4

Managing Networks and Security

# Homework

Last Name:

First Name:

Date Due: February 24, 2016

# Instructions

General

* Answers that show little or no thought or evidence of proper study will not be accepted and will be counted as errors.
* Single-word answers are rarely sufficient. Show me that you understand the situation.

Test Your Understanding Questions

* You must answer all in **boldface**.
* Questions that are ~~crossed out~~ will not be on the exam.
* All that are not crossed out will be the exam. You get up to 5 points of extra credit for answering all that are not crossed out

End of Chapter Questions

* You must do all that are not crossed out

# Failures in the Target Breach

Test Your Understanding

 1. a) What security mistake did Fazio Mechanical Services make?

 **b) Why do you think it did this? (This requires you to give an opinion.)**

 **c) How might segregation of the network have stopped the breach**?

 **d) Why do you think the Minneapolis security staff did not heed the FireEye warning? (This requires you to give an opinion.**)

 e) **What warnings had Target not responded to adequately**?

 f) What happens in a kill chain if a single action fails anywhere in the chain?

 g) **How can kill chain analysis allow companies to identify security actions it should take**?

 h) **Explain why "Security is a process, not a product**.”

# Network Quality of Service (QoS)

 2. a) What are QoS metrics? (Do not just spell out the acronym.)

 b) Why are QoS metrics important?

## Transmission Speed

Test Your Understanding

 3. a) Distinguish between rated speed and throughput.

 b) Distinguish between individual and aggregate throughput.

 c) **You are working at an access point with 20 other people. Three are doing a download at the same time you are. The rest are looking at their screens or sipping coffee. The access point channel you share has a rated speed of 150 Mbps and a throughput of 100 Mbps. How much speed can you expect for your download? (Check figure: 25 Mbps**).

 d) **In a coffee shop, there are 10 people sharing an access point with a rated speed of 20 Mbps. The throughput is half the rated speed. Several people are downloading. Each is getting five Mbps. How many people are using the Internet at that moment**?

## Other Quality-of-Service Metrics

 4. a) What is availability?

 b) **When should you measure error rates? Why**?

 c) What is latency?

 d) In what units is latency measured?

 d) **Give an example not listed in the text of an application for which latency is bad**.

 e) What is jitter?

 f) **Name an application not listed in the text for which jitter is a problem**.

 g) **Why may adding applications that cannot tolerate latency and jitter be expensive**?

## Service Level Agreements (SLAs)

 5. a) What are service level agreements?

 b) **Does an SLA measure the best case or the worst case**?

 c) **Would an SLA specify a highest speed or a lowest speed**?

 d) **Would an SLA specify a highest availability or a lowest availability**?

 e) **Would an SLA specify highest latency or lowest latency**?

 f) **Would an SLA guarantee specify a highest jitter or a lowest jitter**?

 g) What happens if a carrier does not meet its SLA guarantee?

 h) **If carrier speed falls below its guaranteed speed in an SLA, under what circumstances will the carrier *not* have to pay a penalty to the customers**?

 i) **Does residential ISP service usually offer SLA guarantees? Why or why not**?

 j) **A business has an Internet access line with a maximum speed of 100 Mbps. What two things are wrong with this SLA**?

# Network Design

## Traffic Analysis

 6. Do a three-site traffic analysis for the following two scenarios.

 a) **In Figure 4-8, add traffic of 392 Mbps for Seattle-Ogden traffic. Using a picture like the one in the figure, show your work**.

 b) **In Figure 4-7, remove the link between Q and R but add a link between Q and S. Using a picture like the one in the figure, show your work**.

## Traffic Requirements versus Leased Lines

Figure 4-9: Leased Line Speeds in the United States

|  |  |
| --- | --- |
| **Line** | **Transmission Speed** |
| T1 | 1.544 Mbps |
| T3 | 44.7 Mbps |
| OC-3 | 155.58 Mbps |
| OC-12 | 622.08 Mbps |
| OC-48 | 2,488 Mbps |
| OC-192 | 9,953 Mbps |

 7. **For the preceding three examples and the situations in the previous test-your-understanding question, what leased line would each link require**?

## Momentary Traffic Peaks

 8. a) Distinguish between chronic lack of capacity and momentary traffic peaks.

 b) How long do momentary traffic peaks last?

 **c) What two problems do they create**?

 d) What three choices do you have for reducing the impact of delays for latency intolerant traffic?

 **e) What is the advantage of each compared to the others**?

 f**) What is the disadvantage of each compared to the others**?

 g) **Compared to e-mail and voice over IP, what priority would you give to network control messages sent to switches and routers? (The answer is not in the text.) Explain your reasoning**.

 9. a) What do network visibility tools allow a manager to do?

 b) **Why do they save money**?

 c) **Do they cost more money than they save**?

## Ping and Traceroute

 10. a) **If you ping a host and it does not respond, what can you conclude**?

 b) What *two* things does ping tell you about a host that replies?

 c) **If a router fails, how can you diagnose this with ping**?

 d) Distinguish between ping and traceroute.

 e) **In Figure 4-13, what jump causes the most latency? Show your calculations as a table**.

## The Simple Network Management Protocol (SNMP)

 11. a) List the main elements in SNMP.

 b) **Does the manager communicate directly with the managed device? Explain**.

 c) **Distinguish between Get and Set commands**.

 d) Where does the manager store the information it receives from Get commands?

 e) **What kind of message can agents initiate**?

 f) **Why is network automation important**?

 g) What does a network visualization program do?

 h) **Why is the ability to push changes to remote devices useful**?

# Security Management

## Security Is a Management Issue

## The Plan–Protect–Respond Cycle

 13. a) What happens in each stage of the Plan–Protect–Respond cycle?

 b) **Which stage consumes the most time and resources**?

