Reg.No: | | | | | | | | |

SNS College of Technology, Coimbatore-35.
(Autonomous)
B.E/B.Tech- Internal Assessment -II
Academic Year 2023-2024(ODD)
Fifth Semester
Computer Science and Engineering

A

19CSE304 - Cyber Security

Time: 1.5 Hours **Maximum Marks: 50**

Answer All Questions

	PART - A (5x 2 = 10 Marks)	**CO**	**Blooms**
1.	List few aspects of forensic analysis of email. Email messages Email addresses(sender and recipient) IP addresses Date and time User information Attachments Passwords logs (Cloud, server, and local computer)	CO2	Ana
2.	Label few Challenges in Computer Forensics. Data recovery Visibility into cloud system Network log big data Multi-jurisdiction data storage	CO2	Ana
3.	Outline the concept of Denial of Service Denial of service (DoS) is a type of cyber attack designed to disable, shut down or disrupt a network, website or service. Typically, a malware is used to interrupt or inhibit the normal flow of data into and out of a system to render the target useless or inaccessible for a certain period.	CO3	Und

4. Recall the concept of Phishing Attack. CO3 Und

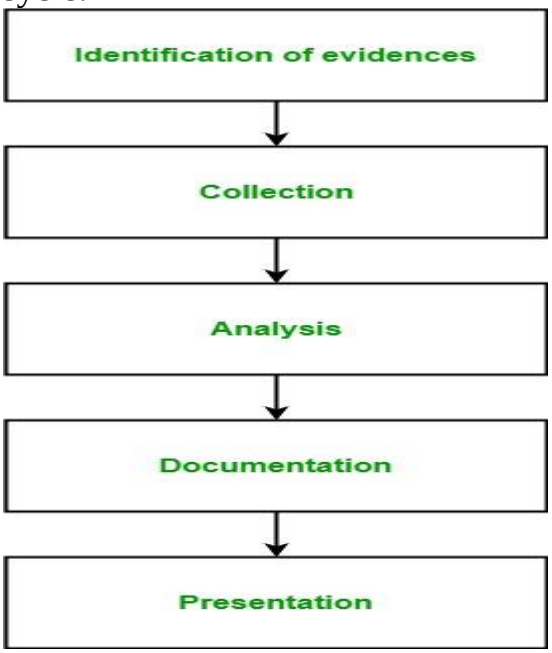
Phishing is one of the most common attack vectors in existence. Most cyberattacks begin with a phishing email that carries a malicious link or an attachment containing malware. On mobile devices, phishing attacks have a variety of media for delivering their links and malware, including email, SMS messaging, social media platforms, and other applications.

5. Define Ransomware Attack. CO3 Und

Ransomware is a malware designed to deny a user or organization access to files on their computer. By encrypting these files and demanding a ransom payment for the decryption key, cyber attackers place organizations in a position where paying the ransom is the easiest and cheapest way to regain access to their files.

PART–B (13+13+14 = 40 Marks)

6. (a) Elaborate in detail about the different phases of digital forensics lifecycle. 13 CO2 Und



1. Identification of evidence: It includes of identifying evidences related to the digital crime in storage media, hardware, operating system, network and/or applications. It is the most important and basic step.
2. Collection: It includes preserving the digital evidences identified in the first step so that they doesn't degrade to vanish with time. Preserving the digital evidences is very important and crucial.
3. Analysis: It includes analyzing the collected digital evidences of the committed computer crime in order to trace the criminal and possible path used to breach into the system.
4. Documentation: It includes the proper documentation of the whole digital investigation, digital evidences, loop holes of the attacked system etc. so that the case can be studied and analysed in future also and can be presented in the court in a proper format.

5. Presentation: It includes the presentation of all the digital evidences and documentation in the court in order to prove the digital crime committed and identify the criminal.

