a2-responses

Student name: Chai Wen Xuan

Student ID: 21052652

WatIAM : wxchai

Written Response Question

Background

ECorp is one of the largest multi-national conglomerates in the world. Among their enterprises, they manufacture computers, phones, and tablets, and maintain a banking and consumer credit division. This makes it critical to protect their infrastructure from malicious hacker groups such as FSociety. AllSafe Cybersecurity Technologies has been hired to conduct a variety of security tests and protect ECorp’ s infrastructure.

You as an employee of ECorp have been hired to conduct a security analysis to identify potential vulnerabilities.

Specifically, you are informed that ECorp uses a Bell-LaPadula security model with the following sensitivity/clearance levels:

Top Secret >c Secret >c Classified >c Unclassified

and the following compartments:

Finance, Human Resources, Operations, Public Relation, Legal

Q1 Access Control

During your security analysis, you know the existence about two files: (a) scandal.txt must be given sensitivity level Top Secret and restricted to the compartments {Human Resources, Operations, Legal}; and (b) audit.txt has sensitivity level Secret and compartments {Human Resources, Operations}. scandal.txt will be a very sensitive document, and ECorp wants to ensure that only the most privileged administrative employees can read it.

In addition to those two documents, you are able to find a list of ECorp’ s employees from an internal memo hosted on an unsecured S3 bucket. You want to use this internal memo to launch

a highly targeted spear phishing attack to compromise a ECorp employee's account. You only have the resources to carefully craft one such attack, so you must choose your target carefully.

1. [6 marks] You want to know whether each employee can:
   a. read audit.txt (Secret, {Human Resources, Operations})
   b. write scandal.txt (Top Secret, {Human Resources, Operations, Legal})
   c. Both
   d. neither

From those 4 options, indicate each employee's abilities:

a. Susan Jacobs: (Secret, {Human Resources, Legal})

   Ans: write scandal.txt (Top Secret, {Human Resources, Operations, Legal})

b. Terry Colby: (Top Secret, {Finance, Human Resources, Operations, Public Relation, Legal})

   Ans: read audit.txt (Secret, {Human Resources, Operations})

c. Scott Knowles: (Classified, {Human Resources, Operations, Legal})

   Ans: write scandal.txt (Top Secret, {Human Resources, Operations, Legal})

d. Saul Weinberg: (Unclassified, ∅)

   Ans: write scandal.txt (Top Secret, {Human Resources, Operations, Legal})

e. Phillip Price: (Secret, {Human Resources, Operations})

   Ans: Both

f. Tyrell Wellick: (Unclassified, {Finance, Public Relation})

   Ans: neither

2. [6 marks] After careful consideration, you decide to target Phillip Price. Your phishing attack succeeds, and you now have access to Phillip Price's computer at ECorp! You quickly find and exfiltrate the audit.txt file, but you decide to look around some more in case there are other interesting things to be found.

   Phillip Price has access to an internal system which instead uses the dynamic Biba Model with the low watermark property. This system uses the same compartments but the following integrity levels:

   $$\text{High Integrity} >_c \text{Medium Integrity} >_c \text{Low Integrity} >_c \text{Untrusted}$$

   Acting as Phillip Price: (Medium Integrity, {Human Resources, Operations}), you want to read and modify a few files. However, as you perform these actions in sequence, the integrity levels of Phillip Price and the files may change. Note: If a change occurs, the modified integrity level is used for the subsequent operations. Indicate:

a. The integrity level of Phillip Price after this action (including the compartments and how the compartments change)

b. The integrity level of the file after this action (including the compartments and how the compartments change)

for each of the following actions performed in order. (Please indicate ” no change” if there is no change.)

a. Write to File 1 with integrity: (Medium Integrity, {Human Resources})

   Ans:

   i. Integrity level of Phillip Price: no change

   ii. Integrity level File 1: no change

b. Read from File 2 with integrity: (High Integrity, {Human Resources, Operations})

   Ans:

   i. Integrity level of Phillip Price: no change

   ii. Integrity level File 2: no change

c. Write to File 3 with integrity: (Medium Integrity, {Human Resources, Operations})

   Ans:

   i. Integrity level of Phillip Price: no change

   ii. Integrity level File 3: no change

d. Write to File 2

   Ans:

   i. Integrity level of Phillip Price: no change

   ii. Integrity level File 2: (Medium Integrity, {Human Resources, Operations})

e. Read from File 4 with integrity: (Untrusted, {Operations})

