Roll. No.: 51810003
Subject : Cyber Security
Subject code: MCA-303

Q3.

A(a) Nessus

Nessus is a remote security scanning tool, which scans a computer & raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have conneted to network. Nessus provide highly-accurate scanning with low false positive and nessus can be scalable to hundreds ~~thound~~ thousands of system in a network and it is easy to deploy and maintaince. It is easy to operate.

(b) Nmap

Nmap is known as network mapper. It is a open source tool for ~~vulens~~ ~~#~~ vulnerability scanning. ~~and~~ Network administrators use Nmap to identify what devices are ~~stil~~ running on their systems, finding open ports and detecting security risks. Most of the time the open ports is the main reason for a system hacker with help of open ports a hacker can get access of a system and stole the data. Nmap uses IP address packets to identify all the devices connected to a network & to provide information on the service and operating systems they are running. It can perform ~~rad~~ rapidly scan large networks. Nmap determine the services like application name & version which host are offering, operating system & version of os they are running, type of packet ~~filet~~ filter or firewall in use etc. So, Nmap provide very useful information of a network.

(C) Netcat

Netcat is a computer network utility for reading from & writing to network connections using TCP or UDP. The command is designed to be dependable back-end that can be used directly or easily driven by by other program. Netcat is a general-purpose command line tool for reading, writing, redirecting and encrypting data accross a network. Netcat handling a wide variety of security testing & administration task.

Q2.

Q2. i) Phishing attack.

Attacker perform a phishing attack in several steps:

i) planning: First attacker plans the attack in which they ~~ploan~~ make a plans of use mass mailing, address collection techniques from targeted house or organization or an individual person.

ii) Setup: He set up emails or webpages to collect the data about the target.

(c) Attack: In this step attacker attacks, he send an ~~se~~ email, ~~as~~ or a message to target which looks like source of a message is ~~genuine~~ from real or trusted company.

(d) collection: After the attack, attacker record all the information of the ~~[illegible]~~ target entering into webpages.

(e) Identity theft and fraud: After collecting all the information, attacker use the information to make illegal purchases.

To ~~preved~~ prevent phishing: In tried phishing once in BCA days, I make a clone of ~~fact~~ 'facebook' login page & sends its to my friends. The login page was real but when they put id & password in it the page will send data to me. ~~So~~ So, I ~~think~~ one think get to ~~ben~~ knew that time is that if you entered wrong information in the webpage and submit or login, then if ~~on~~ you enter ~~the~~ your id & ~~passag~~ password again on that reloaded page then the information will not send to the attacker it will directed to the main server of the webpage.

~~If you have any~~

DoS

- Denail of service is an attempt to make a machine or network resource unavailable to its intended users. Dos attack may do the following like ‘flood the traffic", disrupt service to a specific system or person.
There are many software available you use to send multiple request at same time on ~~an~~ one server so, their server resources g. is unaviable. There ~~A~~ are many more ~~att~~ dos attack like bandwidth, logic, protocol attacks which can be used for a ~~tra~~ target server.

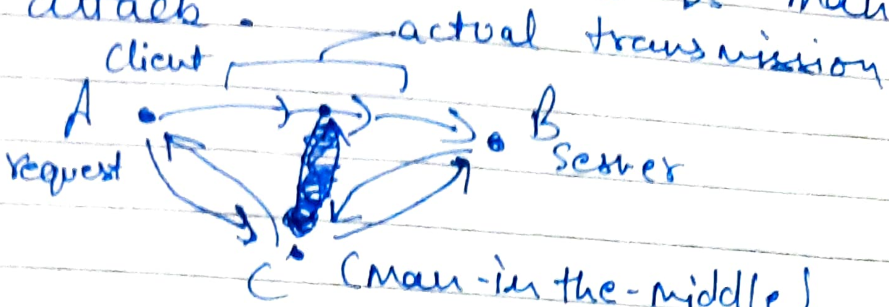
To prevent DOS attack their filtering ~~request~~ which can ~~fit~~ filter all the request & drop the those request which is comming continously from the same ipaddress.
Moving is also help to prevent from DOS it will move the site's ip address to another ipaddress.
The last option to prevent DOS is ‘Blackholing’ in this the request is direct to an address that doesn't exist.

Q1.

A① online password crack

In online password crack ~~the~~ an attacker create a script automated program which try ~~t~~ each password until find the right passwords.

The most popular online attack is man-in-the middle attack.



For ex. Client ~~s~~ send the request to server but man-in-middle capture the client request and he can do what he want like change the request, copy the data etc. then and then forward request to the server. Mostly used used to obtain passwords for email accounts on public websites like Gmail, facebook etc.

- Offline password. crack

Offline password crack means the ~~[illegible]~~ password ~~[illegible]~~ is not ~~s~~ sending by the request. Example for offline password ~~[illegible]~~ crack is we put a password on our computer and computer doesn't saved the password in simple text. In this the attacker uses our system and find out the files in which passwords are saved ~~&~~ ~~copies~~ transfer it into storage device and then try to decrypt the password, that offline password crack performs by the attacker.

Q4.
A4. Civil offences under the IT Act (2000) (section 43)

i)- Unauthorised copying, extracting & downloading of any data.
- Unauthorised access to computer, ~~co~~ computer system or computer network.
- Introduction of virus
- Damage to computer system & network
- Denial of access to authorised person to computer
- Providing assistance to any person to facilitate unauthorised access to a computer.
- Charging the service availed by a person to an account of another person by tampering & manipulation of ~~I~~ other computers.
- Hacking with computer system
- Tampering with computer source document.
- Unauthorised access to protected system.

For offences the person shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Q.5.
A5. Yes, it is possible to fetch the webpages surfed by any user in the past with the help of ~~i~~ the person's gmail account you can fetch not only the information about the webpage you can also see how many time the victim

Open a whatsapp, instagram, facebook, chrome, webpages etc. Gmail keeps the track of all of our phone mobile's phone's activity so we can fetch the webpage also.
Sql injector can be used to get a database of website.