

Course Name: ETHICAL HACKING

Assignment- Week 5

TYPE OF QUESTION: MCQ/MSQ/SA

Number of questions: 10

Total mark: 10 x 1 = 10

QUESTION 1:

Where are the default NMAP scripts stored in a typical Linux system?

- a. /usr/bin/nmap/scripts
- b. /usr/share/nmap/scripts
- c. /opt/nmap/ scripts
- d. /etc/ nmap/scripts

Correct Answer: b

Detail Solution: On Linux, the default NSE script directory is: /usr/share/nmap/scripts

The correct option is (b).

QUESTION 2:

Which of the following NMAP options runs the default set of NSE scripts?

- a. --nse
- b. --script=all
- c. --script=default
- d. --run-default

Correct Answer: c

Detail Solution: --script=default runs the standard/default set of scripts designed for version detection, service discovery, basic vulnerabilities, and more. --script=all runs all available scripts (not recommended unless needed). --nse and --run-default are invalid or non-existent options.

The correct option is (c).



QUESTION 3:

Which of the following NMAP scripts checks for vulnerabilities to a Slowloris DoS attack?

- a. http-slowloris-test
- b. http-slowloris-discovery
- c. http-slowloris-check
- d. http-slowloris-flood
- e. None of these

Correct Answer: c

Detail Solution: http-slowloris-check script is used to check if the webserver is vulnerable to DoS attack without actually launching a DoS attack, http-Slowloris script is used to launch Slowloris attack. There is no script with name http-slowloris-test or flood.

The correct option is (c).

QUESTION 4:

Which of the following NMAP scripts is used to identify the OS of the target system?

- a. http-os-brute
- b. smb-os-brute
- c. smb-brute
- d. smb-os-attack
- e. None of these

Correct Answer: e

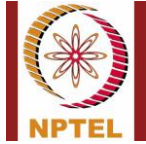
Detail Solution: Nmap does not have a script named http-os-brute, smb-os-brute, smb-brute, or smb-os-attack. The correct script for OS identification via SMB is smb-os-discovery, which is not listed.

The correct option is (e).

QUESTION 5:

Which of the following best describes the function of the crunch tool in hacking?

- a. It scans open ports and running services on a target system.
- b. It generates custom wordlist for password attacks.
- c. It hashes passwords using various algorithms.
- d. It decrypts SSL/TLS encrypted traffic.
- e. None of these.



Correct Answer: b

Detail Solution: Crunch is used to create custom password dictionaries based on rules like length, character set, prefixes/suffixes, etc.

Thus the correct option is (b).

QUESTION 6:

What is the primary function of the hydra tool in penetration testing?

- a. Generating custom wordlist for password attacks.
- b. Performing OS fingerprinting
- c. Performs ARP spoofing attacks
- d. Brute-force login attempts on network services

Correct Answer: d

Detail Solution: Hydra is a fast and flexible login cracker that supports many protocols: SSH, FTP, HTTP, SMB, MySQL, Telnet, etc.

Thus the correct option is (d).

QUESTION 7:

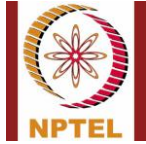
Which tool is most appropriate for performing a brute-force attack against remote login services such as Telnet, FTP, or SSH?

- a. DNSEnum
- b. Crunch
- c. Hydra
- d. Wireshark

Correct Answer: c

Detail Solution: Hydra is a popular login brute-forcer that supports multiple services like Telnet, FTP, SSH, HTTP, SMB, etc. Crunch generates wordlists but does not perform attacks. Wireshark captures network traffic. DNSEnum is used for user enumeration.

Thus the correct option is (c).



QUESTION 8:

What is user enumeration?

- a. Creating multiple user accounts on a system.
- b. Deleting inactive user accounts
- c. Identifying valid usernames on a target system or services
- d. None of these.

Correct Answer: c

Detail Solution: User enumeration is the process of determining valid usernames on a system, often by analyzing different responses from login attempts or error messages.

The correct option is (c).

QUESTION 9:

Which malware records the keystrokes that are typed on the keyboard?

- a. Keylogger
- b. Virus
- c. Adware
- d. None of these.

Correct Answer: a

Detail Solution: A Keylogger monitors and records every keystroke made on a keyboard. It is often used by attackers to steal passwords, credit card numbers, and other sensitive information.

The correct option is (a).

QUESTION 10:

Which of the following best describes the function of the ARP (Address Resolution Protocol)?

- a. It maps IP addresses to MAC addresses in a local network.
- b. It encrypts data at the transport layer.
- c. It maps domain names to IP addresses.
- d. It establishes secure tunnels between routers.

Correct Answer: a

Detail Solution: ARP is used to find the MAC address corresponding to an IP address within a local subnet. It works at the Network Layer (Layer 3) interacting with the Data Link Layer (Layer 2).



NPTEL Online Certification Courses
Indian Institute of Technology Kharagpur



The correct option is (a).

*****END*****