Unit-4

1. Define following terms:

(i) Password Cracking

password cracking is a process of recovering passwords from data that have been stored in or transmitted by a computer system.

password cracking attacks can be classified under 3 categories:

1. Online attacks.
2. Offline attacks
3. non-electronic attacks.

(ii) Keyloggers

Keystroke logging, often called keylogging, is the practice of noting the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that such actions are being monitored.

It can be classified as Software keylogger and hardware keylogger.

(iii) Spywares.

Spyware is a type of malware that is installed on computers which collects information about users without their knowledge

(iv) Virus

Computer virus is a program that can "inject" legitimate programs by modifying them to include a possibly "evolved" copy of itself. Viruses spread themselves, without the knowledge or permission of

to potentially large numbers of programs on many machines.

Types of viruses:

1. Boot Sector Viruses:
2. Program viruses
3. Multipartite viruses
4. Stealth viruses
5. Polymorphic viruses
6. Macroviruses
7. Active X & java Control.

(v) Worms

A computer worm is a self-replicating malware computer program. It uses a computer network to send copies of itself to other nodes and it may do so without any user intervention.

(vii) Trojan Horses:

Trojan Horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and cause harm.

(viii) Steganography:

Steganography is a Greek word that means "Sheltered writing". It is a method that attempt to hide the existence of a message or communication.

2. Write a detail note on SQL Injection.

SQL injection is a code injection technique that exploits a security vulnerability occuring in the database layer of an application.

Attackers target the SQL servers - common database servers used by many organizations to store confidential data.

The prime objective behind SQL injection attack is to obtain the information while accessing a database table that may contain personal information such as credit card numbers, social security numbers or passwords.

Steps for SQL Injection Attack

(1) The attacker looks for the webpages that allow submitting data i.e. login page, search page, feedback etc.

(2) The attacker checks the source code of the HTML, & look for "FORM" tag in the HTML code. The Everything between <FORM> and </FORM> have potential parameters that might be useful to find the vulnerabilities.

(3) The attacker inputs a single quote under the text box provided on the webpage to accept the username & password.

(4) The attacker uses SQL commands such as SELECT statement command to retrieve data from the database or INSERT statement to add information to the database.

Preventing SQL Injection Attacks

The following steps can be taken to prevent SQL injection.

(1) Input validation
(2) Modify error reports
(3) Other preventions like the default system accounts for SQL server 2000 should never be used.

3. Explain in detail DoS Attack with its classification.

DoS Attack (Denial-of-service)

DoS Attack is a can attempt to make computer resource unavailable to its intended users.

A type of criminal attack, the attacker floods the bandwidth of the victim's network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide.

The attackers typically target sites or services hosted on high-profile web servers such as banks, credit cards payment gateways, mobile phone network & even root name servers.

Classification of DoS Attacks

(i) Bandwidth Attacks

The attacker opens 100 pages of a site & keeps on refreshing and consuming all the bandwidth, thus, the site becomes out of service

(ii) Logic Attacks

These kind of attacks can exploit vulnerabilities in network software such as web server or TCP/IP stack.

(iii) Protocol Attacks

~~Protocols here~~ These kind of attacks exploit a specific feature or implementation bug of some protocol installed at the victim's system to consume excess amounts of its resources.

(iv) Unintentional DoS Attack.

This is a scenario where a website ends up denied not due ~~to~~ to attack, but simply due to enormous spike in popularity. This can happen when an extremely popular website posts a prominent link to a second, less-well prepared site.

PAGE No.
DATE / /

4. What do you mean by Buffer Overflow?
Buffer Overflow is an anomaly where a process stores data in buffer outside the memory the programmer has set aside for it.

The extra data overwrites adjacent memory, which may contain other data, including ~~data~~ program variables & program flow control data.

This may result in erratic program behavior, including memory access errors, incorrect results, program termination or a breach of system security.

Types of Buffer Overflow:
(i) Stack-Based Buffer Overflow

(ii) NOP (No peration) or NOOP (No Operation performed)

(iii) Heap Buffer Overflow.

5. Differentiate between Virus and Worm

Virus	Worm
(i) A computer virus is a software program that can itself copy itself & infect the data or information, without the user's knowledge.	(i) A computer worm is a software program, self-replicating in nature, which spreads through a network.
(ii) To spread to another computer, it needs a host program that carries the virus	(ii) It can send copies through the network with or without user intervention.
(iii) Stealth virus, self-modified virus, encryption with variable key virus, polymorphic code virus, metamorphic virus are types of virus.	(iii) E-mail worms, instant messaging worms, Internet worms, IRC worms, file-sharing network worms.
(iv)	

6. What do you mean by Password Cracking? Write down the purpose of password cracking and also list & explain categories of password cracking.

Password cracking is a process of recovering passwords from data that have been stored in or transmitted by a computer system.

The purpose of password cracking
1. To recover a forgotten password.
2. As a preventive measure by system administrators to check for easily crackable passwords.
3. To gain unauthorized access to the system.

Password cracking attacks can be classified under three categories as follows:
1. Online Attacks
2. Offline Attacks
3. Non-Electronic Attacks.

1. Online Attacks

An Attacker creates a script file that will be executed & try each password in a list & when matches the attackers - can gain access to a system.

Popular online attack is Man-in-the-Middle also known as "Bucket-Brigade-Attack" or sometimes "Janus Attack"

This type of Attack is used to obtain the passwords for E-mail accounts on public websites and also used

to get the passwords for financial websites that would gain the access to banking websites.

2. Offline Attack

This Attack require physical access to the computer & copying the password file from the system onto removable disk.

Different types of Offline Attack.

(i) Dictionary Attack → Attempts to match all the words to get the passwords.

(ii) Hybrid Attack → Substitutes numbers & symbols to get the password.

(iii) Brute Force Attack → Attempt all permutations & combinations of letters, numbers & all special characters.

3. Non-electronic Attacks

E.g. Social Engineering
Shoulder surfing and
Dumpster Diving.