sociUniversidad Nacional Abierta y a Distancia
Vicerrectoría Académica y de Investigación
Course: Information Security
Code: 202016905

Activity Guide and Evaluation Rubric – Task 2 - Attacking and defending

1. Activity Description

Type of activity: Collaborative	
Evaluation moment: Intermediate Unit 1	
Highest score of the activity: 125 points	
The activity starts on: Thursday, February 22, 2024	**The activity ends on:** Sunday, March 24, 2024
With this activity, you are expected to achieve the following learning outcomes: Assess information security risks in software development processes in accordance with standards and the organization's security policy to ensure the quality of software products.	

The activity consists of:
 	
Make a review of the readings corresponding to Unit 1 found in the learning environment.
 	
Collaborative work:
 	
This section aims to understand the topics required for the development of the activity. The topics of the unit are:
 	
• Pillars of Computer Security
• Risk Management and Security Controls
• Information security programs, processes and policies
• Continuity Plans
 	
For this, the collaborative group is organized to consult, address and debate the following questions:
 	
  1. What are the pillars of computer security and explain them?
  2. What is risk management in computer security?	

3. What are security controls?
4. Why is it important to implement an information security policy in an organization?
5. What is the objective of carrying out continuity plans in an organization?

Each student chooses one of the questions mentioned above, the question and the reasoned answer are documented and published in the activity forum, based on the readings made and their personal criteria. Additionally, she must make a comment to at least one response from a colleague, to express her support, complement or disagreement in a respectful and reasoned way.

It is important to cite the sources that support the opinions in APA 7 format, so that colleagues can consult them for further information.

Based on the participations made in the forum, the group prepares an online electronic presentation, presenting the relevant information on the topics developed in the questions. This structure is the next one:

Slide 1: Cover.
Slide 2,3,4,5 and 6: Thematic development.
Slide 7: References.
Slide 8. Conclusions.

Individual work:

This activity consists of two parts:

- **PART ONE – Defending:** Are you aware of the information that anyone can find out about us without restrictions on the Internet? The objective is to learn to find what can be known about themselves on the internet, using OSINT tools (Open Source INTelligence), translated as Open Source Intelligence. It refers to the set of techniques and tools to collect public information, analyze the data and correlate it, turning it into useful knowledge.

  In Google there are operators with combination capacity that provide us with very extensive information: intitle, allintitle, inurl, allinurl, filetype, link, inanchor, daterange, view / indexFrame.shtml, among others. On the other hand, there are a multitude of metasearch engines and other great sources of information within the Internet to search for any fingerprint or digital trace.

For the development of this activity, you must document and search for yourself, using the operators mentioned above. Search name, ID in social networks, on web pages, photos, access cameras, search for documents with password.

Examples:
○ Intitle: "My webcamXP server!" inurl: ": 8080. (Access a camera).
○ view / indexFrame.shtml
○ Servers with files called password.txt: intitle "Index of" "Index of /" password.txt (Search a directory structure for a Password file)
○ Robots: site: unir.net inurl: robot.txt

Obtain information from the Metasearch engines mentioned below and attach it to the individual work. In these search engines include your name (Make the search in at least three of the mentioned search engines):

www.yasni.es
http://es.kgbpeople.com
https://pipl.com
http://www.spokeo.com
http://webmii.com

Search your Username in the following metasearch engines to see whether or not it is available on the different social networks:

http://Checkusernames.com
http://namechk.com
http://knowem.com

Finally, it must conclude on what is the criminal capacity of the results obtained in the exercise.

- **SECOND PART Attacking:** TOR (The Onion Router) is a network superimposed on the Internet, which allows the exchange of information between an origin and a destination without revealing the identity of the users. It maintains the integrity and secrecy of the information that travels through it thanks to asymmetric cryptography and the concept of public and private keys. The guarantee of browsing anonymously and accessing the Deep Web (Deep Network) is total, accessing services that are often on the other side of legality.

  ○ The student must install the TOR application.
  ○ You must navigate in the TOR browser.

○ Leave evidence.
○ Conclude on the use in the TOR browser with reference to the criminal part. Check if in Colombia there are restrictions for the use of the TOR Browser and the legal consequences of its use.

The student must deliver the document of the individual work with the following structure:

1. Cover
2. Objectives
3. Part One: OSINT Tools
3.1. Evidence
3.2. To conclude on what is the criminal capacity of the results obtained in the exercise
4. Part Two: TOR Browser
4.1. Evidence of installation
4.2. Evidence of navigation
4.3. To conclude on the use in the TOR browser from the criminal part and its consequences
5. Bibliographic references

For the development of the activity consider that:

In the Initial Information Environment, you must:

• Check the course agenda to check the delivery dates of the activity.

In the Learning Environment, you must:

• Read the suggested readings for Unit 1.
• Enter the forum of the activity to debate with colleagues about the issues referred to.

In the Evaluation Environment, you must:

• Each student sends a digital document (a Word or PDF document) that contains the link of the electronic presentation online and with the evidence of their individual work.

Evidences of individual work:

The individual evidence to be submitted is:

- Participation in the activity forum.
- Digital document with evidence of individual work.

Evidence of collaborative work:

The collaborative evidence to be submitted is:

- Participation in the activity forum with contributions that contribute to the consolidation of group work.
- Link to online electronic filing.

2. General Guidelines for the Development of Evidences to Submit

For **Collaborative** evidence, consider the following:

- Before building the electronic presentation, it is important to analyze and organize the information.
- As you select the information, build the bibliography.
- You can use your preferred online presentation software, some options are: canva, emaze, prezi, genially.
- After building the electronic presentation, copy the link of the presentation into a Word document and send this document through the evaluation environment. Verify that the link works correctly and does not have access restrictions.
- For the consolidation of freelance work, you can use Word or PDF.

