**Case study: Reviewing an assessment reporting template**

* Does this template meet the NCSC stated requirement of preparing a baseline to use as a reference point for pen tests? If not what changes/amendments would you make?

As per the NCSC requirements (2022) of preparing a baseline to be leveraged as a reference for performing penetration testing, the degree of technical risk derived from software and hardware vulnerabilities is identified. This important aspect is included in the template, involving the identification and categorisation of vulnerabilities into the following four groups: critical, high, medium, and low severity. Nevertheless, it is mainly focused on patch management due to missing security updates and system configurations; thus, to fully meet the NCSC requirements (2022), the following sections should be also included in the report: 1) details of black-box testing to be performed as a supplementary testing strategy, since it mimics the way wherein external cyber-attackers may operate; 2) positive testing; 3) information on how likely certain vulnerabilities may occur; 4) relevant risk owners; 5) issues that may impact testing, such as the need for out-of-hours testing; 6) the timeframe of carrying out the required tests; 7) the various use cases to test; 8) compliance or legislative requirements to adhere; 9) specific reporting requirements, such as including the CVSS scores or leveraging CHECK severity levels (Houmb *et al*., 2010).

* What are the two best lessons/examples presented in the report?

The two best examples presented in the report involve: 1) the summary of the vulnerability risks identified, along with their severity, count, detailed descriptions, and proposed solutions to mitigate them; 2) specific remediations and the associated percentage of the network vulnerabilities they would tackle.

* What two things do you think are unnecessary or could be done more effectively?

The recommended password and lockout settings should be supported by industry-relevant references, such as the OWASP’s guidelines (Lala *et al*., 2021); furthermore, references should be provided throughout the report where needed. Given the number of vulnerabilities identified, as well as their rather lengthy descriptions, it would be advisable to move the low-severity vulnerabilities to the appendix, so that the reader could focus more easily on higher-severity vulnerability risks, which have the highest impact.

* Did you have any issues or challenges with this activity?
  + I did not encounter any issues in carrying out this activity.
* How did you overcome them?
  + Fortunately, no issues were encountered in this activity.
* How will they affect your final report?
  + The final report should include references to the NCSC security guidelines for penetration testing.

**References**

Houmb, S. H., Franqueira, V. N., & Engum, E. A. (2010) Quantifying security risk level from CVSS estimates of frequency and impact. *Journal of Systems and Software* 83(9): 1622-1634.

Lala, S. K., Kumar, A., & Subbulakshmi, T. (2021) Secure web development using OWASP guidelines. In *2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS)* (pp. 323-332). IEEE.

NCSC (2022) Penetration testing. Guidance. Retrieved from <https://www.ncsc.gov.uk/guidance/penetration-testing#section_3> on July 15th, 2022.