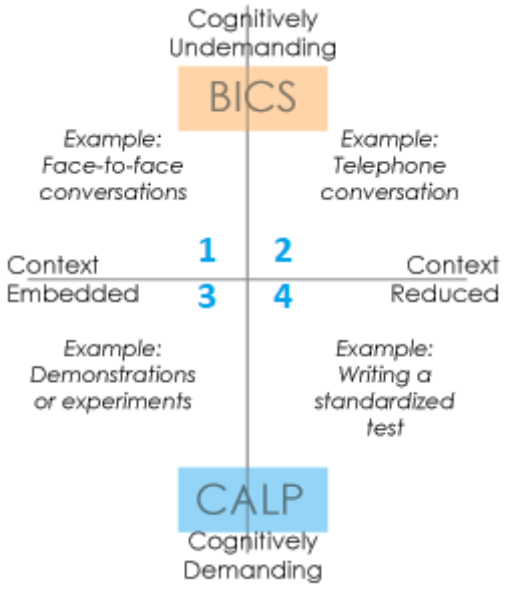


Figure 4-3. BICS/CALP quadrant representation (adapted from Bilash, 2011).

Awareness about the quadrant in which instruction or tasks take place might help CLIL teachers to optimize the use of language. While traditional EFL instruction usually shifts learning from quadrant labelled as 1 to quadrant 4, Ting (2017, p.47) reflects on how CLIL instruction in secondary education already departs from quadrant labelled as 4, whereby

complex academic language is already used to present abstract and cognitively demanding concepts.

Cummings' findings suggest that a student needs 5-7 years to acquire CALP in the second language if the learner has native language literacy. For those students with weak native language literacy, 7-10 years are required. Implications of this difference link with what Cummings calls "Common underlying proficiency", which are the set of skills and implicit metalinguistic knowledge that can be used when working in another language (Figure 4-4). Consequently, any improvement in the common underlying proficiency in one language will result in a beneficial effect on the other language. This framework also explains why it becomes easier to learn additional languages.

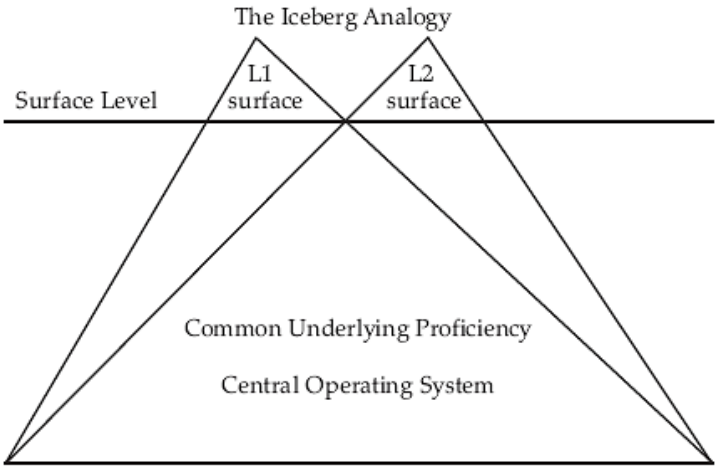


Figure 4-4. Common Underlying Proficiency represented as the bottom of an iceberg (Bligh, 2014).

As Cummins (2000) claims: "Conceptual knowledge developed in one language helps to make input in the other language comprehensible." Consequently, extensive engaged reading, opportunities for collaborative discussion about texts, and writing for academic purposes are key orientations to maximize language and literacy development, both in the mother tongue and the foreign language (Cummins, 2008).

Indeed, *translanguaging* might suppose an effective approach to strategically use different languages in order to learn the same concept (Cenoz & Gorter, 2015; Swain, 2006; Ting, 2017), at the same time that providing the required scaffolding to learn academic registers across languages.

Taking all the previous considerations into account, a well-planned strategy to continuously address both input comprehension and also academic language learning must be defined for CLIL classes. A proposal will be presented in the next section.

5. CLIL Materials on Cybersecurity

5.1. Phases of a hacking attack

The specific content covered by this proposal is "Attack Phases", which is the first content of the unit "Logic Security" within the subject "Security and High Availability" in the VET (vocational education and training) studies of "Computer Network Systems Management".

Understanding how an attack is performed by hackers is of paramount importance when learning how to enhance the security of a system. Although an attacker might compromise a system using many different techniques, the fact that most methods follow the same phases provides us with opportunities to prevent these attacks. Forensics is the part of cybersecurity that analizes these attacks to debug responsibilities and avoid new threats.

Interestingly, in the last few years, cybersecurity forensics is one of the most employable IT positions (Stewart, 2016). One of the main functions of a cybersecurity forensic is to **write reports or analyses** about the vulnerabilities found in a system. Thus, promoting academic output seems crucial, as the best security expert will succeed at work only if after their technical analysis, their reports to the company are organized, formal, and intelligible.

Consequently, after this course, students are expected not only to know about cybersecurity but also to produce academic output analysing how an attack was performed. This writing might well represent a final summative learning assessment to evaluate, at the same time, both content acquisition and academic foreign language performance.

5.2. Context

Having recently earned my first CLIL teaching position as a computer science teacher (AA 2019-2020) in a high school in Seville, now it is a valuable opportunity to put into practice the insights obtained during the last months. The group of students attending the subject "Security and High Availability" is formed by 25 adults highly motivated to finish the course to access the labour market. They have a modest level of English but a good predisposition towards learning.

As for the materials, traditionally, the recommended textbook to cover the *Attack Phases* content has been the manual developed by the *EC-Council* to prepare the *Certified Ethical Hacker Certification* exam (EC-Council, 2009). However, this document is known to be not

only outdated but written in a non-academic and poorly organized style. Figure 5-1 shows readers' reviews on the textbook in Amazon.

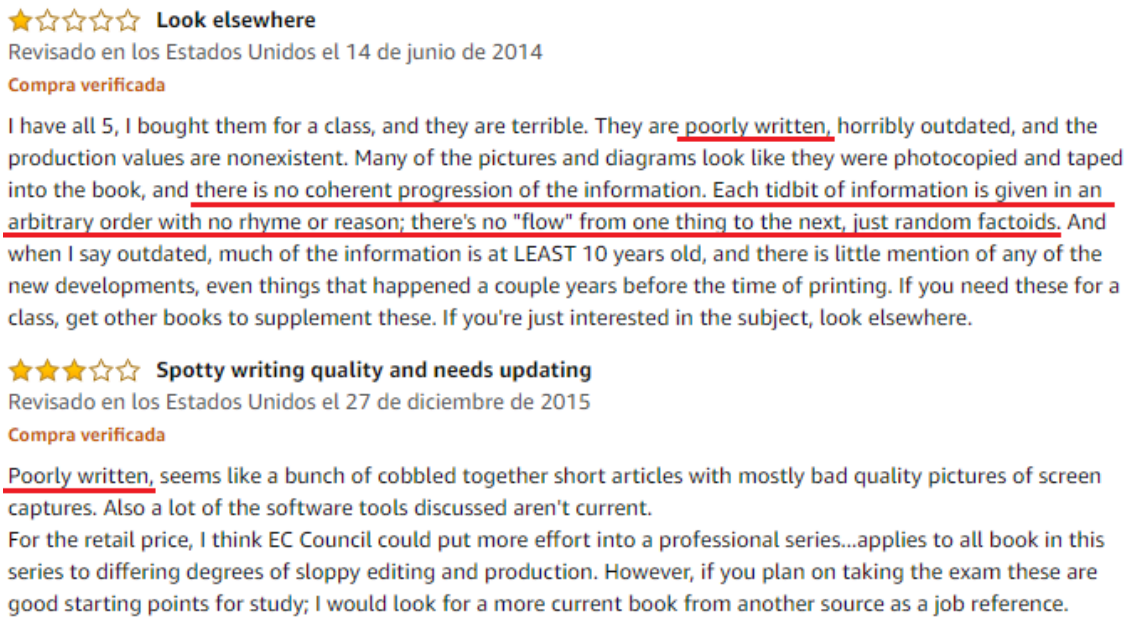


Figure 5-1. Recommended textbook reviews on Amazon

Regarding this lack of academic materials, it is important to notice how cybersecurity is a relatively recent formal field of study. The traditional *community of practice* "languaging" about "system vulnerabilities", "attacks", or "network sniffing techniques" has been composed by hackers, who for both operational and legal reasons maintained their papers unpublished. It was not until cybersecurity turned into a major issue that specific careers on the field emerged and thus the necessity to train new professionals. In Annex II, the pages from the course textbook, (in Spanish), and four internet selected links on the topic are shown. Note how a curation process on Attack Phases materials should be developed before using those texts in the classroom, providing their different sources.

5.3. Proposed learning sequence and results

5.3.1. Previous work

In spite of what a true CLIL lesson should be, and because of curriculum planning timing, I initially delivered the content of "Attack Phases" following a traditional-lecture approach, using as materials:

- Teacher's discourse (in English, and Spanish when needed).
- Slides to support that discourse (in English).

- Reference book (in Spanish, see Annex II)
- Internet selected articles (in English, see Annex II)

Although some students asked relevant questions that revealed that they were understanding the topic, in general, the lesson was passive and not student-centred. I explained Attack Phases while students just listened and – some of them – took notes.

Ten days after this contact with the topic, students were explicitly asked to review this information for the next day session. That day, students were asked to write a document in English, as correct as possible, explaining all they have learnt about attack phases. There was no time restriction to complete this task.

An analysis on the writings revealed a range of issues related to the students' ability to produce academically effective texts, and also to content comprehension. Consequently, I reflected on these results trying to establish improvement points, reaching the conclusion that a CLIL tasks learning sequence must be designed in order to make the content accessible at the same time as fostering academic language. My analysis is detailed in Table 5.1.

FINDING	COMMENTARY	POTENTIAL IMPROVEMENT / LEARNING OPPORTUNITIES
Some students could not write anything about attack phases.	This could be due to lack of attention / later study.	To overcome the volatility of the information in a passive lesson, learning by doing should be the selected approach.
Some students just wrote the attack phases names, but not explained their meaning.	This could be due to the lack of significance in the followed approach.	This topic should not be studied by-heart, but understanding the steps an attacker needs to follow in each phase. Input texts should be broken down into '*chunkable'* tasks.
In turn, some students managed to explain – with different degrees of accuracy – what the phases consist of, but they did not write their names. Actually, only 6/20 students could write the first phase name "Reconnaissance" properly.	This could be due to lack of attention / later study.	Although less important, this pitfall should also be addressed. Students should actually write down phases names while learning, making use of the haptic memory (Mangen & Velay, 2010).
Students tend to mix the processes with the various moments of the "attack", especially phases 1 and 2.	This was expected, providing that they are conceptually similar, being one the logical evolution of the other.	Work out the difference between these two phases in learning tasks.
In general, students produce very schematic writing, lacking discourse connectors.	The input materials were not schematic but followed an organized discourse. However, It is not enough to just be exposed to it – students have to actively be taught and practice discourse.	In fact, academic discourse should be taught through learning activities, making explicit whether the register is academic or not.
Sometimes, English structures were very poor: run-on sentences are present, concordance subject-verb is very frequently missed, the third-person-singular rule for the present tense was too frequently not followed.	Student's conceptions about English reveal they are not comfortable nor motivated with the use of a foreign language at school.	Actively practice English though tasks. Finding language/content mistakes might be a good approach. Even if basic concepts are required to be practised. If needed, why not?

Table 5-1. Issues observed in students' writings.

Having analysed students' written answers, a CLIL task-driven lesson on this topic was designed in order to address the learning of attack phases as well as the improvement of academic output written skills.

5.3.2. Implementing the CLIL approach

Taking into consideration the literature review developed in the previous chapters, a set of tasks have been designed *ad hoc* in order to promote academic language while learning about Attack Phases. A final printable version of the materials is presented in Annex II. Also, this document explains reflections on intermediate draft versions of the proposed learning sequence tasks, that are reproduced in Annex IV. This task-based learning (TBL) progression will scaffold students to understand complex concepts, moving from the already difficult language of cybersecurity texts (CALP) to manageable pieces of information (BICS) that are content and language comprehensible. Then, an additional movement back to academics is needed, providing that improving CALP is at the centre of CLIL instruction.

Task 1 will be used as a warming-up activity whose solutions are easy to extract from the exercise itself. In b) the plural of vulnerability is explicitly presented as it seems students tend to have problems with it. Note that, as a warming-up task, language cognitive load should be simple and content should as well have little weight at this point of the learning progression.

1	Read this short text: One of the tasks of an ethical hacker is to test the security of an organization. In order to do that, a white-hat hacker follows processes similar to those of a malicious hacker, given that the steps to gain and maintain access into a computer system are similar no matter what the hacker's intentions are. Now, use this information and what you already know from previous units to answer the questions below.
a)	A *malicious* / *ethical* hacker is also known as a white-hat hacker.
b)	*Vulnerabilities* / *vulnerability* is the weakness which can be exploited by a threat actor, such as an attacker, to perform unauthorized actions within a computer system.
c)	An *exploit* / *evidences* is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behaviour to occur on a system.
d)	An attacker might *explode* / *exploit* a vulnerability in order to gain unauthorized access to a system.

Key: a) ethical b) Vulnerability c) exploit d) exploit.

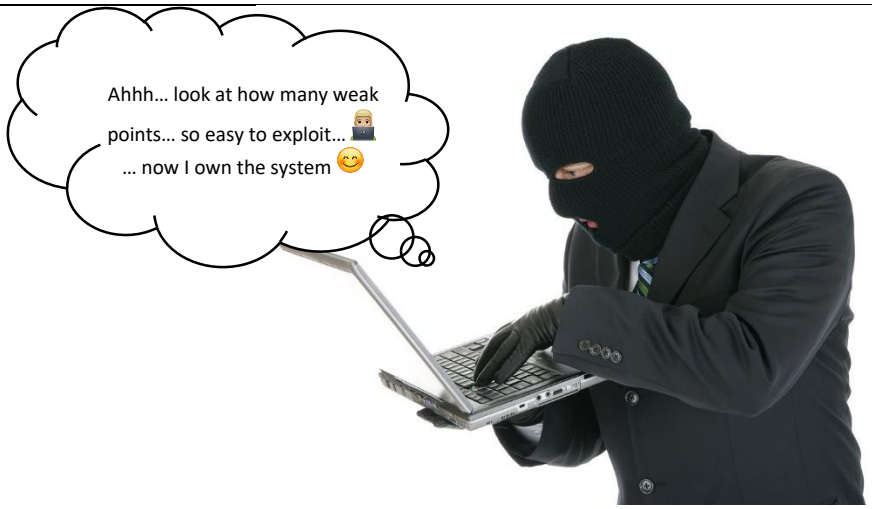
The following Task 1A will be useful to provide solutions for exercise 1, as well as to make explicit that explode and exploit are different verbs. *Threat* is an often misspelled word, and *chunk* might be new to students but is widely used in computer science. Note how for each word, two definitions are provided: one written by Alice, using BICS, and a different one written by Bob showing CALP. Such an explicit demonstration might help students to perceive what it is meant by "good writing", in line with visible pedagogies studied in previous chapters.

