Date:

Syllabus: R16 Class: BE Sub: CSL Sem: VII

RegNo: 2017C02 Seat No- 7278650

Q1 MCQ

1) Option : A : Social engineering attack

2) Option : C : Agreement

3) Option : C : Testmony

4) Option : D : Logos names and brand

5) Option : A : GLBA

6) Option : B : Online Stalkers

7) Option : C : Mishing

8) Option : D : Computer based Social Engineering

9) Option : A : Citizen to Government

10) Option : D : Reject E-filing of data and information due to attack

Date:

Syllabus: R16 Class: BE Sub: CSL Sem: VII
Reg No- 2017C02 Seat No: 7278650

Q2C DOS Attack

① A DOS attack is a Denial of Service attack, in this attack Computer Sends massive amount of traffic to a victims computer and shuts it down.

② DOS attack is a online attack which is used to make the website unavailable for its user when done on a website.

③ This attack make the server of a web site down which is Connected to internet by sending large number of traffic to it or sending large number of requests.

DDOS attack

① A distributed Denial of service attack is DOS attack that comes from more than one Source at a ~~time~~. Same time.

② A DDOS attack is typically generated using multiple Computers or zombie machines.

③ These machine are infected with malware, allowing them to be controlled remotely by an attacker. This devices are reffered as bots and group of bots is botnet.

④ Once botnet has been established, the attacker is able to direct an attack by Sending remote instructions to each bot

⑤ When victim Server or network is targetted by botnet each bot Sends resquests to the target's IP address potentially causing the server or network to be come flooded with requests, resulting an ~~direct~~ Denial of service attack.

Date:

R16|BE|Sem:VII| Sub: CSL| Seat No- 72778650

Q2 B Security Challenges Posed by Mobile Devices

(1) Due to the use of the hand-held devices, information can be taken outside the physically controlled environment

(2) For the protected environment remote access is being granted

(3) It is important that the organization should be aware about these cybersecurity challenges in developing suitable Security operating procedure.

(4) Day by Day mobile users are increasing and due to this there are two challenges:

i) The first problem is a the device level. It is also known as microchallenges

ii) The second problem is at the organizational level. It also known as macrochallenges.

(5) There are few well known technical challenges in mobile Security.

i) Managing the registry security and Configurations.

ii) Authentication Service security, Cryptography Security

iii) Light weight Directory Access Protocol (LDAP) Security

iv) Remote access server (RAS) security, media player Contral Security

v) Networking Application Program interface (API) Security.

Date:

Pg-4

R16/BE/Sem:VII/Sub: CSL / Seat No: 7278650

~~Q2A~~

Q2 E Passive Attack:

(1) In passive attack the attacker collect the information about the target without individual for Company's knowledge. For example, an attacker keep watch on an employee at what time is entering the building and leaving the promises.

(2) attacker can also monitor the network traffic for the emails sent using the monitoring tools.

(3) Attacker can get general information from the following ways

i) Search engines: Searching the information about target on search engine like Google & Yahoo.

ii) Social website: By Surfing the social website like Facebook, Instagram etc an attacker can get information

iii) Organization website: The organizational website also provide the personal information about the employes like Contact details, email address etc.

iv) Network Sniffing: In this attack, the attacker gives the information about the internet protocol address ranges, hidden server or networks and other services on the system or network. The attacker monitors flow of data check at what time certain transactions are taking place and where the traffic is going.

v) People search: It gives details about personal information like, date of birth, residential address, Contact number etc.

vi) Domain name Confirmation: To carry out searches for domain names using multiple keywords in ".com", ".net", ".org", ".edu", etc.

Date:

R16|BE|Sem: VII|Sub: CSL|Seat No- 72786S0

Active attack

① An active attack includes examining the system or network to find individual host to affirm the data (IP address, working framework type and form, and adminstrations on the system) accumulated in the passive attack stage

② It includes the danger of identification and additionally called active reconnaissance.

③ Active reconnaissance can give confirmation to an attacker about security measures setup, However the procedure can like wise expand the opportunity of being gotten or raise a doubt.

④ Tools used during active attacks are

i) Bing : Used for Bandwidth ping

ii) Hping : used to send custom TCP/IP packets

iii) Fping : Uses internet Control message protocol (ICMP) echo request

iv) nmap : used for reconiassiance to get host, OS, version info etc..

v) Netcat : Used to read and write custom ~~TCP/UDP packets~~. TCP/UDP packets and to make Connection with host.

vi) Ping : Used to send ICMP packets to target.

Date:

R16 | BE | Sem: VII | Sub: CSL | Seat No: 7278650

Q3 B Attacks on wireless networks.

(1) Wireless attacks can come at you through different methods like tricking Users, bruteforcing etc..

(2) Types of wireless attacks are Fallows

(3) Packet Sniffing:

i) When information is send back and forth over network it is sent ~~in~~ in what we call packets. Since wireless traffic is Sent over air it is easily Captured.

ii) Lot of traffic (FTP, HTTP, SNMP etc) is Sent over network without any encryption in Cleartext form.

iii) So using tools like wireshark and burpsuite you Can capture the packet and read data in plain text.

(4) Rouge Access point:

i) When an unauthorized access point (AP) appears on a network, it is refferred to as a rogue access point

ii) This APs represents a vulnerability to the network because they leave it open to variety of attacks.

iii) This include Vulnerabilities like, ARP poisoning, packet capture, Denial of Service attack.

