Reg.No. _____

Karunya UNIVERSITY

(Karunya Institute of Technology & Sciences)
(Declared as Deemed-to-be University under Sec.3 of the UGC Act, 1956)

End Semester Examination – Nov/Dec – 2016

Code : 15CS3001 | **Semester : 2016-17 ODD**
Sub. Name : Ethical hacking | **Duration : 3hrs** | **Max. marks : 100**

ANSWER ALL QUESTIONS (5 x 20 = 100 Marks)

Q. No.	Sub Div.	Questions	Course Outcome	Marks
1.	a.	Discuss all the six step-by-step guide about the internet foot printing techniques to gather the information of an organization. (i) People search in search engine and social networking websites.	CO1	20
		(OR)		
2.	a.	(i) Read the following scenario : An email with a link that looked like it was coming from a colleague contained the malicious code, which spread from there like a digital rhinovirus. The hackers recorded everything that happened on the affected computers to learn how the organization did things. When they had mastered the system, they commandeered it for a series of transactions that included the ATM hits, but also a practice of artificially inflating bank balances and then siphoning off that amount, so a customer's account balance might go from $1,000 to $10,000 and then $9,000 would go to the hacker. Explain the social engineering attack based on a. Humansocial engineering attack b. Computersocial engineering attack	CO1	20
3.	a.	Discuss the enumeration process : (i) Service fingerprinting (ii) Vulnerability scanners (iii) Basic banner grabbing	CO1	20
		(OR)		
4.	a.	Examine the hosts which are known for Trojan horses, distributed denial-of-service (DDoS) tools, or other malicious services running on a host to determine whether system is alive or not using the following NMAP tools: (i)ARP Host discovery (ii)ICMP host discovery (iii)TCP/UDP host discovery	CO1	20
5.	a.	(i) Read the following scenario : Bay Pointe Security Consulting (BPSC) provides security consulting services toa wide range of businesses, individuals, schools, and organizations. BPSC hashired you as a technology student to help them with a new project and providereal-world experience to students who are interested in the security field. Pomodoro Fresco is a regional Italian pizza chain that provides free open wireless access to its customers and secure wireless access for its staff. However, Pomodoro Fresco was using WPA for securing its staff network but wasusing a short and weak password, and an attacker accessed the WLAN. Thecompany now wants to install a much more secure wireless network, andthey have asked BPSC to make a presentation about their options.	CO2	20

		(i) Create a PowerPoint presentation for the staff about the threats againstWLANs and the weaknesses of the IEEE 802.11 security protocols. Alsoinclude information about the more secure WPA2. Your presentation should contain at least 10 slides.		
		(OR)		
6.	a.	Read the following scenario and discuss the procedure how the password tampered using Hiren's CD Boot able USB: In 2008, a noteworthy insider attack occurred when Terry Childs, a network engineer for the San Francisco Department of Telecommunications and Information Services, altered the city's network passwords, locking Fiber WAN access for 12 days. Childs was found guilty of felony network tampering. The work required to regain system control cost the city of San Francisco $900,000, and 60 percent of city services were affected by the insider attack.	CO2	**15**
	b.	Elaborate the importance of simulating Insider attack.	CO2	**5**
7.	a.	Expalin the hacking procedure of vulnerability of an "Word-Press" database using google hacking's exploit-DB. (i) File containing the usernames and passwords (ii) Vulnerable servers and files.	CO3	**20**
		(OR)		
8.	a.	(i) Read the following : The City of San Francisco contains approximately 23,000 "smart" electronic parking meters manufactured by MacKay Meters that boast tamper resistance, payment via smartcard, and usage auditing capabilities. Jonny, in collaboration with Jacob Appelbaum and Chris Tarnovsky, evaluated San Francisco's electronic parking meter implementation, which was installed at a cost of $35 million, and successfully compromised the meter via its smartcard interface. One feature of San Francisco's implementation is supporting the use of a stored value smartcard. These non-refillable, disposable cards can be purchased online or at selected locations within San Francisco in $20 and $50 values. When the card is inserted into the meter, the meter first calculates the remaining value on the card and then, every few seconds, deducts a "unit," corresponding to $0.25. When the meter displays the desired amount of time, the user removes the smartcard. While there were many avenues available for attacking the smart parking meter, effort was focused on the easily accessible, external smartcard interface. An unpopulated "shim" placed between the smartcard and parking meter was used to break out the requisite signals and the communication was then captured using an Agilent DSO7054A digital storage oscilloscope. After determining the communication settings (half-duplex, asynchronous serial protocol at 9600bps, 8 bit, even parity, 1 stop bit), the serial decoding function of the DSO was used to display the actual data bytes being transmitted from the meter to the card and received by the meter from the card. (i)Analyze the reverse engineering of the entire conversation of a card communicating with the meter to deposit "coins" using a custom designed Microchip PIC16F877-based smartcard emulator.	CO3	
		Compulsory:		
9.	a.	Discuss the Jailbreaking process of the ios devices by installing the jailbreak app from jailbreakme.com in iPhone,ipad,ipod . show the options as (i) User (ii) Hacker (iii) Developer	CO3	**20**

ALL THE BEST