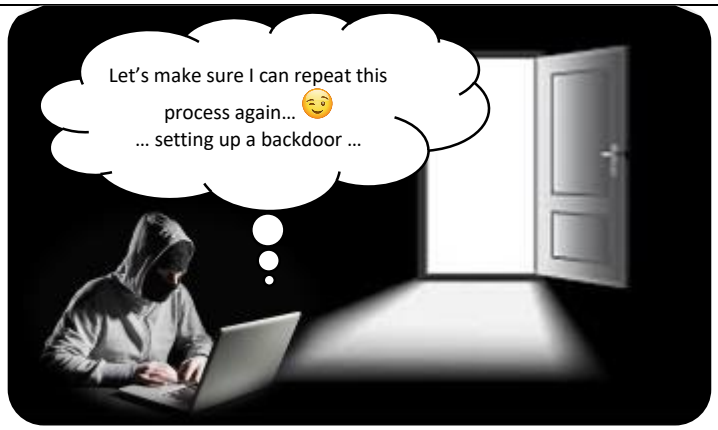
1A	Alice and Bob are two students that have just defined some words from exercise 1. Although both definitions are correct, Bob expressed himself in academic language and consequently obtained better marks. Match the following sentences with a word from exercise 1.	
	Alice	Bob
	A verb meaning "to use something to one's own advantage".	A verb meaning "to use personal skills, aptitudes, resources, or a particular situation in order to obtain an opportunity which is beneficial for the subject".
	A verb meaning "to break up into pieces".	A verb meaning "to burst violently, usually provoking an extremely loud noise".
	The possibility that something bad will happen.	A potential source of imminent danger or harm.
	Some but not all of a thing.	A piece of something, especially a large part.

Key: to take advantage / to explode / threat / chunk.

Task 2 will present the five names of the attack phases to the students, along with a brief graphical explanation of what they consist of. Phases names are provided unordered whereas the pictures follow the logical order of a cyber-attack.

2	Match the following situations with the phase names of an attacking process.
Gaining access Reconnaissance Scanning **Covering tracks Maintaining access**	

1	 AH! Potential target! Let's get some info... ... Gathering info... he he he
2	 I know everything about this target ... Now, let's check their system for vulnerabilities ...
3	 Ahhh... look at how many weak points... so easy to exploit... ... now I own the system

4	
5	

Key: 1-Reconnaissance / 2-Scanning / 3-Gaining access / 4-Maintaining access / 5-Covering tracks.

At this point it is necessary to explain that in the first version of these materials, I had not given students Task 2 for matching "image-to-terminology". Therefore, after Exercise 1, I had expected students to do the task shown in Annex IV.

However, CLIL-training made clear that it was a poor design. Students were provided with descriptions of the learning phases, unordered, and without their names, which were requested to be extracted from the excerpts. This design would force students to process two cognitive tasks at the same time: first, identifying the missing word which is necessary to understand the paragraph; then, putting the paragraphs in order, which can not be done without

the previous understanding. For this reason, the previous comic vignettes task was introduced in order to empower students to order the paragraphs once they know Phases names.

In addition, in task 2A students are requested to order the phases and, because of this, they will have to read the descriptions more than once, focusing on the interdependences between phases (content) and linking words clues (language). Note how students must write down phases names, making use of the haptic memory theory, in order to both make them remember attack phases names and also avoid misspelling.

2A	In the following pieces of text, the different phases of an attack are briefly described. Unfortunately, Mallory[2] has intentionally cluttered the paragraphs. Rearrange the paragraphs and write down the names of the phases.
Order	**Description**
	a. _____, also known as the preparatory phase, involves gathering information about a potential target.
	b. Last, but not least, it is necessary to remove any traces of the attack, so that detection by security personnel and legal actions are avoided.
	c. _____. After vulnerabilities have been exposed during the scanning phase, the actual hacking takes place. Those weak points of the system are now exploited in order to own the system.
	d. _____ involves taking the information discovered during prior reconnaissance and using it to examine the network using different tools, looking for vulnerabilities.
	e. As crucial as the 'Gaining access' phase is the m_____ access. During this phase, it is necessary to secure the access so that it is maintained for future exploitation and attacks.

[2] Characters in the tasks are commonly used names in the field of Cryptography, which is a forthcoming topic during the course.

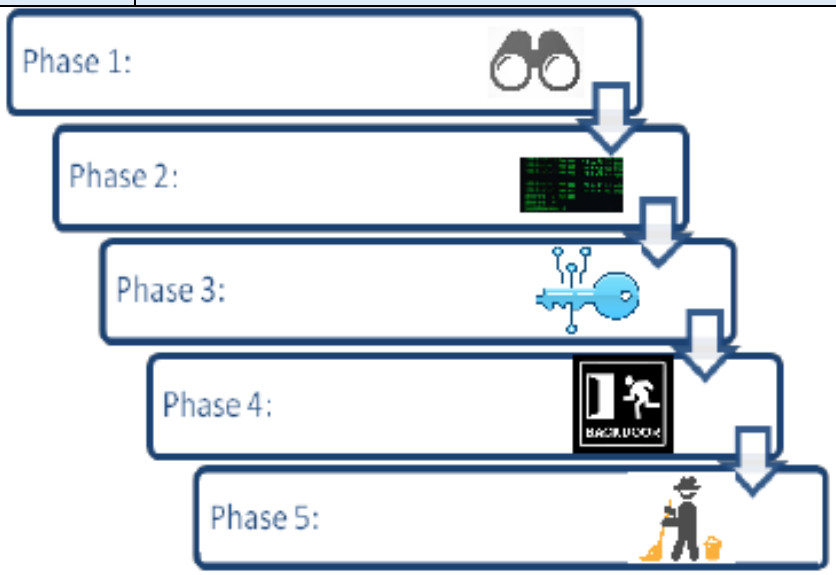
Now, Task 2B will be used as a self-correcting exercise for 2A, but in addition, it will make students reflect on their language-based answers.

2B	Now, check your answers by answering these questions.
What words made you think sentence (a) is the first sentence?	Potential answer: “preparatory”
What words made you think sentence (d) comes after sentence (a)?	Potential answer: “involves gathering information” (from a) and “taking the information discovered” (from d).
What words made you think sentence (c) is the third sentence?	Potential answer: “looking for vulnerabilities” (from d) and “after vulnerabilities have been exposed” (from c)
What words made you think the 4th phase (e) is called ‘Maintaining access’?	Potential answer: “secure the access so that it is maintained”
What words made you think sentence (b) comes last?	Potential answer: “last, but not least”

Task 2C just asks students to write down attack phases again, in order to summarize learnt concepts before moving to higher cognitive demanding tasks. This is in line with the importance of continuously verifying that learning is taking place, performing a formative assessment, before moving on to new concepts.

At the same time, going back again to Attack Phases’ names, students are schematizing, with the consequent reduction of intrinsic cognitive load by breaking down the information into small tasks that require active thinking.

2C	Now write down again the names of the 5 phases of an attack, with the clues provided by the icons.



Thinking that, to do CLIL, I only needed to now present students with English texts about the 5 different phases and put in a little bit of "language-focused" by inserting a few "grammar mistakes" for the students to identify, I designed the task that is presented in Annex IV.

A reflection on this task, and an assessment of it against the principles extracted from the literature review reveals that this task does not represent a digestible way to learn about the topic, but simply a reading task on a long text about unknown content, with the consequent heavy cognitive demand. Even though students have been presented with the Attack Phases already, this long text is in L2 and presents the complete information about

Indeed, the cognitive load ratio between *extremely-high new content* vs *light language* will not work here for the reason that (difficult) content is unknown yet while language does not serve as a scaffold but merely as an *annoying* addition to the task, or as Ting & Ciadamidaro (2016) call them, "tasks of torture".

For this reason, the learning sequence was modified to address the learning of one Attack Phase at a time, giving the students the opportunity to focus on **core concepts** of every phase. Every content in the curriculum is composed of fascinating core concepts, which are easy to understand, and surrounding details that exemplify these concepts (e.g. the core concept "when hot water touches a cold surface, it condenses" might be surrounded by details such as "the influence of atmospheric pressure", "the exact temperature of vapour and the surface", etc.). Distinguishing between core concepts and details is of paramount importance when designing CLIL tasks: it provides a list of micro-content-learning objectives to cover – core concepts. A decision on how many details are considered in CLIL tasks should be taken, considering that when learning, especially through a foreign language, the core concept might be suffocated by the details. After students have effectively learnt core concepts, it is easy to go to the textbooks and embellish those learnt concepts.

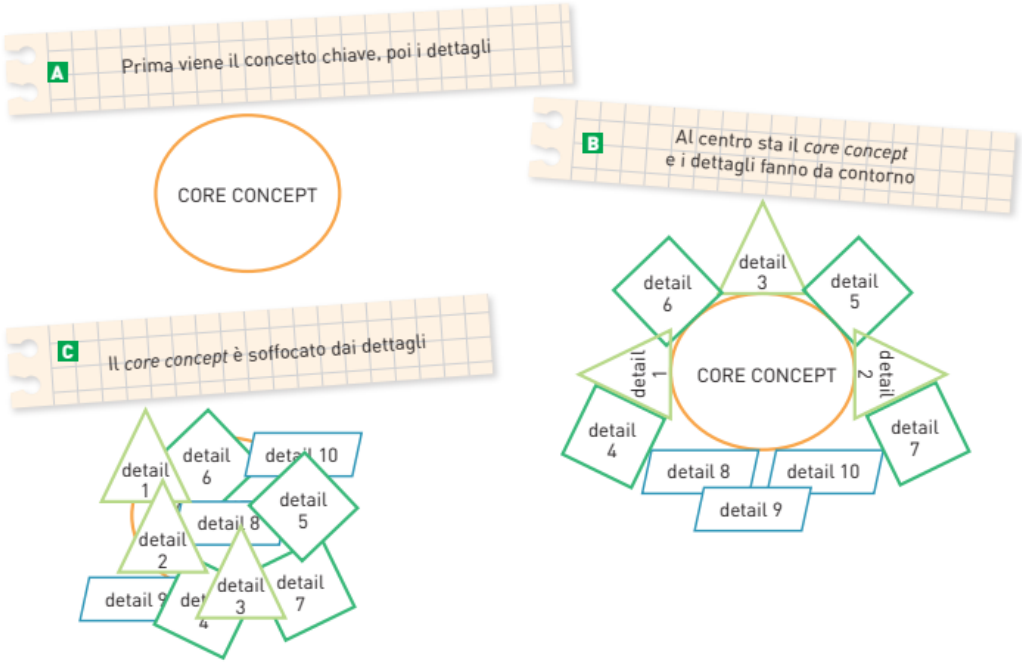


Figure 5-2 from Ting & Ciadamidaro (2016).

To accomplish the partition of that long text into digestible tasks, Task 3 was designed based on principles of "translanguaging" whereby L1 and the L2 are used complementarily to scaffold each other strategically, using both BICS and CALP across languages. Therefore, Task 3 shows how unfamiliar content in the mother tongue (L1-CALP) can be scaffolded upon familiar language in English (L2-BICS). A Spanish academic text on the first Attack Phase is provided. This textbook excerpt (Triviño, 2019, p.43) represents a high cognitive demand for a

student, even in the mother tongue. Through a *translanguaging* task, students are required to re-read challenging academic Spanish with the scaffolding of comprehensible non-academic English.

3	Read the following text about the first phase of a cyber-attack.

Reconocimiento

Fase preparatoria en la que el atacante reúne toda la información posible de su objetivo, basándose en cualquier fuente, incluida la ingeniería social. Esta fase también puede incluir un escaneo no autorizado de la red (interno o externo). El potencial atacante diseña su estrategia de ataque, y para ello tarda el tiempo necesario para recabar la información crucial del objetivo. Para ello acude, si es necesario, a la basura de la víctima (dumpster diving), donde puede encontrar información de nombres de usuarios, contraseñas, números de tarjetas de crédito, recibos bancarios, números de teléfono, etc.

En general, las técnicas de reconocimiento pueden dividirse en activas y pasivas. Las técnicas activas implican la interacción con el sistema informático víctima, por ejemplo, el uso de herramientas para detectar equipos accesibles, routers, etc. Las técnicas pasivas no interactúan directamente con el sistema, sino que acopian información sobre este obtenida de fuentes públicas, ingeniería social, etc.

Write the Spanish equivalent next to each of these English phrases about the first phase of a cyber-attack. The English sentences are not identical to the Spanish ones from the previous excerpt, so you must also modify your Spanish sentence. The English phrases are also in informal English: you should write in academic Spanish.

1. During the reconnaissance phase, an attacker tries to collect as much information as possible about the potential victim, by different ways like social engineering or unauthorized network scanning.	
2. Another trick is to get the victim's information from the rubbish, which is called dumpster diving.	

3. There are two types of reconnaissance techniques: active, which involve interaction with the victim' system; and passive, getting the information from somewhere else.	

Note that some details have been omitted for the sake of learning the core concept of the reconnaissance phase while using L2-BICS to access academic L1-CALP. Once the key structure of knowledge is learnt, students might be able to go back to the textbook or other reliable sources of information to fill it in with details.

Task 3A reproduces a video where a *social engineering* action is accomplished. As a typical example of a reconnaissance activity, understanding this term might help students to comprehend Phase 1, the reconnaissance phase.

3A	The previous task established *Social Engineering* as an activity which is usually performed during the reconnaissance phase. 1. Watch the following video once. 2. Look at these questions and answer them while watching the video again. 3. Check your answers with your partner.

https://www.youtube.com/watch?v=lc7scxvKQOo

4. Social Engineering is basically…	a. voice solicitation
5. A vishing call is…	b. using the phone to extract information or data points that can be used in a later attack.
6. A vishing attack consists of…	c. faking the caller number from which you are supposedly phoning.
7. "Spoofing" from a phone number consists of…	d. hacking without any code.

Language demands of this task are not high, indeed, the video relies on BICS, while cognitive demands require students to understand the meaning of social engineering from the conversation the woman has on the phone. Questions are designed to guide students' focus on the concepts from the video.

3B	Read the following excerpt which summarizes the Reconnaissance phase:

"When hackers are looking for information on a potential target, they commonly run an Internet search on an individual or company to gain information. This can be done either manually or using automatized tools. Social engineering and dumpster diving are considered passive information-gathering methods of the *former*, whereas sniffing the network is an example of the *latter*."

What do the words **former** and **latter** refer to? Think of a rule to remember which word refers to the first, and which one refers to the last.

Former refers to: _____

Latter refers to: _____

Rule to remember the order:

Key: **F**ormer, **F**irst item (done manually); **L**atter, **L**ast item (done using automatized tools).

Task 4 is intended to introduce the second phase – scanning, using some scenarios to help students understand the difference between phases 1, reconnaissance, and 2, scanning. Note that it forms a sort of "BICS-thinking" to prepare students for the upcoming "CALP-thinking" in subsequent tasks.

