Minqi Xu
m259xu
20845758

Q1

a)

1. Write access
2. Read access
3. Read and Write access
4. No access
5. No access

b)

1. Barbara' s clearance level will change into (Trainer, {medical})
2. Barbara' s clearance level will change into (Athlete, {medical})
3. Doc3' s clearance level will change into (Athlete, {})
4. Doc4' s clearance level will change into (Athlete, {medical})
5. Barbara' s clearance level will change into (Fan, {medical})

Q2

a) Password guessing attack

b) May not be able to prevent the attacks in the future since the hash is using the standard hash mechanisms (SHA-256). If the attackers has the computational resources to crack the hash, they still have the ability to determine the new passwords that Carlton used in the past 8 months.

c) One way is to add salt. Since each user' s salt is unique, it makes guessing attacks harder, and can' t just build a single table of fingerprints and passwords and use it for any password file.

Another way is to avoid using standard hash mechanisms, since they are relatively cheap to compute. Instead, use an iterated hash function that is expensive to compute (e.g. bcrypt) and maybe also uses lots of memory (e.g. scrypt)

d) The magnetic key card is the most secure one. For additional pin, it is still the thing that belongs to "user knows" class. Which is not safe since if the password is leaked, the additional key is also likely to be leaked. For SMS message, it may not be safe due to it is vulnerable to SIM card swapping attacks or interception of SMS messages. For magnetic key, this is the most safe one since it is a physical hardware, it requires physical possession of the key card.

e) SHA-256 is relatively cheap to compute. Compared to bcrypt and scrypt. Also, since it is a quite well-known method to hash, there is a large database to match the hashed result and original content.

One way to eliminate is using the key-stretching algorithms such as bcrypt and scrypt, which is expensive to compute. Another way is to use PBKDF which is also aimed to slow the process to crack passwords.

Q3

a)

ALLOW 18.28.148.0/24 => Any FROM all to PORT 80, 443 BY TCP
ALLOW Any=>18.28.148.0/24 FROM PORT 80, 443 to all BY TCP ACK
ALLOW 18.28.148.0/24 => 20.140.130.178 FROM all to PORT 55445 BY TCP
ALLOW 20.140.130.178 => 18.28.148.0/24 FROM 55445 to all BY ACK
DENY 48.67.66.128/25 => Any FROM all to all BY BOTH
ALLOW 123.22.34.23 => 18.28.148.0/24 FROM all to PORT 22 BY TCP
ALLOW 18.28.148.0/24 => 123.22.34.23 FROM PORT 22 to all BY TCP ACK
ALLOW Any => 18.28.148.13 FROM all to PORT 443 BY TCP
ALLOW 18.28.148.13 => Any FROM PORT 443 to all BY TCP ACK
ALLOW Any => 86.243.82.76 FROM PORT 1300-1500 to PORT 53 BY UDP
ALLOW 86.243.82.76 => Any FROM PORT 53 to PORT 1300-1500 BY UDP

b) Using Demilitarized Zone(DMZ). By doing this, web server is placed in a sperate zone , DMZ isolated internal network and external network. There is a subnetwork that contains an organization' s external services accessible to the Internet. And External Firewall are protecting DMZ, Internal firewall protects internal network from attacks lodged in DMZ.