Source: Bing Chat AI

BADGE TABLE USAGE SUGGESTIONS

DEPARTMENT OF COMPUTER SCIENCE. UNIVERSITY OF OVIEDO

Computer Security | 2023 – 2024 (V4.0 *"S-81 Isaac Peral"*)

Content

Badge Tables?

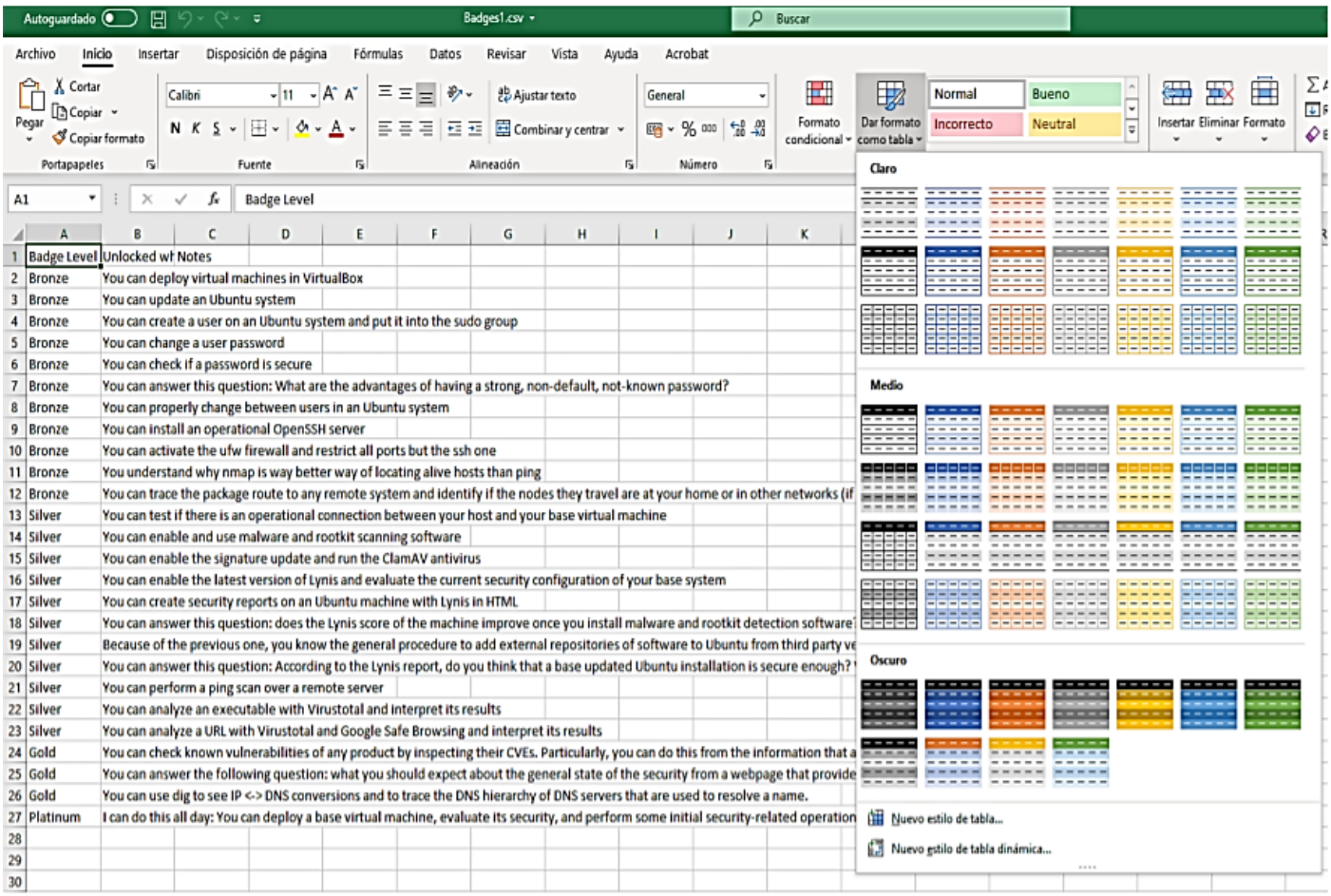
At the end of each lab, **you will find a self-assessment section with a table of concepts/ideas/techniques you have to understand/reproduce to consider you have understood each lab successfully**. Keeping a log of your lab activities **IS KEY** to pass the lab part of this course, and hence we expected students to use this table as a guideline to document their work.

However, on the year 2020-2021, the student Daniel Barrientos (thanks Daniel!) told us the way he used the self-assessment section of each lab to prepare their activities. Instead of using it as a checklist of whether the listed concepts are understood, he used the table to directly take notes associated with each of them, problems encountered, and commands used, that is, **as a complete log** of each action. The main problem was that exporting tables from PDF to *Word* did not work well and gave compatibility issues between different programs reading the generated files and/or operating systems.

As we believe that this alternative form of using the badges is more useful and help more people, we decided to support his idea by providing you with files that contain the badges classified by its level, but that are easily loadable and editable by any *Office*-like program on any OS without formatting problems. That is why we have converted them to the `csv` format (text files separated by `;`) and made them public for all course students.

The `.csv` of the laboratories will be found in a `.zip` file at the end of the laboratories section of the virtual campus.