4	Let's compare a cyber-attack to a bank robbery. Can you match these phases between them? 1. Match bank robbery situations with phases 1, 2, or 3. 2. Match each pair with a cyber-attack situation x, y, or z.
a. Sitting on a bench in the hall of a bank headquarter, just paying attention to every movement of the employees. b. Taking the elevator and walking through the corridors of the bank offices, taking notes of the open hours written on every door. c. Actually going back to the offices at a time where nobody is supposed to be there, and checking whether the doors are locked.	
1. Scanning 2. Passive reconnaissance 3. Active reconnaissance	
x. Running a script on a system website, obtaining just the type of web server and operating system it is installed on. y. Navigating through a system website. z. running an automatized vulnerability scan on the system website.	
_ _ _ _ _ _ _ _ _	

Key: a2y, b3x, c1z

The Scanning phase, Phase 3, is now addressed in task 4A. The text was modified to avoid mentioning some scanning tools that are not important at this moment of the course and might blur the learning of the core concept – what is done in this phase. Consequently, the student might be able to focus on other contents. CALP is promoted through awareness of academic language features.

4A	Last class, Alice wrote a piece of information about the Scanning phase that was marked A+. Can you guess which text corresponds to Alice? _____

Scanning-1

Scanning involves taking the information discovered during reconnaissance and using it to examine the network. It could be considered as the logic evolution of active reconnaissance. Tools that a hacker may employ during the scanning phase include:

- Diallers.
- Port scanners.
- Network mappers (i.e. *Nmap*)

One of the goals might be to map open ports and applications.

Techniques to lessen the chance of detection, consisting of scanning at a very slow rate, might be used. As an example, instead of checking for all potential applications in just a few minutes, the scan might take days to verify what applications are running. Many organizations use *intrusion detection systems* (IDS) to detect just this type of activity.

One key defence against the hacker is the practice of *deny all*. This rule can help reduce the effectiveness of malicious actions at this step. *Deny all* means that all ports and applications are turned off, and only the minimum number of applications and services that are required to accomplish the organization's goals are turned on.

Scanning-2

Scanning is the phase after active reconnaissance that uses the information obtained to scan the network looking for open ports and applications. The following tools are used by a hacker in this phase:

- Diallers.
- Port scanners.
- Network mappers (i.e. *Nmap*)

The hacker uses methods to avoid being detected, for example by scanning slow to not being caught by *intrusion detection systems* (IDS) to detect scanning.

A possible solution is called *deny all*. *Deny all* works turning off all ports and applications except the ones needed by the company to work.	
Now, provide examples of fragments with…	
1. Impersonalized sentences	Potential answer: "It could be consider".
2. Find where the phrase "being identified" is now a "noun" in the sentence (i.e. "nominalization")	Answer: "detection"
3. Repetition / A sentence where repetition was avoided.	Potential answer: "A possible solution is called *deny all*. *Deny all* works…"

Task 5 describes the *Gaining access* phase and is a task which focuses on language, paying attention to structures that will help students to write academic output, in line with Cognitive Discourse Functions (Dalton-Puffer, 2017).

5	Read the following excerpt about the Gaining access phase:
Gaining access As far as potential damage, this phase could be considered one of the most important steps of an attack, which occurs when the hacker moves from simply probing the network to actually attacking it. Vulnerabilities exposed during the reconnaissance and scanning phase are now exploited to gain access to the target system. The hacking attack can be delivered to the target system via a local area network (LAN), either wired or wireless; local access to a PC; the Internet; or offline. Examples include stack-based buffer overflows, denial of service (DoS), and session hijacking. Gaining access is known in the hacker world as *owning the system* because once a system has been hacked, the hacker has control and can use that system as they wish. This is the context where *privilege escalation* takes place, which is the act of gaining elevated access to resources that are normally protected from an application or user, with the intention of performing unauthorized actions.	
Find and write down a sentence used to give examples. Underline the words that denote exemplifying.	

Find and write down a sentence used to express comparison. Underline the words that express comparison.
Find and write down a sentence used to express purpose. Underline the words that denote purpose.
Find and write down a sentence used to express a definition. Underline the words that denote definition.

Task 6 focuses on content by raising awareness on two key expressions to understand this phase: *to harden* and *exclusive access*. Students are requested to discuss with their partners so that they negotiate meaning while communicating in the classroom.

6	Read the following excerpt about the Maintaining access phase:

Maintaining access

In this phase, the attacker tries to retain the ownership of the system for future exploitation and attacks. Sometimes, hackers ***harden*** the system from other hackers or security personnel by securing their **exclusive access** with backdoors, rootkits, and trojans. Once the hacker owns the system, they can use it as a base to launch additional attacks. In this case, the owned system is sometimes referred to as a *zombie system*.

Sometimes hackers might even fix the original problem that they used to gain access so that they can keep the system to themselves, and prevent other hackers from entering.
Providing the dictionary definitions for *harden*, which do not exactly fit in this context. Can you infer its meaning from the text? Write a dictionary-definition for "*to harden (computer science)*". Share it with your partners until you determine the most academic definition.  harden *verb* [I or T] UK /ˈhɑː.dᵊn/ US /ˈhɑːr.dᵊn/ **harden** *verb* [I or T] (SOLID) **to become or make hard:** • *The mixture hardens as it cools.* • *It is thought that high cholesterol levels in the blood can harden the arteries (= make them thicker and stiffer, causing disease).* **harden** *verb* [I or T] (SEVERE) **to become more severe, determined, or unpleasant:** • *Living in the desert hardened the recruits (= made them more strong and determined).* • *As the war progressed, attitudes on both sides hardened (= became more severe and determined).*
Discuss with your partner: After owning a system, why would an attacker want to ensure that access is only limited to them and not accessible to other hackers?

The last phase of an attack consists only in evidence removal. Not supposing a high cognitive demand, it is presented straightaway with a haptics task which is proposed to remember this last phase: crossing the lines of a log file, which represents something students at this stage are already familiar with.

7	Read the following excerpt about the last phase of an attack, and then make the activity below.
Covering tracks	

Reasons for covering tracks of actions vary from avoiding legal action to being able to continue using the system. Evidence removal delays attack detection by deleting tracks in log files or in intrusion detection systems (IDS) alarms.

Mallory has been attacking the server of a company and consequently, there are traces in this log that reveal his unauthorized activity. Help Mallory to cover his tracks and get away with this attack by crossing out traces of his presence in the system:

```
2020-02-10 07:50    Incoming connection: Alice@office
2020-02-10 07:50    Incoming connection: Bob@office
2020-02-10 08:00    Incoming connection: Alice@office
2020-02-10 08:15    Incoming connection: Heidi@office
2020-02-10 08:54    Incoming connection: Trudy@office
2020-02-10 09:14    Incoming connection: Bob@office
2020-02-10 10:00    Incoming connection: Alice@office
2020-02-10 12:25    Incoming connection: Mallory@Unknown-location
2020-02-10 12:30    Incoming connection: Mallory@Unknown-location
2020-02-10 12:35    Incoming connection: Bob@office
2020-02-10 12:39    Incoming connection: Mallory@Unknown-location
2020-02-10 13:00    Incoming connection: Trudy@office
```

The purpose of Task 7B is to check whether the students are understanding what operations are required to be developed in each phase, in line with the principle of continuously verifying that learning is taking place before moving on to the next content. Note that examples of tools used through every different Attack Phase have been provided in its corresponding task, so that this vocabulary should be known at this point. In other case, this task serves as a guide to "where to go back to".

7B	Match the following examples of actions/tools with the phase they are related to:
a) Backdoors, rootkits, and trojans.	
b) Social engineering, dumpster diving, and sniffing.	
c) Deleting traces in registry files (logs) or removing IDS alarms.	
d) Network mappers, port mappers, network scanners, port scanners, and vulnerability scanners.	
e) Buffer overflow, DoS, password filtering, and session hijacking.	

Task 8 summarizes the contents studied, in a context. Once the five Attack Phases have been learnt through step by step tasks, a holistic content and language task is developed to review content and move students into academic language.

<table>
<tr><td>8</td><td colspan="2">- Alice is a professional white-hacker who has written a report for Bob, a client who wants to assess the cybersecurity of his company.
- Mallory is a hacker writing an email to Eve, another hacker, about his last attack.

Both the report and the email have been cluttered. Can you order these fragments into the original documents?

Hints: use a pencil and rubber, and the boxes to set A/M and an order number in the writing. Try to distinguish the report from the email paying attention to the register of the language. Example: A 3</td></tr>
<tr><td colspan="2">An examination of these hosts revealed a password-protected administrative webserver interface. ☐☐</td><td rowspan="6">Alice’s Report:</td></tr>
<tr><td colspan="2">After a closer examination, we discovered that the compromised webserver utilizes a Java applet for administrative users. We added a malicious payload to this applet, which gave us administrative privileges at the same time that permanent access for future accessing. ☐☐</td></tr>
<tr><td colspan="2">Suddenly, I found a post-it note on a screen: “servers room: 4721”. It resulted to be the access code to open the door. It worked! ☐☐</td></tr>
<tr><td colspan="2">I am concerned that I will be discovered because I am having trouble removing a specific log. Could you help me? ☐☐</td></tr>
<tr><td colspan="2">Initial reconnaissance of the company network resulted in the discovery of a misconfigured server that allowed the implementation of a specific attack. The results provided us with a listing of specific hosts to target for this assessment. ☐☐</td></tr>
<tr><td colspan="2">Mallory’s Email:</td></tr>
</table>

I plugged in a very small USB stick from which I will be able to connect remotely any time I want.	
An examination of the administrative interface revealed that it was vulnerable to a remote code injection vulnerability, which was used to obtain interactive access to the underlying operating system.	
So, yesterday I walked into the office and tried to enter the servers' room, which unfortunately was locked up by a password panel on the wall. Then, I started checking all the desks in the office, looking for something helpful.	
Existing network traffic controls were bypassed through encapsulation of malicious traffic into allowed protocols, disguising any evidence. Concerns about the company security arise, providing all the malicious tasks.	
During the last couple of weeks, I have been observing the habits of the employees of the company's data centre that hosts the servers. It turns out that every day from 2 pm to 3 pm there is nobody at the office.	

8A	Now, re-read the texts and discuss with your partner: what features of the language in each excerpt made you distinguish its register? Give examples.	
	Alice's report language features:	Mallory's email language features:

Key:

Report	**Email**
Initial reconnaissance of the company network resulted in the discovery of a misconfigured server that allowed the implementation of a specific attack. The results provided us with a listing of specific hosts to target for this assessment. An examination of these hosts revealed a password-protected administrative webserver interface. An examination of the administrative interface revealed that it was vulnerable to a remote code injection vulnerability, which was used to obtain interactive access to the underlying operating system. After a closer examination, we discovered that the compromised webserver utilizes a Java applet for administrative users. We added a malicious payload to this applet, which gave us administrative privileges at the same time that permanent access for future accessing. Existing network traffic controls were bypassed through encapsulation of malicious traffic into allowed protocols, disguising any evidence. Concerns about the company security arise, providing all the malicious tasks .	During the last couple of weeks, I have been observing the habits of the employees of the company's data centre that hosts the servers. It turns out that every day from 2 pm to 3 pm there is nobody at the office. So, yesterday I walked into the office and tried to enter the servers' room, which unfortunately was locked up by a password panel on the wall. Then, I started checking all the desks in the office, looking for something helpful. Suddenly, I found a post-it note on a screen: "servers room: 4721". It resulted to be the access code to open the door. It worked! I plugged in a very small USB stick from which I will be able to connect remotely any time I want. I am concerned that I will be discovered because I am having trouble removing a specific log. Could you help me?
Possible features: nominalizations, impersonal sentences, or distancing from speech.	Possible features: use of pronoun I or phrasal verbs.

5.3.3. Results

As explained in section 5.3.1, frontal lecturing in L2 about Attack Phases resulted in poor learning and poor attention to academic language. During the process of designing CLIL materials, a first version of them – including the "long-text task", was used in class. Results were similar to direct lecturing in English. Although a shift had been made from passive instruction to reading, the task failed to convey learning as well.

Unfortunately, the final version of these tasks was not implemented in class with students, since the curriculum moved forward while their writing process. However, **some personal insights have been gained thanks to the development of this thesis**. The process of creating CLIL materials trying to meet all the studied principles imposes a reflective practice that promotes awareness on how we should *CLIL*. In spite of the difficulties that the context, the content, or a neophyte teacher might pose to himself, every new experience contributes to increase the teacher development.

6. Conclusions

CLIL implementation in the classroom must be determined by language awareness for different reasons. Firstly, it is the vehicle that conveys concepts, even in the mother tongue. Paying attention to input comprehensibility shifts the classroom dynamics into a new approach that goes beyond the bilingualism. Secondly, academic language is a difficult social construct and consequently must be explicitly taught, not only to succeed in school but in lifelong learning.

A learning sequence proposal has been designed considering all the insights from the literature review, covering a specific content of a VET course while fostering academic language awareness.

Acknowledgements

I would like to show my gratitude to my supervisor, Prof. Teresa Ting, for all the suggested readings, dissertation possibilities, and for sharing her invaluable advice and expertise with me. At the same time, I would like to recognize the commendable work done by the professors involved in this Master programme, especially during its first-year implementation. Finally, I would like to express my appreciation for the labour of all the teachers I have met during my student life, from *Señorita Toñi* to Prof. Ting. Thank you.

Bibliography

Airey, J., & Linder, C. (2006). Necessary Conditions for Learning? Modes of Representation and the Disciplinary Discourse of University Science. *Journal of Research in Science Teaching*, *1*(1).

Allison, S., Runeckles, C., Haynes, F., & Tharby, A. (2017). Words. Retrieved from https://classteaching.wordpress.com/2017/10/08/words/

Beck, I. L., McKeown, M. G., & Kucan, L. (2002). *Bringing words to life : robust vocabulary instruction*. Guilford Press.

Beck, I. L., McKeown, M. G., & Kucan, L. (2019). Choosing Words to Teach. Retrieved from Reading Rockets website: https://www.readingrockets.org/article/choosing-words-teach

Bilash, O. (2011). BICS/CALP. Retrieved from https://sites.educ.ualberta.ca/staff/olenka.bilash/Best of Bilash/bics calp.html

Bligh, C. (2014). The silent experiences of young bilingual learners: A sociocultural study into the silent period. In *The Silent Experiences of Young Bilingual Learners: A Sociocultural Study into the Silent Period*.

Bloom, B. (1979). *Taxonomía de los objetivos de la educación : clasificación de las metas educativas*. Alcoy: Marfil.

Bourdieu, P., & Passeron, J. C. (1977). *Reproduction in education, society and culture*. London: Sage Publications.

Cenoz, J., & Gorter, D. (2015). Translanguaging as a Pedagogical Tool in Multilingual Education. In *Language Awareness and Multilingualism* (pp. 1–14).

Centre for Education Statistics & Evaluation. (2017). *Cognitive load theory: Research that teachers really need to understand*. Sydney.

Chevallard, Y. (1997). *La transposición didáctica. Del saber sabido al saber enseñado.* Buenos Aires: Aiqué.

Clark, R., Kirschner, P., & Sweller, J. (2012). Putting students on the path to learning: The case for fully guided instruction. *American Educator*, (36), 6–11.

Colera, J. (2015). *Matemáticas orientadas a las enseñanzas académicas 3 : Educación Secundaria Obligatoria*. Anaya.

Colera, J. (2016). *Mathematics for academic studies, Secondary Education 3*. Anaya.

Coxhead, A. (2000). A New Academic Word List. *TESOL Quarterly*, *34*(2), 213.