   Ans:

   i. Integrity level of Phillip Price: (Untrusted, {Operations})

   ii. Integrity level File 4: no change

f. Write to File 5 with integrity: (Low Integrity, {Public Relation})

   Ans:

   i. Integrity level of Phillip Price: no change

   ii. Integrity level File 5: (Untrusted, {Public Relation})

Q2 Password Security

Now, you want to evaluate the security of the company’ s password authentication mechanism. Its current scheme stores a password hash (fingerprint) file, and authenticates their employee login attempts against this fingerprint. The process for creating the fingerprint and verifying login attempts is as follows:

- Every password entry P maintains an 8-bit random salt S used for generating a fingerprint F. They use hash function H for this system
- The fingerprint of a password is computed as $F = H(P) \oplus S$ and is stored in their password fingerprint file along with the username and S for that user, where $\oplus$ is the bitwise XOR operator.
- When an employee attempts to log in with a password P′, the system verifies the password by computing $H(P') \oplus S$ where S is the salt for that user in their password fingerprint file.

You are tasked with answering the following questions when writing your report on the security of this password mechanisms.

1. [3 marks] Is this mechanism secure? Why or why not (describe a potential attack if not secure)?

   Ans:

   The password authentication mechanism is not secure against offline attacks. If the attacker gains access to the password fingerprint file, and knowledge of the salt value, an attacker can compute the hash value of any password guess and compare it with the stored hash to see if it matches. Therefore, this mechanism is vulnerable to a brute-force attack where an attacker repeatedly guesses passwords until they find a match.

2. [2 marks] Without changing the underlying hashing function, what two ways can the company improve their authentication scheme?

   Ans:

   a. To make the mechanism more secure, instead of using random salt S, user-specific salt should be used. For example, in UNIX , the salt is initially derived from the time of the day and process ID of /bin/passwd. This approach makes it much more difficult for attackers to guess passwords even if they have access to the password file.

   b. Implement two-factor authentication: Two-factor authentication (2FA) adds an additional layer of security to the authentication process by requiring users to provide two different forms of identification before granting access. For example, after entering a password, a user needs to enter a unique code generated by an app on their phone. This makes it much more difficult for attackers to gain access even if they manage to guess the correct password.

1. [2 marks] You are informed that they are using an implementation of SHA-512 algorithm to hash the passwords. Do you think this is the right choice? Explain the reasoning behind your answer, and provide and alternative function and justification if you don't believe this is the correct choice.

   Ans:

   Although SHA-512 is more secure than its predecessor SHA-256, which produces a 256-bit hash value. It is still a standard cryptographic hash and it is cheaper to compute compared to the other hashing function. An alternative to SHA-512 is bcrypt. Bcrypt is a slower hash function that uses a derived form of the Blowfish cypher. It is more resistant to brute-force attacks, as it is slower and more expensive to compute.

4. [2 mark] Phillip Price read a book on computer security in 1994, and wants to change the hash function used for storing passwords. Here is an example password hash he provides, which he believes was computed with an unbreakable hash function:

   2034f6e32958647fdff75d265b455ebf

   a. Name a hash function that could have produced this hash.

      Ans:

      One hash function that could have produced this hash is MD5, as the hashed password is 32 characters(128-bit) long.

   b. What is a password that hashes to this value? (You may use the internet, but please don't share it with your classmates.)

      Ans:

      secretpassword

   c. Is this a good suggestion for a password hashing function?

      Ans:

      No, this is not a good suggestion for a password-hashing function. MD5 is known to be vulnerable to collision attacks, where two different inputs can produce the same hash value.

Q3 Firewalls

During the security analysis of ECorp's systems, you accidentally mess up the firewall configuration. You have to recreate all the firewall rules based on the requirements below. (For this question, you can ignore the order of the rules.)