These files can be loaded from *Excel* or any other similar program and will be converted to tables automatically. The tables will initially not be formatted, but can be easily fixed with *Excel* autoformat with a simple click:

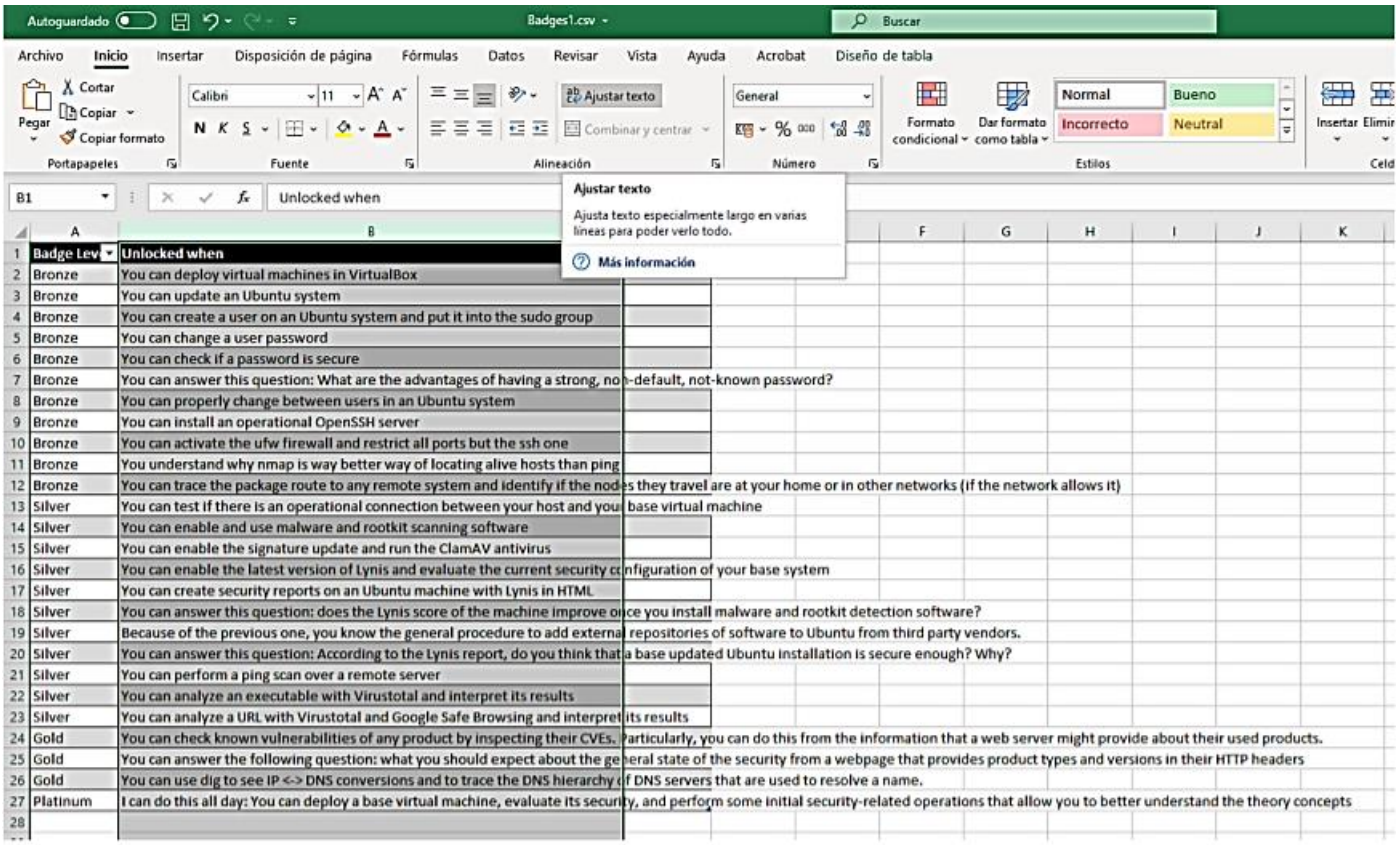


Badge Level	Unlocked wh	Notes
Bronze		You can deploy virtual machines in VirtualBox
Bronze		You can update an Ubuntu system
Bronze		You can create a user on an Ubuntu system and put it into the sudo group
Bronze		You can change a user password
Bronze		You can check if a password is secure
Bronze		You can answer this question: What are the advantages of having a strong, non-default, not-known password?
Bronze		You can properly change between users in an Ubuntu system
Bronze		You can install an operational OpenSSH server
Bronze		You can activate the ufw firewall and restrict all ports but the ssh one
Bronze		You understand why nmap is way better way of locating alive hosts than ping
Bronze		You can trace the package route to any remote system and identify if the nodes they travel are at your home or in other networks (if
Silver		You can test if there is an operational connection between your host and your base virtual machine
Silver		You can enable and use malware and rootkit scanning software
Silver		You can enable the signature update and run the ClamAV antivirus
Silver		You can enable the latest version of Lynis and evaluate the current security configuration of your base system
Silver		You can create security reports on an Ubuntu machine with Lynis in HTML
Silver		You can answer this question: does the Lynis score of the machine improve once you install malware and rootkit detection software?
Silver		Because of the previous one, you know the general procedure to add external repositories of software to Ubuntu from third party ve
Silver		You can answer this question: According to the Lynis report, do you think that a base updated Ubuntu installation is secure enough?
Silver		You can perform a ping scan over a remote server
Silver		You can analyze an executable with Virustotal and interpret its results
Silver		You can analyze a URL with Virustotal and Google Safe Browsing and interpret its results
Gold		You can check known vulnerabilities of any product by inspecting their CVEs. Particularly, you can do this from the information that a
Gold		You can answer the following question: what you should expect about the general state of the security from a webpage that provide
Gold		You can use dig to see IP <-> DNS conversions and to trace the DNS hierarchy of DNS servers that are used to resolve a name.
Platinum		I can do this all day: You can deploy a base virtual machine, evaluate its security, and perform some initial security-related operation

