14-741/18-631: Test 4
Dec. 10th, 2020

Name:

Andrew ID:

Scores

Problem 1 (14 pts max):

Problem 2 (24 pts max):

Problem 3 (20 pts max):

Problem 4 (20 pts max):

Problem 5 (22 pts max):

Total (100 pts max):

Guidelines

- This exam contains 5 problems and is 6 pages long. Check you have all pages.
- **Do not write answers on the back of the pages. They will not be graded**
- To help us grade as anonymously as possible, please **do not write your name or any other identifying information on any page other than this cover page**.
- Be neat and concise in your explanations. Limit your answers to the space provided. You won't be penalized for using incorrect grammar, but you will get penalized if we can't understand what you are writing.
- Show your work clearly. If your reasoning (in other words, steps) is correct, but your final answer is wrong, you will receive most of the credit. On the other hand, answers without proof, explanation, or argumentation get no credit, *even if they are correct*.
- This exam is open-book. All reference books, class notes, and dictionaries are allowed. **Internet access during the exam is strictly prohibited. Accessing the Internet during the exam constitutes an academic integrity violation and will be punished by failure of the class ("R") and other disciplinary measures at the discretion of the University. Turn off your cell phones and devices!**
- Open-book does not mean open neighbor. Cheating on the exam (including accessing the Internet) automatically results in failure of the class and will be reported to the University administration. We do enforce the INI plagiarism policies strictly.
- It is advantageous to partially answer a question than not attempt it at all.

1 Security Economics (14 pts)

1.1 Short answers(7 pts)

1. (3 pts) Provide an example of a positive externality in cybersecurity. The example does not have to come from class discussion (feel free to be creative).

2. (2 pts) What is most likely the common factor that motivates hackers to break into corporate systems and try to leak information from databases?

3. (2 pts) What is most likely the common factor that motivates hackers to perform denial-of-service on government websites?

1.2 Externalities and Nash Equilibrium (7 pts)

A user, Homer, belongs to a company C and does not care about following the best security practices on their device. Homer argues that he likes to focus on his job responsibilities and if a security incident happens, homer trusts that the company will have enough resources to fix it.

1. (3 pts) What kind of externality does Homer create (negative/positive)? Justify your answer.

2. (4 pts) Explain Homer's approach from a Nash Equilibrium/Social optimum perspective.

2 Security Risk Management (24 pts)

You have just been appointed to oversee all security operations of a financial company **F**.

You first analyze all reported incidents, and discover that in the past year, 14 unauthorized root accesses were observed, causing on average, for each of them, 6 hours of work from your two-person IT staff (each costing the company $50/hour) to repair. 12 of these unauthorized root accesses can be traced back to 3 malicious code infections, and the last 2 accesses to an unhappy employee that was let go shortly thereafter.

2.1 Cost (10 pts)

You understand that to convince upper management, you need to provide some numbers related to cost/benefit.

1. (4 pts) How much money did the company lose due to unauthorized root accesses?

2. (6 pts) Installing the `snort` intrusion detection package would have been able to thwart 2 out of the 3 malicious code infections. `snort` is free, but requires a dedicated PC ($2,300), takes 2 man-hour to install, and to have the two IT staff attend a three-day (24-hour) seminar as ongoing education. Do you recommend to install `snort`, or not? (Justify your answer.)

2.2 Insider Threat from Unhappy Users(4 pts)

Provide two recommendations to prevent the situation where an unhappy employee gets unauthorized access as described above.

2.3 Insider Threat from Naive Users (10 pts)

You decided to conduct further analysis to be more thorough. In addition to all the above, you found 4 additional unauthorized accesses that were made by the Chief Financial Officer (CFO) that the company trusts. The CFO travels a lot and is always on the go. The CFO works from wherever possible using their own personal device: home, Coffee shops, airports, etc. The CFO is highly experienced in Finance but is not a fan of learning more about computers and IT.

