***Source**: Bing Chat AI*

GROUP WORK INSTRUCTIONS

DEPARTMENT OF COMPUTER SCIENCE. UNIVERSITY OF OVIEDO

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

Content

Goal of the course work

The work of the course is to create **a PDF document to** describe the steps you have taken to do the work you have been assigned, **based on screenshots,** and **explaining what you have done** to obtain the result shown in the screenshots. You can think of doing it as a kind of step-by-step explanation of the results that appear in the images, including what you have done to make it happen, similar to the KT of the labs.

There is no page limit, although it is recommended **that you try to be as concise as possible** and get to the point in the explanations. The objective is to remark what information you have found and what can be used for (if you were a “bandit” 😊)

Available material

Since all the **works are based on research using data from open sources (OSINT),** you are given a document to help you do the work, which is already available on the campus of the course. This document (**A-21 "Poseidon"**) contains all the information you will need (and some more 😊) to do those jobs, so that you do not have to look too much how to do certain things and focus on doing them. It is an extensive document that has been created with the intention that you keep it for your future, so although it has a lot of content, focus only on those that are relevant to your work.

Obviously, as long as you are compliant with the rules of the next section, you can use any other technique or tool that you find or consider appropriate.

Proposed works

The works are subject to rules, **they are divided into models,** and each model has a **code**. Please take a good look at the code that you have received in groups to works assignment document to know exactly what work you have to do.

Rules

All proposed works have the following **mandatory rules**.

- "***Do not engage***": It is strictly forbidden to **interact with people** who may be the target of an investigation as a result of your work. **Even under a false identity**. They should always be **passive reconnaissance techniques**. We know that the document has descriptions of active techniques, but they are included for your later training and in case you ever fall victim to them. **Do not use that knowledge to interact, or of course harm, others**.
    - As an example, these techniques are considered **acceptable** on any website.
        - Browse a website normally with any browser
        - Examine the contents of a website with HTTP proxies such as *Burp* or browser developer tools
        - Duplicate a website on your hard drive to do offline analysis of its contents
        - Examine the properties and contents of any public files linked on the web
        - Causing 404 errors by navigating to pages you know do not exist
        - Test URLs manually to see if they exist
    - These are considered **unacceptable techniques** against websites that are not yours
        - In general, any technique that involves a large number of requests in a short period of time in order to test the validation of system data or any other reason.
        - Fuzzing, directory enumeration, automated vulnerability testing, etc. It is also not the objective of this work to do these kind of tests, they always need a contract with a client to do it legally.
        - Run `nmap` against them
        - Test *malware*, *exploits*, etc.
- "***Do not disclose***": It is strictly forbidden to **publish sensitive information** that you may have encountered. In your work, if you find sensitive information the captures must **be "censored**" so that only a minimal part of it is seen so that it is not recognizable but proves that you have found "things" (pay special care in the poster in case we could expose it in the future).
- "***Do not harm***": Directly or indirectly harming any person or entity.

In these works, you may not get much information about the objective you have chosen. For this we have to tell you the following:

- **Choose the objective well**: start with someone or something that you see that has a presence on the network or is popular.
- **The focus is not finding information, but properly developing an investigation**: The objective is to execute search techniques correctly and reasonedly. If nothing or almost nothing appears after that, it

is not a bad thing (good for the entity or person investigated! 😊). In other words, the **result of a work can perfectly be to congratulate someone or some entity for managing their presence in the network well**.

General objectives

Although each investigation can take different paths depending on what you find of each person or entity studied, in general it is about answering these questions, although you can add all the extra information that you consider relevant:

- If the person or entity studied makes **appropriate use** of social networks or, in general, the Internet, in the sense of exposing too much information that can potentially be used for some malicious purpose.
- If it is easy to identify the "**environment"** of the person or entity studied, in the sense of with whom it is related/associated, with whom it works, etc., and if you think it may cause a security problem to the objective of the study.
- If you believe that some of what you have found **would facilitate** a ***spear phishing*** attack against the person or entity studied (one of its members), or a physical crime (theft, etc.).

Work models (choose one)

Work model 1: Investigating a politician

Do an investigation with data **exclusively from open sources** and always **WITHOUT contacting** the investigated target in any way (see rules) **of someone you choose** associated with **any political party** (currently or in the past), either nationally or regionally.

- **MODEL1_POLIT_PSOE:** PSOE
- **MODEL1_POLIT_PP:** PP
- **MODEL1_POLIT_VOX**: VOX
- **MODEL1_POLIT_PODEMOS**: PODEMOS
- **MODEL1_POLIT_SUMAR**: SUMAR
- **MODEL1_POLIT_ ERC**: ERC
- **MODEL1_POLIT_AST**: FORO ASTURIAS or any Asturian deputy

Work model 2: Investigate a Spanish streamer

Do an investigation with data **exclusively from open sources** and always **WITHOUT contacting** the investigated target in any way (see rules) **of one of these streamers**.

