CMR INSTITUTE OF TECHNOLOGY

USN | | | | | | | | | | |

Internal Assessment Test 2 – May 2017

Sub:	Cyber Crime and Digital Forensics					Code:	14SCN424
Date:	13/05/2017	Duration:	90 mins	Max :	50	Sem: IV	Branch: M.Tech(CNE)

NOTE: Answer any five full questions. Total marks: 50

		Marks	OBE	
			CO	RBT
1.	a) What are the different phases of attack on network? b) Explain the importance of proxy server and an anonymizer.	[6] [4]	CO4 CO4	L1 L2
2.	Explain the different types of DOS/DDOS attacks.	[10]	CO4	L2
3.	What is phishing? What are the different techniques used by phishers to launch Phishing attacks?	[10]	CO5	L1,L2
4.	Explain how the "chain of custody" concept applies in computer/digital forensic with a suitable example.	[10]	CO6	L2
5.	Explain how an Email can be traced for forensic purpose. Outline the various key steps involved.	[10]	CO6	L2
6.	Explain the importance of reports. Describe guidelines for writing reports. Explain the structure of report.	[10]	CO6	L2
7.	What are the guidelines for giving testimony as a technical/scientific or expert witness? Describe guidelines for testifying in court.	[10]	CO6	L1
8.	Explain how ethics and codes apply to expert witnesses.	[10]	CO6	L2

Scheme & Solution

Internal Assessment Test 2 – May 2017

Sub:	Cyber Crime and Digital Forensics					**Code:**	**14SCN424**
Date:	13/05/2017	Duration: 90 mins	Max Marks: 50	**Sem:**	IV	**Branch:**	M.Tech(CNE)

Total marks: 50

1a) a) What are the different phases of attack on network?

1. **Initial covering:** two stages
    1. Reconnaissance- social networking websites
    2. Uncovers information on company's IP
2. **Network probe:**
    1. Ping sweep- seek out potential targets
    2. Port scanning
3. **Crossing the line toward electronic crime:**
    1. Commits computer crime by exploiting possible holes on the target system

4**. Capturing the network:**
- attackers attempts to own the network
- uses tools to remove any evidence of the attack
- trojan horses, backdoors

5 **. Grab the data:**
- attacker has captured the network
- steal confidential data, customer CC information, deface webpages…

6. Covering the attack:
- extend misuse of the attack without being detected.
- start a fresh reconnaissance to a related target system
- continue use of resources
- remove evidence of hacking---------- 1*6 = 6

b) b) Explain the importance of proxy server and an anonymizer.

- A **proxy server** is a dedicated computer or a software system running on a computer that acts as an intermediary between an endpoint device, such as a computer, and another **server** from which a user or client is requesting a service.

Purposes:

- **Improve Performance:**
- **Filter Requests**
- **Keep system behind the curtain**
- **Used as IP address multiplexer**
- **Its Cache memory can serve all users**

---------- **2 Marks**

- An **anonymizer** or an **anonymous proxy** is a tool that attempts to make activity on the Internet untraceable.
- It is a proxy server computer that acts as an intermediary and privacy shield between a client computer and the rest of the Internet.
- It accesses the Internet on the user's behalf, protecting personal information by hiding the client computer's identifying information.
- For example, large news outlets such as CNN target the viewers according to region and give different information to different populations

---------- **2 Marks**

2.	Explain the different types of DOS/DDOS attacks. **Explain each of the following attacks:** • **Flood attack** • **Ping of death attack** • **SYN attack** • **Teardrop attack** • **Smurf attack** • **nuke - 10 Marks**
3.	What is phishing? What are the different techniques used by phishers to launch Phishing attacks? **Phishing** is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication. --- **1 Mark** Techniques: URL Manipulation, website forgery, Filter evasion, Flash attack, Social attack, Mobile attack Explain each of these techniques – **9 Marks**
4.	Explain how the "chain of custody" concept applies in computer/digital forensic with a suitable example. The route evidence takes from the time the investigator obtains it until the case is closed or goes to court. **Chain of custody** (CoC), in legal contexts, refers to the chronological documentation or paper trail, showing the papertrail, custody, control, transfer, analysis, and disposition of physical or electronic evidence. When evidence can be used in court to convict persons of crimes, it must be handled in a scrupulously careful manner to prevent tampering or contamination. Establishing chain of custody is made of both a chronological and logical procedure, especially important when the evidence consists of fungible goods. An identifiable person must always have the physical custody of a piece of evidence. In practice, this means that a police officer or detective will take charge of a piece of evidence, document its collection, and hand it over to an evidence clerk for storage in a secure place. Maintaining a chain of custody is essential for the forensic scientist that is working on a specific criminal case. The documentation of evidence is key for maintaining a chain of custody because everything that is done to the piece of evidence must be listed and whoever came in contact with that piece of evidence is accountable for what happens to it. This prevents police officers and other law officials from contaminating the evidence or taking the piece of evidence. ---------- **7 Marks** An example of *chain of custody* would be the recovery of a bloody knife at a murder scene: 1. Officer Andrew collects the knife and places it into a container, then gives it to forensics technician Bill. 2. Forensics technician Bill takes the knife to the lab and collects fingerprints and other evidence from the knife. Bill then gives the knife and all evidence gathered from the knife to evidence clerk Charlene. 3. Charlene then stores the evidence until it is needed, documenting everyone who has accessed the original evidence (the knife, and original copies of the lifted fingerprints). The chain of custody requires that from the moment the evidence is collected, every transfer of evidence from person to person be documented *and* that it be provable that nobody else could

