Jashandeep Justin Bains
J24bains
20832856

# Q1: Access Control

1:

1. Susan Jacobs
    a. WRITE SCANDAL. Susan jacobs does not belong to the Operations compartment so she cannot read from audit.txt although the simple security property would allow it if not for her compartment. She can however write to scandal.txt because she matches compartments and is in the legal/HR compartments
2. Terry Colby
    a. BOTH. Due to simple security property and Terry's high clearance he can read audit.txt and he can write to scandal.txt due to * property
3. Scott Knowles
    a. WRITE SCANDAL. By ss property and Scott's lower clearance he can not read audit.txt but he can write to scandal.txt via * property and is in the correct compartments
4. Saul Weinberg
    a. NEITHER. Saul has unclassified clearance as well as belonging to no compartment so he can do neither
5. Phillip Price
    a. BOTH. Due to both being given Secret sensitivity and being a part of Human Resources and Operations Phillip can both read audit.txt and write to scandal.txt
6. Tyrell Wellick
    a. NEITHER. Tyrell belongs to the wrong compartments to be able to read or write from either file

2:

1. Write File 1: Medium, {Human Resources}
    a. NO CHANGE
    b. File integrity does not change because GLB(MED {HR,O}, MED {HR}) = MED {HR}
2. Read file 2: High, {Human Resources, Operations}
    a. NO CHANGE as GLB(MED {HR,O}, HIGH {HR, O}) = MED {HR,O}
    b. NO CHANGE
3. Write File 3: Medium, {Human Resources, Operations}
    a. NO CHANGE
    b. NO CHANGE MED {HR,O} Subject integrity is unchanged because GLB for both subject and object are the same
4. Write to file 2 High, {Human Resources, Operations}
    a. NO CHANGE
    b. File 2 is downgraded to MED {HR, O} due to object low watermark property and Phillip's MED integrity compared to the files previous HIGH integrity. Compartments remain unchanged
5. Read File 4: Untrusted, {Operations}
    a. Philips' integrity is downgraded to UNTRUSTED, {O} due to subject low watermark property
    b. UNTRUSTED {O} Unchanged due to read
6. Write File 5: Low, {public Relations}
    a. UNTRUSTED {O} unchanged due to write
    b. File 5 is downgraded to UNTRUSTED {O} due to object low watermark property

# Q2: Password Security

1. This is unsecure because the hashed password length must match the salt for XOR to work which implies that the hashed password is only 8 bits which is very easy to crack using brute force with modern computing power regardless of if the password was salted or not.
2. Using MAC and adding the salt to the password before hashing which will increase the length of the password as well as making it unique. In conjunction with using MAC with the salt we can create another salt which is stored in a different location than the fingerprint file and also used in the MAC which further improves security and if the fingerprint files are leaked then the secret salt remains secret as long as the other location is not leaked as well.
3. Because SHA-512 is fast it would be better to use a slower hashing algorithm such as bcrypt to impede the speed at which brute forcing attacks can succeed
4. A
    a. MD5 could've been used to compute this hash
    b. The password is "secretpassword"
    c. No. MD5 is riddled with collision vulnerabilities which means that if a single password were to leak then it would be possible to login to multiple accounts because they would share the same hash values and it would be easy to see which accounts the password can access

# Q3: Firewalls

Format:

Action SourceIP SourcePort => DestIP DestPort Connection SYN/ACK/NOFLAG

Note:

HIGH ports are the set of ports that are not reserved

Allow http/s requests

ALLOW 17.34.152.0/24 {HIGH} => 0.0.0.0/0 {80,443} BY TCP
ALLOW 0.0.0.0/0 {80,443} => 17.34.152.0/24 {HIGH} BY TCP ACK

Allow webserver access from anywhere

ALLOW 0.0.0.0/0 {HIGH} => 84.56.32.48 {80,443} BY TCP
ALLOW 84.56.32.48 {80,443} => 0.0.0.0/0 {HIGH} BY TCP

Allow IRC server accessibility

ALLOW 243.82.77.16 {ALL} => 17.34.152.37 {1337} BY TCP
ALLOW 17.34.152.37 {1337} => 243.82.77.16 {ALL} BY TCP

Allow Scott Knowles to work remotely

ALLOW 0.0.0.0/0 {ALL} => 243.132.51.32 {22} BY TCP
ALLOW 243.132.51.32 {22} => 0.0.0.0/0 {ALL} BY TCP ACK

Deny all Fsociety inbound traffic but allow outbound?

DROP 64.56.91.0/24 {ALL} => 17.34.152.0/24 {ALL} BY BOTH
ALLOW 17.34.152.0/24 {ALL} => 64.56.91.0/24 {ALL} BY BOTH

Allow DNS queries and responses

ALLOW 17.34.152.0/24 {1200-1550} => 243.82.76.43 {53} BY UDP
ALLOW 243.82.76.43 {ALL} => 17.34.152.0/24 {ALL} BY UDP
ALLOW 17.34.152.0/24 {1200-1550} => 243.82.76.43 {ALL} BY UDP