(or)

(b) Examine how the forensics investigation is carried out and explain the challenges faced in computer forensics. 13 CO2 Ana

A forensic investigation is a practice of lawfully establishing pieces of evidence that have to be presented in a court of law. It includes all investigations, ranging from cases of financial fraud to murder. When most people think about forensics, they think about crime scene investigation, in which physical evidence is gathered. There are other forms of forensic investigation, however, such as computer forensics and sub-fields that focus on dentistry or insects and crime scenes.

Crime scenes forensics

The type of forensic investigation revolves around crimes. Forensics used in these investigations can uncover scientific evidence that may provide enough proof or evidence to convict a criminal. These methods can also help disprove outdated evidence that could lead to the release of someone who was wrongly convicted.

One of the main kinds of evidence this form of forensic investigation yields is biological evidence. Impression evidence, like fingerprints, helps connect people to a crime scene or victim. After the evidence is carefully collected, it is sent for processing.

Computer forensics

A fast-growing division of forensics involves digital or computer investigations. It is a branch of science that involves evidence found in digital storage mediums and computers. This field of forensic investigation has several subdivisions.

Digital forensic investigation is useful in a variety of situations. Investigators use different programs and utilities to recover lost data after a system-wide computer crash. Careful handling and presentation of digital evidence are necessary for it to remain admissible in a courtroom setting.

Challenges with cyber forensics

Cyber forensics experts extract data from a variety of sources any technologies that may be used by an end-user. These include mobile devices, cloud computing services, IT networks and software applications.

These technologies are developed and operated by distinct vendors. The technology limitations and privacy measures tend to restrict investigative capacity of an individual InfoSec expert as they face the following challenges:

- Data recovery. If the data is encrypted, the investigator will not be able to decrypt the information without access to encryption keys. New storage tools such as SSD devices may not offer immediate factory access to recover lost data, unlike traditional magnetic tape and hard disk drive systems.

- Visibility into cloud system. Investigators may only have access to metadata but not the information content of the files. The underlying resources may be shared and allocated dynamically. That lack of access to physical storage systems means that lost data may not be recovered by third party investigators.

- Network log big data. Network log data grows exponentially and requires advanced analytics and AI tools to connect the dots and find insightful relationships between networking activities.

- Multi-jurisdiction data storage. If the data is stored in a different geographic location, cyber forensics investigators may not have the legal authority to access the required information.

7. (a) Determine the security challenges posed by mobile devices and discuss in detail about few attacks on mobile devices. 13 CO3 Ana

1. Application based threat:

The most of application are downloadable and purposed the most common risk for mobile users; most devices don't do much on their own, and it is the applications that make them so awesome and we all download apps. If it comes to apps the risks run from bugs and basic security risks on the low end of the scale all the way through malicious apps with no other purpose to commit cyber crime.

- Malware
- Spyware
- Privacy
- Zero Day Vulnerabilities

2. Web based threat:

According to the nature of mobile use, the fact that we have our devices with us everywhere we go and are connecting to the Internet while doing so, they face the number of unique web-based threats as well as the run-of-the-mill threats of general Internet use.

- Phishing Scams
- Social Engineering
- Drive By Downloads

- Operating System Flaws

3. Network-based threat:

Any mobile devices which typically support a minimum of three network capabilities making them three-times vulnerable to network-based attack. And a network often found on a mobile include cellular, WiFi and Bluetooth.

- Network exploits
- WiFi sniffing
- Cross-Platform Attacks
- BOYD

4. Physical Threats:

It is happened any time, unlikely a desktop sitting at your workstation, or even a laptop in your bag, a mobile device is subject to a number of everyday physical threats.

- Loss/Theft:

Loss or theft is the most unwanted physical threat to the security of your mobile device. Any devices itself has value and can be sold on the secondary market after all your information is stolen and sold.

Attacks

1.Malicious Apps and Websites

Like desktop computers, mobile devices have software and Internet access. Mobile malware (i.e. malicious applications) and malicious websites can accomplish the same objectives (stealing data, encrypting data, etc.) on mobile phones as on traditional computers.

