188.959 Software Security VU 2,0h

Midterm Exam Retake

June 17^{th}, 2020

Instructions

Please read the instructions BEFORE you start writing!

1. For calculations, write the complete calculation. Your solution needs to be comprehensible.
2. Read the questions carefully. Your answer should include only relevant information.
3. Try to keep your answers short.
4. You may answer in either English or German.
5. You can get up to **25 points** for this exam.
6. Whenever you answer a question, you are not allowed to copy text from websites, lecture slides or other students verbatim, except when the question explicitly tells you to. Otherwise use your own words for your answers.
7. Screenshots or images of answers are not allowed as submission.
8. Upload your questions as pdf file to TUWEL and include your name and student ID on the first page of the document.
9. Make sure that you reference the question numbers in your answers.
10. You have 2 and a half hours to upload your answers, i.e. until 17:30.

1. **(2pt) Describe the relationship between the CVE list and other security databases in detail.**

2. **(2pt) What is the purpose of the Common Vulnerability Scoring System (CVSS)? Describe one of its metric groups.**

3. **(1pt) Describe the design goals (i.e., properties) of the Common Platform Enumeration (CPE).**

4. **(2pt) Describe the process (i.e., information flow in individual steps) how an entry in the National Vulnerabilities Database (NVD) is created.**

5. **(1pt) Describe the properties and rationale behind the Top 25 Most Dangerous Software Errors.**

6. **(2pt) What is Postel's law? Describe a situation where following this principle is desirable. Name and describe one example where it leads to vulnerabilities. Then describe the patch to Postel's law.**

7. **(2pt) Describe the principles of a packet-in-packet attack. Which layer of the OSI model is this attack performed against? Does it work in a theoretical model where the receiver sees exactly the data sent by the sender? Explain why or why not.**

8. **(2pt) A friend of yours recently implemented a communications API used internally by their employer. Because the protocol is rather simple, he just wrote a client and server library in each of the programming languages they commonly employ without documenting the protocol anywhere else. Name and explain three reasons why this is not a good idea in terms of security. What is this type of grammar called?**

9. **(8pt) Write a ABNF specification for "DRS", the *Domain Resolution System*, a simplified version of DNS.**

   A DNS message can be either a request or a response. Each request contains a unique numeric ID, the record type that is being requested and a payload specific to each type (see below). The response contains the ID of the request it is referring to, a field indicating either success (OK), no record found (NX) or server-side error (FAIL), and zero or more response payloads prefixed by the payload type. The payload types and associated payloads are as follows:

   - **A *IP* record request contains a hostname. The response contains an IP (IPv4 only).**
   - ***PTR* requests contain an IP (IPv4 only) and the response contains a hostname.**
   - ***IP* responses (but not requests) may also contain zero or more *ALIAS* records. This is used when a *IP* request refers to a hostname that is an alias for another hostname (e.g. `foo.com` may be an alias for `www.foo.com`). In this case, the response contains the final *IP* response type and payload, and additionally at least one *ALIAS* response type and payload. The payload here is the new hostname (i.e. not the one contained in the request, but the one it is translated/aliased to).**

   After you have completed your grammar, describe how and why a client should validate the ID of a response before using it. (Hint: What happens if a rogue server simply spams responses to everyone?) If your IPv4 grammar permits invalid addresses (e.g. 123.456.789.0), describe how IPs should be validated. (however, if your grammar is already strict enough to prevent invalid addresses, you can skip this step)

   Finally, write a valid DRS request and the associated response.

10. (2pt) What is a binary polyglot? Name and describe at least two reasons why using binary polyglots may be advantageous for malware.

11. (1pt) Describe how inlining of functions as performed by a compiler may reduce security.