# KONNEXIONS 2020

THEORY EXAM – 20 questions 30 mins [40 marks]

1) The absolute code for file permissions that says the following – "***Owner, User-Group and Others are allowed all read, write and execute permissions (rwx rwx rwx)***"
_777__ [3-digit octal number]

2) These are the Cybersecurity experts who help the Govt and organizations by performing penetration testing and identifying loopholes in their security framework. They ensure protection from malicious hackers and other cybercrimes.
    a. Script Kiddies
    b. Black Hat Hackers
    c. Hacktivists
    d. White Hat Hackers

3) The keyword that helps the current user to run commands as a high privileged user (root).
    a. chown
    b. sudo
    c. which
    d. chmod

4) Write the complete combined command for performing an update and upgrade of your Kali Linux OS.
_____sudo apt-get update && apt-get upgrade_____

5) What is the default **HTTPS** service port?
    a. 80
    b. 21
    c. 443
    d. 135

6) DNS and ARP, respectively, stands for
    a. Domain Name Server
    b. Domain Name Service
    c. Database Name Server
    d. Address Recall Protocol
    e. Address Resolution Phase
    f. Address Resolution Protocol

7) Write the command to initiate a netcat listener on port *1234 :*
___nc –nlvp 1234_____

8) Which of these is NOT valid request method in HTTP/1.1?
    a. GET
    b. ACCEPT
    c. POST
    d. DELETE
    e. PUT

9) Which tool is used to create payloads for social engineering attacks on windows and android devices (a Metasploit standalone payload generator)
    a. msfvenom
    b. sqlmap
    c. netstat
    d. arpspoof

10) What is the default location of Webshells and Nmap scripts in Kali Linux?
    a. /mnt/temp
    b. /usr/share
    c. /bin
    d. /var/www

11) The __/etc/passwd__ file stores essential user account information, which is required during login and __/etc/shadow__ contains the encrypted passwords (hashes) for the active users

12) Mention any one tool designed to brute force directories and file names on web/application servers.

_____nikto / dirbuster / gobuster_____

13) Write the N-map keywords for any 4 of the following options –

OS Scan: ___-O_____

Service Version scan: ____-sS_____

Aggressive Scan: ____-A_____

Normal Scan (Default timing template): ____-T3____

Script kiddies Output: ____-oS____

14) A passive information gathering/footprinting technique used to discover vulnerabilities, data exposure, and security misconfigurations in websites. It involves using specialized search query operators to finetune results based on what you are looking for (site, inurl, intext, …)

____Google Dorking____

15) Write a XSS (Cross-site Scripting) example payload for any website with low level of security:

___`<script>alert(0)</script>`___

OR

___`<img src=x onerror=alert("XSS")>`___

16) What is the general sequence of commands for using an exploit from MSFCONSOLE

a. exploit > search > show options > use
b. show options > search > use > exploit
c. use > show options > exploit > search
d. search > use > show options > exploit

17) Which command searches for files in a **pre-existing** database of indexed locations on the system which makes it UNABLE to find recently created files, and hence is fastest.

a. whereis
b. which
c. locate
d. find

18) Identify the type of Web application attack from the sample payload given –

A. User ID ' or 1=1-- __SQL Injection__
B. http://blogpage.com/foo.php?page=../../../../../etc/passwd __File Inclusion__
C. <img src=x onerror=alert(0)> __XSS Attack__

19) Which of the following tools is used to create wordlists (using letters, numbers and symbols according to specific rules or specific to a company from a given URL)

a. Hydra
b. Crunch
c. CeWL
d. John

20) Which of the following commands are related to Process management in Linux

a. route
b. head
c. kill
d. top
e. grep
f. ps