CS458 A2

Justin Cai, t28cai, 20786110

Q1: Access control

1.1:

Alice Zander has top secrete on all, thus he can only read it, cannot write (a)

Bob Yves has secrete clearance on Admin, meaning he can do only write (b)

Carol Xavier has secret on admin again, identical to bob and alice, he can do both (c)

David Wheeler is unclassified, thus he can write to eveything including report.txt but not read anything (b)

Eve Victoria is a Classified individual on Admin, thus he can write to report.txt only (b)

Frank Ulysses is not in any department, he can write to report.txt only (b)

1.2:

(**a)** since you read the file 1 with High integity, nothing hcanges

- Carol is at Medium Integrity, {Administration, Development}
- File 1 is at High Integrity {Administration, Development}

(b): both are medium, no change happens

- Carol is at Medium Integrity {Administration, Development}
- File 2 is at Medium Integrity {Administration}

(c): Carol lower the file security

- Carol is at Medium Integrity {Administration, Development}
- File 3 is at Medium Integrity {Administration, Development}

(d): since you read File with lower integrity, your permission goes down

- Carol is at Low Integrity {Development}
- File 4 is at Low Integrity {Development}

(e): Since you write to file 2 again, this time with lower permission, you downgraded file to to low integrity too. Note that greatest lower bound means the department is completely removed

- Carol is at Low Integrity {Development}
- File 2 is at Low Integrity {}

(f): Carol is now reading a file with Untrusted, thus itself downgrad to untrust

- Carol is untrusted {}
- FIle 5 is untrusted {Marketing}

Q2: Password Security

1

Rule 1's lower bound is really bad. with just 25 AMDS Radeon graphics card you can try 95^8 combinations in 5.5 hours, (note this includes every possible eight-character password containing upper- and lower-case letters, digits, and symbols). Most people are lazy and will set short password, which means this rule is really weak against brute force. I would suggest to go for 12 minimum instead (no limit on how long you want it to be, longer the better) Note that NIST 2017 in my opinion is outdated

Rule 2 is bad because everyone would just use the same trick to satisfy the rule instead of actually making their password more secured (easy password + extra simple character to satisfy)

Rule 3 is a great on the surface but it typically leads to user cycling their password which is not very useful at the end of the day, like helloworld to helloworld_1 to helloworld_2,

2

bcrypt is a great idea for hash, when a leak happens, the following property of bcrypt will give attackers a headache:

- You can define a salt for bcrypt, and you can have a unique salt for every users. this prevent rainbow table attacks as attacker has to recomputer the entire table using the salt, thus making computing very expensive
- More over, you can define salt round, which is how many round you encrypt the password, the more there is the harder to compute the password, making brute forcing even more challenging It might be a reasonable cost in time to compute the exact password once for verification, but for bruteforcing, repeating this process will consume wayyy to much time.

3

Seems like Bob Yves like MD5, if you hash “password123” with MD5Sum, you get this hash. It a pretty terrible hash for following reason

- It fast, the default MD5 cannot have salt and no salt round, means you can compute MD5 hash very fast.
- In fact, people compute these entries so fast these days, we start to have severe issues with people generating table containing k-v table containing the original password to the hash (or the reverse). This means you can just look up the hash and get the original value, especially if the original value is something like “password123”
- Worst of all, it very easy to get a collision in MD5 hash value, which sucks a lot. this means attacker sometimes doesn’t even need to guess your password, just need to put in something that produce identical hash.

4

It very easy to intercept SMS messages, for example, social engineering to trick provider such as dell and get the sim card from another person, another attack is make use of weakness in the SMS protocols, which is a protocol that is well known to have severe weaknesses. More importantly, your phone can be stolen as well.

Q3: Firewalls

129.34.156.0/24 indicate that the last 8 bits are bits which you can control in this case we have address from 129.34.156.0 to 129.34.156.255

1. All employees of CHOWN should be able to browse the internet (both HTTP and HTTPS pages) from within the network. Note that HTTP and HTTPs only relies on TCP protocol, thus we are ignoring the UDP connectoin
    a. ALLOW 129.34.156.0/24 ⇒ all FROM all TO port {80, 443} BY TCP
    b. ALLOW all ⇒ 129.34.156.0/24 FROM port {80, 443} TO all BY TCP ACK
2. CHOWN hosts a Matrix server at 129.34.156.48. This server runs over HTTP and HTTPS and needs to be accessible from anywhere in the world. Note that HTTP and HTTPs only relies on TCP protocol, thus we are ignoring the UDP connectoin
    a. ALLOW all ⇒ 129.34.156.48 FROM all TO port {80, 443} BY TCP
    b. ALLOW 129.34.156.48 ⇒ all FROM port {80, 443} TO all BY TCP ACK
3. The Matrix server also needs to be able to communicate with Root’s own Matrix server (243.82.77.124) on port 8448 via TCP. Either server may initiate this connection.
    a. ALLOW 243.82.77.124 ⇒ 129.34.156.48 FROM port 8448 TO 8448 BY TCP
    b. ALLOW 129.34.156.48 ⇒ 243.82.77.124 FROM port 8448 TO 8448 BY TCP
4. Carol Xavier does much of her work remotely and needs to be able to ssh into her work device from anywhere in the world. She has the IP address 129.34.156.78. Note that this is a one way connection.
    a. ALLOW all ⇒ 129.34.156.78 FROM all TO port 22 BY TCP
    b. ALLOW 129.34.156.48 ⇒ all FROM port 22 TO all BY TCP ACK

5. CHOWN blocks all incoming traffic from the IP address range 84.71.99.0/24, as this range is known for abusive behavior.
    a. DROP 84.71.99.0/24 to all FROM all to all by BOTH
    b. Note that ths rule overpower all other ALLOW rules,
6. Since the acquisition, CHOWN has shifted to exclusively doing DNS lookups through a DNS server operated by its new parent company, Root. 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 1700 through 1750
    a. ALLOW 129.34.156.0/24 to 243.82.76.43 FROM port [1700 - 1750] to port 53 BY UDP
    b. ALLOW 243.82.76.43 to 129.34.156.0/24 FROM port 53 to port [1700 - 1750] BY UDP