Network Security Theory and Practice

Assignment

Due April 10, 2022

POLICIES:

1. **Coverage**
   Lectures 01-07
2. **Grade**
   The ultimate goal for this assignment is review and understand.
   Grading may concentrate more on completeness than correctness.
3. **Individual or Group**
   Individual based, but group discussion is allowed and encouraged
4. **Academic Honesty**
   Violation of academic honesty may result in a penalty more severe than zero credit for an assignment, a test, and/or an exam.
5. **Submission**
   Soft copy on course.zju.edu.cn.
6. **Late Submission**
   NO late submission is permitted.
   Late submissions after April 10, 2022 will NOT be graded.

QUESTIONS:

1. **10 points: DDoS**
   a. What is the difference between DoS attacks and DDoS attacks?
   b. How does the TCP SYN Flood attack work?
   c. How does the solution of SYN Cookies against TCP SYN Flood attacks work?
   d. How does the DNS Amplification Attack work? How to defend against it?
   [Grading Rubric: 10 points = 2 + 2 + 3 + 3.]

2. **10 points: DDoS**
   a. How does Memcached attack work?
   b. What is the difference between HTTP Flood and Fragmented HTTP Flood?
   c. Why is Fragmented HTTP Flood relatively more challenging to detect?
   d. How does Ingress Filtering work?
   e. How does IP Traceback work?
   [Grading Rubric: 10 points = 2 + 2 + 2 + 2 + 2.]

3. **10 points: Secure Routing**
   a. What are the key features of the five typical delivery schemes?
   b. What is the framework of the Dijkstra algorithm?

c. What is the framework of the Bellman-Ford algorithm?
d. How does prefix hijacking work?
e. How does RPKI work? Why is it insufficient for secure routing?
[Grading Rubric: 2 points per sub-question.]

4. **10 points: Anonymous Communication**

a. Why is current Internet communication vulnerable to anonymity or privacy leakage?
b. In which scenarios do users require the communication anonymity or privacy as concerned in sub-question a?
c. How to use proxies to secure communication anonymity? What are the possible limitations?
d. How does Onion Routing provide a better guarantee for anonymity?
e. How to infer anonymity or privacy of Onion Routing traffic?
[Grading Rubric: 2 points per sub-question.]

5. **10 points: Web Security**

a. How does Same Origin Policy work?
b. How does SQL Injection work? How to defend against it
c. Please refer to the slides or search online and provide two concrete examples of SQL Injection.
[Grading Rubric: 10 points = 2 + 5 + 3.]

6. **10 points: Web Security**

a. How does a DNS hijacking attack affect network security?
b. In HTTPS, how does a user verify a certificate for determining the authenticity of the website it connects to?
c. Please provide a concrete example to showcase CSRF.
d. Please provide two concrete examples to showcase Stored XSS and Reflective XSS.
[Grading Rubric: 10 points = 2 + 3 + 2 + 3.]

7. **10 points: Email Security**

a. Please describe common threats against Email security.
b. How should an Email be protected to support both Authentication and Confidentiality?
c. Please describe the differences among DANE, SPF, and DKIM.
[Grading Rubric: 10 points = 2 + 3 + 5.]

8. **10 points: Traffic Analysis**

a. Please describe the properties of the four types of commonly used Firewall.
b. What are the differences among Firewall, IDS, and IPS?
c. Please list commonly used methods for obfuscating traffic to evade detection?
[Grading Rubric: 10 points = 2 + 3 + 5.]

9. 10 points: Open Question - Authentication Efficiency

Consider a time-consuming authentication scenario where a database records all secret keys of a large number of users. When the system authenticates a user, it first issues a challenge message to the user. The user then uses his/her key to encrypt the challenge and then returns the encrypted challenge to the system. The system then encrypts the challenge using one key in the database after another and compares the result with the received encrypted message. Once a match is found, the system accepts the user. Otherwise, the user is denied. This authentication protocol surely takes a lot of time and computation.

Design a possible solution to speed up the authentication process.

666.10 points: SHINE YOUR WAY

[I sincerely thank each and every one of you for taking the "adventure" of Network Security with me, and for your continuing support, understanding, tolerance, and cooperation.
At the very best, I hope you will walk out of this class with not only some security highlights to master but also some fun moments to remember.
When you think of this class once in a while, this is the sweetest I can imagine: Smile because it happened.]

Share your thoughts on the course:
a. To what extent do you devote your time and energy to labs? How do you overcome the associated challenges?
b. Do you think that you have gradually cultivated a research/security mindset? What is the most useful idea that you learned during this process?
c. Provide an example to showcase how you leverage that useful idea to facilitate problem solving in study or life.

Design a question that you think is feasible as an exam question.
a. Which topic among the lectures you would like to consider?
b. Describe a (sufficiently complex) question;
c. Provide also a *correct* sample solution, thanks.

[Finally, the last question of the first, yet last assignment of Network Security. Enjoy.]

waa