You spoke with CFO. The CFO was surprised about the situation and assured you that they do not know about any unauthorized access. The CFO volunteers to turn-in their personal laptop for you to inspect to prove that they are honest. After further investigation and analysis, you and your IT team were convinced that the CFO is innocent and attackers took advantage of the CFO's weak IT background to take-over the machine and access F's network.

Now, you want to make sure that this does not happen again, so you consult with your IT team for possible solutions.

1. (3 pts) The first IT team member, Neo, suggests a strategy of forbidden offsite Network access. Employees can only access resources when on company premises. No offsite access for anyone from anywhere. Provide with brief explanation one advantage and one disadvantage of Neo's approach.

2. (3 pts) The other IT team member, Trinity, argues that Neo's suggestion is impractical. Trinity suggests allowing offsite access but employees must use company provided equipment. Provide with brief explanation one advantage and one disadvantage of Trinity's approach.

3. (4 pts) What approach would you choose? You can follow Neo's approach, Trinity's approach, find another approach the meets them in the middle, or come up with a new suggestion. Please Justify your answer.

3 A Security Breach Incident (20 pts)

A company M that specializes in Travel and Tourism, with branches and hotels all over the world had hired you as a Chief Information Security Officer (CISO) because they need to re-establish their processes and learn from past mistakes. This decision was made after the company suffered a major data breach that leaked the information of one million customers. The first thing you did was to look at the timeline of events and try to put the pieces of the story together.

3.1 Who is Telling the Truth? (8 pts)

The company purchased a security tool that is known to you to be reliable. Shortly after the tool was installed, the tool flagged an unusual database query. When the IT support manager was informed, he ordered the IT team to find out what user name was used to access the database. The team came back to the manager explaining that the user name was for a manager in the accounting division, Bob, who has administrator privileges.

The investigation documents shows a signed affidavits from Bob stating that 1) Bob never initiated any queries and 2) Bob does not know what that means. Bob further state that they only uses the Company's laptop to access the work email and the accounting system. In addition, Other employees testified that Bob had been a loyal employee and never had problems and served the company for 25 years.

The IT manager wrote a report that there is no way Bob did not initiate those queries and that the company must fire Bob and pursue legal action. The IT manager supports their claim by explaining that the investigation found a malicious remote access trojan tool and a malware tool that was leaking out user credentials. These tools cannot be installed in system memory without the administrative privileges that Bob has.

As a security expert who understands how systems work, You are asked to provide input on the following:

Is it true that the digital evidence proves with 100% accuracy that the logs are accessed by Bob? If you argue its true, please provide the technical explanation. If you argue its false, please explain a possible scenario that explains what could have happened. Either way, your explanation need to include 1) Bob's username being attached to the queries; and 2) the malware installed by with Bob's credentials.

3.2 A New Security Plan (12 pts)

You came up with a detailed plan to improve M's Cybersecurity practices. After presenting the plan to M's Chief Executive Officer (CEO), and other top executives, you received feedback that although the plan seems very well-detailed, the CEO is not convinced that it is worth spending that money. The CEO argues that the company no longer keeps credit card information in its databases and all the payment data are handled directly between customers and airlines, hotels, car rental companies, etc. M's responsibility is to provide reservations, travel information and packages to its customers. M's relies on having government contracts where M manages travel of government employees, and no credit card or financial information for those transactions are kept on record.

3.2.1 Decide on Security! (6 pts)

You have two options:

1. Agree with the CEO that this should change the scenario and you offer to revise the plan and provide a cheaper alternative

2. Convince the CEO there is still existing risk and the security cost is highly justified

Which option would you choose? Please justify your answer either way. If you you choose option 1, you need to explain how the minimal plan will still provide the needed security. If you choose option 2, you need to provide a convincing argument to the CEO that the risk exists. Your argument must show: the data at risk, the attacker's incentive/motivation/goal.

