COMP2216 Principles of Cyber Security 19-20

Coursework on Cyber Attack Analysis

Coursework: individual report on the analysis of a cyber attack
Deadline: 3:59pm Wednesday 29th April 2020
(**please note that submitting exactly at 4:00pm will result in a penalty**)
Feedback: by Monday 15th June 2020
Effort: 35 hours per student
Weighting: 30% of module evaluation

Introduction

For this assignment, you will write a report about the analysis of a cyber-attack. In the specific, you will pick a recent attack, identify exploited weaknesses and used attack techniques, analyse the attack according to the kill chain-based model and discuss the attacker profile.

Academic Integrity

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

In particular, you should not "copy and paste" text unless you both (a) put the copied text in quotation marks and (b) provide a full reference to the source. Even if these steps are taken, more than one such direct quotation in an assignment of this length will be considered poor academic practice and result in lower marks.

Furthermore, all the reports will be checked for plagiarism by scanning them in Turnitin.

Assignment

Select one cyber-attack from the list provided here and register your choice.
https://secure.ecs.soton.ac.uk/student/wiki/w/COMP2216-1920-Coursework-CyberAttackChoice
Note that each cyber-attack can be chosen by at most 18 students.

Instructions

Please download the report template from the following link:
https://secure.ecs.soton.ac.uk/noteswiki/images/COMP2216_-_1920_-_Cyber_Attack_Analysis_-_Template.docx
A version of the report template with additional information and guidance can be accessed here:
https://secure.ecs.soton.ac.uk/noteswiki/images/COMP2216_-_1920_-_Cyber_Attack_Analysis_-_Template_with_Detailed_Instructions.pdf

Task 1 – Impact, Response and Recovery Analysis

Describe the impact of the attack, the responses that followed the attack (e.g. by the target, the government, media) and any recovery action that was taken to restore normal operations after the attack.

Task 2 – Weaknesses and Attack Techniques Analysis

Elaborate on what weaknesses were exploited (using CVE, NVD and CWE knowledge bases) and what attack techniques were used (using CAPEC and ATT&CK knowledge bases).

Task 3 – Kill Chain-based Analysis

Perform a "kill chain"-based analysis of the attack, by explaining how it worked in each phase and making explicit references to the weaknesses and attack techniques identified in Task 2.

Task 4 – Attacker Analysis

Discuss what types of actor, among those discussed in this module, are likely to be behind the cyber-attack.

Deliverables

Submit your report to the ECS hand-in system at
https://handin.ecs.soton.ac.uk/handin/1920/COMP2216/1/
before the specified deadline, i.e. **before 4:00pm Wednesday 29th April 2020**.
Note that late submission 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.

Word count

The maximum length of the report is 2500 words and submission must be as a .pdf file in PDF format. The reasons why there is a word limit are (a) it's good practice to write concisely and you should get used to doing this (b) you should not be spending more than 35 nominal hours on this assignment.

The word count of the report will be computed by using Foxit Reader (View -> Word Count). You can download Foxit Reader for free here https://www.foxitsoftware.com/downloads/

For reports longer than 2500 words (i.e. whose length is equal to or greater than 2501 words), only the first 2500 works will be marked, and an ad hoc penalty will be applied (-10 marks, see Marking section). The same penalty will be applied to any submission that is NOT in the required format (i.e. PDF file).

Marking

The report will be graded based on depth and accuracy, clarity and conciseness. Given the word limit, you are not expected to analyse deeply every single aspect of the event. However, we expect a number of well-supported, well-presented analysis points that would benefit another Part II student reading your report to learn about the attack.

Module Learning outcomes

A2. Demonstrate knowledge and understanding of the cyber threat landscape, both in terms of recent emergent issues and those issues, which recur over time.
A3. Demonstrate knowledge and understanding of the roles and influences of governments, commercial and other organisations, citizens and criminals in cyber security affairs.

Assignment Learning outcomes

AS1. Demonstrate knowledge and understanding of real-world cyber security events.
AS2. Use available knowledge bases (i.e. CVE, NVD, CWE, CAPEC, ATT&CK) to identify and correlate exploited weaknesses and employed attack techniques.
AS3. Analyse real-world cyber-attacks by applying the kill chain model.
AS4. Examine the profile of the cyber actors behind a real-world cyber-attack.

Marking Criteria

Your submission will be marked out of 100. The following criteria will be used.

Task	Criteria	Outcomes	Mark
Task 1: Impact, Response and Recovery Analysis	Limited understanding of attack impact, response and recovery. The description includes errors and/or inaccuracies and is incomplete.	A2, A3, AS1	0-3
	Good understanding of attack impact, response and recovery. The description includes most relevant details and is accurate.		4-6
	Excellent understanding of attack impact, response and recovery. All relevant details are included, explained precisely, and commented concisely.		7-10
Task 2: Weaknesses and Attack Techniques Analysis	Little ability to identify and correlate exploited weaknesses and used attack techniques, based on available KBs. Some of the reported weaknesses or vulnerabilities are wrong and/or the justification is inaccurate.	A2, AS2	0-11
	Good at identifying and correlating exploited weaknesses and used attack techniques, based on available KBs. Most of main weaknesses and vulnerabilities are correctly reported and adequately justified.		12-20
	Excellent at identifying and correlating exploited weaknesses and used attack techniques, based on available KBs. All the key weaknesses and vulnerabilities are correctly reported and justified concisely and accurately.		21-30
Task 3: Attack Analysis	Little ability to apply the kill chain model to analyse a cyber-attack. Fail to distinguish between single-step and multi-step cyber-attacks, just a few phases are correctly described.	A2, AS3	0-11
	Good at applying the kill chain model to analyse a cyber-attack. Correctly distinguish between single-step and multi-step cyber-attacks, most of phases are correctly described.		12-20
	Excellent at applying the kill chain model to analyse a cyber-attack. Correctly distinguish between single-step and multi-step cyber-attacks, all the phases are correctly described.		21-30
Task 4: Attacker Analysis	Little ability to examine a cyber actor profile. The analysis is incomplete (i.e. not all the possible cyber actors are discussed) and partially correct (i.e. the discussion of some cyber actor is wrong).	A3, AS4	0-7
	Good at examining a cyber actor profile. The analysis is either complete (i.e. all the possible cyber actors are discussed) and partially correct, or incomplete but correct (i.e. all considered cyber actors are discussed correctly).		8-13
	Excellent at examining a cyber actor profile. The analysis is complete and correct.		13-20
Readability, file format, report length	Submitted file is in PDF format, the report is compliant with the provided template, it is not longer than 2500 word, the readability of the report is good. If the report is more than 2500 words or the format is not PDF, 0 marks will be awarded for this assessment criterion.	-	0-10

Support

Detailed instructions will be given in a dedicated lecture. If you need any additional support in completing this coursework, please email any queries to l.aniello@soton.ac.uk.