Part-B

Answer all the questions

11) a) TCP/IP:

definition:

=> The TCP(transmission control protocol) is used to communicate between two different network computers in the local area network.

=> The IP (Internet protocol) is used to map the unique address of ip address of the computer device.

=> they usually categorised into two testing of

i) active

ii) passive.

i) active testing:

* it is used to gather information directly from the organisation.
* it is highly risk.
* it is a faster process.

ii) passive testing:

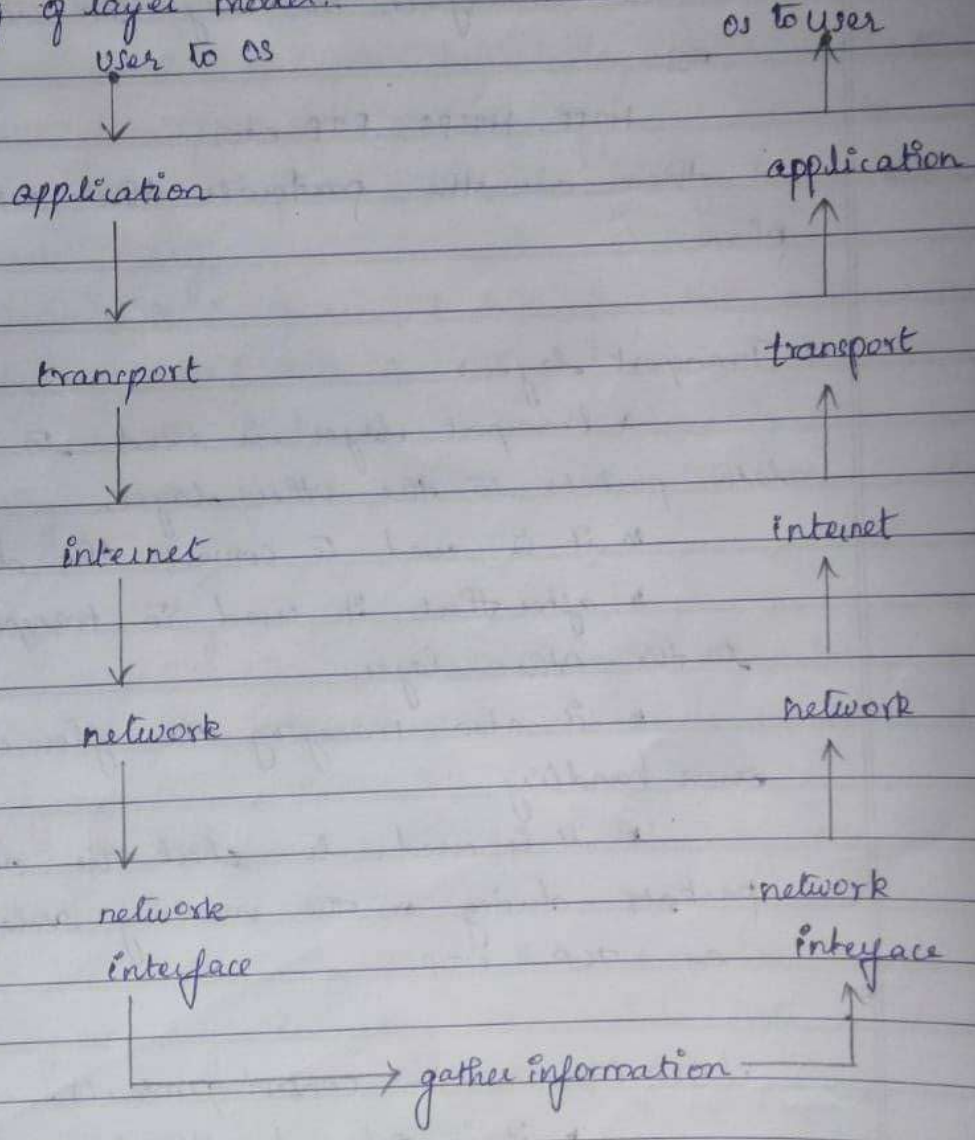
* it is used to gather information indirectly like any sources of links, platforms from the organisation.
* it is low risk.
* it slower process.