Coyle, D., Hood, P., & Marsh, D. (2010). *CLIL : content and language integrated learning*.

Crouch, C., Watkins, J., Fagen, A., & Mazur, E. (2007). Peer Instruction: engaging students one-on-one, all at once. In *Research-Based Reform of University Physics* (p. 55).

Cummins, J. (1979). Cognitive/Academic Language Proficiency, Linguistic Interdependence, the optimum age question and some other matters. *Working Papers on Bilingualism*, *19*,

198–205.

Cummins, J. (2000). *Language, power, and pedagogy : bilingual children in the crossfire*. Multilingual Matters.

Cummins, J. (2008). BICS and CALP: Empirical and Theoretical Status of the Distinction. In *Encyclopedia of Language and Education*.

Dalton-Puffer, C. (2017). A construct of cognitive discourse functions for conceptualising content-language integration in CLIL and multilingual education. *European Journal of Applied Linguistics*.

Dearden, J., & Macaro, E. (2016). Higher education teachers' attitudes towards English medium instruction: A three-country comparison. *Studies in Second Language Learning and Teaching*.

Didau, D. (2017, February 23). Education isn't natural – that's why it's hard. Retrieved February 9, 2020, from https://learningspy.co.uk/psychology/can-learn-evolutionary-psychology/

EAP Foundation. (2020). AWL Highlighter. Retrieved from https://www.eapfoundation.com/vocab/academic/highlighter/

EC-Council. (2009). *Ethical Hacking and Countermeasures: Attack Phases*. New York: EC-Council Press.

European Commission. (1995). Teaching and Learning - Towards the Learning Society. *White Paper on Education and Training*.

Geary, D. C. (2008). An Evolutionarily Informed Education Science. *Educational Psychologist*, *43*(4), 179–195.

Grandinetti, M., Langellotti, M., & Ting, Y. L. T. (2013). How CLIL can provide a pragmatic means to renovate science education – even in a sub-optimally bilingual context. *International Journal of Bilingual Education and Bilingualism*, *16*(3), 354–374.

Halliday, M., & Martin, J. R. (1993). *Writing science : literacy and discursive power*. London: Falmer Press.

Hattie, J. (2009). *Visible learning. A syntesis of over 800 meta-analyses relating to achievement*. London: Routledge.

Hattie, J., & Yates, G. C. R. (2013). Visible learning and the science of how we learn. In *Visible Learning and the Science of How We Learn*.

Huynh, T. (2016). A17. Tier 2 Words: Words that Make a Difference. Retrieved from Empowering ELLs website: https://www.empoweringells.com/a17-tier-two-words/

Hyland, K. (2009). *Academic discourse English in a global context*. New York: Continuum.

Johnson, K., & Golombek, P. (2003). Teachers' narrative inquiry as professional development. *TESOL Quarterly*.

Lave, J., & Wenger, E. (1991). *Situated learning : legitimate peripheral participation*. Cambridge University Press.

Leong, D. J. (1998). Scaffolding emergent writing in the zone of proximal development. *Literacy1*, *3*(2), 1–18.

Mangen, A., & Velay, J.-L. (2010). Digitizing Literacy: Reflections on the Haptics of Writing. In *Advances in Haptics*.

Mazur, E. (1997). *Peer Instruction: A User's Manual*. Upper Saddle River, NJ: Addison-Wesley.

OCDE. (2019). *PISA 2018 Results (Volume I): What Students Know and Can Do*.

OECD. (2020). Young people struggling in digital world, finds latest OECD PISA survey. Retrieved January 26, 2020, from https://www.oecd.org/newsroom/young-people-struggling-in-digital-world-finds-latest-oecd-pisa-survey.htm

Onrubia, J. (1993). Enseñar: crear zonas de desarrollo próximo e intervenir en ellas. In C. Coll (Ed.), *El constructivismo en el aula* (6th ed., pp. 101–124).

Pérez Cañado, M. L. (2016). Are teachers ready for CLIL? Evidence from a European study. *European Journal of Teacher Education*, *39*(2).

Pérez Cañado, M. L. (2018a). CLIL and educational level: A longitudinal study on the impact of CLIL on language outcomes and content mastery. *Porta Linguarum*, *29*, 51–70.

Pérez Cañado, M. L. (2018b). The effects of CLIL on L1 and content learning: Updated empirical evidence from monolingual contexts. *Learning and Instruction*, *57*, 18–33.

Pérez Cañado, M. L. (2019). CLIL and elitism: myth or reality? *The Language Learning Journal*, 1–14.

Pertierra, T. (2019, December 26). La incomunicación PISA fuerte en las aulas. *La Opinión Coruña*. Retrieved from https://www.laopinioncoruna.es/opinion/2019/12/27/incomunicacion-pisa-fuerte-aulas/1463514.html

Piaget, J. (1936). *Origins of intelligence in the child*. London: Routledge & Kegan Paul.

Sato, M., & Curis, M. (2008). *Making good choices: a support guide for the PACT teaching event*. 33. Retrieved from http://www.pacttpa.org/_files/Supporting_Documents/Making Good Choices 4.11.08.doc

Schleppegrell, M. (2004). *The language of schooling : a functional linguistics perspective*. Lawrence Erlbaum.

Shanahan, T., & Shanahan, C. (2008). Teaching disciplinary literacy to adolescents: Rethinking content-area literacy. *Harvard Educational Review*, *78*(1), 40–59.

Snow, C. E. (2010, April 23). Academic language and the challenge of reading for learning about science. *Science*, Vol. 328, pp. 450–452.

Stewart, J. M. (2016). *Cybersecurity Training White Paper: 10 Reasons You Should Consider a Career in Cybersecurity*. Retrieved from https://www.globalknowledge.com/us-en/resources/resource-library/white-papers/10-reasons-you-should-consider-a-career-in-cybersecurity/

Swain, M. (2006). Languaging, agency and collaboration in advanced second language proficiency. In H. Byrnes (Ed.), *Advanced Language Learning : The Contribution of Halliday and Vygotsky* (pp. 95–108).

Sweller, J. (1994). Cognitive load theory, learning difficulty, and instructional design. *Learning and Instruction*, (4), 295–312.

Sweller, J. (2010). Element interactivity and intrinsic, extraneous and germane cognitive load. *Educational Psychology Review*, *22*(2), 123–138.

Sweller, John. (2008). Instructional Implications of David C. Geary's Evolutionary Educational Psychology. *Educational Psychologist*, *43*(4), 214–216.

Ting, Y. L. T. (2005). *The value of Narrative Inquiry in Professional Development: A case study in recognising the value of equilibrated qualitative and quantitative methodologies in teacher-led classroom research*. Rende: Università della Calabria.

Ting, Y. L. T. (2011). CLIL ... not only not immersion but also more than the sum of its parts. *ELT Journal*, *65*(3), 314–317.

Ting, Y. L. T. (2014). A Concrete Directive Towards Literacy. *British Council. Regional Policy Dialogues 2013-14*, 105–112.

Ting, Y. L. T. (2017). CLIL at upper secondary: strategizing foreign language for the deep reading of complex academic L1-text. *Lend. Lingua e Nuova Didattica*, *2017*(1), 37–48.

Ting, Y. L. T., & Ciadamidaro, A. (2016). *A CLIL handbook for Maths.CLIL and Natural Science.CLIL*. Bologna: Zanichelli.

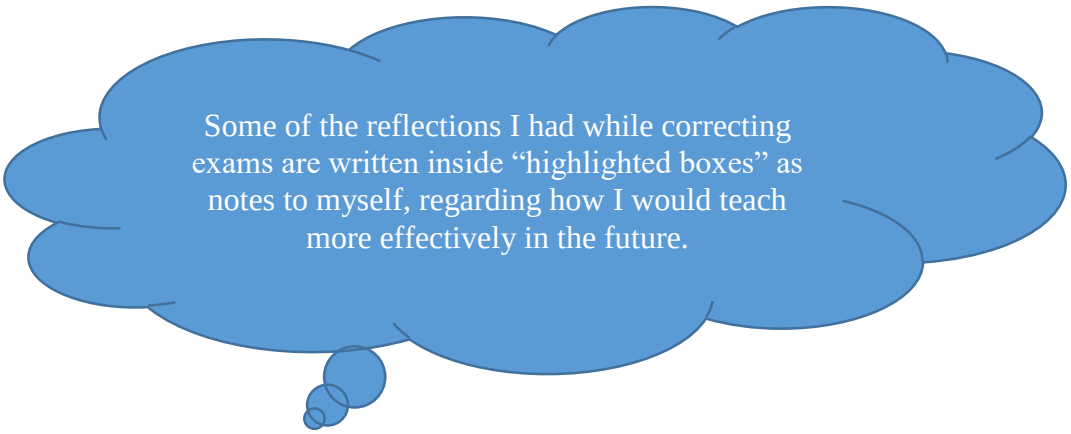
Triviño, I. (2019). *Seguridad y alta disponibilidad*. Madrid: Síntesis.

Vygotsky, L. (1979). *El desarrollo de los procesos psicológicos superiores*. Barcelona: Grijalbo.

Wellington, J., & Osborne, J. (2001). Language and Literacy in Science Education. *McGraw-Hill Education (UK)*.

Annex I. Correcting diary

This document was written as a diary while correcting exams during my first teaching position as a computer science teacher in a Vocational Education Training (VET) programme. Despite preparing references, activities, and tasks that would make my classes meaningful, when I started correcting exams I discovered that most of the students performed incredibly poor.



The purpose of this document is to reflect on my practices, to identify strengths and improvement points, and to find connections between the difficulties students face and their management of academic language.

Notice that the course was not CLIL. For this reason, excerpts from exams in this document are written in Spanish.

Context: the programme

“Ciclo Formativo de Grado Superior en Desarrollo de Aplicaciones Web” (DAW) is a course within vocational education and training (VET) programmes, in the category of Informatics and Communications, whose learning objective focuses on training professionals in the field of web programming. It corresponds to level 5 in the European Qualifications Framework (EQF). To access its modules, students are required to have graduated in:

- Compulsory secondary education (CSE) + Baccalaureate, or
- CSE + medium level VET (level 4 of EQF), or
- CSE + entrance test (although all students are required to be +18 years old)

Programme modules (which is how subjects are called in VET) are presented in the next table. I was responsible to teach all technical modules, which were labour-market-oriented and specifically focused on training students to work in companies in, at maximum, two-years’ time.

First Course	
Computer Systems	Vocational Training and Guidance *
Databases	Technical English *
Programming	
Markup languages and Information Management Systems	
Development Environments	

* Not taught by me

A common issue facing "informatics" instruction at CSE, VET, or even university-level courses is students' misunderstanding of what "computer science" courses involve: playing computer games, offimatics, typing. For example, I once overheard a student proclaiming her "bravura" at the typing academy. It was not only surprising that she equated the objectives of a typing academy with a VET "computer science" course, but that typing academies still exist! Generally speaking, many of the VET students were unaware of the logical-mathematical aspects of "informatics". This may reflect the fact that "using the computer" is a ubiquitous sport in today's society, so much so that I often receive invitations such as: "Are you an informatics guy? Could you fix my internet connection, make me a webpage and fix my microwave?" In my humble opinion, misconstruing "using a computer to play video games" for "computer scientist" poses a problem for informatics instruction that will only get worse as today's digital-natives grow up surrounded by technology which make them believe they want to "study informatics". Basically, all of us drive cars, but only a few of us are mechanical engineers. As "driving well" may have been equated with "good at mechanical engineering" in the eighteen century when cars appeared, those of us who teach "computer science" wonder whether today's youth actually know "how to use ICTs" despite being digital natives, a discussion for another context.

Context: the centre

The centre was a CEPA (Centro de Educación de Personas Adultas), where CSE for adults was taught. In addition, some courses to improve the qualifications of the unemployed were offered. There is a rate of 23% of unemployment in the city. The main occupations are construction workers and grape pickers. It is a small school. 50 adults approximately were studying CSE.

This is the only centre ruled by a local administration – the city council – instead of the regional educational administration, as usual. This has led to recurrent controversies, causing that DAW VET programme misses its teacher year after year, usually in the middle of the course. Since its implementation, there has not been a course without teacher replacement. The reason is that teachers quit the position as soon as they are called from the substitution list from the regional educational administration. Not only that, as this centre is local administration dependant, there is not that substitution list for them, and consequently every year students lose around 1 month of classes until a new teacher is recruited.

One aspect that surprised me was the fact that DAW modules are offered every other year, so that 1st course modules were offered this academic year, and will not be available until 2020/2021 course. What is more, some of the students enrolled and took 2nd year modules last academic course, before taking this years' 1st course modules. This course offering configuration represents a difficulty for students "starting the programme in the second year", as they will have to learn complex contents about programming without the basic pillars from first year's modules.

Context: the students

It was a nineteen students heterogeneous group regarding their:

- Access to the studies (from CSE, access exam or baccalaureate).
- Personal maturity (ages from 18 to 26).

It was a homogeneous group, in general, in terms of:

- Low motivation and commitment to work.
- Low previous knowledge about IT.
- Low general previous knowledge about maths or reading comprehension (even in L1).

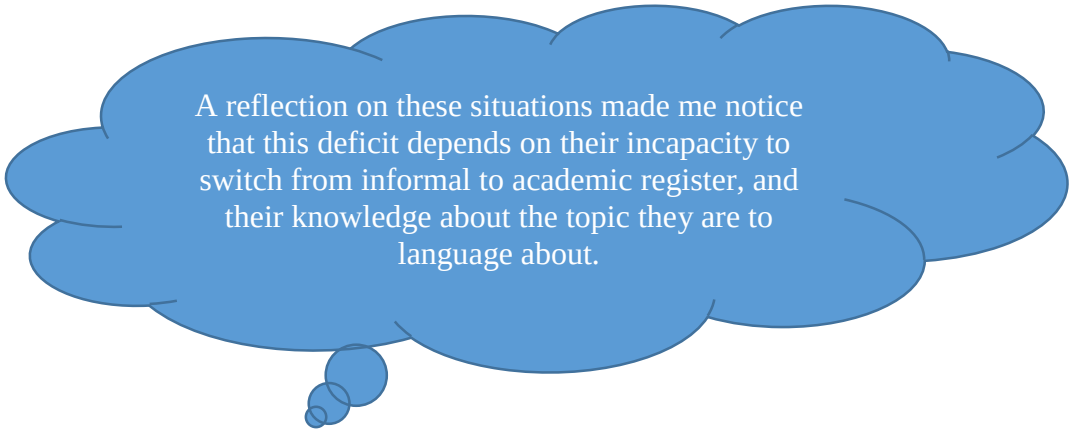
Exceptions to the later were 4 students:

- JDOM comes from nursing university studies. He entered the studies last year – so he learnt 2nd year subjects first.
- JDP comes from baccalaureate, this is his 1st year.
- APO entered the studies 4 years ago. Her high motivation was founded on her desire to finally graduate. This year, she was an example of "learning success if doing the homework".
- TPM comes from 4-EQF level IT VET. He entered the studies last year – so he learnt 2nd year subjects first.

I was shocked in the first exam that most of them did not know their ID number. When I shared this with the principal, she told me that many of the students came to register at the school with their mothers and when asked about their previous studies (CSE, VET level 4, etc.), they had to ask their mothers whether they have studied those programs.

