CS458 Assignment 2
Insung Chung
i4chung
20576619

Written Response Questions

Question 1. Access Control

Part 1. No read up, no write down

(i) A

(ii) B

(iii) C

(iv) D

(v) B

(vi) B

Part 2.

Carol Xavier: (Medium Integrity, {Administration, Development})

action	Integrity level of Carol	Integrity level of the file
A	Not changed	Not changed
B	Not changed	Not changed
C	Not changed	Medium Integrity, {Administration, Development}
D	Low Integrity, {Development}	Not changed
E	Not changed	Low Integrity, { }
F	Untrusted, { }	Not changed

Question 2. Password Security

Part 1.

1. Bad. NIST 2017 suggest at least 8 characters minimum length to at least 64 characters maximum length. As range from 8 to 12 characters is not as wide range as 8 to 64 characters passwords, this will end up limiting the range of the passwords, and potentially make it easy to guess.

2. Bad. Forcing composition rules will not help making secure passwords as everyone uses same simple trick to bypass the rule. For example, enforcing special characters in the password might end up resulting a lot of simple passwords with "!" appended at the end.

3. Bad. As people are easily get annoyed to remember passwords, it is most likely that the users will periodically cycle over similar passwords.

Part 2. Bcrypt is a reasonable choice. As it is expensive to compute, it takes longer time for attackers to guess.

Part 3.

a) MD5

b) password123

c) High message collision, easy to guess, there is known huge dictionary online. If same messages are hashed using MD5, it will produce duplicated hash values, making it easy to spot patterns. In addition, MD5 is also old, easy to spot what hash function it is.

Part 4.

SMS based authentication is not the best approach to take, as there are multiple ways to forge the authentication. For instance, attackers can forge the authentication by including methods such as spoofing or phishing, SIM swapping, RDP.

Question 3. Firewalls

Rule	**Src**		**Dest**		**Protocol**	**Flags**
	IP	port	IP	Port		
Deny	84.71.99.0/24	*	*	*	*	*
Allow	129.34.156.*	*	*	80 or 443	TCP	SYN xor ACK
Allow	*	80 or 443	129.34.156.*	*	TCP	SYN and ACK
Allow	*	*	129.34.156.48	80 or 443	TCP	SYN xor ACK
Allow	129.34.156.48	80 or 443	*	*	TCP	SYN and ACK
Allow	129.34.156.48	*	243.82.77.124	8448	TCP	SYN xor ACK
Allow	243.82.77.124	8448	129.34.156.48	*	TCP	SYN or ACK
Allow	129.34.156.48	*	243.82.77.124	8448	TCP	SYN or ACK
Allow	*	*	129.34.156.78	22	TCP	SYN xor ACK
Allow	129.34.156.78	22	*	*	TCP	SYN and ACK
Allow	*	1700 to 1750	243.82.76.43	53	UDP	*
Deny	*	*	*	*	*	*