- ECorp owns the IP range 17.34.152.0/24. (You don't need an explicit rule for this)

- AllSafe Cybersecurity uses a “DENY by default” firewall policy. (You don’t need an explicit rule for this)
- All employees of AllSafe Cybersecurity should be able to browse the internet (both HTTP and HTTPS pages) from within the network.
- AllSafe Cybersecurity hosts a webserver at 84.56.32.48. This server runs over HTTP and HTTPS and needs to be accessible from anywhere in the world.
- Finally, ECorp hosts an IRC server with IP 17.34.152.37 on port 1337. AllSafe Cybersecurity needs to be able to connect to this IRC server with address 243.82.77.16.
- Scott Knowles does much of their work remotely and needs to be able to ssh into their work device from anywhere in the world. They work device has the IP address 243.132.51.32.
- ECorp blocks all incoming traffic from the IP address range 64.56.91.0/24, as this range is known for abusive behavior from FSociety.
- ECorp has shifted to exclusively doing DNS lookups through a DNS server. This DNS server is hosted on IP address 243.82.76.43. This server only listens for DNS requests on port 53 and expects clients to send requests only from ports 1200 through 1550. Assume DNS goes over UDP.

1. [12 marks] Configure the firewall by adding the required rules to meet the aforementioned requirements of ECorp. Rules must include the following:
    - DROP or ALLOW
    - Source IP Address(es)
    - Destination IP Address(es)
    - Source Port(s)
    - Destination Port(s)
    - TCP or UDP or BOTH
    - For TCP, a set of TCP flags that must be set (SYN and/or ACK). Note not all TCP rules may require these flags

    Here is an example rule that allows a server at 5.5.5.5 to serve HTTP pages to ECorp’s network but prevents it from creating new connections:

    ALLOW 5.5.5.5 => 17.34.152.0/24 FROM PORT 80 TO all BY TCP ACK

    For multiple ports 80 and 443:

    ALLOW 5.5.5.5 => 17.34.152.0/24 FROM PORT all TO {80,443} BY TCP

    For a range of ports ”1700-1750”:

ALLOW 5.5.5.5 => 17.34.152.0/24 FROM PORT all TO [1700-1750] BY TCP

For connection to any IP address:

ALLOW 5.5.5.5 => 0.0.0.0/0 FROM PORT all TO [1700-1750] BY TCP

HINTS:

- CIDR Notation may be helpful for this portion of the assignment.
- Some requirements may need more than one rule.
- Ports can be specified as a singular value, range, as a set, or as ‘all’ as seen in the example above.
- Section 10.1 of of the van Oorschot textbook may be helpful in this task.

Ans:

- All employees of AllSafe Cybersecurity should be able to browse the internet (both HTTP and HTTPS pages) from within the network.

  ALLOW 17.34.152.0/24 => 0.0.0.0/0 FROM PORT all TO {80, 443} BY TCP

  ALLOW 0.0.0.0/0 => 17.34.152.0/24 FROM PORT {80, 443} TO all BY TCP ACK

- AllSafe Cybersecurity hosts a webserver at 84.56.32.48. This server runs over HTTP and HTTPS and needs to be accessible from anywhere in the world.

  ALLOW 0.0.0.0/0 => 84.56.32.48 FROM PORT all TO {80, 443} BY TCP

  ALLOW 84.56.32.48 => 0.0.0.0/0 FROM PORT {80, 443} TO all BY TCP ACK

- Finally, ECorp hosts an IRC server with IP 17.34.152.37 on port 1337. AllSafe Cybersecurity needs to be able to connect to this IRC server with address 243.82.77.16.

  ALLOW 243.82.77.16 => 17.34.152.37 FROM PORT all TO 1337 BY TCP

  ALLOW 17.34.152.37 => 243.82.77.16 FROM PORT 1337 TO all BY TCP ACK

- Scott Knowles does much of their work remotely and needs to be able to ssh into their work device from anywhere in the world. Their work device has the IP address 243.132.51.32.

  ALLOW 0.0.0.0/0 => 243.132.51.32 FROM PORT all TO 22 BY TCP

  ALLOW 243.132.51.32 => 0.0.0.0/0 FROM PORT 22 TO all BY TCP ACK

- ECorp blocks all incoming traffic from the IP address range 64.56.91.0/24, as this range is known for abusive behavior from FSociety.

  DROP 64.56.91.0/24 => 17.34.152.0/24 FROM PORT all TO all BY BOTH

- ECorp has shifted to exclusively doing DNS lookups through a DNS server. This DNS server is hosted on IP address 243.82.76.43. This server only listens for DNS requests on port 53 and expects clients to send requests only from ports 1200 through 1550. Assume DNS goes over UDP.
  ALLOW 17.34.152.0/24 => 243.82.76.43 FROM PORT [1200-1550] TO 53 BY UDP