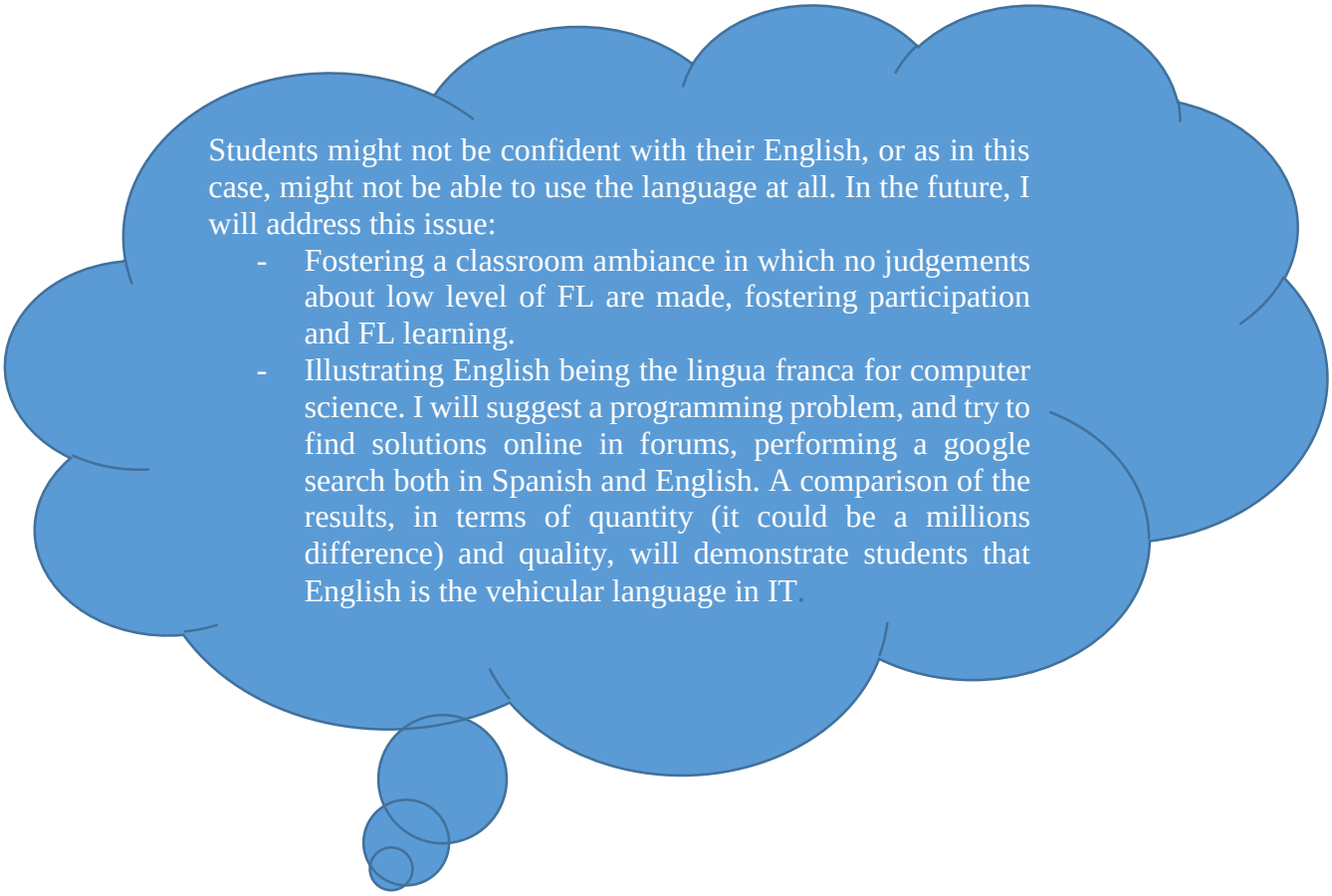
Students' proficiency in L1 and English

Students, in general, showed a deficit regarding **academic** communicative skills in L1, although the severity of it varied from one student to another. Their oral discourse was extremely hesitant; their written discourse, when present, was not structured and sometimes not even correct according to Spanish language rules. Occasionally, I overheard students talking about weekend plans or videogames and they seemed to be different people: their **informal** speech was completely fluent, although they still made some grammar mistakes.



Regarding reading comprehension, students, in general, showed an incapacity to effectively read and understand. This happened not only during learning lessons but also during the exams: they would keep asking doubts that were explicitly explained in the instructions of the tasks. I am aware this is something that happens in most of the classes but it was shocking, providing that students were, at least, 18 years old.

In the same manner, students' **English** skills were awfully poor. Only one student was studying English regularly, outside school, to prepare for a B1 level exam. During classes, as this VET programme was not CLIL, they all complained every time I would show some materials in English, although at some point I decided to explicitly explain the character of English as lingua franca for many topics, being IT one of them.



It was observed how the first thing they do after accessing a webpage written in English is to click on the browser "translate" button. Most webpages including code and explanations are not well-formed to be read by translating software, and so, the "code parts" (begin, loop, for, if, then…) keywords were translated into Spanish too. Students struggled with these issues instead of paying attention to my explanations.

They had a module called "Technical English", two hours a week. In the teacher's words: "their level is 'to-be-verb-like' so I am happy if next week they can remember the basic IT vocabulary we learn this week".

To be honest, I maintained an intransigent position with respect to the exposure of materials in English. It is a must. The explanations in those materials were short and explained by me in Spanish in class. But I have to admit that if I had to read IT documentation in Japanese I would have to rely on google translator too.

PROGRAMMING EXAM

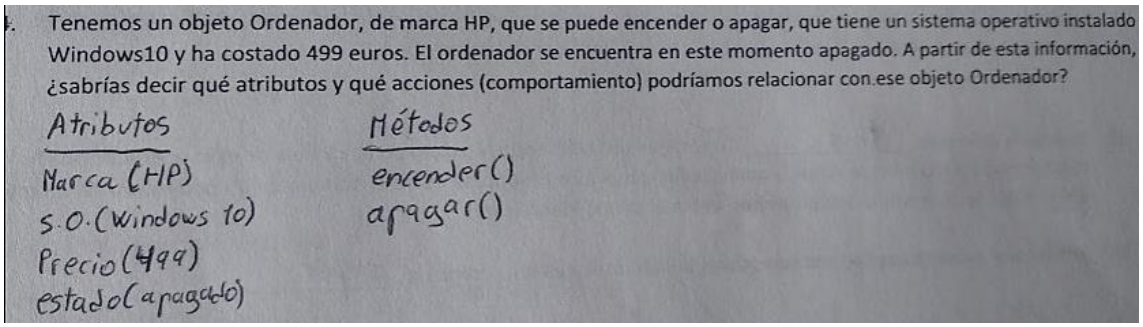
Commentaries on the exam

The final exam consisted of a written test that was worth 30% of the grade and a practicum worth 70% of the grade.

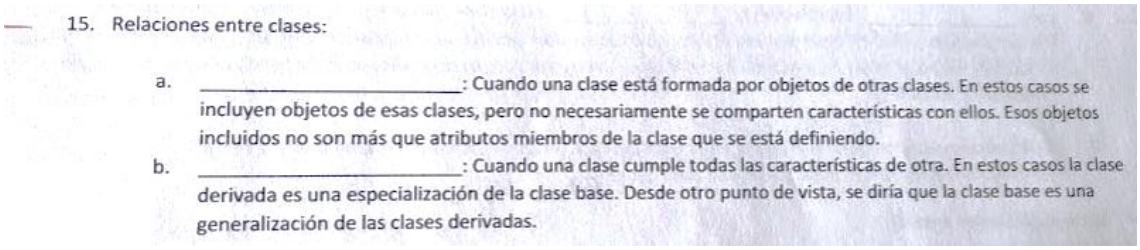
Students could make use of their materials, either printed or digital. This includes notes or even source code of programs we coded in class. The auto-completion feature of the development environment is enabled, as it is something they should have learnt to use and take advantage of it. In turn, they do not have Internet access in order to prevent task-splitting between them.

Student JPD

Correction (test): He performs well in questions involving thinking – I can actually "see him thinking" in class, and also his "aha moment". He understands the concepts. Example:



In turn, he does not answer "more theoretical questions". Even though he knows about these concepts, he has not studied, and consequently, he is not able to identify them:



He understands but does not formally study.

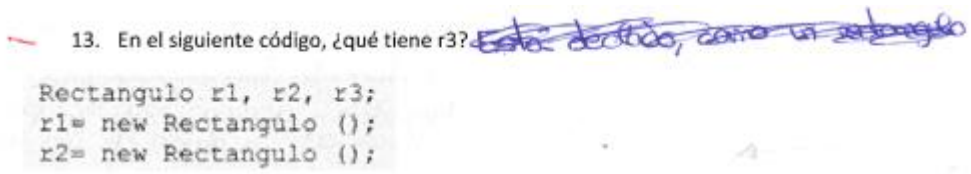
Usually, there is a worse case: those who do not understand – and consequently cannot properly code anything – but *try* to study memorizing without understanding. These ones might answer Q15, but will not have enough points to pass the exam (it is prepared to test whether the student *actually* knows or not about programming, and so, the amount of these questions is not enough to pass the exam).

JPD understands the language that I use in classroom to discuss about programming problems. When he has doubts, he usually calls items by their technical name. Consequently, he understands concepts and know "what to do". On the other hand, as he does not "study" (meaning memorize), he struggles to answer questions "from the book".

Student SGAA

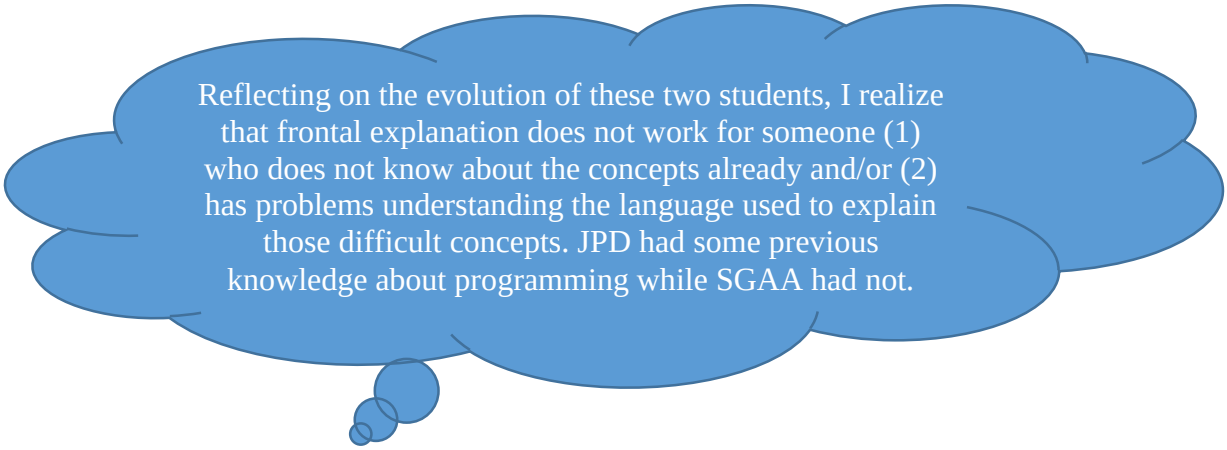
Pre: He pays attention in class, but usually do not understand concepts. Comes with a minimum level of maths, English, and reading comprehension. When given explanations, I can't assure 100% that he has finally understood. He is able to memorize, but not reasoning (even in trivial problems).

Correction (test): Questions literally extracted from the materials they were provided, were answered right. Some questions involving thinking or explaining were answered right, others were left blank.


13. En el siguiente código, ¿qué tiene r3?

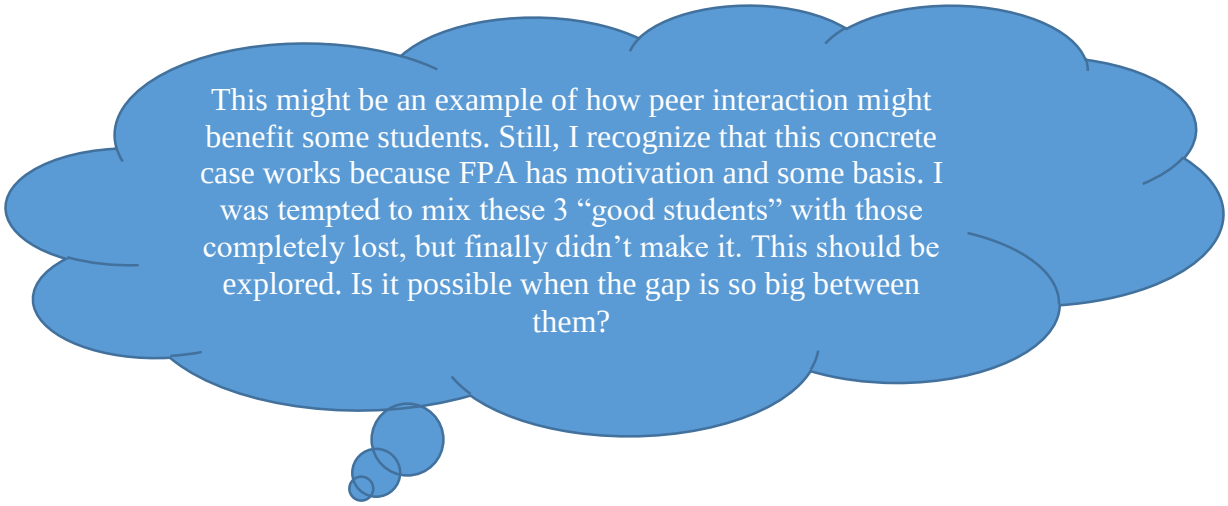
```
Rectangulo r1, r2, r3;
r1= new Rectangulo ();
r2= new Rectangulo ();
```

This student represents the opposite case. The fact that this student performs well answering questions "from the textbook" but fails when questions address the practical aspects of those concepts, makes me suspect that he just memorises concepts **without understanding the language.**



Student FPA

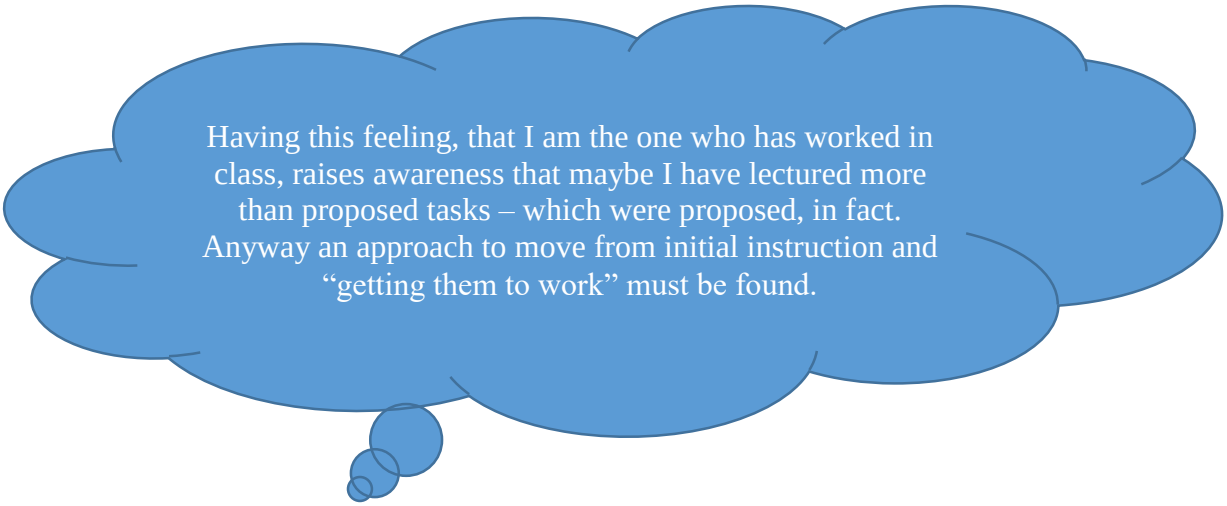
Pre: He entered the studies last year (2nd course modules studied first) and passed, so he must have some idea of programming. He teams with JDOM and TPM, who perform well in all the modules, and so does FPA who benefits from their help but still clearly is not at the same top level.