3.2.2 Decide on Privacy! (6 pts)

You are concerned with *Privacy*. The CEO assures you, that the government employees privacy is ensured and their names are hashed with SHA-256. If the information get leaked, hackers will see hashes and since hashes are one-way functions, there is no way that others can infer the name from the hash.

Do you agree with the CEO. Justify your answer.

4 A New Merger (20 pts)

Company M decides on a merger with company S. You are asked to meet with the Chief Information Security Officer (CISO) of Company S to coordinate and share best security solutions. The CISO of S makes the following suggestions:

4.1 Usable Solutions (12 pts)

In response to a rash of phishing attacks on employees, the IT division should consider the following proposals for the company's email server:

1. All incoming and outgoing emails have to be PGP-signed and PGP-encrypted. The mail client, when it detects problems, will display certificate warning and/or signature invalid warning and give the user the option to proceed.

2. All incoming HTML or graphical email is to be blocked–only text messages can be received. (Attachments are permitted, however.)

The objectives are to maintain high usability, while drastically reducing phishing emails. **Discuss briefly the advantages and drawbacks of each proposal, citing case studies discussed in class**. Make sure to comment on what the users would do that might defeat the purpose of the proposal for each.

4.2 Team Management (8 pts)

The CISO of S leaves the company, and you became the CISO of both merged companies: M and S. The CEO of both merged companies is worried that staff from S are going to leave following their CISO. The CEO suggests to you firing all IT staff from company S within a week period because the CEO believes that you and your team from M are capable of handling systems of both M and S. The CEO also assures you that you will be allowed to hire replacement staff later.

The CEO asks for your input. You disagree with the CEO and argue that firing S's IT staff could have serious security implications.

1. (4 pts) Provide two reasons that supports your argument.

2. (2pts) Provide one non-technical management strategy that you will follow to handle the situation and manage the new team of staff from Company S after the departure of their CISO.

3. (2pts) Provide one technical IT security strategy that you will follow to handle the situation and help provide more reliable security after the merger with the new team of staff from Company S and the departure of their CISO.

5 Understanding Users (22 pts)

5.1 The CEO Password Dilemma (16 pts)

Your Company's CEO tells you that they hate password manager software and they cannot find a good way to use it. The CEO is willing to use the generator feature in the password manager and write-down the password manually using pen-and-paper in the CEO's personal physical note-book.

You consult with three of your IT team members and you get the following suggestions:

(A) Offer training for the CEO. With more training, the CEO will be comfortable using the password manager.

(B) Have the CEO store the passwords in a password protected Excel sheet. This could offer more usability (the CEO can copy and paste) when compared to typing. The password protection helps secure the Excel sheet.

(C) Allow the CEO to manually store passwords in their note-book, but you need to explain to the CEO the importance of maintaining physical security. The notebook should be protected just like how someone protects their personal belongings (e.g. wallet, cellphone, etc.). You can also suggest that the CEO keeps the notebook in a security safe box inside the office along with company's important documents to protect the notebook when the CEO is not present in the office.

1. (12 pts) Provide one advantage and one disadvantage for each suggestion
2. (4 pts) What solution would you prefer. Justify your answer.

5.2 Email Inspection(4 pts)

You are a Netflix subscriber, but you decided to leave the service and return to it later. You receive an email from Netflix asking you to come back and renew your membership. The email provides a link that reads "Renew my Membership" that you can click on. These emails are common and Netflix is not the first company that asks its customer to return. You take a look at the body of the email: content, language, grammar, graphics, logo, etc. and everything looks legit.

1. (2 pts) List one more thing you can check that help you understand if the email is legit or not.
2. (2 pts) You want to renew the Netflix membership after reading the email. Provide an approach that will be safe regardless of the authenticity of the email.

5.3 Patching(2 pts)

Considering usability for IT personnel; provide one reason why patching software and servers is an inconvenient process.