COMP6224 Foundations of Cyber Security 2022/23

Coursework on Cyber Attack Analysis and Password Cracking

Coursework: individual report on kill chain-based attack analysis and password cracking tasks

Deadline: 3:59pm Monday 28th November 2022
(**please note that submitting exactly at 4:00pm will result in a penalty**)

Feedback: by Monday 9th January 2023

Weighting: 25% of module evaluation

Introduction

For this assignment, you will write a report covering the two following points

- The analysis of a cyber-attack, based on the kill chain model
- A number of password cracking activities

Academic Integrity

This coursework is an individual piece of work and the usual rules regarding individual coursework and academic integrity apply. In particular, please refer to the University Academic Integrity Regulations: http://www.calendar.soton.ac.uk/sectionIV/academic-integrity-regs.html

Instructions

Please download the report template [coursework template]

Part 1 – Cyber-Attack Analysis

Consider the following cyber-attack.

A large-scale cryptomining campaign has been uncovered, compromising tens of thousands of routers manufactured by vendor XYZ. Forensic analysis of the cryptominer malware found in these routers showed that it propagated over the Internet and infected those XYZ routers that were exposed to the Internet and had firmware version 1.2.3 installed. This version of the firmware had a vulnerability that could be exploited via network and allowed to execute arbitrary code on the router. Once activated, the cryptominer malware connected to a remote server to register the infection and receive instructions regarding the cryptomining activities to perform; it also propagated over the Internet to infect as many other vulnerable XYZ routers as possible. Further investigation unveiled that this was a supply chain attack because the vulnerability was introduced on purpose in the source code of the firmware by attackers that intruded the internal network of XYZ. The threat actor compromised the machine of a developer to push the vulnerable firmware update into the internal repository where XYZ keeps all the source code; when a new version of the firmware is to be released, the source code stored in this repository is used to generate the new firmware, which is installed in the routers they sell. The *initial intrusion was performed via social engineering, using a spear-phishing email with a malicious attachment, which, once opened, activated a remote access trojan (RAT) that registered itself as auto-start service in the machine and connected back to the attackers via HTTPS to give them remote access to the machine. The analysis also showed that the adversary spent several months monitoring the activities of the targeted developers, probably to figure out how to develop and integrate the piece of software that made the router firmware vulnerable, as well as the internal procedures to upload updated software to the internal repository.*

Task 1.1 – Kill Chain-based Analysis

The goal of this task is to analyse the cyber-attack described above by using the Lockheed Martin's kill chain model of cyber-attack life cycle. Firstly, identify all the phases used in this attack, choosing from *Reconnaissance*, *Weaponisation*, *Delivery*, *Exploitation*, *Installation*, *Command & Control* and *Actions on Objectives*. Describe what happened in each phase in the appropriate subsection of the template (for example, "Reconnaissance Phase", "Weaponization Phase", …). When describing what happened in a certain phase, limit the description to what you think took place during that phase; avoid mentioning events that occurred in previous or following phases. If it is considered that nothing happened in a phase, write it explicitly and justify why. If no information is available about what happened in a phase, make hypotheses about what might have happened and discuss them. Some cyber-attacks may develop over more phases, for example multi-step cyber-attacks; in that case, add a subsection for each additional phase, using the name of the phase as title of the subsection (for example, another "Reconnaissance Phase" subsection). Please note that, whenever lateral movement takes place, the attack should be considered as multi-step. The maximum length of the description of each phase is 100 words. If more than 100 words are used, only the first 100 words will be marked.

Task 1.2 – Cyber Actor Analysis

Discuss the most likely type of cyber actor that launched this cyber-attack, in terms of attack strategy and motivations. A cyber actor profile can be classified as either *Cybercriminal*, *Nation State*, *Hacktivist*, *Script Kiddie*, *Insider*, or a combination of them. The maximum length of the description of attack strategy or attack motivation is 100 words. If more than 100 words are used, only the first 100 words will be marked.

Part 2 – Password Cracking

Task 2.1 - Dictionary-based cracking of passwords

The goal of this task is to crack all the 20 (twenty) passwords included in this file [ZipFileWithPasswordsToCrack].

Depending on the configuration of your virtual machine and where you are opening this document you may experience different permissions regarding uploading the required files.

Within the Kali distribution there is a Firefox browser. I was able to access and download the required files via email (use your favoured email server). The files are saved into the Download directory within root.

You will use John the Ripper software and a number of different dictionaries. In particular, you will experiment with the following 4 (four) dictionaries and select the 2 (two) that overall give you the highest number of cracked passwords. [ZipFileWithDictionaries]

- Cain
- Facebook pastebay

- Hotmail
- MySpace

In order to crack all the passwords, you will also need to create by yourself and use a third dictionary, on the basis of recent lists of popular passwords (e.g., List of the most common passwords - Wikipedia). Remember that these need to be text only files.

