Diploma in Network Security (2009 Course) SUMMER-2019

SUBJECT : NETWORK SECURITY MODULE - II

Day : Friday
Date : 07-06-2019 S-2019-3703

Time 10.00 AM TO 01.00 PM
Max. Marks : 100

N.B.:

1) Attempt **ANY THREE** questions from each section.
2) Answer to both the sections should be written in **SAME** Answer book.
3) Figures to the right indicate **FULL** marks.
4) Assume suitable data if necessary.

SECTION - I

Q.1 **a)** Enlist countermeasures of **DOS/DDOS** Attack. **[08]**

b) Explain following **Password Cracking Method**: **[08]**
i) Rainbow Tables **ii)** Salting.

Q.2 **a)** What is Scanning? Explain **Advanced Port Scanning** Techniques in detail. **[08]**

b) Explain **Null Session** Method used for Enumeration. State any two tool used for Enumeration. **[08]**

Q.3 **a)** What is Active and Passive sniffing? Explain **Arp-Poisoining**. **[08]**

b) Explain **Wireless Hacking** Techniques in detail. Write down the methods used to secure wireless network. **[08]**

Q.4 Write short notes on **ANY THREE** of the following **[18]**
a) Smurf and Teardrop
b) Ping Sweep Techniques
c) Phases of Hacking
d) Side Jacking

SECTION - II

Q.5 **a)** Explain types of SQL Injection. How does an attacker compromise your SQL Server? **[08]**

b) **i)** Explain the working of an **IDS**? **[08]**
ii) Enlist **Firewall Evasion** Techniques.

Q.6 **a)** Why to conduct a **Penetration Test**? Explain Penetration Testing Techniques. **[08]**

b) Explain the purpose and working of **Proxy Server** in detail. **[08]**

Q.7 **a)** How does computer get infected with a **Rootkit**? Explain the ways to manually detect and remove the Rootkit. **[08]**

b) Explain **Web Application** Threats in detail. **[08]**

Q.8 Write short notes on **ANY THREE** of the following **[18]**
a) Stack-Based Buffer Overflows
b) Mobile - Based Attack
c) Vulnerability Assessment Vs. Security Audit
d) URL Obfuscation

* * * *