IV/IV B.Tech (Regular) DEGREE EXAMINATION

Advanced Cyber Security (14IT701)

Scheme of Evaluation

Maximum: 60 Marks

1. Write briefly about the following 1*12= 12 Marks

a) Define exploit?
Ans: A breach of IT system security through vulnerabilities

b) What is a Pen Test?
Ans: pen testing or ethical hacking, is the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit.

c) Distinguish between passive and active attacks.
Ans: Active attack, an attacker tries to modify the content of the messages. Whereas in Passive attack, an attacker observes the messages, copy them and may use them for malicious purposes.

d) What is meant by XSS attack?
Ans: Cross-Site Scripting (XSS): XSS enables attackers to inject malicious client side scripts into the web pages viewed by other users.

e) What is an IP Sniffing?
Ans: Sniffing is a process of monitoring and capturing all data packets passing through given network.

f) Define DNS Foot printing?
Ans: Attacker can gather DNS information to determine key hosts in the network and can perform social engineering attacks.

g) Define DDOS.
Ans: A distributed denial-of-service (DDoS) attack involves a multitude of compromised systems attacking a single target, thereby causing denial of service for users of the targeted system.

h) Define DNS Poisoning.
Ans: DNS poisoning is a technique that trick a DNS server into believing that it has received authentic information when, in reality, it has not.

i) What are the limitations of Firewalls?
Ans:
1. A firewall cannot prevent users or attackers with modems from dialing in to or out of the internal network, thus bypassing the firewall and its protection completely.
2. Firewalls cannot enforce your password policy or prevent misuse of passwords.

j) When will Back door attacks encounter give some examples?
Ans: A backdoor attack is a type of malware that gives cybercriminals. adequate research to detect and review new types of malware on a regular basis.

k) Describe any two password attacks?

Ans:

- Password Guessing:
  The most common type of attack is password guessing. Attackers can guess passwords locally or remotely using either a manual or automated approach. Password guessing isn't always as difficult as you'd expect.
- Password Resetting:
  Attackers often find it much easier to reset passwords than to guess them. Many password cracking programs are actually password resetters.

l) What is a Malware?

Ans: The contraction of malicious software known as malware. Malware is any piece of software that is designed with the intent to damage, disrupt or gain unauthorized access to your device and inflict harm to data and/or people in multiple ways.

UNIT- I

2. a) Explain in – detail different Hacker classes with an examples. 6 Marks

Ans: [any six classes for 6 Marks]

Hacker Classes:

Black Hats: Individuals with extraordinary computing skills, resorting to malicious or destructive activities and are also known as crackers.

White Hats: Individuals professing hacker skills and using them for defensive purposes and are also known as security analysts.

Gray Hats: Individuals who work both offensively and defensively at various times.

Suicide Hackers: Individuals who aim to bring down critical infrastructure for a "cause“ and are not worried about facing jail terms or any other kind of punishment.

Script Kiddies: An unskilled hacker who compromises system by running scripts, tools, and software developed by real hackers.

Cyber Terrorists: Individuals with wide range of skills, motivated by religious or political beliefs to create fear by large-scale disruption of computer networks.

State Sponsored Hackers: Individuals employed by the government to penetrate and gain top-secret information and to damage information systems of other governments.

Hacktivist: Individuals who promote a political agenda by hacking, especially by defacing or disabling websites.

2. b) Define enumeration? Explain any two types of enumeration. 6 Marks

Ans: [Definition – 1Mark, each type – 2.5*2=5 Marks]

In the enumeration phase, attacker creates active connections to system and performs directed queries to gain more information about the target.

Attackers use extracted information to identify system attack points and perform password attacks to gain unauthorized access to information system resources. Enumeration techniques are conducted in an intranet environment.

- Information Enumerated by Intruders:
- Network resources
- Network shares
- Routing tables
- Audit and service settings
- SNMP and DNS details
- Machine names
- Users and groups
- Applications and banners

NetBIOS Enumeration: NetBIOS name is a unique 16 ASCII character string used to identify the network devices over TCP/IP, 15 characters are used for the device name and 16th character is reserved for the service or name record type.