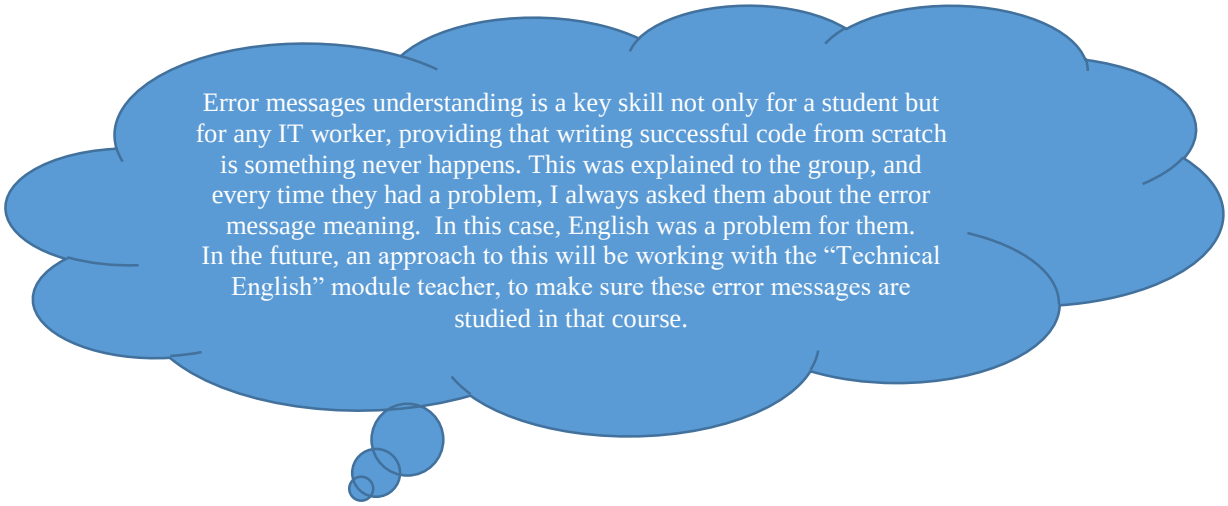
Correction (test): He clearly has not studied theory for the exam. He answers correctly thinking questions (Q13) – which wasn't so difficult after all – but then didn't answer questions "from the book" (Q14, Q15), or answer wrong (Q16, where he answers exactly the opposite of the concept: "Con otras palabras" when it should be "con las mismas palabras").

Correction (practice): He has coded Q1 (Abstract class) right. Hasn't even tried Q3 (Hashmap). Program 4 does not work because he is using an object which is not instantiated

and initialized. This is a key concept in object oriented programing which has been worked in class (only by me, the teacher?).



Still, they were taught to read the compiler's error messages in order to overcome these problems, but they kept not doing it. They have an issue here: those messages are in English, providing accurate technical information about the error, **which, even in Spanish might sound strange to them if they are not very confident to what they are doing and are "just trying"**. (i.e. in this case: *Unresolved compilation problem: The local variable Statement may not have been initialized*)

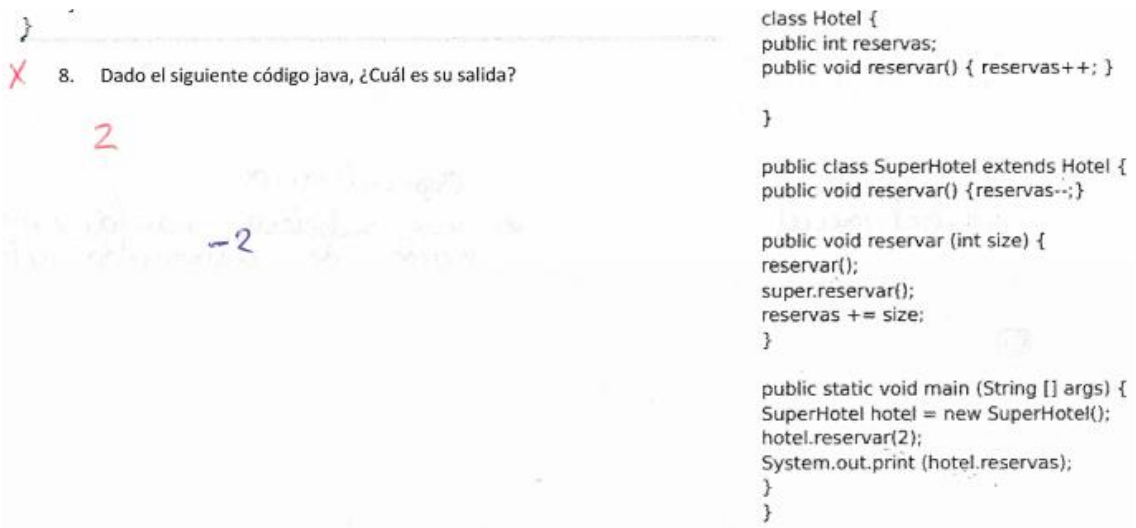


PROGRAMMING (RESIT)

Between the exam and the resit exam, the HashMap and ArrayList data structures were explained to them again. I explained the original exam problem requirements in the whiteboard and gave them a photocopy with an empty table so that they could start to solve it paper-and-pencil. Some of them caught it up, but others still don't.

I could witness something while they were working paper-and-pencil. One of the students who finally had understood the concept of this data structure was explaining it to a student who still hadn't, on her paper. The explanation wasn't very accurate, but it seemed that the second student finally could see how it works. Cooperative learning belongs to the category of things I have studied during these teacher-training masters but then I have failed to implement.
This finding was casual, but in the future, I ought to foster cooperative learning by tasks explicitly designed to do so.

Students frequently fail in Q8, which focused on reading and understanding the given code, to tell the value of a variable at a specific point.

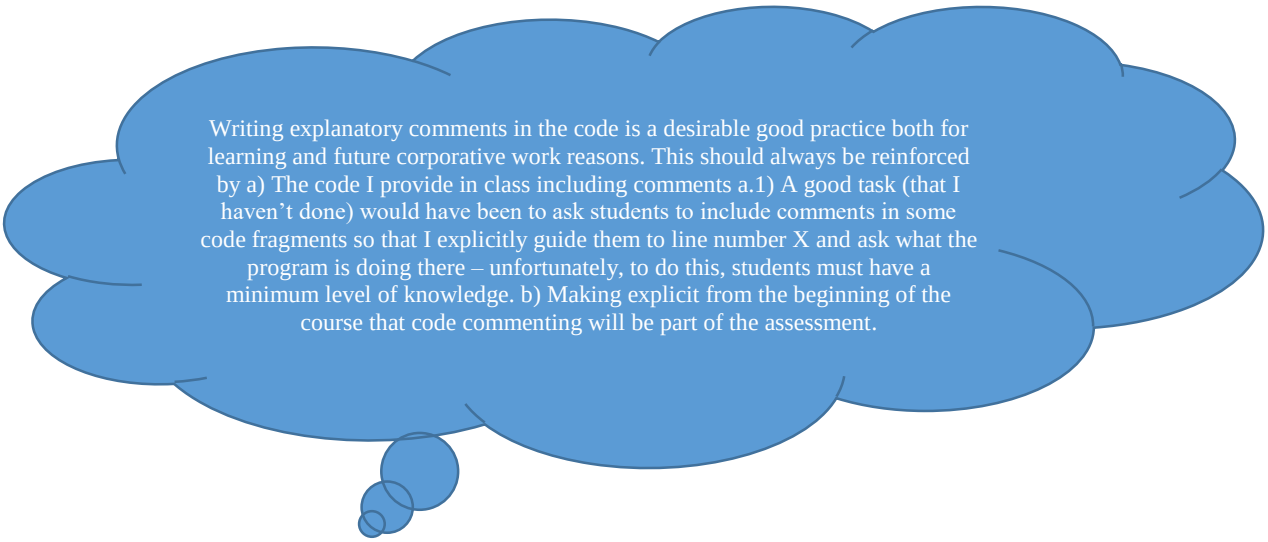


Even though "reading code" is a skill inherent to all the tasks that were carried out, this type of exercise could have been worked more in class (explicitly).

Student APO

Pre: As said in the group description, she is very committed to finally finish the studies. She enrolled in the program 4 years ago. She and JDOM are the only students who made the homework and come to class with doubts.

She always writes explanatory comments in the code – this has helped her to learn programming and databases and, what is more, will help her when finally working in a company; this is a very important aspect that we Engineers with coding experience usually miss, resulting in a mess when we work in teams (almost always).



Correction: As expected, she has passed the exam, doing all the tasks right, with minor pitfalls.

FINAL REFLECTIONS

After these initial months as a teacher, I have experienced that putting into practice what has been theoretically studied in teacher-training programs is not trivial nor as easy as it could have seemed. Learning processes take place in a context and in – as is the case – heterogeneous groups which add many variables to the learning-teaching experiences.

Catering for diversity is an essential part of the teaching practices, especially in groups with diverse degrees of previous knowledge. Multi-level tasking is a suitable approach to meet students' needs for both low and high achievers. Still, there is a feeling that this was not enough in order to make the former succeed. Learning progressions were planned from simple to complex concepts for all the group. High achievers were provided more tasks while low achievers were provided with explanations, suggestions to induce their "aha moment" – if they

were at least in the right track-, or simplified versions of the tasks, but many times this was non-successful because students' previous knowledge was completely void.

In Vygotskyan terms: where is students' "proximal development zone"? and, if as I suppose, it is somewhere back at the beginning of CSE, where do I start to scaffold from? Will they eventually catch up?

> As a VET teacher, I believe I should not bother about gaps like "we don't know the formula of the square or the triangle area". But as a prospective CSE level teacher, especially in maths, I should be ready and trained to deal with knowledge deficiencies from previous courses. At the moment of writing this diary, I am not sure how I will deal with this. As theoretically studied, student-centred approach might help every student develop their knowledge about the subject. But will this adapted, personalized approach be affordable in a thirty students classroom?

In some cases, it was frustrating reformulating the input trying to be understood without success. There were some occasions where I could witness students finally understanding a concept after another student's clumsy explanation. This "talking to your neighbour" approach might be useful in the future, and so peer instruction (Crouch et al., 2007) will be taken into account.

Humbly, this indicates that I could have still "gone less accurate but understandable", trying to "see learning through the eyes of the student" (Hattie, 2009), and consequently, making sure that a proper didactic transposition (Chevallard, 1997) to students' level was carried out when presenting complex concepts to students.

Future teaching experience and readings will provide more tools to be able to meet all students' learning needs.

Talking about **complex content**, it has been experienced how its learning cannot rely on traditional lecture nor a "misunderstood constructivism". Of course, I still believe students should be actually doing something in class: learning tasks. But my mistake here was to think of learning tasks as the combo *task + teacher guidance*, when it is actually more than that. *Task + teacher guidance* would be an approach when students have already learnt something about the topic - in fact, that is what scaffolding is- but this was not the case due to the impossibility to connect with inexistent previous knowledge.

In turn, learning tasks should be carefully planned taking into account cognitive load theory (Sweller, 1994) and consequently, complex content – or what Geary (2008) identifies as secondary biological knowledge - should be explicitly taught, making use of multi-modal inputs, rehearsing, imaging, mnemonics, elaboration, chunking, etc.

This was realized at the end of the course when I tried to address the data-structure learning problems with a paper-and-pencil, step-by-step approach, aside with previously explained programming codes. But even though some students finally understood, their apprehension to the topic was too difficult to be allayed.

In fact, from this experience, I can also estimate that lack of **motivation** is a handicap to succeed in studies. In the future, I will try to overcome this issue by

- Paying attention to tasks being meaningful, real-life related, and job-oriented.
- Making expected outcomes visible (Hattie & Yates, 2013) to students regularly, so that they can use this meta-knowledge to situate themselves in the learning process, not only when they are lost but also when they are making progress.

Regarding the **IT studies misconception**, and in order to deal with it in the future, at the beginning of the course, I could prepare videos where former colleagues explain their current projects, showing not only the coding part but also the previous required logical-mathematical thinking processes. Also talking about management (deadlines, workload etc.) should be done - finding a balance between making students realize what this is really about, and not de-motivating them-. In addition, some problem resolution in class could work in this "warming-up/presenting the profession" phase: dining philosophers' problem (concurrency), Konigsberg bridges problem (graph theory), etc. After carrying out these tasks, I should present concrete real examples of their applicability.

Talking about **evaluation**, which was the reason why I started writing this document, it is clear that formative assessment should be promoted by mandatory tasks which would provide the opportunity to give feedback to students (both remedial but also positive). Consecutive self-assess tasks are a good opportunity to foster student's self-sufficiency – and this can be easily done in programming tasks.

Writing these lines, I recall how students would not read my detailed and personalized feedback in their exams solutions: they would just sum their points to check that I had not made a mistake. How to deal with this issue? I believe that in a classroom everything is connected, and consequently, a better approach in previous paragraphs topics (how to help to learn complex

content, how to boost students' motivation, etc.) will also help students to deal with feedback – I must admit some of them would not pay attention to the provided suggestions just because they thought they would not understand them at all.

In addition, and as aforementioned, assessment should be visible (Hattie, 2009; Hattie & Yates, 2013) to students, that is, they know what is expected and how it is going to be evaluated. This would help them to situate themselves in the learning path.

I cannot finish my reflection about evaluation without a question that has been on my mind: what is my role in the system? (in this case VET). At the end of the course, despite their lack of knowledge, I have marked some students to pass too, so I have contributed to the same issue I criticise – what will next teacher think about those students who have passed, but have little idea of the subjects?

Annex II. Textbook and selected links for the topic

Recommended book

2.1. Introducción

Todo sistema informático debe ser asegurado mediante la correcta instalación, configuración y actualización del software de seguridad adecuado, para protegerlo ante posibles ataques que aprovechen vulnerabilidades o servicios mal configurados o protegidos.

2.1.1. Fases de un ataque

Todo ataque a un sistema informático suele llevarse a cabo en cinco fases muy definidas, según la certificación CEH (*Certified Ethical Hacker*):

Figura 2.1
Fases de un ataque informático.