Malicious apps come in a variety of different forms. The most common types of malicious mobile apps are trojans that also perform ad and click scams.

2. Mobile Ransomware

Mobile ransomware is a particular type of mobile malware, but the increased usage of mobile devices for business has made it a more common and damaging malware variant. Mobile ransomware encrypts files on a mobile device and then requires a ransom payment for the decryption key to restore access to the encrypted data.

3. Phishing

Phishing is one of the most common attack vectors in existence. Most cyberattacks begin with a phishing email that carries a

malicious link or an attachment containing malware. On mobile devices, phishing attacks have a variety of media for delivering their links and malware, including email, SMS messaging, social media platforms, and other applications.

In fact, while emails are what people most commonly think of when they hear phishing, they are not even close to the most commonly phishing vector on mobile devices. In fact, emails only account for 15% of mobile phishing attacks, placing them behind messaging, social media and "other" apps (not social, messaging, gaming, or productivity).

4. Man-in-the-Middle (MitM) Attacks

Man-in-the-Middle (MitM) attacks involve an attacker intercepting network communications to either eavesdrop on or modify the data being transmitted. While this type of attack may be possible on different systems, mobile devices are especially susceptible to MitM attacks. Unlike web traffic, which commonly uses encrypted HTTPS for communication, SMS messages can be easily intercepted, and mobile applications may use unencrypted HTTP for transfer of potentially sensitive information.

(or)

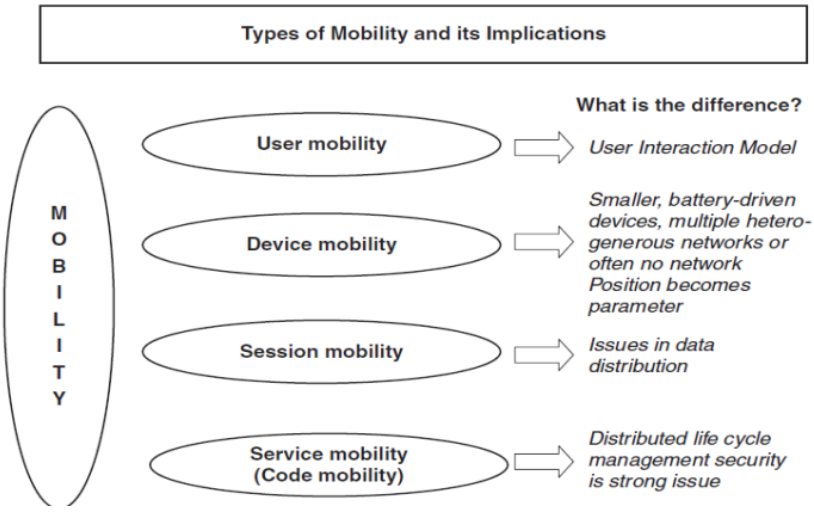
(b)	Discover the proliferation of mobile and wireless devices and discuss about the different aspects of trends in mobility.	13	CO3	Ana

Mobile computing is "taking a computer and all necessary files and software out into the
field." Many types of mobile computers have been introduced since 1990s.
They are as follows:
1. Portable computer: It is a general-purpose computer that can be easily moved from one place to another, but cannot be used while in transit, usually because it requires some
"setting-up" and an AC power source.
2. Tablet PC: It lacks a keyboard, is shaped like a slate or a paper notebook and has features of a touch screen with a stylus and handwriting recognition software. Tablets may not be best
suited for applications requiring a physical keyboard for typing, but are otherwise capable of carrying out most tasks that an ordinary laptop would be able to perform.
3. Internet tablet: It is the Internet appliance in tablet form. Unlike a Tablet PC, the Internet tablet does not have much computing power and its applications suite is limited. Also it
cannot replace a general-purpose computer. The Internet tablets typically feature an MP3 and video player, a Web browser, a chat