Comparatively active testing process is best for simulate a real-world attack with directly to the organization, but it is easy to identify the attacker.

Scenario:

Conduct a comprehensive test on A multinational company, by covering application, transport and internet layers.

Working of layer model:



this, the work phase of the protocols, while each layer doing the separate job and send the data to the next layer.

⇒ Application layer:

* it is the first layer of OSI.
* it is used to interact with the user and the system.
* this is the layer where the user can see the interface and they can understand.

eg;

HTTP, HTTPS, FTP, etc...

* these are the protocols that are used in this phase.

⇒ Transport layer:

* transport layer is used to transfer the data packets to the other layer.
* it is used to convert the data into segments.
* after that, it used to transport the data to the other layer.
* it also managing the flow control and error handling.
* it is used to check the order of the packets during on the receiving side.

eg; TCP, UDP.

i) TCP (Transmission Control protocol):

* it is enhanced with connection establishment.
* it has some error.

ii) UDP (user datagram protocol):

* it is a connectionless protocol.
* it has no error.

(ii) a) Foot printing techniques:

definition:

⇒ Foot printing is the first and most important phase of ethical hacking. it is a step-by-step framework used to gather information about the target organisation.

⇒ after gathering the information, it will be used to exploit the vulnerabilities or simulates a real-world hacking attacks to identify, analyse, fix the vulnerabilities of the organisation.

⇒ the testing can be broadly classified into two of..

i) Active

ii) passive.

i) Active technique:

* it is used to gathering information directly from the organisation.

* which is highly risk due to direct interaction with those organisation.

* it is faster, reliable but high Risky.

ii) passive technique:

* it is used to gathering information indirectly. like the sources from the organisation

* which it is very low risk because of indirect interaction.

* it is slower process but low risk.

iii) Internet layer:

* it is used to share the packets among the different system by using some internet.
* this method is possible to send any data to other packets layer / networks.

iv) Network layer:

* the network layer layer is used to share the data packets to the different networks.
* it is processed and managed by the network layer.
* it is processed by using the address of the devices, which it is unique.
* the sender know the address of the receiving network so, it can send with those addresses.

i) physical layer

* it is used to convert the data to machine coded signal that are understandable by the system.
* it can't be understandable by the humans/users.
* it is used to interact with the core system by converting raw data into machine bit code.

So, these are the main five layers to process / assessing the test on the multinational company to prevent from the attacks by using security mechanisms, authentication factor, authorisation and updates.

⇒ used in social network interface.

* enumerate the information about the employees, customers and more sensitive data.

* Social network interface is defined as online entertainment platform which it contains all information about the organisations.

* it may like,

i) Youtube, facebook

ii) instagram, twitter (x)

iii) linked.in and so on,

⇒ used in websites:

* gathering information from the organization websites.

* it may contain the overview of the organization which it is very useful to enter in the database access.

* it may like,

i) about us

ii) contact

iii) working life

iv) relevant data content.

v) site (robots.xml)

⇒ used in webservers:

* gathering information from the webservers.

* it is used to get the more information about the organization by giving only DNS.

* tools like,

Eg; WHOIS, netcraft.

DATE:
PAGE:

=) used in emails:

* if the email look like the original site but it contains some malicious code or Malware on the page.
* if the user get in the mail, then it will redirect to the other, they supposed to know about this user detailed information.
* even we can get a ip address through the message from the email.
* it is same like phishing, cross site scrapping and any other attacks.

Counter measurements:

* raising firewalls to protect the organisation
* maintain security mechanisms.
* maintain & test the authentication, authorisation.
* keep the software updated.
* don't do unnecessary installed files.
* By testing and analysing the site of the organisation will improve the security mechanisms, include,
  - => prevent sensitive data
  - => prevent from cyber attacks
  - => maintain customer trust
  - => ensure compliance with standard testing.

So, these are the phases to mainly looking for, and if the organisation has the testers then they split us into of security and penetration testers. One is used to monitor and give the solution and another one is used to practically implement the exploitation of vulnerability to identify the loop hole and used to make a final document to build a defence mechanism for that.

