NAME: Connor Raymond Stewart
ID: 20673233

CS658 WINTER 2022 – ASSIGNMENNT TWO

Written Response Questions

Question 1: Bell La Padula Model / Biba Model

1. Using the Bell La Padula Model:
   a. Neither read nor write access
   b. Read access
   c. Neither read nor write access
   d. Write access
   e. Both read and write access
2. Dynamic Biba model using the low watermark properties:
   a. Alice: (Administrator, {attendance, employee record, equipment})
   record1 (unchanged): (Administrator, {attendance, employee record, equipment})
   b. Alice (unchanged): (Administrator, {attendance, employee record, equipment})
   record2: (Support Staff, {attendance, equipment})
   c. Alice: (Student, {equipment})
   record3 (unchanged): (Student, {equipment})
   d. Alice (unchanged): (Student, {equipment})
   record4: (Student, {equipment})
   e. Alice (unchanged): (Student, {equipment})
   record5 (unchanged): (Student, {equipment})

Question 2: Firewall

1. Firewall configuration rules:
   [A] – ALLOW 15.5.5.0/25 => all FROM PORT all to ports 80 and 443 BY TCP
   [B] – ALLOW all => 15.5.5.31 FROM PORT all to port 443 BY TCP
   [C] – ALLOW any => 15.5.5.0/25 FROM PORT all to port 22 BY TCP
   [D] – ALLOW 15.5.5.0/25 => 14.19.21.22 FROM PORT 6556 to port 1552 BY both TCP and UDP
   [D] – ALLOW 14.19.21.22 => 15.5.5.0/25 FROM PORT 1552 to port 6556 BY both TCP and UDP
   [E] – ALLOW 15.5.5.0/25 => 10.16.21.21 FROM PORT all to port 3221 by TCP
   [F] – ALLOW 15.5.5.121 => all FROM PORT 25 to port >1023 by TCP
   [F] – ALLOW all => 15.5.5.121 FROM port 25 to PORT >1023 BY TCP
   [G] – we essentially drop all internet traffic which is not given in the above rules. Preferably: ALLOW {rules A, B, C, D, E, F} => FROM all to all BY both. Alternatively, we can express this as: DROP complement{A,B,C,D,E,F} => FROM all to all BY both.
2. The services of IP packets from outside the company network with IPs set to 15.5.5.18 is an example of a spoofing attack with an external IP address spoofing as an internal IP address. A packet filtering gateway can defend against a spoofing attack.
3. DMZ configuration:

a. In a DMZ network configuration, the internal network (users, printers, user-databases, etc.) are separated from services which connect to the internet (i.e., the servers). Therefore, the SMTP mail server, the IRC server, and the Webpage server should all be located within the DMZ. Likewise, the users A, B, and C should be placed within the internal network zone. A firewall should separate the DMZ from the internet, and another firewall should separate the DMZ from the internal zone so that the DMZ acts as a zone between the internet and the internal network. A switcher can still be used within the DMZ and within the internal zone to connect the systems. The router can be used to connect the internal system with the DMZ and internet.

b. Since the DMZ separates the internal network from the internet, and since the webpage hose machine is within the DMZ, the attacker would only have unauthorized access to the DMZ, not the internal zone. Therefore, the internal zone (which contains users A, B, and C) would be the part of the network that the attackers would not have access to.

Question 3: Securing password authentication

a) Eve can utilize her dictionary to find a password to find a password-hash and salt to generate a fingerprint and find a matching fingerprint to get the username and password to login. There are 500000 * 500000 = 250000000000 attempts to try and match each password (hashing and salting) to a fingerprint.

b) Two ways we can improve the scheme without changing the hash function are that we can use a salt greater then 8-bits, and when computing the fingerprint, we can use a message authentication code that has a secret key.