- **MODEL2_STREAMER_IBAI**: Ibai Llanos
- **MODEL2_STREAMER_ZELING**: Alicia Gonzáles Zeling
- **MODEL2_STREAMER_ILLO**: illojuan
- **MODEL2_STREAMER_NISSAXTER:** Nissaxter
- **MODEL2_STREAMER_AURON**: AuronPlay

- **MODEL2_STREAMER_PARACETAMOR:** Paracetamor
- **MODEL2_STREAMER_RUBIUS**: ElRubius
- **MODEL2_STREAMER_LITTLERAGER:** Littleragergirl
- **MODEL2_STREAMER_GREFG**: TheGrefg
- **MODEL2_STREAMER_MAYICHI:** Mayichi
- **MODEL2_STREAMER_JWILD**: Jordi Wild
- **MODEL2_STREAMER_CRISTININI:** Cristinini
- **MODEL2_STREAMER_DJMARIIO**: ERC

Work model 3: Investigate the web presence of a worker syndicate

Do research with data **exclusively from open sources** and always **WITHOUT active techniques** (e.g.: `nmap`, see rules) of a **machine, machines, or services** (e.g.: RRSS) that belong to the **web infrastructure** of a Spanish **worker syndicate**. The investigation can include people if through them it is possible to find out some data of the web studied, is a provider or similar (someone relevant) of the web.

- **MODEL3_WEBSINDICATO_CCOO:** Comisiones Obreras (CCOO)
- **MODEL3_WEBSINDICATO_UGT:** Unión General de Trabajadores (UGT)
- **MODEL3_WEBSINDICATO_USO:** Unión Sindical Obrera (USO)
- **MODEL3_WEBSINDICATO_CSIF:** Central Sindical Independiente y de Funcionarios (CSIF)
- **MODEL3_WEBSINDICATO_CGT:** Confederación General del Trabajo (España) (CGT)

Work model 4: Investigate the web infrastructure of a national political party

Do research with data **exclusively from open sources** and always **WITHOUT active techniques** (e.g.: `nmap`, see rules) of a **machine, machines, or services** (e.g.: RRSS) that belong to the **web infrastructure** of a Spanish **political party**. The investigation can include people if through them it is possible to find out some data of the web studied, is a provider or similar (someone relevant) of the web.

- **MODEL4_WEBPOLIT_PSOE**: PSOE
- **MODEL4_WEBPOLIT_PP**: PP
- **MODEL4_WEBPOLIT_VOX**: VOX
- **MODEL4_WEBPOLIT_PODEMOS**: PODEMOS
- **MODEL4_WEBPOLIT_SUMAR**: SUMAR

Work model 5: Investigate a political party's web presence

Do research with data **exclusively from open sources** and always **WITHOUT active techniques** (eg: `nmap`, see standards) of a **machine, machines, or services** (eg: RRSS) that belong to the **web infrastructure** of a **political party** either at national or regional level. The investigation can include people if through them it is possible to find out some data of the web studied, is a provider or similar (someone relevant) of the web.

- **MODEL2_WEB_PSOE : PSOE**
- **MODEL2_WEB_PP**: PP
- **MODEL2_WEB_VOX**: VOX
- **MODEL2_WEB_PODEMOS**: PODEMOS
- **MODEL2_WEB_CIUDADANOS**: CIUDADANOS
- **MODEL2_WEB_ERC**: ERC

Work model 6: Investigate the web presence of a town hall

Do research with data **exclusively from open sources** and always **WITHOUT active techniques** (Ex: `nmap`, see standards) of a machine, machines, or services (Ex: RRSS) that belong to the **web infrastructure** of an **Asturian municipality**. The investigation may include people if through them it is possible to find out some data from the website studied, it is a provider, or similar (someone relevant) of the web.

- **MODEL3_WEB_OVIEDO:** Oviedo
- **MODEL3_WEB_GIJÓN:** Gijón
- **MODEL3_WEB_AVILÉS:** Avilés
- **MODEL3_WEB_SIERO:** Siero
- **MODEL3_WEB_LANGREO:** Langreo
- **MODEL3_WEB_MIERES:** Mieres
- **MODEL3_WEB_CASTRILLÓN:** Castrillón

Work model 7: Investigate a worker from a relevant company

Do an investigation with data exclusively from open sources and always **WITHOUT contacting** the investigated in any way (see rules) of **someone** you choose with a **position of any responsibility** associated with **a large company** (currently or in the past), either nationally or regionally.

- **MODEL4_EMP_ECI**: El Corte Inglés
- **MODEL4_EMP_ZARA**: Zara
- **MODEL4_EMP_REPSOL:** Repsol Petróleo SA.
- **MODEL4_EMP_CEPSA**: Compañía Española de Petróleos SAU. (CEPSA)
- **MODEL4_EMP_MERCADONA:** Mercadona SA.
- **MODEL4_EMP_ENDESA:** Endesa Energía SAU.
- **MODEL4_EMP_ENEL:** Enel Iberoamérica SRL.
- **MODEL4_EMP_INDRA:** INDRA S. A.
- **MODEL4_EMP_TOTAL**: Total Energies (the former EDP)
- **MODEL4_EMP_ELCOMERCIO:** El Comercio
- **MODEL4_EMP_LNE:** La Nueva España
- **MODEL4_EMP_LAVOZ:** La Voz de Asturias