Please keep in mind that all individual or collaborative written products must comply with the spelling rules and presentation conditions defined in this activity guide. Regarding the use of references, consider that the product of this activity must comply with **APA** style.

In any case, make sure you comply with the rules and avoid academic plagiarism. You can review your written products using the Turnitin tool found in the virtual campus.

Under the Academic Code of Conduct, the actions that infringe the academic order, among others, are the following: paragraph e) Plagiarism is to present as your own work all or part of a written report, task or document of invention carried out by another person. It also implies the use of citations or lack of references, or it includes citations where there is no match between these and the reference and paragraph f) To reproduce, or copy for profit, educational resources or results of research products,

which have rights reserved for the University. (Agreement 029 - 13 de December de 2013, article 99)

The academic penalties students will face are:
a) In case of academic fraud demonstrated in the academic work or evaluation, the score obtained will be zero (0.0) without any disciplinary measures being derived.
b) In case of proven plagiarism in academic work of any nature, the score obtained will be zero (0.0), without any disciplinary measures being derived.

3. Evaluation Rubric Template

Type of activity: Collaborative	
Evaluation moment: Intermediate Unit 1	
The highest score in this activity is 125 points	
First evaluation criterion: **Contents:** Appropriation of the concepts of the pillars of computer security, risk management and controls, the importance of security policy and the objective of contingency plans. **This criterion represents 40 points of the total of 125 points of the activity.**	**High level:** Appropriate and argue the concepts of the pillars of computer security, risk management and controls, the importance of security policy and the objective of contingency plans. **If your work is at this level, you can get between 26 and 40 points.** **Average Level:** Some ideas expressed in the electronic presentation are not coherent or not all of the requested concepts are presented. **If your work is at this level, you can get between 11 and 25 points.** **Low level:** The concepts embodied in the presentation do not present an understanding of the concepts of the pillars of computer security, risk management and controls, the importance of security policy and the objective of contingency plans. **If your work is at this level, you can get between 0 and 10 points.**
Second evaluation criterion:	**High level:** The presentation is structured appropriately, is carried out using online electronic presentation software and includes references in APA format.

Form: Presentation of the collaborative work document. This criterion represents 5 points of the total of 125 points of the activity.	If your work is at this level, you can get between 4 and 5 points. **Medium Level:** The presentation does not include references, is not structured in a totally orderly manner, or is not done in online electronic presentation software. If your work is at this level, you can get between 2 and 3 points. **Low level:** The presentation is not structured in an organized way. If your work is at this level, you can get between 0 points and 1 point.
Third evaluation criterion: **Participation** Participation in the forum in collaborative work. **This criterion represents 5 points of the total of 125 points of the activity.**	**High level:** Promotes the generation of different points of view related to the topic, enriching the discussion and adding value to it. If your work is at this level, you can get between 4 and 5 points. **Medium Level:** The content of some messages is not coherent with the subject matter, not all of them are original or they do not always promote the generation of different points of view, enriching the discussion and adding value to it. If your work is at this level, you can get between 2 and 3 points. **Low level:** The contents of the messages are not coherent with the subject matter; they are not original or they do not promote the generation of different points of view for the discussion and adding value to it. If your work is at this level, you can get between 0 points and 1 point.
Fourth evaluation criterion: **Contents** Obtaining public information through tools and	**High level:** Each student performs adequately obtaining information about themselves through OSINT tools, making use of the operators and the suggested metasearch engines and correctly concludes on what is the criminal capacity of the results obtained in the exercise. If your work is at this level, you can get between 21 points and 30 points.

techniques to analyze the data. **This criterion represents 30 points of the total of 125 points of the activity.**	**Medium Level:** The student partially obtains information about themselves through OSINT tools, making use of the operators and the suggested metasearch engines and partially concludes on what the criminal capacity of the results obtained in the exercise is. **If your work is at this level, you can get between 10 and 20 points.** **Low level:** Each student does not adequately obtain information about themselves through OSINT tools, and does not make use of the operators and the suggested metasearch engines and does not correctly conclude on what the criminal capacity of the results is obtained in the exercise, or the activity does not deliver. **If your work is at this level, you can get between 0 and 9 points.**
Fifth evaluation criterion: **Contents:** Appropriation of the installation and proper use of tools to navigate (TOR) in the Deep Web. **This criterion represents 30 points of the total of 125 points of the activity.**	**High level:** Each student performs properly the installation, navigation in TOR and correctly concludes on what is the criminal capacity of the results obtained in the exercise. **If her work is at this level, she can get between 21 and 30 points.** **Medium Level:** The student partially performs the installation, navigation in TOR and partially concludes on what is the criminal capacity of the results obtained in the exercise. **If your work is at this level, you can get between 10 and 20 points.** **Low level:** Each student does not correctly install, navigate in TOR and does not correctly conclude about the criminal capacity of the results obtained in the exercise or does not deliver the activity. **If your work is at this level, you can get between 0 and 9 points.**
Sixth evaluation criterion: **Form:**	**High level:** The student presents a document in Word or PDF with all the elements: Cover, objectives, first part obtaining information, second part with the installation, navigation in TOR, and includes references in APA format and without spelling errors and good drafting.

Presentation of the independent work document. **This criterion represents 15 points of the total of 125 points of the activity.**	**If your work is at this level, you can get between 11 and 15 points.** **Medium Level:** The student presents a document in Word or PDF with some of the requested elements and includes references in APA format and / or with spelling errors and / or good writing. **If your work is at this level, you can get between 6 and 10 points.** Low level: The document is not structured in an organized way, has spelling errors and bad writing, does not include APA standards or the activity was not carried out. **If your work is at this level, you can get between 0 and 5 points.**