IERG 4130 - Introduction to Cyber Security (2022 Fall)

Assignment 3: Network and Web Security

Total: 70 points

Due Date: Nov. 25, 11:59pm

Note:

- Please answer the following questions. Please write down your student id and answers in a single pdf file, then submit to Blackboard.

Q1: (9 points) Please write at least three types of man-in-the-middle attacks.

Q2:(9 points) Answer the following questions related to Adversary Model.

1. Which part(s) of the CIA triad does the Smurf Amplification attack violated? Please explain briefly.
2. Which part(s) of the CIA triad does the Sniffing attack violated? Please explain briefly.
3. Which part(s) of the CIA triad does the Man-in-the-Middle attack violated? Please explain briefly.

Q3: (12 points) Answer the following questions related to SYN flooding attacks.

1. Does a SYN flooding attack cause the victim server to freeze? Why or why not?
2. In the SYN flooding attack, why do we randomize the source IP address? Why cannot we just use the same IP address?
3. What will happen if the spoofed source IP address in a SYN flooding attack does belong to a machine that is currently running?

Q4: (12 points) For DNS query, it is natural to expect that the local DNS server may not know how to resolve an address. In this case, further queries will be made by this local DNS server. If a hacker can find "a way" to make a certain DNS server report back the wrong IP address, then anyone trying to get to one Web address will be sent to a bogus one, without any obvious way for the user to detect that anything is wrong. Likewise, email could be delivered to the wrong destination.

1. Describe two possible attacks to make the resolver report the wrong IP address.
2. How can an administrator secure the network against the above two attacks correspondingly?

Q5: (6 points) We can use `arp -a` to print out arp table in Unix-like operating system (e.g., macOS, Ubuntu, etc.). What kind of attack will cause the following output result? why?

```
server:~$ arp -a
? (10.13.42.1) at a8:6d:f4:72:b6:65 on en0 ifscope [ethernet]
? (10.13.63.144) at b4:c:28:ef:0:11 on en0 ifscope [ethernet]
? (10.13.42.178) at a8:6d:f4:72:b6:65 on en0 ifscope [ethernet]
```

Q6: (8 points) Consider an application that lets users log in with a userid and password. The following SQL statement is sent to the database, where $userid and $passwd contain data provided by the user. If the query result returns the details of a user, then the login is successful. Otherwise, the login is failed.

```
$sql = "SELECT * FROM users_table WHERE userid='$userid' and password='$passwd'"
```

Answer the following questions realted to SQL injection.

1. An attacker, who knows a victim's userid "Alice" but does not know his password, wants to login the victim's account. What should the attacker put inside $userid or $passwd to achieve that goal?
2. How to prevent above attack as an application developer? Please write at least two ways of prevention.

Q7: (8 points) Cross-Site Scripting (XSS) is a way to inject malicious javascript code into web pages. Answer the following questions related to XSS attacks.

1. To prevent stored XSS, a website developer designs a defense mechanism rejecting any user input that contains `<script>` or `</script>`. Is this defense effective against XSS attack? Why or why not?
2. What can a reflected XSS harm in real-world websites? Please write at least two examples.

Q8:(6 points) Does using SSL/TLS prevent Man-in-the-Middle attack? Why or why not?