Name1 : _____ Student Id : _____ Group :_____ Date : _____

Lab 1 – Nmap IP Scanning in Windows (5%) | **DUE DATE : 3 MAY 2019**

Instructions : Please make sure you have the latest version og nmap installed in your PC. Connect your PC to UiTM Raub WiFi. Open your PC's command line and do the following assessment. Please do not scan any website outside the UiTM Network.

1. Basic understanding on **Nmap:**
   a) Explain the features available in nmap.
   b) What is the version of Nmap you are running?
   c) What is the option for a ping scan?
2. Finding the number of connected systems (In your own Network)
   a) What is the nmap command to find the total number of connected system in our network?
   b) How many hosts did it find?
   c) How long did the scan take?
3. TCP / UDP Open Ports (For your own PC)
   a) What is the nmap command to look the TCP and UDP connections?
   b) How many ports did it find?
   c) How long did the scan take?
   d) For all open ports detected, what is the latest vulerabilites/exploits detected associated with the port number? Please find the vulnerabilties/exploits in SecurityFocus and exploit-db.com. Give only ONE and LATEST vulnerabilities/exploits for each port. p/s 10.73.YY.XX is your machine.
4. Nmap Stealth Scan (For your own PC)
   a) What is the nmap command to scan in depts to find the services and open ports?
   b) How many ports did it find? Compare this to the number of ports found with a TCP scan
   c) How long did the scan take? Compare this to the amount of time it took with the TCP scan
5. OS Fingerptint (For your own PC)
   a) What is the nmap command to find the types of operating system used by the target system?
   b) What was the guess made by Nmap? Was it correct?

6. How to detect HeartBleed SSL Vulnerability ? (For your own PC)

   Specify the command and show your answer. (For Nmap version 6.46 and above)

7. What is the nmap command to search for DDoS Reflection UDP Service ?

   Specify the command and show your answer. (For Nmap version 6.46 and above). This is a handy Nmap command that will scan a target list for systems with open UDP services that allow these attacks to take place.

HTTP Service Information

8. What is the command to get page Title from HTTP Services ? Find the page Title from HTTP Services for https://apambalik2u.com
9. What is the command to get HTTP Headers of Web Services ? Find the HTTP Headers of Web Services https://apambalik2u.com
10. What is NSE Scripts? Give 2 example of NSE Scripts in nmap (DO NOT SCAN ANY IP USING NSE Script)

END OF QUESTION