Attackers use the NetBIOS enumeration to obtain:

- List of computers that belong to a domain
- List of shares on the individual hosts in the network
- Policies and passwords

SNMP enumeration: SNMP enumeration is a process of enumerating user accounts and devices on a target system using SNMP. SNMP consists of a manager and an agent; agents are embedded on every network device, and the manager is installed on a separate computer.

SNMP holds two passwords to access and configure the SNMP agent from the management station.

Read community string: It is public by default; allows viewing of device/system configuration.
Read/write community string: It is private by default; allows remote editing of configuration.

Lightweight Directory Access Protocol (LDAP) is an Internet protocol for accessing distributed directory services.

- Directory services may provide any organized set of records, often in a hierarchical and logical structure, such as a corporate email directory.
- A client starts an LDAP session by connecting to a Directory System Agent (DSA) on TCP port 389 and sends an operation request to the DSA.
- Information is transmitted between the client and the server using Basic Encoding Rules (BER).
  Attacker queries LDAP service to gather information such as valid user names, addresses, departmental details, etc. that can be further used to perform attacks.

Network Time Protocol (NTP) is designed to synchronize clocks of networked computers. Attacker queries NTP server to gather valuable information such as:

- List of hosts connected to NTP server
- Clients IP addresses in a network, their system names and Oss.
- Internal IPs can also be obtained if NTP server is in the DMZ

NTP Enumeration Commands:

ntptrace:

- Traces a chain of NTP servers back to the primary source
- ntptrace [-vdn] [-r retries] [-t timeout] [server]

ntpdc:

- Monitors operation of the NTP daemon, ntpd
- /usr/bin/ntpdc [-n] [-v] host1 | IPaddress1...

ntpq:

- Monitors NTP daemon ntpd operations and determines performance
- ntpq [-inp] [-c command] [host] [...]

Enumeration Countermeasures:

SNMP:

- Remove the SNMP agent or turn off the SNMP service
- If shutting off SNMP is not an option, then change the default community string name
- Upgrade to SNMP3, which encrypts passwords and messages

DNS:

- Disable the DNS zone transfers to the untrusted hosts make sure that the private hosts and their IP addresses are not published into DNS zone files of public DNS server.

3. a) Explain in detail different Hacking Phases.

Ans: [any three - 6 Marks]

Hacking Phases:

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Clearing Tracks

Reconnaissance:

- Reconnaissance refers to the preparatory phase where an attacker seeks to gather information about a target prior to launching an attack.
- Reconnaissance target range may include the target organization's clients, employees, operations, network, and systems.

Reconnaissance Types:

Passive Reconnaissance:

- Passive Reconnaissance involves acquiring information without directly interacting with the target.
- For example, searching public records or news releases.

Active Reconnaissance:

- Active Reconnaissance involves interacting with the target directly by any means.

For example, telephone calls to the help desk or technical department

Scanning:

- **Pre-Attacks Phase**: Scanning refers to the pre-attack phase when the attacker scans the network for specific information on the basis of information gathered during reconnaissance.
- **Port Scanner:** Scanning can include use of dialers, port scanners, network mappers, ping tools, vulnerability scanners, etc.

Extract Information: Attackers extract information such as live machines, port, port status, OS details, device type, system uptime, etc. to launch attack.

Gaining Access:

- Gaining access refers to the point where the attacker obtains access to the operating system or applications on the computer or network.
- The attacker can gain access at operating system level, application level, or network level.
- The attacker can escalate privileges to obtain complete control of the system. In the process, intermediate systems that are connected to it are also compromised.

Example includes password cracking, buffer overflows, denial of service, session hijacking, etc.

Maintaining Access:

- Maintaining access refers to the phase when the attacker tries to retain his or her ownership of the system.
- Attackers may prevent the system from being owned by other attackers by securing their exclusive access with Backdoors, RootKits, or Trojans.
- Attackers can upload, download, or manipulate data, applications, and configurations on the owned system.
- Attackers use the compromised system to launch further attacks.

Clearing Tracks:

- Covering tracks refers to the activities carried out by an attacker to hide malicious acts.
- The attacker's intentions include: Continuing access to the victim's system, remaining unnoticed and uncaught, deleting evidence that might lead to his prosecution.
- The attacker overwrites the server, system, and application logs to avoid suspicion.
- Attackers always cover tracks to hide their identity.