By doing this we will have this table:

Badge Lev	Unlocked	Notes
Bronze		You can deploy virtual machines in VirtualBox
Bronze		You can update an Ubuntu system
Bronze		You can create a user on an Ubuntu system and put it into the sudo group
Bronze		You can change a user password
Bronze		You can check if a password is secure
Bronze		You can answer this question: What are the advantages of having a strong, nor
Bronze		You can properly change between users in an Ubuntu system
Bronze		You can install an operational OpenSSH server
Bronze		You can activate the ufw firewall and restrict all ports but the ssh one
Bronze		You understand why nmap is way better way of locating alive hosts than ping
Bronze		You can trace the package route to any remote system and identify if the node
Silver		You can test if there is an operational connection between your host and your
Silver		You can enable and use malware and rootkit scanning software
Silver		You can enable the signature update and run the ClamAV antivirus
Silver		You can enable the latest version of Lynis and evaluate the current security co
Silver		You can create security reports on an Ubuntu machine with Lynis in HTML
Silver		You can answer this question: does the Lynis score of the machine improve on
Silver		Because of the previous one, you know the general procedure to add external
Silver		You can answer this question: According to the Lynis report, do you think that
Silver		You can perform a ping scan over a remote server
Silver		You can analyze an executable with Virustotal and interpret its results
Silver		You can analyze a URL with Virustotal and Google Safe Browsing and interpret
Gold		You can check known vulnerabilities of any product by inspecting their CVEs. F
Gold		You can answer the following question: what you should expect about the ger
Gold		You can use dig to see IP <-> DNS conversions and to trace the DNS hierarchy o
Platinum		I can do this all day: You can deploy a base virtual machine, evaluate its securit

Then, by simply widen the "*Unlocked When*" column and click "***Adjust Text***" we obtain a usable and well-formatted table.



Badge Level	Unlocked when
Bronze	You can deploy virtual machines in VirtualBox
Bronze	You can update an Ubuntu system
Bronze	You can create a user on an Ubuntu system and put it into the sudo group
Bronze	You can change a user password
Bronze	You can check if a password is secure
Bronze	You can answer this question: What are the advantages of having a strong, non-default, not-known password?
Bronze	You can properly change between users in an Ubuntu system
Bronze	You can install an operational OpenSSH server
Bronze	You can activate the ufw firewall and restrict all ports but the ssh one
Bronze	You understand why nmap is way better way of locating alive hosts than ping
Bronze	You can trace the package route to any remote system and identify if the nodes they travel are at your home or in other networks (if the network allows it)
Silver	You can test if there is an operational connection between your host and your base virtual machine
Silver	You can enable and use malware and rootkit scanning software
Silver	You can enable the signature update and run the ClamAV antivirus
Silver	You can enable the latest version of Lynis and evaluate the current security configuration of your base system
Silver	You can create security reports on an Ubuntu machine with Lynis in HTML
Silver	You can answer this question: does the Lynis score of the machine improve once you install malware and rootkit detection software?
Silver	Because of the previous one, you know the general procedure to add external repositories of software to Ubuntu from third party vendors.
Silver	You can answer this question: According to the Lynis report, do you think that a base updated Ubuntu installation is secure enough? Why?
Silver	You can perform a ping scan over a remote server
Silver	You can analyze an executable with Virustotal and interpret its results
Silver	You can analyze a URL with Virustotal and Google Safe Browsing and interpret its results
Gold	You can check known vulnerabilities of any product by inspecting their CVEs. Particularly, you can do this from the information that a web server might provide about their used products.
Gold	You can answer the following question: what you should expect about the general state of the security from a webpage that provides product types and versions in their HTTP headers
Gold	You can use dig to see IP <-> DNS conversions and to trace the DNS hierarchy of DNS servers that are used to resolve a name.
Platinum	I can do this all day: You can deploy a base virtual machine, evaluate its security, and perform some initial security-related operations that allow you to better understand the theory concepts