application and a picture viewer.
4. Personal digital assistant (PDA): It is a small, usually pocket-sized, computer with limited functionality. It is intended to supplement and synchronize with a desktop computer, giving access to contacts, address book, notes, E-Mail and other features.
5. Ultramobile PC: It is a full-featured, PDA-sized computer running a general-purpose operating system (OS).
6. Smartphone: It is a PDA with integrated cell phone functionality. Current Smartphones have a wide range of features and installable applications.
7. Carputer: It is a computing device installed in an automobile. It operates as a wireless computer, sound system, global positioning system (GPS) and DVD player. It also contains word processing software and is Bluetooth compatible.
8. Fly Fusion Pentop computer: It is a computing device with the size and shape of a pen. It functions as a writing utensil, MP3 player, language translator, digital storage device and calculator.

Trends in Mobility

 Mobile computing is moving into a new era, third generation (3G), which promises greater variety in applications and have highly improved usability as well as speedier networking.
"iPhone" from Apple and Google-led "Android" phones are the best examples of this trend and there are plenty of other developments that point in this direction.
 This smart mobile technology is rapidly gaining popularity and the attackers (hackers and crackers) are among its biggest fans.
 It is worth noting the trends in mobile computing; this will help readers to realize the seriousness of cybersecurity issues in the mobile computing domain.



8. (a) Analyze the different aspects of Forensics Analysis of Email and infer the steps involved in communication establishment in email. 14 CO2 Ana

Email forensics is dedicated to investigating, extracting, and analyzing emails to collect digital evidence as findings in order to crack crimes and certain incidents, in a forensically sound manner.

The process of email forensics, it's conducted across various aspects of emails, which mainly includes

- Email messages
- Email addresses(sender and recipient)
- IP addresses
- Date and time
- User information
- Attachments
- Passwords
- logs (Cloud, server, and local computer)

If you're still not familiar with the fields, check the below explanations:

- From: Address of the actual sender acting on behalf of the author listed in the From field
- To: The email address and, optionally, the name of the message's primary recipient(s)
- Cc: Carbon copy; a copy is sent to secondary recipients
- Bcc: Blind carbon copy; a copy is sent to addresses added to
- Subject: A brief summary of the topic of the message
- Date: A brief summary of the topic of the message
- (In)Reply-To: The message-ID of the message that this is a reply to; used to link related messages together
- Message-ID: An automatically generated field
- Content-Type: Information about how the message is to be displayed, usually a Multipurpose Internet Mail Extensions (MIME) type
- Precedence: —Commonly with values "bulk," "junk," or "list"; used to indicate that automated "vacation" or "out of office" responses should not be returned for this mail, for example, to prevent vacation notices from being sent to all other subscribers of a mailing list
- Received: Tracking information generated by mail servers that have previously handled a message, in reverse order (last handler first)
- References: Message-ID of the message to which this is a reply

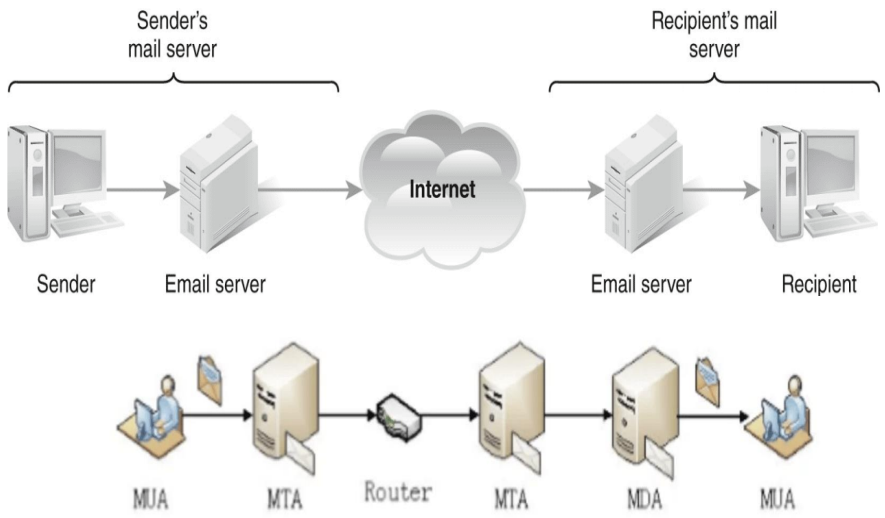


Figure 1: E-mail architecture
Source: Guo,Hong. Jin,Bo. Qian, Wei. 2013 [1]