A) Reconocimiento (reconnaissance)

Fase preparatoria en la que el atacante reúne toda la información posible de su objetivo, basándose en cualquier fuente, incluida la ingeniería social. Esta fase también puede incluir un escaneo no autorizado de la red (interno o externo).

El potencial atacante diseña su estrategia de ataque, y para ello tarda el tiempo necesario para recabar la información crucial del objetivo. Para ello acude, si es necesario, a la basura de la víctima (*dumpster diving*), donde puede encontrar información de nombres de usuarios, contraseñas, números de tarjetas de crédito, recibos bancarios, números de teléfono, etc.

En general, las técnicas de reconocimiento pueden dividirse en activas y pasivas. Las técnicas activas implican la interacción con el sistema informático víctima, por ejemplo, el uso de herramientas para detectar equipos accesibles, routers, etc. Las técnicas pasivas no interactúan directamente con el sistema, sino que acopian información sobre este obtenida de fuentes públicas, ingeniería social, etc.

Figure II-1. Course recommended textbook page on the topic (Triviño, 2019, p.44)

B) *Escaneo* (scanning)

El escaneo es el método que un atacante lleva a cabo antes de atacar realmente el sistema víctima. Utiliza toda la información obtenida en la fase anterior para identificar vulnerabilidades específicas, por lo que esta fase puede considerarse una continuación lógica del reconocimiento activo.

En el escaneo habitualmente se utilizan herramientas automatizadas. Puede reunirse información crítica de la red utilizando comandos tan simples como un *traceroute*. Una vez identificados los equipos activos (*live systems*), se escanean los puertos abiertos, se identifican los servicios que están a la escucha, se identifica el sistema operativo subyacente, se elabora un mapa de equipos vulnerables alcanzables y, por último, se buscan las vulnerabilidades con software específico para esta misión (*vulnerability scanners*). Un administrador del sistema debe preocuparse de tapar todos los agujeros, pero un *hacker* solo necesita uno para entrar, por lo que siempre se encontrará en ventaja.

C) *Obtención de acceso* (gaining access)

Esta fase es la más importante dentro del ataque, en términos de daño potencial, aunque no siempre es necesario ganar acceso al sistema para causar algún daño (por ejemplo, en las técnicas de denegación de servicio, agotando los recursos de la máquina).

Varios factores influyen en las posibilidades que tiene el atacante de ganar acceso al sistema objetivo: la arquitectura y configuración del sistema y, por supuesto, el nivel de destreza del atacante.

D) *Mantenimiento del acceso* (maintaining access)

Una vez que el atacante ha conseguido acceder al sistema objetivo, este puede elegir entre utilizar los recursos de dicho sistema para lanzar un ataque posterior a otros equipos o permanecer explotando el sistema con un perfil bajo que le impida ser detectado. Sea cual sea la decisión, el atacante instala una puerta trasera (*backdoor*) que le permita volver a entrar sin ser detectado. Dicha puerta trasera puede inocularse en la forma de un troyano, un *rootkit*, etc. (encontrarás más información sobre estos métodos en el capítulo 4).

Los atacantes pueden mantener el control sobre "sus" sistemas durante mucho tiempo, a lo largo del cual pueden dedicarse a robar datos, consumir ciclos de CPU, alterar información sensible, etc.

E) *Borrado de huellas* (covering tracks)

Un atacante siempre quiere destruir las evidencias de su presencia y actuaciones en el sistema, principalmente por dos motivos: mantener el acceso y evitar consecuencias penales. Las huellas para borrar se encuentran en múltiples ficheros log del sistema: registro de inicios de sesión, posibles errores provocados por la fase de escaneo o la de penetración en el sistema, etc.

Es primordial para un atacante que el sistema tenga la misma apariencia que antes de que ganara acceso y estableciera la puerta trasera, por lo que no basta con eliminar líneas de ficheros log, sino que debe restaurar atributos de los ficheros alterados (tamaño, fecha de modificación, permisos).

Figure II-2. Course recommended textbook page on the topic (Triviño, 2019, p.45)

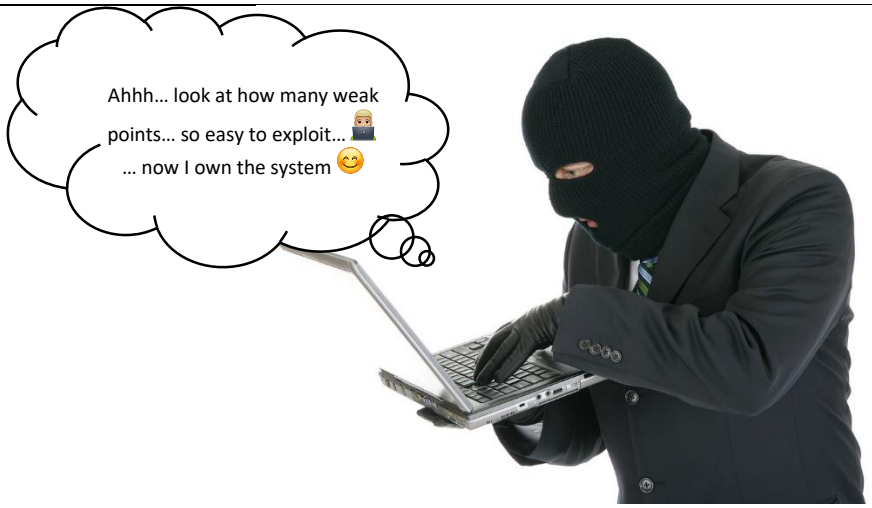
Selected Internet links

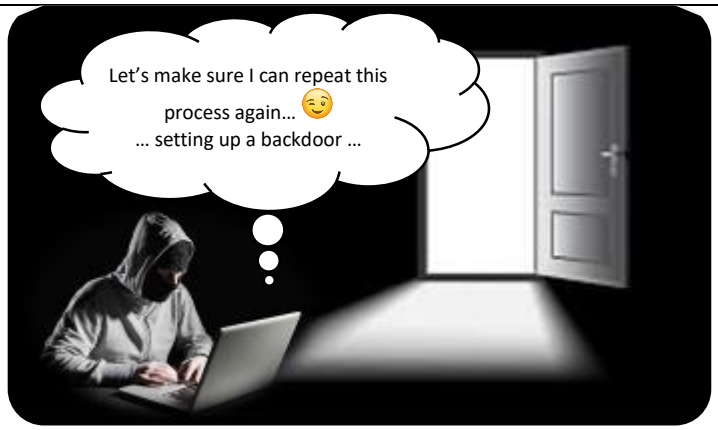
Title:	CEH: Certified Ethical Hacker: The phases of ethical hacking
Url:	http://certifiedethicalhackerceh.blogspot.com/2011/08/phases-of-ethical-hacking.html
Last accessed:	16/02/2020
Title:	The Five Phases of Ethical Hacking
Url:	https://www.simplilearn.com/phases-of-ethical-hacking-article
Last accessed:	16/02/2020
Title:	The Attacker's process
Url:	http://www.pearsonitcertification.com/articles/article.aspx?p=462199&seqNum=2
Last accessed:	16/02/2020
Title:	5 Phases of Hacking
Url:	https://www.geeksforgeeks.org/5-phases-hacking/
Last accessed:	16/02/2020

Annex III. Printable tasks

1	Read this short text: One of the tasks of an ethical hacker is to test the security of an organization. In order to do that, a white-hat hacker follows processes similar to those of a malicious hacker, given that the steps to gain and maintain access into a computer system are similar no matter what the hacker's intentions are. Now, use this information and what you already know from previous units to answer the questions below.
a)	A *malicious* / *ethical* hacker is also known as a white-hat hacker.
b)	*Vulnerabilities* / *vulnerability* is the weakness which can be exploited by a threat actor, such as an attacker, to perform unauthorized actions within a computer system.
c)	An *exploit* / *evidences* is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behaviour to occur on a system.
d)	An attacker might *explode* / *exploit* a vulnerability in order to gain unauthorized access to a system.

1A	Alice and Bob are two students that have just defined some words from exercise 1. Although both definitions are correct, Bob expressed himself in academic language and consequently obtained better marks. Match the following sentences with a word from exercise 1.	
	Alice	Bob
	A verb meaning "to use something to one's own advantage".	A verb meaning "to use personal skills, aptitudes, resources, or a particular situation in order to obtain an opportunity which is beneficial for the subject".
	A verb meaning "to break up into pieces".	A verb meaning "to burst violently, usually provoking an extremely loud noise".
	The possibility that something bad will happen.	A potential source of imminent danger or harm.
	Some but not all of a thing.	A piece of something, especially a large part.

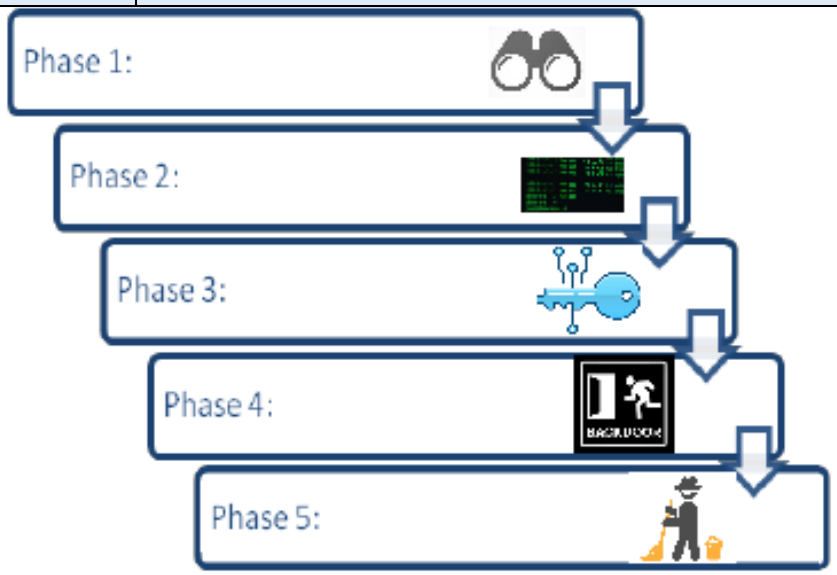
2	Match the following situations with the phase names of an attacking process.
	Gaining access Reconnaissance Scanning **Covering tracks Maintaining access**
1	
2	
3	

4	 Let's make sure I can repeat this process again… 😌 … setting up a backdoor …
5	 I wasn't here 😝 … Removing my traces so that nobody can find me

2A	In the following pieces of text, the different phases of an attack are briefly described. Unfortunately, Mallory has intentionally cluttered the paragraphs. Rearrange the paragraphs and write down the names of the phases.
Order	**Description**
	a. _____, also known as the preparatory phase, involves gathering information about a potential target.
	b. Last, but not least, it is necessary to remove any traces of the attack, so that detection by security personnel and legal actions are avoided.
	c. _____. After vulnerabilities have been exposed during the scanning phase, the actual hacking takes place. Those weak points of the system are now exploited in order to own the system.
	d. _____ involves taking the information discovered during prior reconnaissance and using it to examine the network using different tools, looking for vulnerabilities.
	e. As crucial as the 'Gaining access' phase is the m_____ access. During this phase, it is necessary to secure the access so that it is maintained for future exploitation and attacks.

2B	Now, check your answers by answering these questions.
What words made you think sentence (a) is the first sentence?	
What words made you think sentence (d) comes after sentence (a)?	
What words made you think sentence (c) is the third sentence?	
What words made you think the 4th phase (e) is called 'Maintaining access'?	
What words made you think sentence (b) comes last?	

2C	Now write down again the names of the 5 phases of an attack, with the clues provided by the icons.



3	Read the following text about the first phase of a cyber-attack.

Reconocimiento

Fase preparatoria en la que el atacante reúne toda la información posible de su objetivo, basándose en cualquier fuente, incluida la ingeniería social. Esta fase también puede incluir un escaneo no autorizado de la red (interno o externo). El potencial atacante diseña su estrategia de ataque, y para ello tarda el tiempo necesario para recabar la información crucial del objetivo. Para ello acude, si es necesario, a la basura de la víctima (dumpster diving), donde puede encontrar información de nombres de usuarios, contraseñas, números de tarjetas de crédito, recibos bancarios, números de teléfono, etc.

En general, las técnicas de reconocimiento pueden dividirse en activas y pasivas. Las técnicas activas implican la interacción con el sistema informático víctima, por ejemplo, el uso de herramientas para detectar equipos accesibles, routers, etc. Las técnicas pasivas no interactúan directamente con el sistema, sino que acopian información sobre este obtenida de fuentes públicas, ingeniería social, etc.

Write the Spanish equivalent next to each of these English phrases about the first phase of a cyber-attack. The English sentences are not identical to the Spanish ones from the previous excerpt, so you must also modify your Spanish sentence. The English phrases are also in informal English: you should write in academic Spanish.

1. During the reconnaissance phase, an attacker tries to collect as much information as possible about the potential victim, by different ways like social engineering or unauthorized network scanning.	
2. Another trick is to get the victim's information from the rubbish, which is called dumpster diving.	
3. There are two types of reconnaissance techniques: active, which involve interaction with the victim' system; and passive, getting the information from somewhere else.	

3A	The previous task established *Social Engineering* as an activity which is usually performed during the reconnaissance phase. 8. Watch the following video once. 9. Look at these questions and answer them while watching the video again. 10. Check your answers with your partner.

https://www.youtube.com/watch?v=lc7scxvKQOo

11. Social Engineering is basically…	e. voice solicitation
12. A vishing call is…	f. using the phone to extract information or data points that can be used in a later attack.
13. A vishing attack consists of…	g. faking the caller number from which you are supposedly phoning.
14. "Spoofing" from a phone number consists of…	h. hacking without any code.

3B	Read the following excerpt which summarizes the Reconnaissance phase:

"When hackers are looking for information on a potential target, they commonly run an Internet search on an individual or company to gain information. This can be done either manually or using automatized tools. Social engineering and dumpster diving are considered passive information-gathering methods of the *former*, whereas sniffing the network is an example of the *latter*."

What do the words **former** and **latter** refer to? Think of a rule to remember which word refers to the first, and which one refers to the last.

Former refers to: _____

Latter refers to: _____

Rule to remember the order:

4	Let's compare a cyber-attack to a bank robbery. Can you match these phases between them? 1. Match bank robbery situations with phases 1, 2, or 3. 2. Match each pair with a cyber-attack situation x, y, or z.

a. Sitting on a bench in the hall of a bank headquarter, just paying attention to every movement of the employees.
b. Taking the elevator and walking through the corridors of the bank offices, taking notes of the open hours written on every door.
c. Actually going back to the offices at a time where nobody is supposed to be there, and checking whether the doors are locked.

1. Scanning
2. Passive reconnaissance
3. Active reconnaissance

x. Running a script on a system website, obtaining just the type of web server and operating system it is installed on.

y. Navigating through a system website.

z. running an automatized vulnerability scan on the system website.

_ _ _ _ _ _ _ _ _

4A	Last class, Alice wrote a piece of information about the Scanning phase that was marked A+. Can you guess which text corresponds to Alice? _____

Scanning-1

Scanning involves taking the information discovered during reconnaissance and using it to examine the network. It could be considered as the logic evolution of active reconnaissance. Tools that a hacker may employ during the scanning phase include:

- Diallers.
- Port scanners.
- Network mappers (i.e. *Nmap*)

One of the goals might be to map open ports and applications.