13) a) NetBIOS enumeration techniques:

definition:

* the netBIOS (network Basic Input/output service) is used to gathering information for the vulnerability testing.
* it is used to follow in the protocols of
  i) TCP/IP
  ii) UDP.

i) TCP/IP:

* it is a connection established testing.
* IP is used to identify the address of the device, network, application.

ii) UDP:

* user datagram protol is a connectionless testing.
* it has no ~~error~~.

process of netBIOS is,

planning & scope
↓
Reconnaissance
↓
scanning & enumeration
↓
vulnerability assessment
↓
exploitation
↓
post-exploitation
↓
reporting
↓
remedy & follow up

Objectives of footprinting:

* to gathering information about the target organisation.
* and to get into deep to gather information about their senitive data.
* exploit the vulnerabilities to the organisation.
* it is used to identify vulnerabilities
* prevent from cybercrime attacks.
* protect the senitive data.
* maintain the customer trust
* testing and ensuring the existing security mechanisms.

process of footprinting techniques:

=> used in search engines
=> used in social network interface
=> used in websites
=> used in webservers
=> used in email.

=> used in search engine:

* the attacker used to analyse / gathering the information about the target organisation from the online search engines like
  i) google.
  ii) wikipedia,
  iii) github. repositories,
  iv) source links,
  v) sources like pdf, docx.

Success
DATE:
PAGE:

Part-A

Answer all the question.

1) Penetration tester:

* the penetration tester is used to exploit the data in unauthorised manner.

* it will be useful to detect the vulnerability in the organisation and make sure to build a safety or security mechanisms.

2) Ethical hacking:

* It is the authorised manner to exploit the data for identify the vulnerability and analysing it.

* Objectives:

=) prevent from cyber attacks

=) protect sensitive data.

3) TCP/IP:

* used to check the connection between the devices, network and application.

* check and apply the techniques of four layers are application, transport, internet, network and physical.

4) Network attack:

* it is held in the network protocol like it may be happened due to the slow security-mechanisms

Malware attacks:

* it is done with help of the user, it may include from downloading file, phishing, etc...

5) Footprinting:

* the footprinting is the step-by-step framework and it is the important phase in ethical hacking to enumerate the information from the organisation used to identify the vulnerability.

DATE:
PAGE:

6) footprint through webservices:
* you can gather information about the organisation by the tools of,
WHOIS, Scratify.

footprint through search engines:
* you can gather information about the target by using
online search engine such as google, github. etc.

7) network Scanning:
* it is used to scan the network of TCP/IP for the data to passes through.
* used to check the active networks.

Port Scanning:
* it is used to scan the ports which are open, closed, filtered.
* open → can receive data.
* close → can't receive any data
* filter → inbetween blocked by firewall.

8) * Scanning technique is used to gather information about the loop hole of vulnerabilities of the target.
* if you need to identify the vulnerability, then Scanning is the important method to detect it.

9) NetBIOS:
* Network basic input/output service is used to enumerate the information from the target.
* it is used to identify the vulnerability, assess the risk and managing the security mechanisms.

Success
DATE:
PAGE:

=) planning and scope:

* it is used to define the target of the Organisation
* after that we need to define the scope of this testing like,
  what we are testing, which technique, is it scalable or not,

=) Recoinnancense:

* it is used to gathering the information about the Organisation.

=) Scanning & enumeration:

* after defining the organisation, we had to gather information in deep way such as users, employee and other data.

=) Vulnerability assesment:

* it is used to identify the vulnerability in the Organisation and make the document about it to build a defensive mechanism.

=) exploitation:

after gathering information, then they simulate the real-world attacks to identify the vulnerability.

=) post-exploitation:

* after exploitation, check whether it is accessible the data or not.

=) reporting:

after these process, you need to create a document about the vulnerability of loopholes in the Organisation.

=) remedy & followup:

giving solutions to the each vulnerability.

IMPRESS
DATE:
PAGE:

10) Vulnerability assessment technique :-

* footprint techniques used in search engine
* footprint technique used in social network interface
* footprint technique used in webservice
* footprint technique used in website
* footprint technique used in email.
* also, scanning & enumeration are also the technique