(5) Password theft:

i) When Communicating over in wireless networks, like login in to website using username and password, and if the site doesn't use SSL or TLS, That password is Sitting in plain text for an attacker to read.

Date:

R16 | BE | Sem: VII | Sub: CSL | SeatNo: 7278650

⑥ Manin the middle attack.

i) It is possible for hackers to trick communicating devices in to sending their transmissions to the attackers System.

ii) Here they can record the traffic to view. Cliter in packet Sniffing) and even change the contents of files.

iii) Various types of malware can be inserted into these packets, emails content could be changed or the traffic could be dropped so that communication is blocked.

⑦ Jamming: There are number of ways to jam a wireless network

i) Flooding an AP with deauthentication frames overwhelmes the network and prevents legtimate transmissions from getting through.

ii) This attack is little unusual because there probably isn't anything in it.

⑧ Bluetooth attacks: There are variety of Bluetooth exploits out there. These ranges from popup messages to controll over victims bluetooth device.

⑨ WEP/WPA attacks:

i) Attacks on wireless router can be huge problem. Older encryption Standards are extremely vulnerable.

ii) APs and routers are hiding your IP address from the broader internet usind Network Address translation(NAT)

iii) It helps to prevent attacks but doesent stops it Completely.

Date:

RIb|BE|Sem:VII|Sub:CSL|SeatNo-7278650

Q3 A Digital Signature.

→ ① A digital Signature is an electronic ~~device~~ method of illustrating the authenticity of a digital message or record. A substantial digital Signature gives the recipent motivation to trust that he message was made by a known sendir and that it was not changed in transit.

② ~~Digitia~~ Digital Signature are regolarly utilized for software conveyance, money related ~~exe~~ exchanges and in different ~~Sitio~~ Situations where it is imperative to ~~recigni~~ recognize impersonation or altering.

③ Following are the functions of digital signature

a) To authenticate the document

b) To identify the document

c) Securing the document from forgery

d) To make the contents of the document binding on person putting digital Signature.

e) Evidance for identification of document.

④ Digital Signature are used in e-commerce and by e-gurernance for the purpose of authentication. Digital Signature in ITACT 2000 means authentication of electronic record. Section 3 of IT Act 2000, describes authentication of electronic records.

~~Leg~~ Legal Architecture required for validation of Digital Signature.

① Intent to sign & opt-out clause.

Electronic Signatures are valid if only a user demonstrates a clear intent to sign.

Date:

R16|BE| Sem: VII| Sub: CSL | Seat No: 7278650

(2) Consent to do business electronically
The respective parties must either express or imply their consent to do business electronically.

(3) Clear signature attribution.
The context and circumstances under which the document was signed can indicate the attribution of an electronic signature.

(4) Association of Signature in record.
It is critical for electronic signatures to be connected to ~~de~~ the document being signed.

(5) Record retention.
Electronic Signature act ensures ~~the~~ the validity of records as long as they accurately reflect the agreement and can be reproduced as required.

Date:

R16|BE|Sem: VII | Sub: CSL | SeatNo - 7278650

Q4 A

a) Cybercrime and Indian IT Act 2000

→ (1) Cyber Crime is defined as the crimes which are mentioned in Information Technology act 2000. The Cybercrimes are restricted to tamper dow with the computer Source code, cyber pornography, harking, email abuse, harrassment, defamation, IPR theft, Cyber fraud etc

(2) Cyber Crime is an act of commission committed or omission or with the help of internet, whether Connected directly or indirectly, which is prohibited by law and for which punishment, monetary and/or corporal is provided

Indian IT A 2000

→ (1) Tampering with the computer Source documents

(2) Hacking with computer System

(3) Publishing of information which is obscence in electronic form

(4) Power of Controller to give directions

(5) Protected System

(6) Penalty for misrepresentation

(7) Penalty for breach of confidentiality and privacy.

(8) Publication for fraud purpose.

(9) Power to invistigate offences.

(10) Penalties or confiscation not to interfere with other punishments.

etc.

Date:

R16|BE|Sem:VII|Sub:CSL|SeatNo:7278650

Q4 B2) E-commerce.

→① E-commerce in simple language is defined as buying and selling goods and rendering the services on the internet.

② The E-commerce transactions are of four types that blend and correlate.

i) Information Access
ii) Interpersonal Communication
iii) Shopping Services.
iv) Virtual enterprises.

③ Information access
It gives the user search and retrives facility, that involves the transfer of information across the internet.

④ Interpersonal Communication.
It provides the methods to exchange information discuss ideas and improve their co-operation.

⑤ Shopping services.
It permits the user to seek and purchase good on the internet or to avail the service through the internet.

⑥ Virtual enterprises.
i) These are the business arrangements when trading partners who are separated by geographies and expertise are able to engage in joint business activities.
ii) Every e-Commerce transaction is like any other transaction but there involves Contractual relationship between

transacting parties. The Indian Contract Act 1872 states the law of Contract and the sales of goods act 1930 states the law ~~pt~~ pertaining to the Sale of goods.

iii) In this ~~[redacted]~~ IT Act 2000 Some provisions have been incorporated related to the distance natur of e-commerce transaction.

iv) In this important implication on a Contract is given. Every Contract needs to be tailored in accordance with the need of transaction

v) The industries that are using IT in Their Setup should be awar of various leagel aspects of e-contracts the same way every Consumer must understand the terms of the contract before entering into a transaction.