SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)

SRM Nagar, Kattankulathur – 603 203

DEPARTMENT OF

COMPUTER SCIENCE AND ENGINEERING

QUESTION BANK

II SEMESTER

1912202-SECURITY PRACTICES

Regulation – 2019

Academic Year 2019-2020 (Even Semester)

Prepared by

V.Prema AP/CSE

SRM VALLIAMMAI ENGINEERING COLLEGE

SRM Nagar, Kattankulathur – 603 203.

DEPARTMENT OF INFORMATION TECHNOLOGY

QUESTION BANK

SUBJECT : CP5291 - Security Practices

SEM / YEAR: II Sem / I Year

UNIT I - System Security			
Building a secure organization- A Cryptography prime – Detecting system intrusion- Preventing system intrusion –Fault tolerance and resilience in cloud computing environments – security web applications, services and servers.			
PART – A			
Q. No	**Questions**	**BT Level**	**Competence**
1	**Illustrate** the evolutionary trend towards building a secure organization?	BTL 3	Applying
2	**List and explain** in brief about security types?	BTL 1	Remembering
3	**Describe** the applications of high performance and high throughput systems?	BTL 1	Remembering
4	**Define** cryptography and encryption.	BTL 1	Remembering
5	**Analyze** the working parts of cryptography.	BTL 4	Analyzing
6	**Give** the basic operations when risk and threats are identified.	BTL 3	Applying
7	**List** out various cipher techniques.	BTL 1	Remembering
8	**Differentiate** modern and earlier type cryptography.	BTL 4	Analyzing
9	**Examine** the weaknesses of one time pad?	BTL 3	Applying
10	**Explain** zero day attack?	BTL 2	Understanding
11	**Differentiate** between hackers and crackers	BTL 2	Understanding
12	**Formulate** the features of vulnerability management phases.	BTL 6	Creating
13	**Summarize** the technologies of BOTS and its types.	BTL 5	Evaluating

14	**Highlight** the importance of risk analysis"	BTL 2	Understanding
15	**How** faults are classified?	BTL 1	Remembering
16	**Tabulate the different types of firewalls.**	BTL 4	Analyzing
17	**List the various intrusion monitoring**	BTL 1	Remembering
18	**Bring Antivirus and Antispyware Tools**	BTL 2	Understanding
19	**Summarize Signature -Based deduction**	BTL 5	Evaluating
20	**Generalize Network Access Control.**	BTL 6	Creating
	PART-B		
1	i)**Identify** and explain in detail about ten steps to build a secure Organization. (6) ii)**Explain** the types of cipher in detail (7)	BTL 1	Remembering
2	i)Explain DES in detail with an example (6) ii) Explain AES in detail with an example (7)	BTL 2	Understanding
3	i)Write about the security objectives in detecting system intrusions (7) ii)Explain Zero-day attack and Good known state in detail (6)	BTL 3	Applying
4	List the types of Rootkit in detail. (13)	BTL 1	Remembering
5	**Analyze** in Full-packet capture devices in detail (13)	BTL 4	Analyzing
6	**Explain** data correlation with an example (13)	BTL 5	Evaluating
7	**Generalize** the ideas of i) SIEM. (7) ii) How the system is prevented from intrusion (6)	BTL 6	Creating
8	Explain the tools for preventing system intrusions (13)	BTL 2	Understanding
9	i)**Explain** user access is controlled within the network? (6) **ii)** Describe cloud computing fault model (7)	BTL 4	Analyzing
10	**i)Demonstrate** in detail about **fault tolerance** (7) ii)**Illustrate** in detail about cloud computing (6)	BTL 1	Remembering
11	**Describe Network Access control** (13)	BTL 1	Remembering

12	**Illustrate** Reactive Measures with example(13)	BTL 3	Applying
13	**Brief** the Spam filtering with an example (13)	BTL 4	Analyzing
14	**i)Describe** Authorization patterns (6) **ii)Describe** the architecture about the security considerations for avoiding common errors. (7)	BTL 2	Understanding
	PART-C		
1	**Evaluate** the strategic to follow in the implementation of the Following i) Intrusion detection system (7) ii) prevention of IDS (8)	BTL 5	Evaluating
2	**Create** and **justify** Vulnerability Testing and Patching**?** (15)	BTL 6	Creating
3	**Explain** the Defense in Depth with an example. .(15)	BTL 5	Evaluating
4	**Elaborate** the features of following in the computing system design. i) Traffic Monitoring (8) ii) Behavior Anomalies (7)	BTL 6	Creating

