Penetration Testing

Penetration Testing or Pen test is a security exercise where a cyber security expert attempts to find and exploit vulnerabilities in a computer system. The purpose of this simulated attack is to identify any weak spots in a system's defense which attackers could take advantage of

Penetration testers use the same tools, techniques and process as attackers to find the weakness.

Benefits

1. Find weaknesses in systems
2. Determine the robustness of controls
3. support compliance with data privacy & security regulation.
4. Provide qualitative and quantitative eg of current security posture.

Stages

1. Planning
2. Scanning
3. Gaining access
4. Maintaining access
5. Analysis and WAF configuration (Web Application Firewall)

IPSGMA

Spiral

DT. ☐☐ ☐☐ ☐☐☐☐

1. Planning
→ Defining the scope and goals of a test · including systems to be addressed and the testing methods to be used.
→ Gathering intelligence — how a target works.

2. Scanning
↳ to understand how the target application will respond to various intrusion attempts

3. Gaining access
This stage uses web application attacks such as cross-site scripting, SQL injection and backdoors to uncover a target vulnerabilities.
Tester then try and exploit these vuln. by stealing data, intercepting traffic etc. to understand the damage they can cause

4. maintaing access.
The goal of this stage is to see if the vulnerability can be used to achieve a peersistent presence in the system

5. Analysis
The result of the test are compiled into detailed report
↳ sensitive data that was accessed
↳ specific vulnerabilities that were exploited
↳ amount of time pen test was able to remain in the system undetected.

DT.

Methods

① Internal Testing → In this, the ethical hacker performs the test from the company's internal network. Eg. a employee whose credentials were stolen due to a phishing attack.

② External Testing → In this, the hacker ~~tests~~ target the assets of a company that are visible on the Internet eg. web application, website, email, domain name servers

The goal is to gain access and extract valuable data

③ Blind testing → a tester is only given the name of the enterprise that's being target.

④ Double blind → security personnel has no prior knowledge of the simulated attack. As in real world, they won't have time to shore up their defenses before an breach

⑤ Targeted testing → In this scenario, both tester & security personnel work together & keep each other appraised of the movements.

DT. ☐☐ ☐☐ ☐☐☐☐

FRAME RELAY	ATM
1. FR has variable packet size	1. ATM has fixed packet size
2. Cost is low	2. costlier
3. Packet delay is more	3. Packet delay is less
4. Reliability is less	4. Reliable
5. Packet trasfer speed is low	5. High
6. Does not provide error control and flow control	6. provides error & flow control

SMDS → Switched multimegabit Data Service
SMDS is a high speed packet based WAN networking tech. used for communications over public data networks (PDN).
↳ uses copper or fiber optic based media
↳ support speed of 1544 Mbps over DS 1 or 44736 Mbps over DS-3
↳ It extends the performance & efficiency of the company's LAN.
↳ designed for moderate bandwidth connection 1-34 Mbps.

ATM :- Asynchronous Transfer mode :-
ATM is a cell switching, connection oriented technology.
↳ uses asych. time-division multiplexing to encode data into small, fixed sized cells.
↳ provide support for virtual network
↳ Higher transmission capabilities
↳ low operating cost & low error rate

Spiral

DT. □□ □□ □□□□

SDLC
↳ Software Development Lifecycle
process used by the software industry to design, develop and test high quality softwares.

Planning → Defining → Designing → Building → Testing → Depl.

HDLC → High level Data Link Control

It is a group of communication protocols of the data link layer for transmitting data b/w network points or nodes.
Since it is a data link protocol, data is organized into frames.
A frame is transmitted via the network to the destination that verifies its successful arrival.
Applicable for both point-to-point & multipoint communication

Normal response mode
↳ one station send command other receives
↳ used for both p-2-p & mult.

Asynch. balanced mode
each station can send & respond.
→ p-2-p communication.

ISDN → Integrated Digital Network services

ISDN is a network in which digital switching connections are used to transmit digital signals. Multiple devices can be connected to the line and sent as needed.
↳ offers symmetrical transfer rate →
↳ consistent transfer rate 64 Kbps
→ support both circuit switching & packet switching.
Is are transmission of voice, data, video and other network services over the digitalized circuit.

Spiral

DT.

Frame Relay:

It is a packet switching network protocol that is designed to work at the data link layer of the network.
It is used to connect LAN and transmit data across WAN.
It does not have an error control and flow management mechanism.
It is a fast packet technology based on X.25.
Data is transmitted by encapsulating them in multiple size frames and sent in high speed bursts through digital network.
It uses the technology of fast packet in which error checking does not occur in any intermediate node

RAID : Redundant array of independent disks is a data storage visualization technology that combines multiple physical disk drive components into one or more logical units for data redundancy, performance improvement or both.

It is a way of storing the same data in diff places on a multiple hard disks or solid state drives to protect data in case of drive failure. consists of 2 or more drives working in parallel.

Disk mirroring → copy identical data onto more than one drive.

Disk stripping → partitions help spread data over multiple disk drive.

Spiral

DT. ☐☐ ☐☐ ☐☐☐☐

~~Redundant Server~~

IBM NetView

IBM Netview helps to determine the highest degree availability of IBM networks.

⇒ Netview program enables the management of networks and systems through graphical display and automation.
⇒ Extensive tools are included to manage and maintain complex systems from a single point of control.

→ Also provide a set of user interface to meet the needs of any user that work with other product.

Advantages

↳ Increased network and system efficiency and availability
↳ Reduce the need for duplicate network management syst.
↳ enhanced operations and message management

Components

1. Command facility → send & receive messages
2. Hardware monitor → collect & display events & data
3. Session Monitor → provide info. about sessions like status, connectivity, response time
4. Terminal Access facility → provide operator control from one terminal
5. Automated Operation Network
   ↳ monitor messages, alerts and automatically perform action

Spiral

DT.

Sun Net Manager is the primary network management system for Sun Microsystem.

↳ used to monitor and improve Performance in multiprotocol networks.

SNM has 4 categories of elements

1. components → elements like printer, workstation, system etc
2. View → collection of elements
3. Bus → represent LAN segments
4. Connection → connect two elements Eg. P2P

It is a platform for the management of distributed work group networks.

↳ Architecture → relies on manager / agent model.

↳ manager is a process initiated by the user.
The agent is the process that access the managed object and collect data on behalf of manager.