Department of Computer Science

Gujarat University

Certificate

Roll No: 25 Seat No: _____

This is to certify that Mr./Ms. Shaikh Faizanahemad student of MCA Semester – V has duly completed his/her term work for the semester ending in December 2020, in the subject of Network Security (NS) towards partial fulfillment of his/her Degree of Masters in Computer Applications.

11-12-2020
Date of Submission

Internal Faculty

Head of Department

Department Of Computer Science
Rollwala Computer Centre
Gujarat University

MCA – 5

Subject: - Network Security – (NS)

Name: - Shaikh Faizanahemad

Roll No.: - 25 **Exam Seat No.: -**

Sr. No.	Contents	Pg. No	Date	Signature
1	Assignment 1	3-4	12-08-20	
2	Assignment 2	5-8	15-09-20	
3	Assignment 3	9-10	10-11-20	
4	Assignment 4	11-14	24-11-20	

ASSIGNMENT-1

Q1) List all symmetric key algorithms.

→ (1) AES (Advanced Encryption Standard)
(2) DES (Data Encryption Standard)
(3) IDEA (International Data Encryption Algo.)
(4) Blowfish (Drop-in replacement for DES or IDEA)
(5) Triple DES
(6) RC4 (Rivest Cipher 4)
(7) RC5 (Rivest Cipher 5)
(8) RC6 (Rivest cipher 6)

Q2) List all Asymmetric key algorithms.

→ (1) RSA (Rivest Shamir Adleman).
(2) Ed25519 Signing.
(3) DSA (Digital Signature Algorithm)
(4) Diffie-Hellmann key agreement
(5) Ecc (Elliptic Curve Cryptography)
(6) El Gamal
(7) X25519 key exchange
(8) Ed448 Signing.
(9) key Serializations.

Q3) List the algorithms for Message Digest.

→ (1) MD4 hash
(2) MD5 hash
(3) RIPEMD160 hash
(4) SHA-1 hash
(5) SHA-256 hash
(6) SHA-512 hash
(7) NTLM (NT LAN Manager)
(8) LANMAN (LAN Manager)

ASSIGNMENT-2

Q:) Discuss Briefly:-

(a) PII (Personally Identifiable Information):-

It defines "personally identifiable" as information like name, social security number, and biometric records which can be used to distinguish or trace an individual's identity.

(b) U.S. Privacy Act of 1974:-

The privacy Act of 1974, Public law 93-579, was created in response to concerns about how the creation & use of computerized databases might impact individuals privacy rights. It safeguards privacy through creating four procedural & substantive rights in personal data.

(c) FOIA:-

Freedom Of Information Act (FOIA) has established a gateway for Americans to access a wealth of data and knowledge maintained by govt. agencies about virtually everything. And through public-facing websites, citizens are generating FOIA requests at a dizzying pace - well more than 550,000 annually for the 15 US departments & agencies that receive 90% of all such requests.

(d) FERPA:-

It guarantees students access to their academic records while prohibiting unauthorized access by others. Computer systems maintaining student information applicable to FERPA must have computer security controls in place to protect the confidentiality & integrity of this information.

(e) CFAA

→ The Computer Fraud & Abuse Act (CFAA) - title 18 U.S.C, Statute 1030 - is a law designed to address legal & illegal access to federal & financial IT systems. It was intended to reduce cracking of computer systems & to address federal computer related offences.

(f) COPPA

→ The Children's Online Privacy Protection Act of 1998 is a US federal law, located at 15 USC. The act, effective April 21, 2000, applies to the online collection of personal information by persons or entities under US jurisdiction about children under 13 years of age. including children outside of US, if the company is US based.

(g) VPPA

→ The Video Privacy Protection Act of 1988, An act to amend title 18, US code, to preserve personal privacy with respect to the rental, purchase or delivery of video tapes or similar audio visual materials.

(h) HIPAA

→ The Health Insurance Portability and Accountability Act (HIPAA) sets the standard for sensitive patient data protection. Companies that deal with protected Health Information (PHI) must have physical, network & process security measures in place & follow them to ensure HIPAA Compliance.