UNIT II - Network Security

Internet Security- Botnet Problem – Internet Security – Local area network security- wireless network security –wireless sensor network security- cellular network security

PART – A

Q. No	Questions	BT Level	Competence
1	**Define** internet security.	BTL 1	Remembering
2	**Illustrate** the various primitives of communication service interface.	BTL 3	Applying
3	**List** the major goals of internet protocol architecture.	BTL 1	Remembering
4	**Summarize** the layers of communication module.	BTL 2	Understanding
5	**Classify** the MAC layer.	BTL 3	Applying
6	**Formulate** physical and virtual link.	BTL 6	Creating

7	**Compare** MAC with internet protocol.	BTL 5	Evaluating
8	**Analyze** the MAC layers.	BTL 4	Analyzing
9	**What** is the purpose of best effort MAC?	BTL 2	Understanding
10	**List** the requirements of router in network layer.	BTL 1	Remembering
11	**Differentiate** parallel data transfer versus striped data transfer.	BTL 2	Understanding
12	**What** do you understand by forward function supported in network layer.	BTL 2	Understanding
13	**Define** Address resolution protocol	BTL 1	Remembering
14	**Point** out the trouble shooting tool in internet.	BTL 4	Analyzing
15	**Deduce** the threat at each component of internet exposes to internet protocol Suite	BTL 5	Evaluating
16	**Define** Black hole attack.	BTL 1	Remembering
17	**Name** the concepts involved in defending against eaves dropping	BTL 1	Remembering
18	**Illustrate** the independence of keys.	BTL 3	Applying
19	**Analyze** the Botnet attack	BTL 4	Analyzing
20	**Formulate** the network security threats.	BTL 6	Creating
	PART-B		
1	**With** a neat sketch, discuss the Internet protocol architecture (13)	BTL 1	Remembering
2	**Write** a detailed note on MAC layers. (13)	BTL 2	Understanding
3	**Explain** the Internet Control Message Protocol. (13)	BTL 3	Applying
4	i) **Analyze** the Threat layers(6) ii) **Explain** the services of message deletion attack. (7)	BTL 4	Analyzing
5	**Describe** in detail about the defending against eaves dropping attack(13)	BTL 1	Remembering
6	i) **Examine** the Independence of keys. (6) ii) **Demonstrate** in detail about internet security checklist. (7)	BTL 3	Applying

7	i) **Discriminate** how the MAC and internet protocol works. (6) ii) **Explain** Botnet life cycle (7)	BTL 5	Evaluating
8	**Explain** how botnet attacks are prevented. (13)	BTL 6	Creating
9	**Describe** in detail about internet security.(13)	BTL 1	Remembering
10	**What** are security considerations explain in detail .(13)	BTL 4	Analyzing
11	i) **Tabulate** the Local area network security (7) ii) **Examine** the Network threat category in detail. (6)	BTL 1	Remembering
12	**Express** in detail about the Security Implications of Internet Connectivity (13)	BTL 2	Understanding
13	**What** is Firewalls? **Explain** in detail about different types of firewall **.**(13)	BTL 4	Analyzing
14	**Discuss** in detail about the Cellular network security. (13)	BTL 2	Understanding
	PART-C		
1	**Discuss** in detail about the motivation in wireless network security. (15)	BTL 6	Creating
2	i) **Evaluate** the Taxonomy of attacks for cellular network attack. (8) ii) **Discuss** the difference between wireless and wireless sensor network security.(7)	BTL 5	Evaluating
3	**Formulate** the requirement of Security in WSN using a Layered Approach (15)	BTL 6	Creating
4	**Evaluate** the features of Routing Classifications in WSN.(15)	BTL5	Evaluating

UNIT III – Security Management
Information security essentials for IT MANAGERS – Security management system- Policy driven system management- IT Security – Online identity and user management system- Intrusion and detection and prevention system.