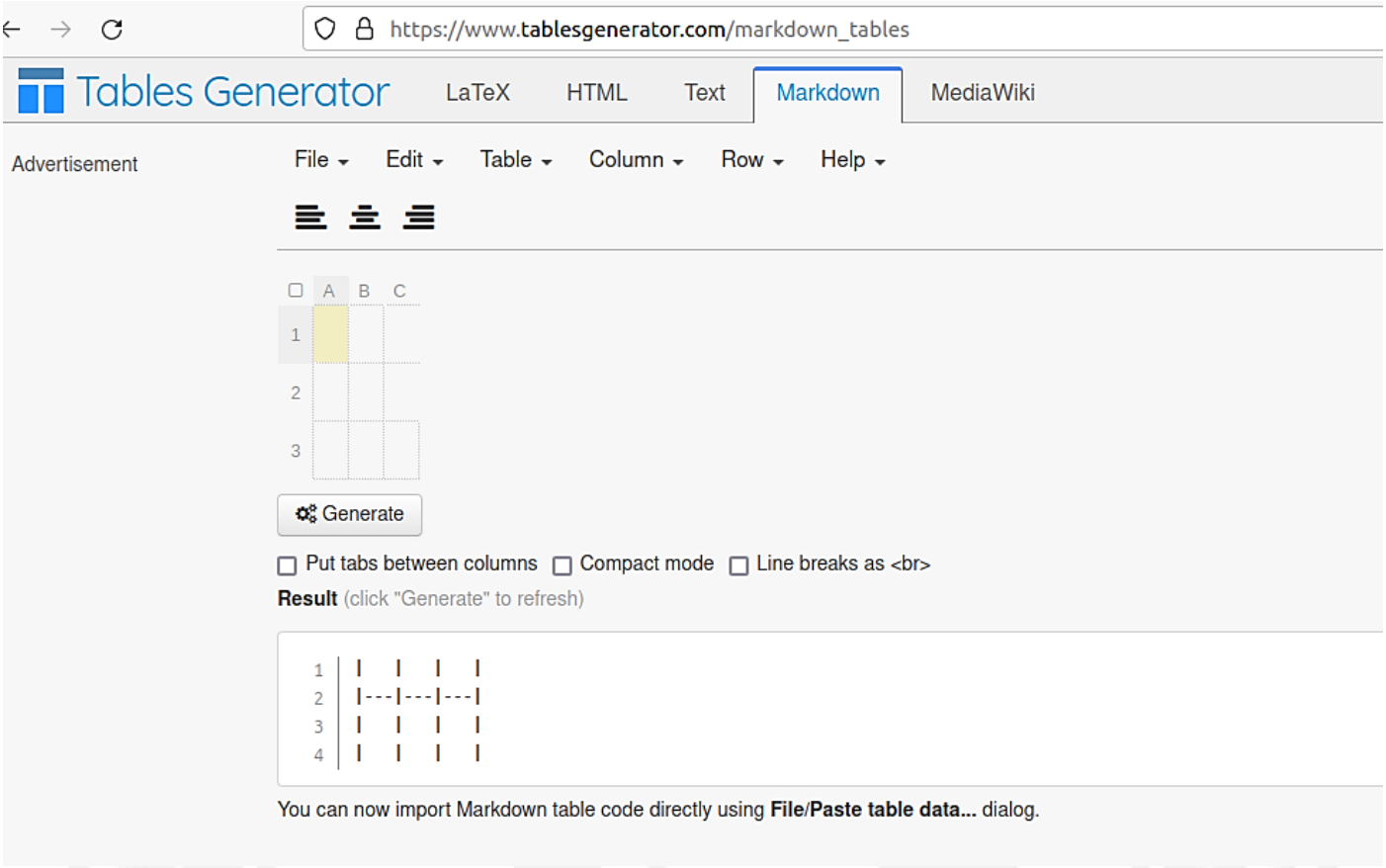
And with this, and a little format adjustment to your own liking, you will have a table to make notes the way you want, compatible with many programs.

Using this with *Word*

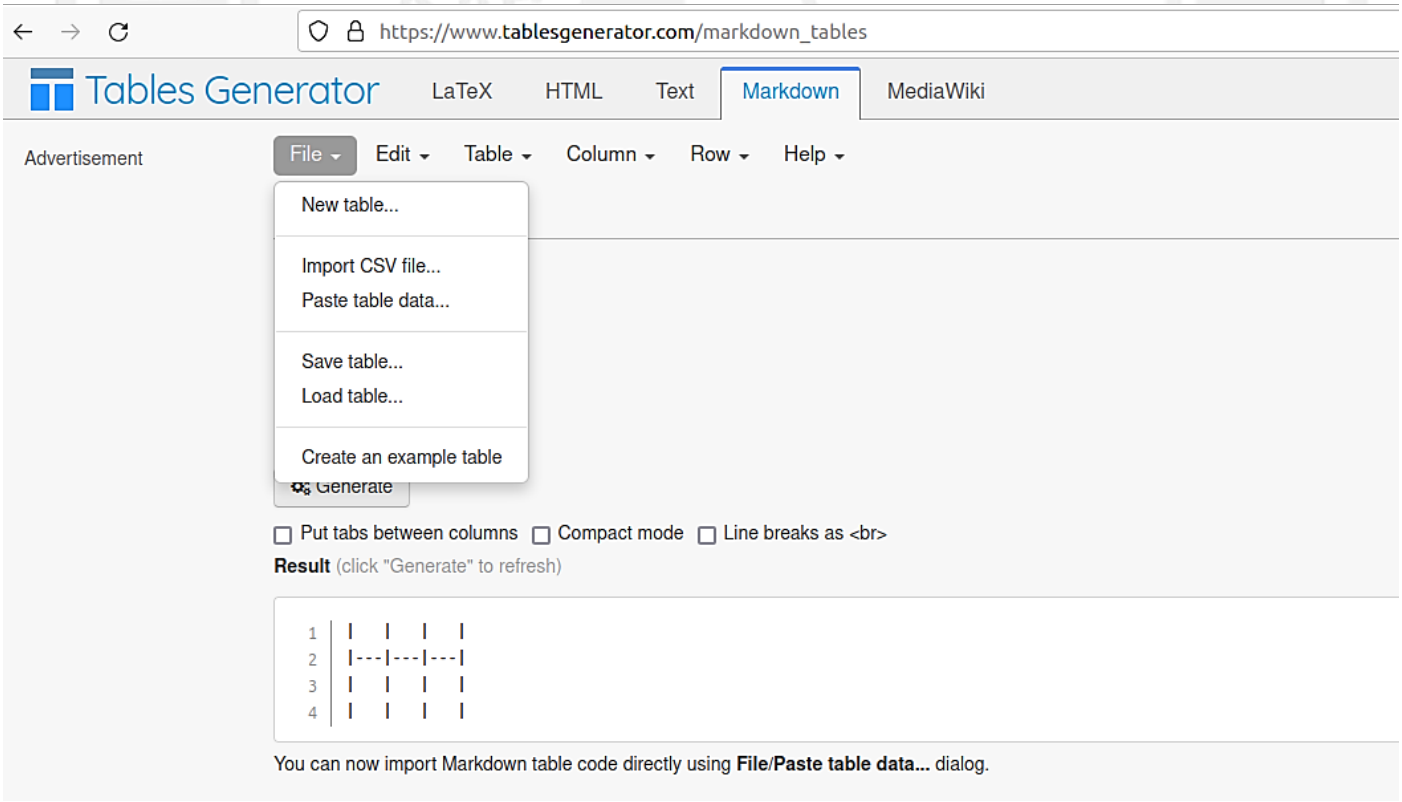
We know that *Excel* is not precisely the best tool to take notes, but these formatted tables **can be also directly copied and pasted in *Word***. Another way to do this is to open the table in *Excel*, copy it "raw" to *Word* and do the formatting directly in *Word*, which is usually faster and leave a more interesting format. In any case, these files are designed to adapt them to your liking and not to follow a specific format, so modify them as you please 😊.

