(Q1) What is the purpose of the -sn option in nmap?

(Q2) In the previous lab, you used nmap to find what services are running on what ports in the Metasploitable2 VM. Which nmap option gives you the version of those services? why is it important for vulnerability scanning?

**nmap -S**

It’s important to check the version of software as outdated software likely has vulnerabilities that are easily patched if updated to the newest version.

(Q3) Try scanning Metasploitable2 VM from your Kali machine using -A option with nmap. What additional information about the open ports on Metasploitable2 VM can you get by using this option? o Watch this video for more info

(Q4) What vulnerabilities did you find – both from Google and using the script?

(Q5) Some of the information on a vulnerability scan report might be incorrect. What kind of potential errors should you be looking for on such a scan report?

(Q6) Look at how found vulnerabilities were scored high, medium, and low using their CVSS score. Watch this video and list different parts of the CVSS Base Vector.

(Q7) List different solution types suggested in the report for found vulnerabilities.

(Q8) Watch this video and list the factors to consider when prioritizing found vulnerabilities for remediation.