PART – A

Q. No	Questions	BT Level	Competence
1	**Define** security, threat and vulnerability.	BTL 1	Remembering
2	**Distinguish** between physical security and data security.	BTL 2	Understanding
3	**Mention** Risk analysis.	BTL 1	Remembering
4	**Define** IaaS.	BTL 1	Remembering
5	**Summarize** the steps required for host based security.	BTL 6	Creating
6	**Show** the levels of security controls.	BTL 3	Applying
7	**List** the requirements of information technology security aspects?	BTL 2	Understanding
8	**Why** do we need a XRI/XDI?	BTL 4	Analyzing
9	**How** does the SMS based OTP works?	BTL 5	Evaluating
10	**Compare** insider with outsider threat.	BTL 4	Analyzing
11	**Demonstrate** the abuse of privilege.	BTL 3	Applying
12	**Discuss** the design issues of openID protocol stack.	BTL 2	Understanding
13	**List** the forms of malware.	BTL 1	Remembering
14	**Give** the The Rogue's Gallery attack and motivation.	BTL 1	Remembering
15	**Describe** the Role Of The '0-Day.	BTL 2	Understanding
16	**How** the Anti malware software works?	BTL 3	Applying
17	**Formulate** the features of TCP/IP.	BTL 6	Creating
18	**Where** digital forensics are used ?	BTL 1	Remembering
19	**Discuss** the model of NIDS.	BTL 5	Evaluating
20	Why do we need system integrity validation .	BTL 4	Analyzing
PART-B			
1	**List** the deployment models and give a detailed note about Information security.(13)	BTL 1	Remembering

2	**Analyze** the uses of i) Mission critical systems. (4) ii) Risk analysis. (4) iii) Contingency planning. (5)	BTL 4	Analyzing
3	**Describe** service and deployment models of a security monitoring mechanisms with illustrations.?(13)	BTL 2	Understanding
4	i) **List** the advantages and disadvantages of security policies. (6) ii) **Identify** the support of security control. (7)	BTL 1	Remembering
5	i) **Summarize** the support of policy driven system management(6) ii) **Describe** the security based objective relate to CIA. (7)	BTL 2	Understanding
6	**Give** the importance of Information Technology security aspects(13)	BTL 6	Creating
7	i) **Illustrate** in detail about the security organization techniques. (6) ii) **Examine** in detail IT security processess(7)	BTL 3	Applying
8	i) **Point** out the importance of online identity and user management systems.(6) ii) **Explain** in detail about the principles to maintain privacy and security. (7)	BTL 4	Analyzing
9	**What** is Identity management? **Describe** the identity silo model**.**(13)	BTL 1	Remembering
10	i) **Differentiate** Centralized vs. Federation Identity Management. (7) ii) **Discuss** Single-Sign-On (SSO) in detail. (6)	BTL 2	Understanding
11	**Illustrate** the openID protocol stack in detail. (13)	BTL 3	Applying
12	i) **Explain** the SMS Based One-Time Password (OTP). (6) ii) **Analyze** the various types of Malware infection in detail. (7)	BTL 4	Analyzing
13	Explain in detail about TCP/IP Data Architecture And Data Encapsulation. (13)	BTL 5	Evaluating
14	**What** do you mean by host based intrusion detection system.(13)	BTL 1	Remembering
	PART-C		
1	**Compare** how the security management system is designed to provide security. (15)	BTL 5	Evaluating

2	**Discuss** the need of security management system.(15)	BTL 6	Creating
3	**Evaluate** and contrast the merits and demerit of online identity and user management systems.(15)	BTL 5	Evaluating
4	**Test** the significant benefit of using the following service in application design i) Intrusion detection. (5) ii) Prevention mechanism. (5) iii) IT srcurity. (5)	BTL 6	Creating

UNIT-IV Cyber security and cryptography

Cyber forensics- Cyber Forensics and incidence response – security e- Discovery- Network Forensics – Data Encryption-Satellite Encryption -Password based authenticated Key establishment Protocols.