In summary, you will select 3 (three) dictionaries: 2 (two) out of the four previously listed and 1 (one) created by yourself.

For each dictionary you use (up to three), please report the following information:

- Name of the file
- File source, i.e., from the module wiki page or created based on a list of popular passwords; in the latter case, please also specify where you picked the list from
- What command you launched to crack the passwords using this dictionary (please also include a screenshot)
- What passwords were successfully cracked

Task 2.2 - Password cracking of Linux accounts

The goal of this task is to crack the passwords of 5 (five) distinct Linux accounts. You can download here the [ZipFileWithAccountsToCrack] where account information is stored.

Note that you need to use the account files you just downloaded (usually stored in the Download folder), not those already configured in your system. Furthermore, make sure you do not overwrite your system account files with those you downloaded, otherwise you would break the OS.

Once you have unshadowed those files (*unshadow* command), you will use John the Ripper software in the following two modes:

- Firstly, in brute force mode
- Secondly, with the default password.lst dictionary

For each of those modes, please report the following information:

- What command you launched to crack the passwords (please also include a screenshot)
- What passwords were successfully cracked

Finally, compare the results you obtained in those two cases (i.e., brute force vs dictionary) and elaborate on any difference you noticed in the results by explaining the reason(s) behind those differences. The maximum length of this comparison is 200 words. If more than 200 words are used, only the first 200 words will be marked.

Task 2.3 - Password analysis

For each password you successfully cracked in Task 2.1 or Task 2.2 (up to 25), identify the characteristics that made it easy to crack it. In particular, identify for each password at most four weaknesses. If more than four weaknesses are provided, only the first four will be marked. Note that each password has at least four weaknesses.

Describe each weakness very briefly. Just a bullet point with **very** brief text (only the first 30 words will be marked) is required. Some possible examples are given below:

- This password does not contain any numbers, making it more vulnerable to brute force attacks

- This password does not contain any special characters, making it more vulnerable to brute force attacks
- This password is contained in publicly available password cracking dictionaries

Deliverables

Submit your report before the specified deadline, i.e., **before 4:00pm Monday 28th November 2022** to the ECS hand-in system at https://handin.ecs.soton.ac.uk/handin/2223/COMP6224/1/

The report must be in PDF format. An ad hoc penalty will be applied if a different format is used (see Marking section). *Note that late submissions will be penalized using the standard University rules (10% per working day) and that no work will be accepted that is more than five working days late.*

Marking Scheme

The learning outcomes that will be assessed in this assignment are

- LO1 Analyse a cyber-attack using the kill chain model
- LO2 Analyse the cyber actor who launched a cyber-attack
- LO3 Use John the Ripper software to crack passwords
- LO4 Analyse strengths and weaknesses of passwords

Task	Criteria	LOs	Marking scheme
Task 1.1	Ability to apply the kill chain model to analyse a cyber-attack [0-40 marks]	LO1	Up to 40 marks, awarded based on the number of phases (i) correctly identified, (ii) well-placed in the chain, and (iii) properly described, in proportion to the total number of phases included in the model answer.
Task 1.2	Ability to examine a cyber actor profile [0-10 marks]	LO2	Up to 10 marks will be awarded based on whether attack strategy and motivations are correctly examined.
Task 2.1	Number of passwords successfully cracked [0-13 marks]	LO3	0.5 marks for each unique[1] password successfully cracked; up to 10 marks
			1 mark for each dictionary correctly reported (i.e., filename, source, command, and screenshot); up to 3 marks
Task 2.2	Number of accounts successfully cracked [0-5 marks]	LO3	1 mark for each unique[2] account successfully cracked; up to 5 marks
	Appropriateness of the explanation of the differences between cracked passwords [0-7 marks]	LO4	Up to 7 marks, based on the following criteria • [0-2] the reasons behind the differences are not explained at all • [3-5] some reasons are identified and described • [6-7] all the reasons are recognised and properly discussed
Task 2.3	Correctness of the identification of the weaknesses of cracked passwords [0-25 marks]	LO4	Up to 25 marks, based on the following criteria • 1 mark for each password for which all the weaknesses (up to 4) are correctly identified • 0.5 marks for each password for which one to three weaknesses are determined
Penalties	Not compliant with the template[3]		1 mark penalty for each non-compliance
	Wrong report format (includes corrupted PDF)		10% penalty if the report can be read; 0 marks will be awarded otherwise
	Late submission		10% penalty per working day; 0 marks will be awarded if more than 5 working days late
	Academic integrity breach		To be decided on a case-by-case basis

[1] If the same password is cracked using different dictionaries, it counts as one password successfully cracked

[2] If the same account password is cracked using both brute force and a dictionary, it counts as one password successfully cracked

[3] Possible non-compliances include (but are not limited to) changing the structure (i.e., the way it is organised in sections and subsections) of the report