COMP6224 Foundations of Cyber Security 2020-21

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 30th November 2020
(**please note that submitting exactly at 4:00pm will result in a penalty**)

Feedback: by Monday 22nd December 2020

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.

Just before the start of important national elections, the website of a political party was targeted with a distributed denial of service (DDoS) attack and remained unavailable for several hours. This DDoS attack was launched from a large botnet built by infecting home Internet routers spread, all of the same popular model. These routers were exploited using a zero-day vulnerability. The leader of the targeted political party did not reveal whether they were asked for a ransom to stop the attack.

A few months before, the servers of the manufacturer of the model of router used in the attack above were hacked, and confidential documents were likely stolen from these servers, including detailed design and technical specification of produced devices. A forensic analysis of the attack against the manufacturer was carried out, and gave evidence that the initial intrusion took place via a malicious PDF document attached to an email sent to an employee of the manufacturer, which gave the adversary remote control of the employee's computer.

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 three possible profiles of the adversary that launched this cyber-attack, in terms of attack strategy and motivations. Each adversary 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
[zip file with passwords to crack].

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. [zip file with the four dictionaries]

- 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.

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 on the basis of a list of popular passwords (where does this list come 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 [zip file with passwd and shadow files] where account information are 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 them, 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 1 and Task 2 (up to 25), identify the characteristics that made it easy to crack. In particular, identify for each passwords 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 in 50 words at most. If more than 50 words are used, only the first 50 words will be marked.

Deliverables

Submit your report before the specified deadline, i.e. **before 4:00pm Monday 30th November 2020** to the ECS hand-in system at https://handin.ecs.soton.ac.uk/handin/2021/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 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 [0-35 marks]	LO1	Up to 35 points, awarded on the basis of 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 [0-15 marks]	LO2	Up to 5 points for each relevant[1] cyber actor profile (or combination of cyber actor profiles) discussed. 5 points will be awarded if both attack strategy and motivations are correctly examined.
Task 2.1	Number of passwords successfully cracked [0-13 marks]	LO3	0.5 points for each unique[2] password successfully cracked; up to 10 points
			1 point for each dictionary correctly reported (i.e. filename, source, command, and screenshot); up to 3 points
Task 2.2	Number of accounts successfully cracked [0-5 marks]	LO3	1 point for each unique[3] account successfully cracked; up to 5 points
	Appropriateness of the explanation of the differences between cracked passwords [0-7 marks]	LO4	Up to 7 points, 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 points, based on the following criteria • 1 point for each password for which all the weaknesses (up to 4) are correctly identified • 0.5 points for each password for which some the weaknesses are determined
Penalties	Not compliant with the template[4]		1 point 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, up to 5 days; 0 marks will be awarded if more than 5 days late
	Academic integrity breach		To be decided on a case-by-case basis

[1] A cyber actor profile (or combination of cyber actor profiles) is relevant if, according to your discussion, it makes sense to consider it as the possible author of the cyber-attack

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

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

[4] 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