Using this with other formats (that you might prefer…)

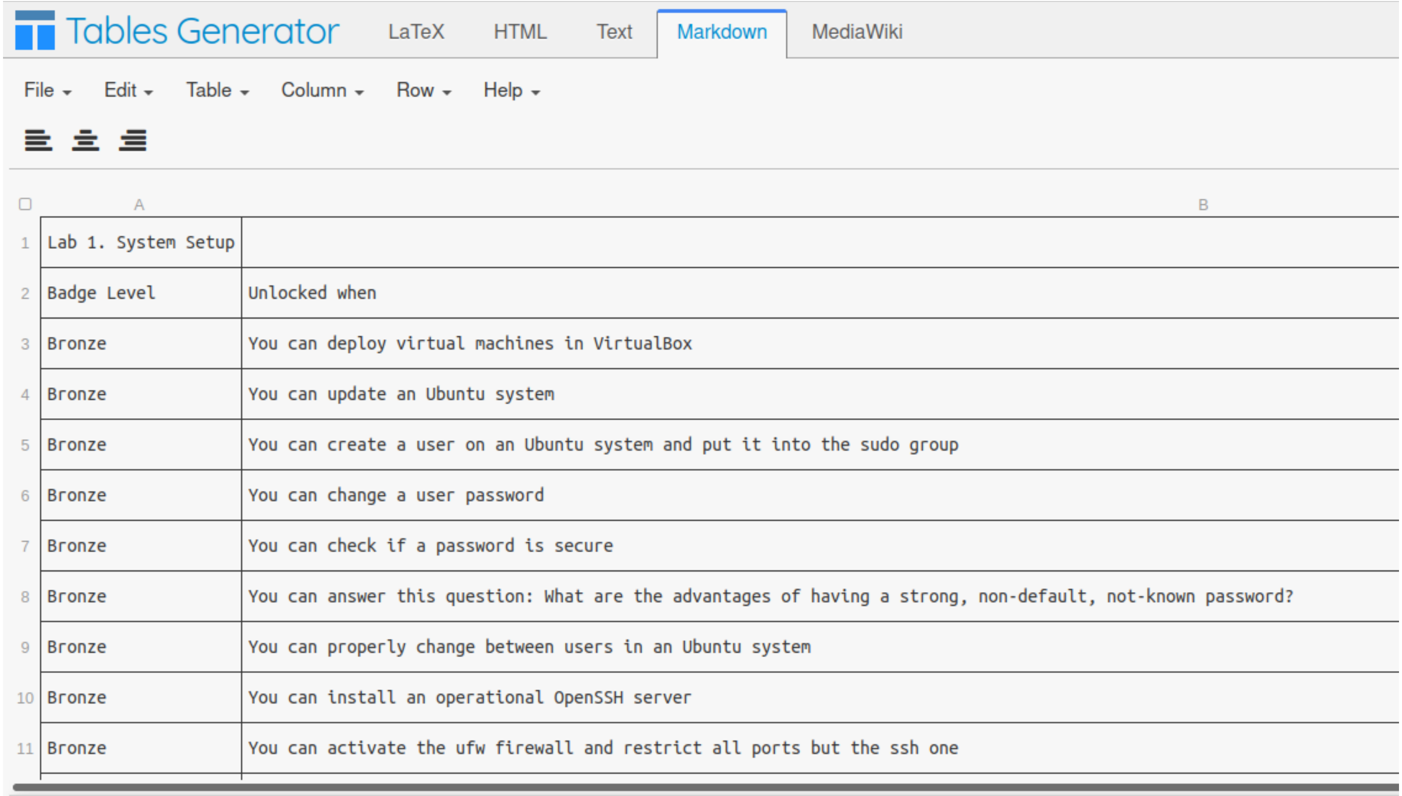
Last year some students told us that they use other formats for taking their notes, and while the CSV format is highly compatible, converting them to these other formats may be problematic. This section aims to help you with that, finding a format that make you feel comfortable with. To do that, you can use the features of this web page: https://www.tablesgenerator.com/markdown_tables



This page accepts uploading `csv` files like the ones with the badges, so you can import and convert them to many formats! The following image shows you the option:

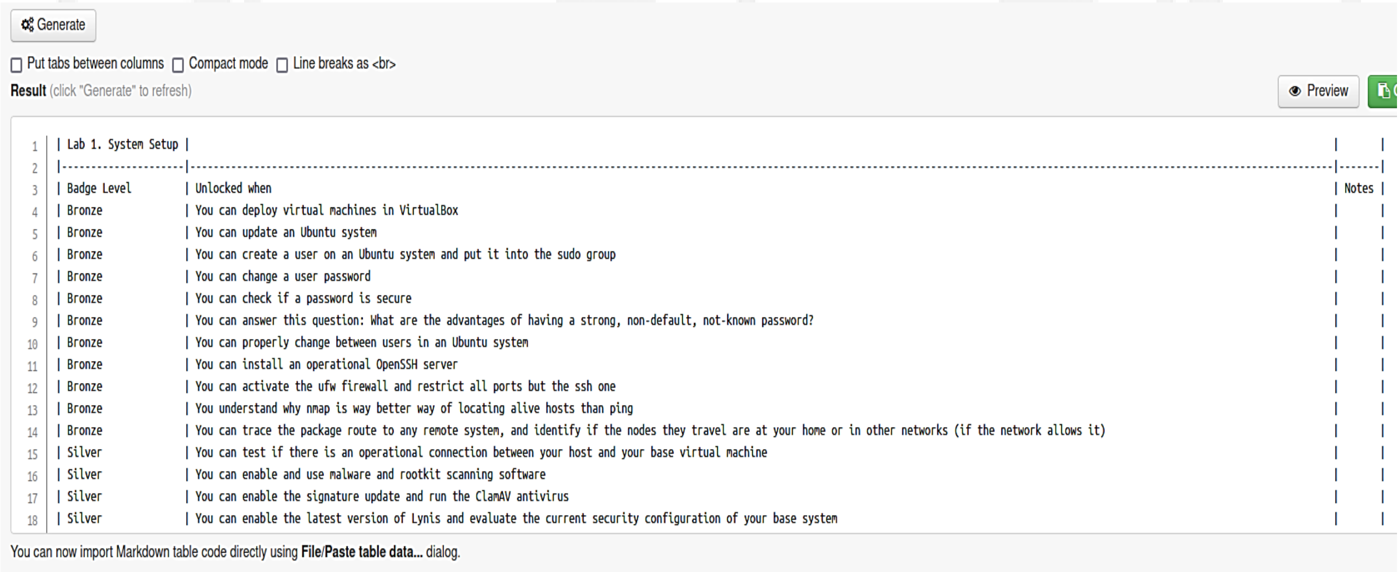


As you see, the default option is the ***Markdown*** format (the one that *GitHub* uses). This is a quite simple format and even *Visual Studio Code* (that is installed on the course VM 😉 😉) can edit it.



Lab 1. System Setup	
Badge Level	Unlocked when
Bronze	You can deploy virtual machines in VirtualBox
Bronze	You can update an Ubuntu system
Bronze	You can create a user on an Ubuntu system and put it into the sudo group
Bronze	You can change a user password
Bronze	You can check if a password is secure
Bronze	You can answer this question: What are the advantages of having a strong, non-default, not-known password?
Bronze	You can properly change between users in an Ubuntu system
Bronze	You can install an operational OpenSSH server
Bronze	You can activate the ufw firewall and restrict all ports but the ssh one

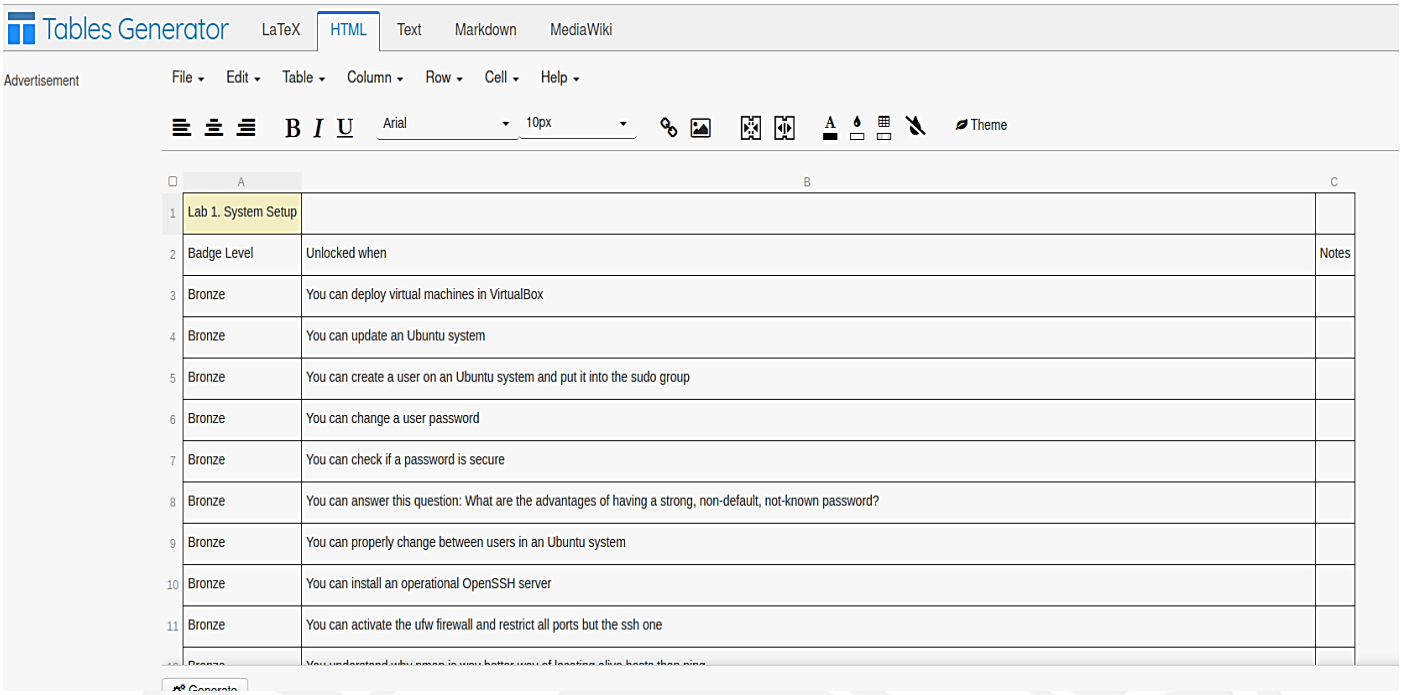
You can scroll down to find the table in the *Markdown* format you can copy and paste to your document and start working with it. This procedure is the same for any format you want to use from this page:



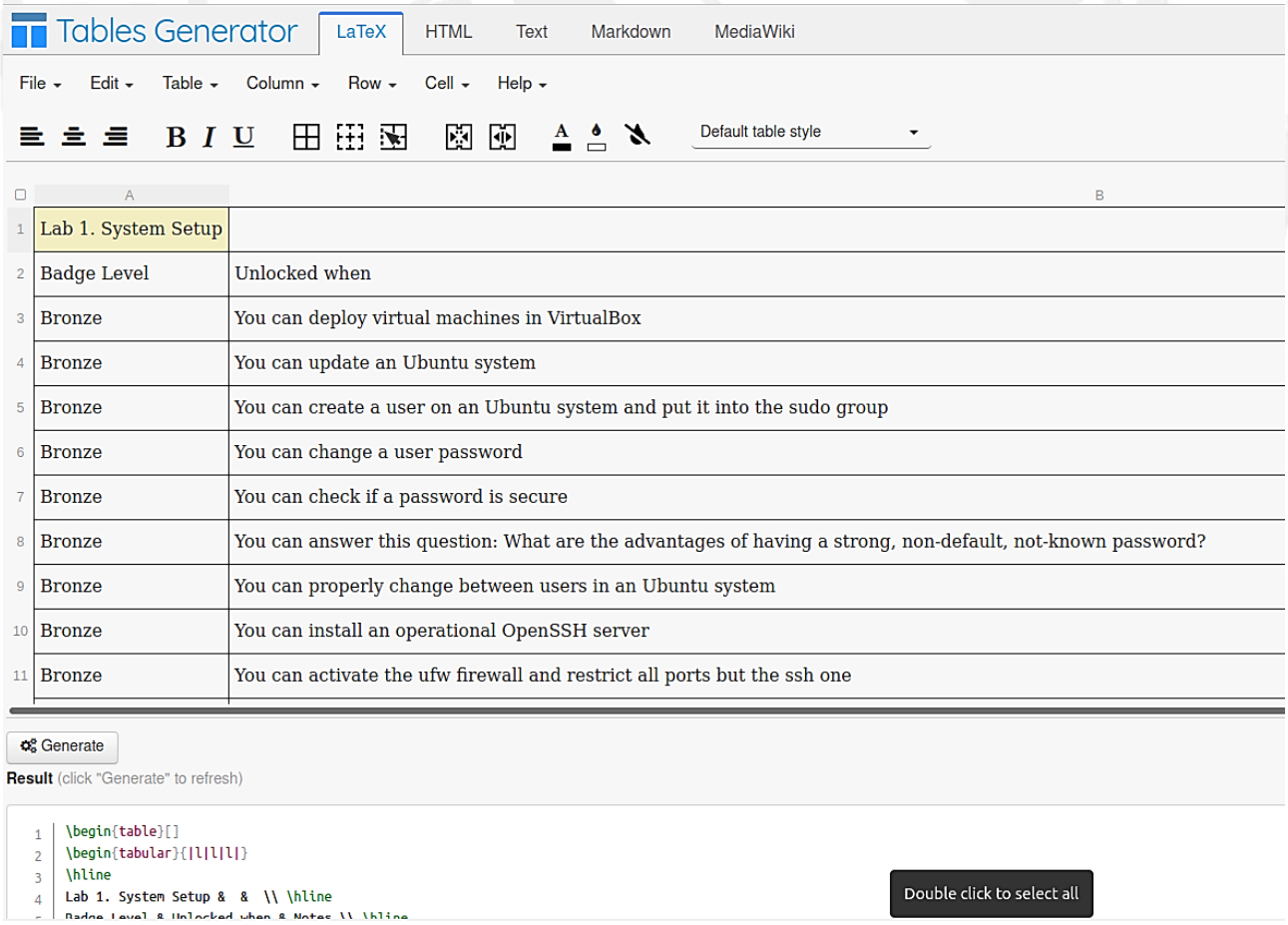

```
| Lab 1. System Setup |                                                                                                                              |       |
|---------------------|------------------------------------------------------------------------------------------------------------------------------|-------|
| Badge Level         | Unlocked when                                                                                                                | Notes |
| Bronze              | You can deploy virtual machines in VirtualBox                                                                                |       |
| Bronze              | You can update an Ubuntu system                                                                                              |       |
| Bronze              | You can create a user on an Ubuntu system and put it into the sudo group                                                     |       |
| Bronze              | You can change a user password                                                                                               |       |
| Bronze              | You can check if a password is secure                                                                                        |       |
| Bronze              | You can answer this question: What are the advantages of having a strong, non-default, not-known password?                   |       |
| Bronze              | You can properly change between users in an Ubuntu system                                                                    |       |
| Bronze              | You can install an operational OpenSSH server                                                                                |       |
| Bronze              | You can activate the ufw firewall and restrict all ports but the ssh one                                                     |       |
| Bronze              | You understand why nmap is way better way of locating alive hosts than ping                                                  |       |
| Bronze              | You can trace the package route to any remote system, and identify if the nodes they travel are at your home or in other networks (if the network allows it) |       |
| Silver              | You can test if there is an operational connection between your host and your base virtual machine                           |       |
| Silver              | You can enable and use malware and rootkit scanning software                                                                 |       |
| Silver              | You can enable the signature update and run the ClamAV antivirus                                                             |       |
| Silver              | You can enable the latest version of Lynis and evaluate the current security configuration of your base system               |       |
```

You can now import Markdown table code directly using **File/Paste table data...** dialog.