(i) GLBA

→ The Financial Services Modernization Act, better known as the Gramm-Leach-Bliley Act (GLBA), requires that financial institutions ensures the security of customer data, Protect data against known or anticipated risks and secure data to protect it from unauthorized access.

(j) PCI DSS

→ The PCI DSS is an information security standard created to enhance cardholder data security for

organisations that store and process credit card data. To attend Compliances, organizations must pass an assessment that audits all parts of the network that interact with cardholder environment.

(k) FCRA:-

⇒ The Fair Credit Reporting Act (FCRA) adds provisions designed to improve the accuracy of consumers credit related records. The Act also requires the provisions of "risk-based-pricing" notices & credit scores to consumers in connection with denials or loss favourable offers of credit.

(l) FACTA

⇒ Fairs and Accurate Credit Transactions Act (FACTA) is an amendment to FCRA that was added primarily to protect consumers from identity theft. The Act stipulates requirements for Information Privacy, accuracy & disposal & limits the way consumer information can be shared.

ASSIGNMENT-3

Q) Stateful Usecase for :-

(1) RADIUS

→ Remote Authentication Dial-In User Service.

(2) TACACS

→ Terminal Access Controller Access Control System.

(3) L2TP & PPTP

→ Layer 2 Tunneling Protocol.
Point to Point Tunneling Protocol.

(4) PPP

→ Point-to-Point Protocol.

(5) EAP

→ Extensible Authentication Protocol

(6) CHAP

→ Challenge-Handshake Authentication Protocol

(7) NTLM

→ NT (New Technology) LAN Managers.

(8) PAP

→ Pulmonary Alveolar Proteinosis.

(9) SSH

→ Secure Shell

(10) LDAP

→ Lightweight Directory Access Protocol.

ASSIGNMENT-4

Q) List the name of softwares/s:-

(1) Firewall:-

- FortiGate
- CheckPoint Next Generation Firewalls (NGFWs)
- Sophos XG Firewall
- WatchGuard Network Security
- SonicWall
- Cisco
- ZoneAlarm
- Glasswire
- TinyWall

(2) Intrusion Detection & Prevention:-

- SolarWinds Security Event Manager
- CrowdStrike Falcon
- ManageEngine Eventlog Analyzer
- Snort
- OSSEC
- Suricata
- Zeek
- Sagan
- McAfee Network Security Platforms
- FireEye Network Security & Forensics

(3) Anti-Virus:-

- Bitdefender Antivirus
- Norton Antivirus
- kaspersky Antivirus
- Avira Antivirus
- Webroot Secure Anywhere Antivirus
- Avast Antivirus
- Sophos Antivirus
- ESET Antivirus
- AVG Antivirus

(4) Packet Sniffing:-

- Paessless PRTG Network Monitor
- ManageEngine Netflow Analyzer
- Savvius Omnipeek
- Wireshark
- Telerik Fiddler
- NETRESEC Network Miner
- Colasoft Capsa

Q2) State any 10 security softwares used by ethical hackers.

→ 1. Netspoofer
2. Acunetrix
3. Traceroute NG
4. Burp Suite
5. EtterCap
6. Aircrack
7. Angry IP Scanner
8. GFI LanGuard
9. Saavius
10. QualysGuard
11. WebInspect
12. Nashcat
13. LOphtCrack
14. Rainbow Crack
15. IKE Crack
16. IronWASP
17. Medusa
18. Net Stumbler
19. SQL Map
20. Cain & abel

Q3) What is the role of CERT?

→ CERT-In's primary role is to raise security awareness among Indian Cyber Community & to provide technical assistance & advise them to help them recover from computer security incidents. CERT-IN provides technical advice to System Administrator's and users to respond to computer security incidents.

Q4) List top 10 OWASP

→
- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfigurations
- Cross Site Scripting (XSS)
- Insecure Deserialization
- Using Components with known vulnerabilities
- Insufficient logging & monitoring