Zizhong Zhu
20530820
z63zhu

Assignment 2

Written Response Questions

1) Hashing Password

a. An salted hash can defend against guessing attacks, use a salt can make guessing attacks harder, can't just build a single table of fingerprints and passwords and use it for any password file.

b.1. Use SHA-1 is relatively cheap to compute, Alice can use an iterated hash function that is expensive to compute (e.g., bcrypt) and maybe also uses lots of memory (e.g., scrypt).

2. It can not defend interception attacks, attacker can intercept password while it is in transmission from client to server, Alice can use Challenge-response protocols to defend.

3. A password cannot normally be recovered from a hash value (fingerprint), it is necessary to store an encrypted version of the password in the password file, and Alice need to keep encryption key away from attacker.

2) Security Policies & Models

a.1. Bob only has read access.

2. Bob neither has read or write access

3. Bob neither has read or write access

4. Bob only has read access.

5. Bob only has write access.

b.1. Carol does not change
D201 change to (Secret, {D,E})

2. Carol and D202 both do not change

3. Eve change to (Unclassified, {B,C})
D203 does not change

4. Eve does not change
D204 change to (Confidential, {C,D})

5. Carol change to (Secret, {D})

3) Firewall

a. It is a Integrity attacks which use IP address spoofing attack, can use Packet filtering gateways / screening routers firewall to defend against it.

b. It is a TCP SYN attack, The server will wait for the acknowledgement for some time, as simple network congestion could also be the cause of the missing ACK. However, in an attack, the half-open connections created by the malicious client bind resources on the server and may eventually exceed the resources available on the server. At that point, the server cannot connect to any clients, whether legitimate or otherwise. This

effectively denies service to legitimate clients. Some systems may also malfunction or crash when other operating system functions are starved of resources in this way.

c. Because IP layer can fragment packets, so firewall might have to re-assemble packets for stateful inspection, so the crash and jamming at the firewall, and it would cause the problem of accessing the web services too.

Programming Response Questions

1. a) First check the url/robots.txt know the url/docs, so I check the url/docs and download the website_db.db, from this Sqlite database,know the hash value for the user nvolodin is “cafebabe", then let hash equal to“cafebabe” and save the cookie, then post a link which means need to set type=2.

   b) Let username equal to “'or 1=1 /*”, which always equal to true, so the check would pass let us be the user uhengartner, which is the first one in user.

   c) It’s easy to guess sengler’s password is “bluejays” because he loves bluejays so much.

   d) First download the url/docs/website_db.db as data.db, then use the same way for part a, I wanna use sql injection, which sql code is:
   ';INSERT INTO users (username,password,confirm,active)VALUES ("z63zhu", "zzz", '', 1); INSERT INTO ref (id_perm,id_user) VALUES (1,10)—“
   encoded them and let hash equal these, after that, the code would be ran and save the new user into the database.