(or)

(b) Consider the scenario of a victim affected by credit card fraud, with this discover the concept involved in credit card frauds and its techniques and recommend few tips to prevent from credit card frauds. 14 CO3 Ana

These are new trends in cybercrime that are coming up with mobile computing – mobile commerce (M- Commerce) and mobile banking (M-Banking).

 Credit card frauds are now becoming commonplace given the ever- increasing power and the ever-reducing prices of the mobile hand-held devices, factors that result in easy availability of these gadgets to almost anyone.

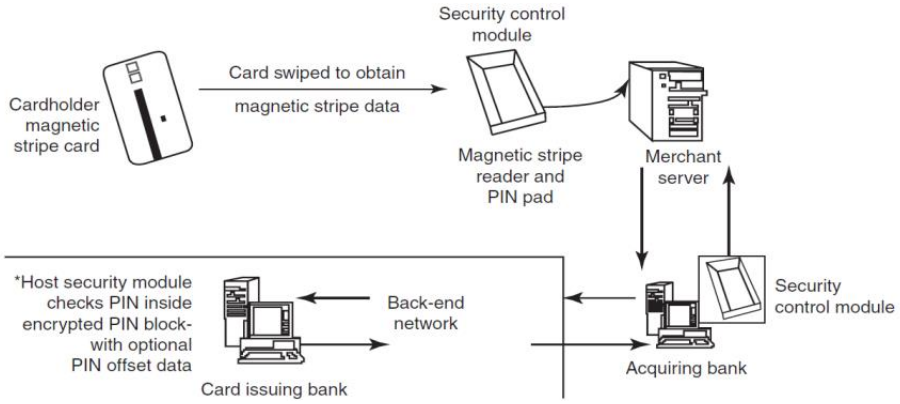
 Mobile credit card transactions are now very common; new technologies combine lowcost mobile phone technologies with the capabilities of a point-of-sale (POS) terminal.

 Today belongs to "mobile computing," that is, anywhere anytime computing.

 The developments in wireless technology have fuelled this new mode of working for white collar workers.

 Wireless credit card processing is a very desirable system, because it allows businesses to process transactions from mobile locations quickly, efficiently and professionally.

 It is most often used by businesses that operate mainly in a mobile environment.



Preventive Steps

1. Put your signature on the card immediately upon its receipt.
2. Make the photocopy of both the sides of your card and preserve it at a safe place to Remember the card number, expiration date in case of loss of card.
3. Change the default personal identification number (PIN) received from the bank before doing any transaction.
4. Always carry the details about contact numbers of your bank in case of loss of your card.
5. Carry your cards in a separate pouch/card holder than your wallet.
6. Keep an eye on your card during the transaction, and ensure to get it back immediately.
7. Preserve all the receipts to compare with credit card invoice.
8. Reconcile your monthly invoice/statement with your receipts.
9. Report immediately any discrepancy observed in the monthly invoice/statement.
10. Destroy all the receipts after reconciling it with the monthly invoice/statement.
11. Inform your bank in advance, about any change in your contact details such as home address, cell phone number and E-Mail address.
12. Ensure the legitimacy of the website before providing any of your card details.
13. Report the loss of the card immediately in your bank and at the police station, if necessary.

****

(Note: Und-Understand Rem-Remember Ana-Analyze App-Apply)

Prepared By Verified By HoD