PART-A

Q. No	Questions	BT Level	Competence
1	**Analyze** on grid software support and middleware packages.	BTL 4	Analyzing
2	**Define** RAID.	BTL 1	Remembering
3	**Examine** how the data are analyzed.	BTL 3	Applying
4	**Summarize** how information is stored in FAT.	BTL 2	Understanding
5	**List** the types of evidence.	BTL 1	Remembering
6	**Write** the significant of file carving.	BTL 6	Creating
7	**Define** CSIRT AND CERT.	BTL 1	Remembering
8	**Analyze** the password hacking.	BTL 4	Analyzing
9	**Illustrate** the building blocks of Incident life cycle.	BTL 3	Applying
10	**Name** any four services offered in Forensic analysis team.	BTL 1	Remembering
11	Justify how a network forensic is useful in data analysis.	BTL 5	Evaluating
12	**Differentiate** MFT with ADS.	BTL 2	Understanding

13	**What** are Data retention policies?	BTL 2	Understanding
14	**Name** the different types of attacks.	BTL 6	Creating
15	**Analyze** how a IP traceback is categorized.	BTL 4	Analyzing
16	**Define** Euclidean Algorithm.	BTL 1	Remembering
17	**Generalize** as to how as Online Fraudster Detection is done.	BTL 6	Creating
18	**What is password based authenticated key**	BTL 2	Understanding
19	**Name** the Need For Satellite Encryption.	BTL 1	Remembering
20	**Demonstrate** establishment protocols	BTL 3	Applying
	PART-B		
1	**Describe** the relative strength and limitation of Cyber Forensics In The Court System.(13)	BTL 1	Remembering
2	i) **List** the features in Hacking A Windows Xp Password (7) ii) **Describe** User Artifact Analysis in detail. (6)	BTL 1	Remembering
3	i) **Summarize** the Network Analysis. (6) ii) **Discuss** on Cyber Forensics and Incident Response. (7)	BTL 2	Understanding
4	**Draw** and **explain** the Identifying the Incident Life Cycle (13)	BTL 3	Applying
5	i) **Explain** the concepts involved in Scrutinizing Email. (7) ii) **Classify** the Securing e-Discovery. (6)	BTL 4	Analyzing
6	**Evaluate** the Information Management with Legal And Regulatory Obligation (13)	BTL 5	Evaluating
7	i) **Generalize** the functional components of Network Forensics. (6) ii) **Design** the functional building blocks in Online Fraudster Detection and Attribution. (7)	BTL 6	Creating
8	**What** is Data encryption? **Describe** in detail about the need for cryptography with a suitable diagram**.**	BTL 1	Remembering
9	**Discuss** classical cryptography with modern cryptography with suitable diagrams.(13)	BTL 2	Understanding
10	i) **Classify** the various ways in Substitution Cipher.(6) ii) **Show** how will you have the use of Modern Block Ciphers.(7)	BTL 3	Applying
11	**Illustrate** dataflow in Satellite Encryptionduring file read/write operation with suitable diagrams.(13)	BTL 4	Analyzing
12	**Examine** the basic Implementation of Satellite Encryption. (13)	BTL 1	Remembering

13	**Discuss** in detail about Pirate Decryption Of Satellite Transmissions. (13)	BTL 2	Understanding
14	**Give** a detailed note on Password based authenticated Key establishment Protocols. (13)	BTL 4	Analyzing
	PART-C		
1	**Evaluate** the Cyber Forensics and Incidence Response with suitable illustrations. (15)	BTL 5	Evaluating
2	**Formulate** the significant use of Security e-Discovery of i) Network Forensics. (8) ii) **Propose** the feature of Data encryption in detail. (7)	BTL 6	Creating
3	**Choose** and architect an application system by using Satellite encryption, List its benefit. (15)	BTL 5	Creating
4	**Construct** the Design of Password based authenticated Key establishment Protocols application with neat sketch. (15)	BTL 6	Creating

UNIT V – Privacy and Storage Security

Privacy on the internet – Privacy enhancing technologies –Personal privacy polices- Detection of conflicts in security policies- Privacy and security in environment monitoring systems. Storage Area network security –storage area network security devices- risk management- physical security essentials.