# Security Planning Principles

## Apply Risk Analysis Thinking

Figure 4-17: Risk Analysis Calculation

|  |  |
| --- | --- |
| Parameter | Countermeasure |
| None | A | B |
| Damage in Successful Attack | $1,000,000 | $500,000 | $1,000,000 |
| Annual Probability | 20% | 20% | 15% |
| Annual Probable Damage | $200,000 | $100,000 | $150,000 |
| Annual Cost of Countermeasure | $0 | $20,000 | $60,000 |
| Annual Outlay | $200,000 | $120,000 | $210,000 |
| Countermeasure Value | NA | $80,000 | (10,000) |

Countermeasure A cuts the damage from a successful attack in half.

Countermeasure A does not reduce the annual probability of a compromise.

Countermeasure B does not reduce the damage from a successful attack.

Countermeasure B reduces the probability of a successful attack by a quarter.

 14. a) **Comment on the statement, “The goal of security is to eliminate risk**.”

 b) **Why do you think Target did not take action to protect its POS terminal**?

 c) **Repeat the risk analysis in Figure 4-17, this time with Countermeasure C, which reduces damage severity by a quarter and the likelihood of attack by 75%. The annual cost of Countermeasure C is $175,000. Show the full table. What do you conclude? Justify your answer**.

## Provide Comprehensive Security

 15. a) What is comprehensive security?

 b) Why is it important?

 c) **Which avenues into and out of its network did Target fail to protect adequately**?

 d) **Give your own example of a failure in comprehensive security**.

## Provide Defense in Depth

 16. a) What is defense in depth?

 b) Why is defense in depth necessary?

 c) **Give your own example of defense in depth inside or outside of networking**.

## Limit Access with Minimum Permissions

 17. a) **Distinguish between authentication and authorizations**.

 b) What is another term for authorizations?

 c) **What is the principle of least permissions**?

 d) **Why is it important**?

 e) **To assign least permissions to someone, what must you know**?

 f) **Give your own example of a least permissions inside or outside of networking**.

## Segment the Network

 18. a) Why is it important to segment different parts of the network and provide access control limits on each path between segments?

 b) How would network segmentation have stopped the attack on Target? Be specific.

 c) **Give your own example of segmenting communication to provide security inside or outside of networking**.

## Identifying and Protecting Single Points of Takeover and Single Points of Failure

 19. a) **Come up with an example of a single point of takeover inside or outside of networking**.

 b) **Come up with an example of a single point of failure inside or outside of networking**.

## Identifying and Protecting Weakest Links

 20. a) What are the two things that distinguish defense in depth from weakest links?

 a) **Come up with an example of a weakest link inside or outside of networking**.

# Conclusion

## Synopsis

## End-of-Chapter Questions

Thought Questions

4-1. Your home is connected to the Internet. You get to create SLAs that the ISP must follow. Being reasonable, write SLAs you would like to have for the following things:

 a) Write an SLA for speed.

 b) Write an SLA for availability. c) Write an SLA for latency. **Do not just say what each SLA should include; actually write the SLAs as the ISP would write them in the form of specific guarantees**. **Begin each with, “We guarantee …).**

4-2. Redo the analysis in Figure 4-8. Remove the link between Ogden and Seattle but add a link between Seattle and Dublin.

4-3. a) Suppose that an attack would do $100,000 in damage and has a 15% annual probability of success. Spending $11,000 per year on Countermeasure A would cut the annual probability of success in half and reduce the damage of a successful attack by 25%. Do a risk analysis to compare benefits and costs. Show your work clearly.

 b) Should the company spend the money? Explain.

 c) What is the maximum a company should be willing to pay for Countermeasure A?

|  |  |  |
| --- | --- | --- |
|  | Base | A |
| Damage | $100,000  | $75,000  |
| Annualized Rate of Occurrence | 15% | 7.5% |
| Annualized Damage | $15,000  | $5,625.0  |
| Annualized Cost of Countermeasure | $11,000  |
| Outlay | $15,000  | $16,625.0  |
|  |  |  |
| Damage | $100,000  | $75,000  |
| Annualized Rate of Occurrence | 15% | 7.5% |
| Annualized Damage | $15,000  | $5,625.0  |
| Annualized Cost of Countermeasure | **$9,375**  |
| Outlay | $15,000  | $15,000  |

4-4. An executive opened an e-mail attachment because the content looked like it came from a subordinate. In addition, the executive knew that the company did antivirus filtering. Actually, this was a spear phishing attempt, and the attachment contained malware. What security planning principle does this breakdown represent?

4-5. Edward Snowden, a server administrator, was able to copy many CIA secret and top secret files to a USB RAM stick. What security planning principle breakdown allowed this?

4-6. For the following table, list the security planning principle involve in each example and justify your choices. More than one principle may be involved.

|  |  |  |
| --- | --- | --- |
| **Example** | **Principle** | **Justification** |
| Deciding whether to place a combination lock on the door to the computer center. |  |  |
| Protecting a building with many entry points. |  |  |
| Two-factor authentication for a debit card—the card itself and a PIN |  |  |
| Parental controls on a television |  |  |
| Compromising a client PC’s password. |  |  |
| Failing to sanction an employee for tailgating—following another employee through a door without swiping his or her access card. |  |  |
| Taking over a firm’s login system. |  |  |
| Failing to update antivirus signatures. |  |  |
| In a public storage facility, the elevator has a different combination for each customer. It will only take the person to the floor that contains his or her storage locker. |  |  |
| Attacking your systems itself in order to identify vulnerabilities before attackers can. |  |  |
| Compromising a border firewall. |  |  |

Perspective Questions

 4-7. What was the most surprising thing you learned in this chapter?

 4-8. What was the most difficult part of this chapter for you?