3. b) Define Vulnerability? Discuss in – detail different vulnerabilities encountered in Hacking process. 6 M

Ans:

Vulnerability is a weakness in design, implementation, operation or internal control. Most of the vulnerabilities that have been discovered are documented in the Common Vulnerabilities and Exposures (CVE) database.

An exploitable vulnerability is one for which at least one working attack or "exploit" exists. Vulnerabilities are often hunted or exploited with the aid of automated tools or manually using customized scripts. ---2 Marks

Any organization can fortify their security defenses by addressing these vulnerabilities:

1. **Insecure or Misconfigured Services**
   Many Web services come with advanced capabilities that, if not properly secured, can allow a malicious attacker to gain access to a system or network. Some problems can be detected by easily obtainable security scanning tools, then exploited to compromise a website or backend system including databases or other network systems. To properly configure services, most companies do not need to spend thousands of dollars for third-party products that do little more than change system settings. With proper research and time, companies can secure their internal, external and mobile systems themselves. Flat networks, misconfigured firewalls and perimeter devices, and higher security permissions across the domain are also culprits.
2. **Input Validation**
   Input validation issues, such as Cross-site Scripting and SQL Injection, have been a constant target for cyber attacks. While the techniques used to exploit these issues have been well documented, there are also many automated tools which can be used to quickly search for and exploit these types of issues. To protect against potential security holes and vulnerabilities, all input should be tested.
3. **Social Engineering**
   Social engineering attacks are one of the most effective ways for attackers to gain access to internal systems. The tactic typically exploits people’s desire to either help others or make their own jobs easier.

Whether through a well-crafted email or phone pretext, and sometimes by simply dressing the part, the attacker will often obtain information or access to what was previously unavailable. ---4 Marks

UNIT - II

4. a) Explain the differences between IP Spoofing and IP Sniffing and give some related attacks. 6 Marks

Ans:

In sniffing, the attacker listens into a networks' data traffic and captures data packets using packet sniffers. In spoofing, the attacker steals the credentials of a user and uses them in a system as a legitimate user. Spoofing attacks are also referred to as man-in-the–middle attacks since the attacker gets in the middle of a user and a system. -2 Marks

MAC duplicating attack is launched by sniffing a network for MAC addresses of clients who are actively associated with a switch port and re-using one of those addresses. By listening to the traffic on the network, a malicious user can intercept and use a legitimate user's MAC address to receive all the traffic destined for the user. This attack allows an attacker to gain access to the network and take over someone's identity already on the network.—2 Marks

Attacker sends spoofed IRDP router advertisement message to the host on the subnet, causing it to change its default router to whatever the attacker chooses. This attack allows attacker to sniff the traffic and collect the valuable information from the packets. Attackers can use IRDP spoofing to launch man-in-the-middle, denial-of-service, and passive sniffing attacks.—2 Marks

4. b) What is a poisoning? Explain DNS poisoning process. 6 M

Ans: Incorrect data quietly slithers into your system and changes its overall functioning, which can lead to a data breach and loss of user trust. ---1 Mark

DNS poisoning is a technique that trick a DNS server into believing that it has received authentic information when, in reality, it has not. It results in substitution of a false IP address at the DNS level where web addresses are converted into numeric IP addresses. It allows attacker to replace IP address entries for a target site on a given DNS server with IP address of the server he/she controls. Attacker can create fake DNS entries for the server (containing malicious content) with same names as that of the target server. ---3 Marks

DNS cache poisoning refers to altering or adding forged DNS records into the DNS resolver cache so that a DNS query is redirected to a malicious site. If the DNS resolver cannot validate that the DNS responses have come from an authoritative source, it will cache the incorrect entries locally and serve them to users who make the same request. –2 Mark

5. a) What is a firewall? How to enable packet filter firewall in applications.