Techniques to lessen the chance of detection, consisting of scanning at a very slow rate, might be used. As an example, instead of checking for all potential applications in just a few minutes, the scan might take days to verify what applications are running. Many organizations use *intrusion detection systems* (IDS) to detect just this type of activity.

One key defence against the hacker is the practice of *deny all*. This rule can help reduce the effectiveness of malicious actions at this step. *Deny all* means that all ports and applications are turned off, and only the minimum number of applications and services that are required to accomplish the organization's goals are turned on.

Scanning-2

Scanning is the phase after active reconnaissance that uses the information obtained to scan the network looking for open ports and applications. The following tools are used by a hacker in this phase:

- Diallers.
- Port scanners.
- Network mappers (i.e. *Nmap*)

The hacker uses methods to avoid being detected, for example by scanning slow to not being caught by *intrusion detection systems* (IDS) to detect scanning.

A possible solution is called *deny all*. *Deny all* works turning off all ports and applications except the ones needed by the company to work.

Now, provide examples of fragments with…	
4. Impersonalized sentences	Potential answer: "It could be consider".
5. Find where the phrase "being identified" is now a "noun" in the sentence (i.e. "nominalization")	Answer: "detection"
6. Repetition / A sentence where repetition was avoided.	Potential answer: "A possible solution is called *deny all*. *Deny all* works…"

5	Read the following excerpt about the Gaining access phase:

Gaining access

As far as potential damage, this phase could be considered one of the most important steps of an attack, which occurs when the hacker moves from simply probing the network to actually attacking it. Vulnerabilities exposed during the reconnaissance and scanning phase are now exploited to gain access to the target system. The hacking attack can be delivered to the target system via a local area network (LAN), either wired or wireless; local access to a PC; the Internet; or offline.

Examples include stack-based buffer overflows, denial of service (DoS), and session hijacking. Gaining access is known in the hacker world as *owning the system* because once a system has been hacked, the hacker has control and can use that system as they wish.

This is the context where *privilege escalation* takes place, which is the act of gaining elevated access to resources that are normally protected from an application or user, with the intention of performing unauthorized actions.

Find and write down a sentence used to give examples. Underline the words that denote exemplifying.
Find and write down a sentence used to express comparison. Underline the words that express comparison.
Find and write down a sentence used to express purpose. Underline the words that denote purpose.
Find and write down a sentence used to express a definition. Underline the words that denote definition.

6	Read the following excerpt about the Maintaining access phase:

Maintaining access

In this phase, the attacker tries to retain the ownership of the system for future exploitation and attacks. Sometimes, hackers ***harden*** the system from other hackers or security personnel by securing their **exclusive access** with backdoors, rootkits, and trojans. Once the hacker owns the system, they can use it as a base to launch additional attacks. In this case, the owned system is sometimes referred to as a *zombie system*.

Sometimes hackers might even fix the original problem that they used to gain access so that they can keep the system to themselves, and prevent other hackers from entering.

Providing the dictionary definitions for *harden*, which do not exactly fit in this context. Can you infer its meaning from the text? Write a dictionary-definition for "*to harden (computer science)*". Share it with your partners until you determine the most academic definition.

harden

verb [I or T]

UK /ˈhɑː.dᵊn/ US /ˈhɑːr.dᵊn/

harden *verb* [I or T] **(SOLID)**

to become or make hard:

- *The mixture hardens as it cools.*
- *It is thought that high cholesterol levels in the blood can harden the arteries (= make them thicker and stiffer, causing disease).*

harden *verb* [I or T] **(SEVERE)**

to become more severe, determined, or unpleasant:

- *Living in the desert hardened the recruits (= made them more strong and determined).*
- *As the war progressed, attitudes on both sides hardened (= became more severe and determined).*

Discuss with your partner: After owning a system, why would an attacker want to ensure that access is only limited to them and not accessible to other hackers?

7	Read the following excerpt about the last phase of an attack, and then make the activity below.

Covering tracks

Reasons for covering tracks of actions vary from avoiding legal action to being able to continue using the system. Evidence removal delays attack detection by deleting tracks in log files or in intrusion detection systems (IDS) alarms.

Mallory has been attacking the server of a company and consequently, there are traces in this log that reveal his unauthorized activity. Help Mallory to cover his tracks and get away with this attack by crossing out traces of his presence in the system:

```
2020-02-10 07:50    Incoming connection: Alice@office
2020-02-10 07:50    Incoming connection: Bob@office
2020-02-10 08:00    Incoming connection: Alice@office
2020-02-10 08:15    Incoming connection: Heidi@office
2020-02-10 08:54    Incoming connection: Trudy@office
2020-02-10 09:14    Incoming connection: Bob@office
2020-02-10 10:00    Incoming connection: Alice@office
2020-02-10 12:25    Incoming connection: Mallory@Unknown-location
2020-02-10 12:30    Incoming connection: Mallory@Unknown-location
2020-02-10 12:35    Incoming connection: Bob@office
2020-02-10 12:39    Incoming connection: Mallory@Unknown-location
2020-02-10 13:00    Incoming connection: Trudy@office
```

7B	Match the following examples of actions/tools with the phase they are related to:
a) Backdoors, rootkits, and trojans.	
b) Social engineering, dumpster diving, and sniffing.	
c) Deleting traces in registry files (logs) or removing IDS alarms.	
d) Network mappers, port mappers, network scanners, port scanners, and vulnerability scanners.	
e) Buffer overflow, DoS, password filtering, and session hijacking.	

8	- Alice is a professional white-hacker who has written a report for Bob, a client who wants to assess the cybersecurity of his company. - Mallory is a hacker writing an email to Eve, another hacker, about his last attack. Both the report and the email have been cluttered. Can you order these fragments into the original documents? Hints: use a pencil and rubber, and the boxes to set A/M and an order number in the writing. Try to distinguish the report from the email paying attention to the register of the language. Example: A 3

An examination of these hosts revealed a password-protected administrative webserver interface. ☐☐	Alice's Report:
After a closer examination, we discovered that the compromised webserver utilizes a Java applet for administrative users. We added a malicious payload to this applet, which gave us administrative privileges at the same time that permanent access for future accessing. ☐☐	
Suddenly, I found a post-it note on a screen: "servers room: 4721". It resulted to be the access code to open the door. It worked! ☐☐	
I am concerned that I will be discovered because I am having trouble removing a specific log. Could you help me? ☐☐	
Initial reconnaissance of the company network resulted in the discovery of a misconfigured server that allowed the implementation of a specific attack. The results provided us with a listing of specific hosts to target for this assessment. ☐☐	
I plugged in a very small USB stick from which I will be able to connect remotely any time I want. ☐☐	Mallory's Email:
An examination of the administrative interface revealed that it was vulnerable to a remote code injection vulnerability, which was used to obtain interactive access to the underlying operating system. ☐☐	
So, yesterday I walked into the office and tried to enter the servers' room, which unfortunately was locked up by a password panel on the wall. Then, I started checking all the desks in the office, looking for something helpful. ☐☐	
Existing network traffic controls were bypassed through encapsulation of malicious traffic into allowed protocols, disguising any evidence. Concerns about the company security arise, providing all the malicious tasks. ☐☐	
During the last couple of weeks, I have been observing the habits of the employees of the company's data centre that hosts the servers. It turns out that every day from 2 pm to 3 pm there is nobody at the office. ☐☐	

8A	Now, re-read the texts and discuss with your partner: what features of the language in each excerpt made you distinguish its register? Give examples.	
	Alice's report language features:	Mallory's email language features:

Annex IV. Draft versions of tasks

The original draft versions of the CLIL materials presented below are intended to illustrate weak points in the original materials, which were then modified, informed by literature regarding cognitive load theory (see section 2.1.1).

Draft of the task originally proposed as Task 2: now substituted by Task 2

Draft	In the following pieces of text, the different phases of an attack are briefly described. Unfortunately, Mallory has intentionally deleted the names of the phases and has cluttered the paragraphs. Write in the names of the "Attack Phases" and rearrange the sentences into a proper paragraphs.	
Order	**Phase name**	**Description**
		a. _____, also known as the preparatory phase, involves gathering information about a potential target.
		b. Last, but not least, it is necessary to remove any traces of the attack, so that detection by security personnel and legal actions are avoided.
		c. _____. After vulnerabilities have been exposed during the scanning phase, the actual hacking takes place. Those weak points of the system are now exploited in order to own the system.
		d. _____ involves taking the information discovered during prior reconnaissance and using it to examine the network using different tools, looking for vulnerabilities.
		e. As crucial as the 'Gaining access' phase is the m_____ access. During this phase, it is necessary to secure the access so that it is maintained for future exploitation and attacks.

Professional Development Commentary: in light of what we know about the limitations of working memory (section 2.1.1), this CLIL task was weak for numerous reasons, not least of which it involved students in (1) reading a complex text in CALP-FL about (2) an unfamiliar topic so to (3) fill in missing words and then (4) re-organize the five complex texts (which (5) the students probably do not totally comprehend).

Back to page 34

Draft of the task originally proposed as Task 3: now substituted by all the tasks in the sequence

Note that language errors are in red; they were supposed to be deleted for the printable, student version.

Draft	Eve has intercepted the following paragraphs, which complete the information about attack phases. She does not know English well and, consequently, she has transcribed them committing some *language* mistakes. Read them carefully and correct any error. The number of mistakes per phase is given between parentheses.
(7)	**Reconnaissance** Also known as the preparatory phase, it consists consist of the systematic attempt to locate, gather, identify, and record information about a potential target. Reconnaissance phase can be classified clasify in two types: - Passive reconnaissance: involves gathering to gather information about a potential target without the targeted individual's or company's knowledge. Passive reconnaissance can be as simple as watching a building to identify what time employees enter the building and when they leave. However, in the case of cyber hackers, reconnaissance is done sitting in front of a computer. When hackers are looking for information on a potential target, they commonly run an Internet search on an individual or company to gain information. This can be done either manually or using automatized tools. Social engineering and dumpster diving are considered passive information-gathering methods of the *former*, whereas sniffing the network is an example of the *latter*. Performing a sniffing, one can yield useful information such as IP address ranges, naming conventions, hidden servers or networks, and other available services on the system or network. Sniffing tools are simple and easy to use and yield a great deal of valuable information which literally let you see all the data that is transmitted on the network. Many times this includes usernames and passwords and other sensitive data. This is usually quite an eye-opening experience for many network administrators and security professionals and leads to serious security concerns. - Active reconnaissance: involves involve probing the network to discover individual hosts, IP addresses, and services on the network. This process involves more risk of detection than passive reconnaissance due to the use of software tools that can be traced back to the computer that is running them, thus increasing the chance of detection for the hacker. Still, active reconnaissance is performed in order to obtain an indication of security measures in place (is the front door locked? – one have has to actually pull it to check it, assuming the risk of getting caught – this is why active reconnaissance is usually called rattling the doorknobs).

	Both passive and active reconnaissance can lead to the discovery of useful information to use in an attack. For example, it's usually easy to find the type of web server and the operating system (OS) version number that a company is using. This information may to enable a hacker to find a vulnerability in that OS version and explode exploit the vulnerability to gain more access.
(3)	**Scanning** Scanning involves taking the information discovered during reconnaissance and using it to examine the network. It could be considered as the logic evolution of active reconnaissance. Tools that a hacker may employ during the scanning phase include includes diallers, port scanners, Internet control message protocol (ICMP) scanners, ping sweeps, network mappers (i.e. *Nmap*), or simple network management protocol (SNMP) sweepers. One of the goals might be to map open ports and applications. The hacker might use using techniques to lessen the chance of being detected by scanning at a very slow rate. As an example, instead of checking for all potential applications in just a few minutes, the scan might take days to verify what applications are running. Many organizations use *intrusion detection systems* (IDS) to detect just this type of activity. One key defence against the hacker is the practice of deny all. The practice of the deny all rule can help reduce the effectiveness of the hacker's activities at this step. Deny all means that all ports and applications are turned off, and only the minimum number of applications and services are turn turned on that are needed to accomplish the organization's goals.
(2)	**Gaining access** As far as potential damage, this could be considered one of the most important steps of an attack. This phase of the attack occurs when the hacker moves from simply probing the network to actually attacking it. Vulnerabilities exposed during the reconnaissance and scanning phase are now exploit exploited to gain access to the target system. The hacking attack can be delivered to the target system via a local area network (LAN), either wired or wireless; local access to a PC; the Internet; or offline. Examples include stack-based buffer overflows, denial of service, and session hijacking. Gaining access is known in the hacker world as *owning the system* because once a system has been hacked, the hacker has control and can use that system as they wish. This is the context where *privilege escalation* takes place, which is the act of gaining elevated access to resources that are normally protected from an application or user, with the intention of perform performing unauthorized actions.
(3)	**Maintaining access** Once a hacker has gained access to a target system, they want to keep that access for future exploitation and attacks. Sometimes, hackers *harden* the

	system from other hackers or security personal personnel by securing their exclusive access with backdoors, rootkits, and trojans. Once the hacker owns the system, they can use it as a base to launch additional attacks. In this case, the owned system is sometimes referred to as a *zombie system*. Sometimes hackers might even fixing fix the original problem that they used to gain access so that they can keep the system to themselfs themselves.
(1)	**Covering tracks** Once hackers have been able gaining to gain and maintain access, they cover their tracks to avoid detection by security personnel, to continue to use the owned system, to remove evidence of hacking, or to avoid legal action. Hackers try to remove all traces of the attack; such as log files or intrusion detection system (IDS) alarms. Examples of activities during this phase of the attack include steganography, using a tunnelling protocol or altering log files.

3	Solutions
(7)	**Reconnaissance** It ~~consist~~ → it consists Reconnaissance phase can be ~~classify~~ → classified Involves ~~to gather~~ → gathering Active reconnaissance: ~~involve~~ → involves one ~~have~~ → one has This information ~~may to enable~~ → This information may enable ~~Explode~~ the vulnerability → exploit the vulnerability
(3)	**Scanning** Tools […] ~~includes~~ → Tools […] include The hacker might ~~using~~ → The hacker might use Services are ~~turn~~ on → services are turned on
(2)	**Gaining access** Vulnerabilities […] are now ~~exploit~~ → Vulnerabilities […] are now exploited With the intention of ~~perform~~ → With the intention of performing
(3)	**Maintaining access** Other hackers or security ~~personal~~ → Other hackers or security personnel

	Sometimes hackers might even ~~fixing~~ the original problem → Sometimes hackers might even fix the original problem keep the system to ~~themselfs~~ → keep the system to themselves.
(1)	**Covering tracks** Once hackers have been able ~~gaining access~~ → Once hackers have been able to gain access

Professional Development Commentary: again, evaluating this CLIL task through what we know about working memory and cognitive load theories, this CLIL task was weak for reasons very similar to those listed in the "weak" task presented above. In addition, involving students in the reading of such long texts about very complex concepts, only to perform very minor "choose the correct word" task may discourage students: although they can choose the correct word a handful of times, they still may not totally comprehend these long texts.

Back to page 37