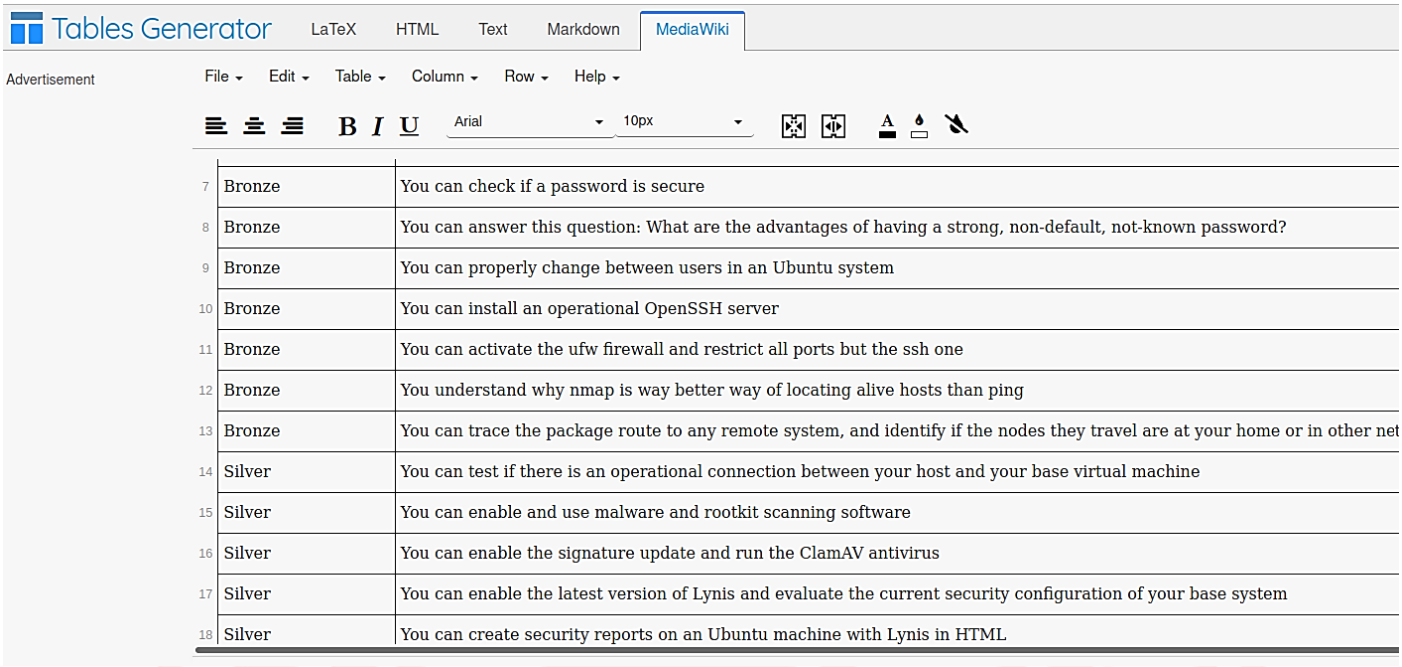
Of course, you can convert the table to ***HTML*** if you feel like, with the option that appears in another tab:



If you are a ***Latex*** fan, this page also has something for you, although bear in mind that this only provides you the table, not the whole document. Therefore, you need to copy and paste the table to *Latex* document to use it. There are plenty of *Latex* document templates available on Internet that you can use as a base. However, we discourage you to use *Latex* format unless you are already familiar with it. It certainly produces prettier documents, but if you have no previous experience, it may impair your productivity.



Finally, you also have the option to generate a ***MediaWiki*** document. This is the format used by the *Wikipedia*, and of course requires a suitable editor that supports it. You may have one already, so this is just to remind you that it is also a viable option.



7	Bronze	You can check if a password is secure
8	Bronze	You can answer this question: What are the advantages of having a strong, non-default, not-known password?
9	Bronze	You can properly change between users in an Ubuntu system
10	Bronze	You can install an operational OpenSSH server
11	Bronze	You can activate the ufw firewall and restrict all ports but the ssh one
12	Bronze	You understand why nmap is way better way of locating alive hosts than ping
13	Bronze	You can trace the package route to any remote system, and identify if the nodes they travel are at your home or in other net
14	Silver	You can test if there is an operational connection between your host and your base virtual machine
15	Silver	You can enable and use malware and rootkit scanning software
16	Silver	You can enable the signature update and run the ClamAV antivirus
17	Silver	You can enable the latest version of Lynis and evaluate the current security configuration of your base system
18	Silver	You can create security reports on an Ubuntu machine with Lynis in HTML

Finally, we also want to point out that Markdown documents are quite easy to use with a special tool called **pandoc** (installable in *Ubuntu*, like the one we provide 😉 😉). This tool **is a universal document format converter** and may be able to help you achieve the format you like to take your notes. You have a full list of examples here: https://pandoc.org/demos.html