Ans: Firewall are hardware and/or software designed to prevent unauthorized access to or from a private network. They are placed at the junction or gateway between the two networks, which is usually a private network and a public network such as the Internet. --- 2 Marks

Packet Filtering Firewall:

Packet filtering firewalls work at the network layer of the OSI model (or the IP layer or TCP/IP), they are usually a part of a router. In a packet filtering firewall, each packet is compared to a set of criteria before it is forwarded. Depending on the packet and the criteria, the firewall can drop the packet and forward it, or send a message to the originator. Rules can include the source and the destination IP address, the source and the destination port number, and the protocol used. ---2 Marks

Sufficient Diagram --- 2 Marks

5. b) Explain in – detail any four Information gathering tools. 6 M

Ans:

Recon-ng: Recon-ng is a framework. It is a very powerful, flexible, and has moving parts similar to the Metasploit framework. Recon-ng is an interactive framework that is not a menu driven UI. Recon-ng uses many different sources to gather data.

Installing recon-ng on Kali Linux

We are going to install recon-ng on Kali Linux. To install recon-ng and place it in the opt directory; we are going to use git clone by typing in the following command in the terminal window.

cd /opt; git clone https://LaNMaSteR53@bitbucket.org/LaNMaSteR53/recon-ng.git

cd /opt/recon-ng

./recon-ng

Net discover:

Net discover is an active/passive address reconnaissance tool, mainly developed for those wireless networks without DHCP server, when you are war driving. It can be also used on hub/switched networks.

sage: netdiscover [-i device] [-r range | -p] [-s time] [-n node] [-c count] [-f] [-S]

Ex: bt ~ # netdiscover -i ath0 -r 192.168.1.0/24

bt ~ # netdiscover -i ath1 –p (scan common networks)

- -i device: your network device
- -r range: scan a given range instead of auto scan. 192.168.6.0/24,/16,/8
- -p passive mode do not send anything, only sniff
- -s time: time to sleep between each arp request (miliseconds)
- -c count: number of times to send each arp reques (for nets with packet loss)
- -n node: last ip octet used for scanning (from 2 to 253)

Nmap:

Nmap is a free, open-source port scanner available for both UNIX and Windows. It has an optional graphical front-end, NmapFE, and supports a wide variety of scan types

Basic Scan Types [-sT, -sS]

- TCP connect() Scan [-sT]
- SYN Stealth Scan [-sS]
- FIN, Null and Xmas Tree Scans [-sF, -sN, -sX]
  Ex: # nmap -sS 127.0.0.1
- Ping Scan [-sP]
- UDP Scan [-sU]
- IP Protocol Scans [-sO]
  Ex: # nmap -sO 127.0.0.1
- Idle Scanning [-sI]
- Version Detection [-sV]
- ACK Scan [-sA]
- Window Scan, RPC Scan, List Scan [-sW, -sR, -sL]

Dmitry: - Deepmagic Information Gathering Tool

- Syntax
- **dmitry** [Options] host
- DMitry (Deepmagic Information Gathering Tool) is a UNIX/(GNU)Linux Command Line program coded purely in C with the ability to gather as much information as possible about a host.

- DMitry has a base functionality with the ability to add new functions. Basic functionality of DMitry allows for information to be gathered about a target host from a simple whois lookup on the target to UpTime reports and TCP portscans.

Options should be passed to DMitry in the form of '-option'. Only options known by DMitry will be used and others will be ignored. If options are not passed as a group block, the trailing options will be considered a host target.

- **-o filename** Create an ascii text output of the results to the "filename" specified.
- **-i** Perform an Internet Number whois lookup on the target. For example, "./dmitry -i 255.255.255.255".
- **-w** Perform a whois lookup on the 'host' target.
- **-n** Retrieve netcraft.com data concerning the host, this includes Operating System, Web Server release and UpTime information where available
- **-s** Perform a Sub Domain search on the specified target
- **-e** Perform an Email Address search on the specified target
- **-p** Perform a TCP Portscan on the host target

Ex: dmitry -w example-host.com
dmitry -winsepo sometextfile.txt example-host.com
dmitry -winsepfbo 127.0.0.1

UNIT - III

6. a) Explain in – detail Privilege escalation process in some sort of attacks. 6 Marks

Ans: Privilege escalation is a common way for attackers to gain unauthorized access to systems within a security perimeter.

Attackers start by finding weak points in an organization's defenses and gaining access to a system. In many cases that first point of penetration will not grant attackers with the level of access or data they need. They will then attempt privilege escalation to gain more permission or obtain access to additional, more sensitive systems.

