National Forensics Sciences University, Goa Campus

TA-2/ Assignment No 2

M.Sc. Cyber Security- Semester -II

Branch – Cyber Security	**Sem – II**	**Submission Date- 03/06/2024**
Subject Name- Network Security & Forensic		**Subject Code- CTMSCS SII P1**
Max. Marks- 10		

Instructions - 1) Answer all questions. 2) Assume suitable data. 3) ONLY Handwritten Note.

Q.1	Attempt all.	**10** **MARKS**
	a. Drawing inspiration from the News International phone hacking scandal involving News of the World and other newspapers owned by Rupert Murdoch, consider a scenario where a newspaper owner notices unusual traffic patterns on their network during non-business hours. How would you investigate whether this is a sign of a security breach, and what steps would you take to prevent similar incidents in the future, leveraging principles of network security, cryptography, and network forensics?	
	b. Describe the ransomware attack that occurred at AIIMS (All India Institute of Medical Sciences) in New Delhi, using your own words. Additionally, elucidate the forensic process undertaken by the investigative team to analyze and understand the scope of the incident. As a security provider tasked with preventing future attacks of this nature, outline the proactive steps you would recommend to counter such threats. Provide a comprehensive list of technical solutions that could bolster AIIMS' cybersecurity defenses against ransomware attacks in the future.	
Q.2		
	a. Discuss the delicate balance between user privacy and the functionalities of social media platforms such as WhatsApp and Facebook, especially in light of recent social media cases in India. How do these platforms navigate concerns regarding privacy while providing valuable services to users? Provide examples of recent social media cases in India that have sparked discussions about privacy, and analyze the	

	implications for users and platform providers. Additionally, propose strategies for improving user privacy protections on social media platforms without compromising user experience and functionality.	
	b. Digital Signature Standard (DSS) plays a pivotal role in ensuring the authenticity, integrity, and non-repudiation of digital documents and transactions. In detail, elucidate the Digital Signature Standard, its components, and its cryptographic mechanisms. Furthermore, delve into the mathematical principles behind DSS, explaining how it generates and verifies digital signatures. Discuss the significance of DSS in modern digital communication and commerce, highlighting its applications and advantages. Finally, address any potential vulnerabilities or criticisms of DSS and propose potential enhancements or alternatives to address these concerns.	
	c.	
Q. 3		
	a. Explain in detail the concepts of MAC and HMAC, including their purpose, construction, and applications in ensuring message integrity and authentication. Compare and contrast MAC and HMAC in terms of their design, security properties, and suitability for different use cases. Provide examples of scenarios where MAC and HMAC are commonly employed, highlighting their effectiveness in protecting against message tampering and unauthorized access.	
	b. Using the Indian software industry as a context, explore the implementation and significance of Role-Based Access Control (RBAC) in network security. Define RBAC and elaborate on its principles, mechanisms, and benefits in regulating access to digital resources within software companies.	
	c.	

Q.4		
	a. Illustrate the vulnerability of the Wi-Fi infrastructure at NFSU (National Forensic Sciences University) in Goa to an Evil Twin attack. Describe in detail how an Evil Twin attack could be executed within the campus environment, taking into account the layout and configuration of the Wi-Fi network.	
	b. As a network security professional tasked with mitigating online banking fraud in India, how would you approach the challenge of combating cybercriminal tactics such as phishing emails, malware, and social engineering? Discuss specific strategies and technologies you would recommend implementing to strengthen the security posture of banking institutions and protect customers' sensitive financial information. Additionally, outline the role of proactive threat intelligence, employee training programs, and collaboration with law enforcement agencies in detecting and preventing online banking fraud incidents.	