Jennifer Shi 20662230
CS458 j77shi@uwaterloo.ca

A2

Written Response Questions

Question 1

1. Bell-La Padula Confidentiality Model: no read up, no write down

Eve: (Secret, {US, G})

(a) (Top Secret, {US, G, M})

Write access

(b) (Confidential, {G})

Read access

(c) (Top Secret, {US,G})

Write access

(d) (Secret, {US, G})

Both

(e) (Confidential, {US, M})

No access?

2. Dynamic Biba Integrity Model

Carol: (Top Secret, {US, M})

(a) Carol reads from record1 having integrity: (Top Secret, {US, G})

Integrity of Carol: (Top Secret, {US})

(b) Carol writes to record2 having integrity: (Confidential, {US})

Integrity of record2: (Confidential, {US})

(c) Carol reads from record3 having integrity: (Top Secret, {US,M})

Integrity of Carol: (Top Secret, {US})

(d) Carol writes to record4 having integrity: (Top Secret, {US, G, M})

Integrity of record4: (Top Secret, {US})

(e) Carol reads from record5 having integrity: (Confidential,{US})

Integrity of Carol: (Confidential, {US})

Jennifer Shi 20662230
CS458 j77shi@uwaterloo.ca

Question 2

1.
   (1) qwerty1234
   (2) iloveyou
   (3) 123456789
   (4) password
2. Total number of possible characters:

   26 + 26 + 10 + 8 = 70

   Total number of possible passwords: 70^8

   For one machine: 70^8/(5*10^6) = 115296020 seconds

   115296020/60/60/24/365 = 3.656 years

   3.656/2=1.828 years needed to complete on average

   115296020/60/60 = 32026.6722222

   32027 machines needed to complete in an hour or 16014 machines needed on average

3. password of length 8 is 8 bytes, SHA256 is 32 bytes.
   Each <password, h(password)> is 40 bytes.
   There are 70^8 of possible passwords. Therefore the amount of data needed to be stored is 70^8*40 bytes = 23 059 204 gigabytes

4. 70^8/60000*16 bytes = 153.728 GB of data needed

5. For each chain, there will be a maximum of 59999*60000/2 = 1799970000 hashes computed

   Assume the average is midpoint, 29999*30000/2 = 449985000 hashes computed per chain

   And there is 70^8/60000 chains, so in the worst case there will be 70^8/60000*1799970000 hashes computed =1.7294115 *10^19

   Average case: 70^8/60000*449985000=4.3234566*10^18 hashes computed

   Worst Case
   1.7294115 *10^19/ 5000000 = 3.458823 * 10^12 seconds = 109678.556316 years

   Average case:
   70^8/60000*449985000/5000000 = 864691325995 seconds = 27419.182 years

6. The rainbow table helps by reducing the number of data needed to be stored in a database. It is space efficient. However, the computational cost of the rainbow table is large. Inevitably, the attacker needs either large computational power or large database.
7. This protects against the rainbow table attack as the same password will end up with different hash values due to the concatenation of a random 64 bit salt value. The attacker would not be able to guess the password from the hash value without knowing the salt. It would increase the computational cost of brute forcing to solve the solution.

Question 3

1. [2 marks] Bruce says we should reinstate a blacklist with a list of all known malicious IP addresses along with the source IP address of the recent breach to protect against any future attacks. Is this a solid defense strategy? Elaborate why or why not? Based on that what do you advise be the default rule on the firewall?

   This is not a solid defense strategy, because we should not use a blacklist filtering. Using a blacklist will let in a lot of unwanted traffic. We should use whitelist of allowable source/destinations instead of a blacklist.

2. [2 marks] While configuring the firewall, you get a request to give access to an internal FTP server to a range of IPs owned by the new branch of the organization in a different location. With further inspection, you find out that there have been outbound responses from the FTP server. What kind of attack is done on the organization? How does the request exacerbate it? What can you suggest to prevent such attacks?

   Outbound responses from the FTP server means that there has been spoofed traffic on the network. This attack tries to send a packet from outside towards the internal network. The request exacerbates the attack by allowing more range of IPs owned by the internal FTP, allowing the attacker to have more branches to be attacked on. We can prevent it by discard packets that arrive at the incoming side of the firewall, with source IP equal to the internal IP.

3. [6 marks] Go ahead and configure the firewall by adding the required rules to meet the afore mentioned requirements. 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
   Here is an example rule to allow access to HTTP pages from a server with IP address 5.5.5.5:
   ALLOW 5.5.5.5 => 16.18.20.0/25 FROM PORT 80 to all 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.

Rule	Action	Source Address	Destination Address	Source Port	Destination Port	Type
1	Allow	*	16.18.20.0/25	80	*	TCP
2	Allow	16.18.20.25	*	*	80	TCP
3	Allow	16.18.20.0/25	16.18.20.85	25	25	TCP
4	Allow	16.18.20.85	16.18.20.0/25	25	25	TCP
5	Allow	53.16.71.12	16.18.20.0/25	1773	6000	BOTH
6	Allow	16.18.20.0/25	53.16.71.12	6000	1773	BOTH
7	Allow	8.18.10.218	16.18.20.10	*	3223	TCP
8	Allow	16.18.20.10	16.18.20.0/25	3223	*	TCP
9	Drop	*	16.18.20.0/25	*	*	BOTH

4. [2 marks] After setting up the firewall, Bruce suggests to migrate the DNS server to an internal server and also make it possible for employees to access the mail server from outside the organization. Using a DMZ (which includes your Web, FTP, Mail and DNS servers), you configure two firewalls. But instead of dropping illegitimate requests to the DMZ on the external firewall, you reject those requests and respond with ~~either a TCP ”RST” or a UDP ”Destination Unreachable~~” an ICMP ”Destination Unreachable” packet. Analyze how can this affect the security of your network.

   By moving the DNS server to an internal server and DMZ will increase the safety of the internal network, because it reduces the number of outside traffic from coming in. And DMZ adds in an additional layer of protection. Making it possible for employees to access the mail server from outside the organization may poses potential threats from malicious users accessing the mail server. Rejecting illegitimate requests with ICMP “Destination Unreachable” packet may adds in extra work for the internal server, it may make the network vulnerable to denial of service attack where the malicious attacker sends in millions of illegal requests to stop the network from sending method.

Jennifer Shi 20662230
CS458 j77shi@uwaterloo.ca

Question 4

1. Is the concept of least privilege followed here? What about complete mediation? Explain your answers. **[4 marks]**

The concept of least privilege is not followed here since services are provided with all available privileges regardless of their function. Complete mediation is not followed here as file/memory access is not checked for programs with administrator privileges.

2. A file creation service assigns read and write permissions to every file it creates by default, unless specific permissions are provided to the service when called. Which OS design policy is violated and how? **[2 marks]**

This violates the OS design policy of permission-based access (fail-safe default). We should not allow access directly upon creation, we should set the default to be not be able to read and write by default and only changing the permission if necessary.

3. Describe two potential vulnerabilities of this system and explain a potential solution for each. **[4 marks]**

The complete mediation and least privilege may be violated if the attacker maliciously trick an admin to download a malware. Then, unsigned programs will be installed by administrators. And then, the malware would have admin privileges and have full file and memory access since "File/memory access is checked for programs without administrator privileges".