There are two types of privilege escalation:

- Horizontal privilege escalation—an attacker expands their privileges by taking over another account and misusing the legitimate privileges granted to the other user.
- Vertical privilege escalation—an attacker attempts to gain more permissions or access with an existing account they have compromised. For example, an attacker takes over a regular user account on a network and attempts to gain administrative permissions. This requires more sophistication and may take the shape of an Advanced Persistent Threat.

There are many privilege escalation methods in Windows operating systems. Here is a brief review of three common methods and how you can prevent them.

Access Token Manipulation

- **Attack description**
  Windows users access tokens to determine the owners of running processes. When a process tries to perform a task that requires privileges, the system checks who owns the process and to see if they have sufficient permissions. Access token manipulation involves fooling the system into believing that the running process belongs to someone other than the user who started the process, granting the process the permissions of the other user.
- **Techniques**
  There are three ways to achieve access token manipulation:
- **Duplicating an access token** using the Windows DuplicateToken(Ex) and then using ImpersonateLoggedOnUserfunction or SetThreadToken function to assign the impersonated token to a thread.

- **Creating a new process with an impersonated token** using the DuplicateToken(Ex) function together with the CreateProcessWithTokenW function.
- **Leveraging username and password to create a token** using the LogonUser function. The attacker possesses a username and password, and without logging on, they create a logon session, obtain the new token and use SetThreadToken to assign it to a thread. In this method, an adversary has a username and password, but the user is not logged
- **Mitigation**
  There is no way to disable access tokens in Windows. However, to perform this technique an attacker must already have administrative-level access. The best way to prevent the attack is to assign administrative rights in line with the least-privilege principle, regularly review administrative accounts and revoke them if access is no longer needed. Also, monitor privileged accounts for any sign of anomalous behavior.
-

Bypass User Account Control

- **Attack description**
  The Windows user account control (UAC) mechanism creates a distinction between regular users and administrators. It limits all applications to standard user permissions unless specifically authorized by an administrator, to prevent malware from compromising the operating system. However, if UAC protection is not at the highest level, some Windows programs can escalate privileges, or execute COM objects with administrative privileges.
- **Mitigation**
  Review IT systems and ensure UAC protection is set to the highest level, or if this is not possible, apply other security measures. Regularly review which accounts are a local administrator group on sensitive systems and remove regular users who should not have administrative rights. ---6 Marks

6. b) What is a DOS? Discuss different DOS attacks. 6 Marks

Ans: [DoS – 2 Marks, any three attacks - 4 Marks]

Denial of Service (DoS) is an attack on a computer or network that reduces, restricts or prevents accessibility of system resources to its legitimate users. In a DoS attack, attackers flood a victim system with non-legitimate service requests or traffic to overload its resources. DoS attack leads to unavailability of a particular website and show network performance.

Basic Categories of DoS Attack Vectors

Volumetric Attacks: Consumes the bandwidth of target network or service.

Fragmentation Attacks: Overwhelms target's ability of re-assembling the fragmented packets.

TCP State-Exhaustion Attacks: Consumes the connection state tables present in the network infrastructure components such as load-balancers, firewalls, and application servers.

Application Layer Attacks: Consumes the application resources or service thereby making it unavailable to other legitimate users.

DoS Attack Techniques

Bandwidth Attacks and Service Request Floods
SYN Flooding Attack
ICMP Flood Attack
Peer-to-Peer Attacks
Application-Level Flood Attacks
Permanent Denial-of-Service Attack
Distributed Reflection Denial of Service (DrDoS)

Service Request Floods:
An attacker or group of zombies attempts to exhaust server resources by setting up and tearing down TCP connections. Service request flood attacks flood servers with a high rate of connections from a valid source.
It initiates a request on every connection.

SYN Attack:
The attacker sends a large number of SYN request to target server (victim) with fake source IP addresses.
The target machine sends back a SYN/ACK in response to the request and waits for the ACK to complete the session setup. The target machine does not get the response because the source address is fake.

ICMP Flood Attack:
ICMP flood attack is a type DoS attack in which perpetrators send a large number of ICMP packets directly or through reflection networks to victims causing it to be overwhelmed and subsequently stop responding to legitimate TCP/IP requests. To protect against ICMP flood attack, set a threshold limit that when exceeds invokes the ICMP flood attack protection feature.