PART-A

Q. No	Questions	BT Level	Competence
1	**Give** the challenges in building the Privacy on the Internet?	BTL 2	Understanding
2	**Define** privacy threats.	BTL 1	Remembering
3	**Summarize** on access control models.	BTL 2	Understanding
4	**List** the steps to accomplish privacy policies.	BTL 1	Remembering
5	**Relate** how privacy protection could be exploited by adversaries.	BTL 3	Applying
6	**Evaluate** the Onion Routing and TOR.	BTL 5	Evaluating
7	**Define** PETs	BTL 1	Remembering
8	**Formulate** the categories of PETs.	BTL 6	Creating
9	**Identify** the Data Minimization Technologies.	BTL 2	Understanding

10	**Differentiate** Mix nets with AN.ON	BTL 4	Analyzing
11	**Write** a brief note on flow of eCash's untraceable electronic money .	BTL 6	Creating
12	**Mention** the importance of Privacy Management Model.	BTL 5	Evaluating
13	**Illustrate** the sequence Conflicts in Security Policies.	BTL 3	Applying
14	**Discuss** the Conflicts In Network Security Policies.	BTL 2	Understanding
15	**Tabulate** the security levels at the network level.	BTL 1	Remembering
16	**Compare** Advantages of Tor over AN.ON.	BTL 4	Analyzing
17	**Show** how you will categorize security risk with privacy risks.	BTL 3	Applying
18	**Discuss** on the application and use of FCAP and FCPAP.	BTL 1	Remembering
19	**List** any four Best Practices for Disaster Recovery	BTL 1	Remembering
20	**Point** out Risk Management Methods.	BTL 4	Analyzing
	PART-B		
1	**Examine** in detail about privacy threats and privacy in the internet.(13)	BTL 3	Applying
2	i) **Define** privacy and explain in detail about Privacy in Mobile Environments.(6) ii) **Discuss** in detail about Data Minimization at Application Level.(7)	BTL 1	Remembering
3	**Explain** Personal Privacy Policies in detail . (13)	BTL 1	Remembering
4	i) **Demonstrate the** Detection of Conflicts in Security Policies.(6) ii) **Classify** the issues in Conflicts In Executable Security Policies.(7)	BTL 3	Applying
5	i) **Analyze** the Conflicts in network Security Policies.(7) ii) **Explain** about Semantic Web Technology for Conflict Detection.(6)	BTL 4	Analyzing
6	**Describe** in detail about the functional architecture of Security And Privacy Issues In Environmental Monitoring.(13)	BTL 4	Analyzing
7	i) **Compose** in detail about Storage Area Network Security.(6) ii) **Generalize** on data security and password policies.(7)	BTL 6	Creating
8	**Evaluate** the concepts involved in Data protection.(13)	BTL 5	Evaluating
9	i) **Express** in detail about the need of SAN.(6) ii) **Give** the challenges in SAN.(7)	BTL 2	Understanding
10	i) **Summarize** on the basic concepts of SAN General Threats And Issues.(6) ii) **Evaluate** and explain the practices of Logical level threats.(7)	BTL 2	Understanding

11	**Describe** in detail about the Risk management Standards and Risk Management methodology.(13)	BTL 1	Remembering
12	i) **Analyze** in detail about Integrating Risk Management into the System Development Life Cycle.(6) ii) **Compare** the various types of security attacks.(7)	BTL 4	Analyzing
13	**Describe** the functionality of Risk Management Laws And Regulations.(13)	BTL 1	Remembering
14	**Write** detailed note on Physical Security Threats. (13)	BTL 2	Understanding
	PART-C		
1	**Evaluate** the Privacy on the Internet and Privacy Enhancing Technologies. (15)	BTL 5	Evaluating
2	**Discuss** in detail about the application level security in following services i) Personal privacy policies(5) ii) Detection of security policies (5) iii) Conflicts of security policies (5)	BTL 6	Creating
3	**Improve** the benefit of Storage area network security and Authorization methods for privacy and security in environment monitoring systems system design.(15)	BTL6	Creating
4	**Evaluate** and **summarize** the Key privacy issues in Risk management - Physical Security Essentials**..**(15)	BTL 5	Evaluating