* What does the article teach you about carrying out vulnerability scans using Kali?
  + Gathering and understanding the target information
  + Dmitry is a deep magic information gathering tool, which used to identify
  + Test on the exploits and other attacks
* What issues might you encounter?
  + The assessment need to be carried out on systems with anti virus and firewalls to get the precise final result.
  + Security system might prevent on the penetration testing WAF
* How would you overcome them?
  + Clone the system and test it without security system
* How do their results compare with your initial evaluation?
  + Mostly the same
* What do you think of their criteria?
  + Better to quantify the criteria instead of Yes/ No.
* What are the pros and cons of using Kali Linux vs. Nessus?
* Kali Linux pros: Capability to run it “live” from a USB drive / DVD, included most of the common free tools.
* Kali Linux cons: Required Linux and system knowledge.
* Nessus pros: Provided plugins for most of the vulnerability. It is easy to use and can run the scan in large scale by scheduling.
* Nessus cons: It is not actively prevented attacks but a tool that checks your computers to find vulnerabilities that exploited.
* Has this changed your original evaluation score?
* The initial evaluation based on different criteria which balanced from the normal user point of view. Technical wise, it should include accuracy, exploit discovered rate, etc. Kali Linux should be the most powerful tools to coverage the whole penetration testing process. In which included most of the common free tools and capability to install and customization.