Permanent Denial-of-Service (PDoS) Attack
Phlashing: Permanent DoS, also known as phlashing, refers to attacks that cause irreversible damage to system hardware.
Sabotage: Unlike other DoS attacks, it sabotages the system hardware, requiring the victim to replace or reinstall the hardware.
Bricking a system: This attack is carried out using a method known as "bricking a system" Using this method, attackers send fraudulent hardware updates to the victims.

Distributed Reflection Denial of Service (DRDoS) : A distributed reflected denial of service attack (DRDoS), also known as spoofed attack, involves the use of multiple intermediary and secondary machines that contribute to the actual DDoS attack against the target machine or application. Attacker launches this attack by sending requests to the intermediary hosts, these requests are then redirected to the secondary machines which in turn reflects the attack traffic to the target.

7. a) Explain key – logger and social engineering password attacks.
Ans: [key logger -3 Marks, Social engineering - 3 Marks]
Keyloggers are a type of monitoring software designed to record keystrokes made by a user. One of the oldest forms of cyber threat, these keystroke loggers record the information you type into a website or application and send to back to a third party.

Criminals use keyloggers to steal personal or financial information such as banking details, which they can then sell or use for profit. However, they also have legitimate uses within businesses to troubleshoot, improve user experience, or monitor employees. Law enforcement and intelligence agencies also use keylogging for surveillance purposes.

Attack tactics like phishing and social engineering are some of the common ways keyloggers are installed. But there is another way this software can find its way to your computer. Imagine a scenario where you make your way to a file sharing site and choose a software download. While doing so, you get something extra in the – your software came bundled with a keylogger. This way a keylogger can infiltrate your “safe” computer.

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Social engineering attacks happen in one or more steps. A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack. Then, the attacker moves to gain the victim's trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources.

Phishing

As one of the most popular social engineering attack types, phishing scams are email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims. It then prods them into revealing sensitive information, clicking on links to malicious websites, or opening attachments that contain malware.

An example is an email sent to users of an online service that alerts them of a policy violation requiring immediate action on their part, such as a required password change. It includes a link to an illegitimate website—nearly identical in appearance to its legitimate version—prompting the unsuspecting user to enter their current credentials and new password. Upon form submittal the information is sent to the attacker.

7. b) Describe and discuss the different malwares. 6 Marks

Ans: [Decribe – 2 Mark, any three – 4 Marks]

The contraction of malicious software known as malware. Malware is any piece of software that is designed with the intent to damage, disrupt or gain unauthorized access to your device and inflict harm to data and/or people in multiple ways. It is one of the biggest threats on the internet and it comes in a bewildering variety of forms, each with its own method of delivery.

Malware discussion typically encompasses three main aspects:

- Objective: What the malware is designed to achieve
- Delivery: How the malware is delivered to the target
- Concealment: How the malware avoids detection (this item is beyond the scope of this discussion)

1. Worms

- Worms are spread via software vulnerabilities or phishing attacks. Once a worm has installed itself into your computer's memory, it starts to infect the whole machine and in some cases… your whole network.
- Depending on the type of worm and your security measures, they can do serious damage. These parasitic nasties can…
- **Modify and delete files**
- **Inject malicious software onto computers**
- **Replicate themselves over and over to deplete system resources**
- **Steal your data**
- **Install a convenient backdoor for hackers**

They can infect large numbers of computers fast, consuming bandwidth and overloading your web server as they go.

2. Viruses

- Unlike worms, viruses need an already-infected active operating system or program to work. Viruses are typically attached to an executable file or a word document.

- Most people are probably aware that a .exe file extension could lead to issues if it's not from a trusted source. But there are hundreds of other file extensions that denote an executable file.

Usually spread via infected websites, file sharing, or email attachment downloads, a virus will lie dormant until the infected host file or program is activated. Once that happens, the virus is able to replicate itself and spread through your systems.

