COMP2216 Principles of Cyber Security 2021/22

Coursework on Cyber-Attack and Corporate Security Analysis

Coursework: individual report on (i) the analysis of a cyber-attack and (ii) the analysis of the security of a corporate environment
Deadline: 3:59pm Wednesday 11th May 2022
(**please note that submitting exactly at 4:00pm will result in a penalty**)
Feedback: by Wednesday 8th June 2022
Weighting: 30% of module evaluation

Introduction

For this assignment, you will analyse a given cyber-attack using the kill chain model. You will also analyse the profile of the attacker. Furthermore, you will be provided with the description of the IT infrastructure of a company and be asked to analyse its security with respect to the UK Cyber Essentials and another security control.

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

All the reports will be checked for plagiarism by scanning them in Turnitin.

Instructions

Please download the report template from the following link:
https://secure.ecs.soton.ac.uk/noteswiki/images/COMP2216-2122-CourseworkTemplate.docx
A version of the report template with additional information and guidance can be accessed here: https://secure.ecs.soton.ac.uk/noteswiki/images/COMP2216-2122-CourseworkTemplateWithDetailedInstructions.pdf

Part 1 – Cyber-Attack Analysis

The water distribution company CyberWater has been targeted by a cyber-attack, which disrupted the water distribution service for a few hours. The IT infrastructure of CyberWater includes a standard, flat IT network with employees' computers, and an air-gapped network with machines monitoring/controlling the physical water distribution process. The IT network is connected to the Internet via a well configured firewall, while the air-gapped network is not connected to the Internet. For analysis purposes, monitoring data collected inside the air-gapped network is manually transferred daily to the IT network using a dedicated laptop. Forensic analysis showed that the adversary attacked the machine that directly controls the water distribution process by exploiting vulnerability CVE-2020-10615 over the network, which caused the machine to halt. Also, it was found that the adversary compromised the laptop used to transfer monitoring data by exploiting vulnerability CVE-2021-22803, which allows executing arbitrary code and can be exploited via network. A malware was discovered inside the laptop, which was dissected and analysed to understand its behaviour. The analysis showed that the malware registered itself as auto-start service and was quite advanced as it included several functionalities, such as automatic reconnaissance (with recon data saved locally) when in the air-gapped network, and connection to an external machine over the Internet when in the IT network. An employee confessed to have been bribed by someone to install a software inside their computer in the IT network and disclose information about operational procedures inside CyberWater, including the fact that the machinery controlling the physical water distribution process is in an air-gapped network, and that a laptop is used to transfer monitoring data daily between the two networks. This employee is not technically skilled at all, and has no access to the laptop used to transfer monitoring data.

Task 1.1 – Kill Chain-based Analysis

Perform a "kill chain"-based analysis of the attack, by explaining how it worked in each phase.

Task 1.2 – Attacker Analysis

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

Part 2 – Corporate Security Analysis

The internal network of an SME is protected by a boundary firewall that blocks any unauthenticated inbound connection but those towards the machine hosting the company's website. This website was created by a development company. All default passwords are changed, and policies are enforced to ensure employees choose strong passwords for their accounts. In particular, all passwords must be at least 16 characters long and must be changed at least once every six months, or whenever a user suspects their password has been compromised; a clear process is established to help employees change their password. Also, employees are discouraged from picking common or discoverable passwords, and encouraged instead to use the password manager provided by company. Each employee is given a unique account, regardless of their role. Each account is configured to provide access to only those services actually required for the user to perform their role. There is a clear process in place to create and approve new accounts. Access to any service and resource of the company is only granted to authenticated users. Users are authenticated using username and password. The privileges of all accounts are routinely checked and updated if required (e.g., if an employee changes their role). All employees' computers require unlocking to be accessed by a user. Employees can unlock their computers using their credentials; however, after 5 unsuccessful unlocking attempts, a computer requires the intervention of an administrator to be unlocked. Each device has an anti-malware software installed, which is updated daily and scans any file that is accessed and any website that is visited. All software is automatically updated weekly to ensure available security patches are installed promptly. Any special update that requires manual installation is installed within 7 days from its release. The company adopts a no BYOD policy, where no employee is allowed to use their own devices to access organisational data or services, or connect them to the company's internal network. Also, no home working is permitted. The company does not rely on or use any externally managed service.

Task 2.1 – Cyber Essentials

For each of the five UK Cyber Essentials controls (firewalls, secure configuration, user access control, malware protection, security update management), discuss concisely what else the company needs to do to meet the requirements of the control. Please avoid generic statements that are only based on the definition of the Cyber Essentials; rather, make explicit references to the characteristics of the company's internal network and clarify what else the company should do, that is not doing yet, to meet controls requirements.

Task 2.2 – Network Fragmentation and Monitoring

Explain how the company can use the "network fragmentation & monitoring" control to further improve security. Please detail how the network should be fragmented and what kind of monitoring could be deployed, by making explicit references to the characteristics of the company's internal network. Please also discuss why using this control can improve the security of the network.

Deliverables

Submit your report to the ECS Handin system at
https://handin.ecs.soton.ac.uk/handin/2122/COMP2216/1/
before the specified deadline, i.e., **before 4:00pm Wednesday 11th May 2022**.
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 reason why there is a word limit is that it is good practice to write concisely, and you should get used to doing this.

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

For reports longer than 2500 words, only the first 2500 words 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., not a 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.
A4. Demonstrate knowledge and understanding of general principles and strategies that can be applied to systems to make them more robust to attack

Assignment Learning Outcomes (ALO)

AS1. Analyse cyber-attacks by applying the kill chain model.
AS2. Examine the profile of the cyber actors behind a cyber-attack.
AS3. Analyse the security of an enterprise network with respect to the UK Cyber Essentials.
AS4. Analyse the security of an enterprise network with respect to the "network fragmentation & monitoring" control.

Marking Criteria

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

Task	Criteria	ALO	Marking scheme
Task 1.1	Ability to apply the kill chain model to analyse a cyber-attack	AS1	Up to 50 marks, awarded based on how many phases are (i) correctly identified, (ii) well-placed in the chain, and (iii) accurately described
Task 1.2	Ability to examine a cyber actor profile	AS2	Up to 10 marks, awarded based on whether the proposed profile fits the given cyber-attack in terms of attack strategy and motivations.
Task 2.1	Ability to analyse the compliance of a corporate network with the UK Cyber Essentials	AS3	Up to 30 marks, awarded based on how many Cyber Essentials controls are correctly analysed.
Task 2.2	Ability to apply the Network Fragmentation and Monitoring control	AS4	Up to 10 marks, awarded based on whether the control is applied correctly, and its security discussed properly.
File format, report length	Submitted file is in PDF format, the report is compliant with the provided template and is not longer than 2500 word. If the report is more than 2500 words or the format is not PDF, a 10 marks penalty will be applied. <u>If the report is corrupted or cannot be opened, 0 marks will be awarded for the coursework</u>.	-	-

Support

If you need any additional support in completing this coursework, please email any queries to l.aniello@soton.ac.uk.