	have accessed that evidence. It is best to keep the number of transfers as low as possible. ---------- **3 Marks**
5.	Explain how an Email can be traced for forensic purpose. Outline the various key steps involved. Explain each of these steps: Header Analysis Bait Tactics Server Investigation Network Device Investigation Software Embedded Identifiers Sender Mailer Fingerprints ---------- 8 Marks - List few E-MAIL FORENSIC TOOLS --------- 2 Marks
6.	Explain the importance of reports. Describe guidelines for writing reports. Explain the structure of report. Importance of reports: • Communicate the results of your investigation – Including expert opinion • Courts require expert witness to submit written reports • Written report must specify fees paid for the expert's services – And list all other civil or criminal cases in which the expert has testified • **Deposition banks** – Examples of expert witness' previous testimonies **(3 Marks)** Guidelines: • Hypothetical questions based on factual evidence – Less favored today – Guide and support your opinion – Can be abused and overly complex • Opinions based on knowledge and experience • Exclude from hypothetical questions – Facts that can change, cannot be used, or are not relevant to your opinion • As an expert witness, you may testify to an opinion, or conclusion, if four basic conditions are met: – Opinion, inferences, or conclusions depend on special knowledge or skills – Expert should qualify as a true expert – Expert must testify to a certain degree of certainty – Experts must describe facts on which their opinions are based, or they must testify to a hypothetical question **(5 marks)** • Structure – Abstract – Table of contents – Body of report – Conclusion – References – Glossary – Acknowledgements – Appendixes **(2 Marks)**

7.	What are the guidelines for giving testimony as a technical/scientific or expert witness? Describe guidelines for testifying in court.

Preparing for testimony

- Technical or scientific witness
  - Provides facts found in investigation
  - Does not offer conclusions
  - Prepares testimony
- Expert witness
  - Has opinions based on observations
  - Opinions make the witness an expert
  - Works for the attorney
- Confirm your findings with documentation
  - Corroborate them with other peers
  - Social networking and professional organizations will help to locate peers
- Check opposing experts
  - Internet
  - Deposition banks
  - Curriculum vitae, strengths, and weaknesses

Documenting and Preparing Evidence

- Document your steps
  - To prove them repeatable
- Preserve evidence and document it
- Do not use formal checklist
  - Do not include checklist in final report
  - Opposing attorneys can challenge them
- Collect evidence and document employed tools
- Maintain chain of custody
- Collect the right amount of information
  - Collect only what was asked for
- Note the date and time of your forensic workstation when starting your analysis
  - Check your clock with time.gov
- Keep only successful output
  - Do not keep previous runs

Search for keywords using well-defined parameters

Reviewing Your Role as a Consulting Expert or an Expert Witness- Include points on this

---------- **6 Marks**

Testifying in court

- Procedures during a trial
  - Your attorney presents you as a competent expert
  - Opposing attorney might attempt to discredit you
  - Your attorney leads you through the evidence
  - Opposing attorney cross-examines you
- Typical order of trial
  - Motion in limine (pretrial motion to exclude evidence)
  - Empaneling the jury
  - Opening statements
  - Plaintiff
  - Defendant
  - Rebuttal
  - Closing arguments
  - Jury instructions

---------- **4 Marks**

-

8.	Explain how ethics and codes apply to expert witnesses • **Ethics** – Rules you internalize and use to measure your performance • **Codes of professional conduct or responsibility** – Standards that others apply to you or that you are compelled to adhere to by external forces • Such as licensing bodies • People need ethics to help maintain their balance – And self-respect and the respect of their profession • Laws governing codes of professional conduct or responsibility – Define the lowest level of action or performance required to avoid liability • Expert witnesses should present unbiased, specialized, and technical evidence to a jury • Expert witnesses testify in more than 80% of trials – And in many trials, multiple expert witnesses testify • The most important laws applying to attorneys and witnesses are the rules of evidence • Experts are bound by their own personal ethics and the ethics of their professional organizations • In the United States, there's no state or national licensing body for computer forensics examiners ---------- 1*10= **10 Marks**