3. Bots & Botnets
   - A bot is a computer that's been infected with malware so it can be controlled remotely by a hacker.
   - That bot (aka a zombie computer), can then be used to launch more attacks or to become part of a collection of bots (aka a botnet).
   - Botnets are popular with hacker show-offs (the more bots you collect, the mightier a hacker you are) and cyber criminals spreading ransomware. Botnets can include millions of devices as they spread undetected.

4. Trojan Horses
   - Just as it sounds, a Trojan Horse is a malicious program that disguises itself as a legitimate file. Because it looks trustworthy, users download it and… hey presto, in storms the enemy.
   - Trojans themselves are a doorway. Unlike a worm, they need a host to work. Once you've got the Trojan on your device, hackers can use it to.

5. Ransomware
   - Ransomware denies or restricts access to your own files. Then it demands payment (usually with crypto-currencies) in return for letting you back in.
   - In May 2017, a ransomware attack spread across 150 countries and compromised over 200k computers within just one day. Aptly named WannaCry, the attack caused damage estimated in the hundreds of millions to billions of dollars.
6. Adware & Scams
   - Adware is one of the better-known types of malware. It serves pop-ups and display ads that often have no relevance to you.
   - Some users will put up with certain types of adware in return for free software (games for example). But not all adware is equal. At best, it's annoying and slows down your machine.

UNIT - IV

8. a) What is Buffer overflow? Explain different Buffer overflow issues. 6 Marks

Ans:

Buffers are memory storage regions that temporarily hold data while it is being transferred from one location to another. A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations.

For example, a buffer for log-in credentials may be designed to expect username and password inputs of 8 bytes, so if a transaction involves an input of 10 bytes (that is, 2 bytes more than expected), the program may write the excess data past the buffer boundary.

Buffer overflows can affect all types of software. They typically result from malformed inputs or failure to allocate enough space for the buffer. If the transaction overwrites executable code, it can cause the program to behave unpredictably and generate incorrect results, memory access errors, or crashes.

Buffer Overflow Attack: Attackers exploit buffer overflow issues by overwriting the memory of an application. This changes the execution path of the program, triggering a response that damages files or exposes private information. For example, an attacker may introduce extra code, sending new instructions to the application to gain access to IT systems.

If attackers know the memory layout of a program, they can intentionally feed input that the buffer cannot store, and overwrite areas that hold executable code, replacing it with their own code. For example, an attacker can overwrite a pointer (an object that points to another area in memory) and point it to an exploit payload, to gain control over the program.

Types of Buffer Overflow Attacks

- Stack overflow attack - This is the most common type of buffer overflow attack and involves overflowing a buffer on the call stack*.
- Heap overflow attack - This type of attack targets data in the open memory pool known as the heap*.
- Integer overflow attack - In an integer overflow, an arithmetic operation results in an integer (whole number) that is too large for the integer type meant to store it; this can result in a buffer overflow.
- Unicode overflow - A unicode overflow creates a buffer overflow by inserting unicode characters into an input that expect ASCII characters. ----6 Marks

8. b) Discuss in – detail Improper error handling and exception management. 6 Marks

Ans:

Improper error handling: ----3 Marks

- Improper handling of errors can introduce a variety of security problems for a web site. The most common problem is when detailed internal error messages such as stack traces, database dumps, and error codes are displayed to the user (hacker).
- These messages reveal implementation details that should never be revealed. Such details can provide hackers important clues on potential flaws in the site and such messages are also disturbing to normal users.
- Web applications frequently generate error conditions during normal operation. Out of memory, null pointer exceptions, system call failure, database unavailable, network timeout, and hundreds of other common conditions can cause errors to be generated.
- These errors must be handled according to a well thought out scheme that will provide a meaningful error message to the user, diagnostic information to the site maintainers, and no useful information to an attacker.
- One common security problem caused by improper error handling is the fail-open security check. All security mechanisms should deny access until specifically granted, not grant access until denied, which is a common reason why fail open errors occur.
- Other errors can cause the system to crash or consume significant resources, effectively denying or reducing service to legitimate users.
- Good error handling mechanisms should be able to handle any feasible set of inputs, while enforcing proper security. Simple error messages should be produced and logged so that their cause, whether an error in the site or a hacking attempt, can be reviewed.

- Error handling should not focus solely on input provided by the user, but should also include any errors that can be generated by internal components such as system calls, database queries, or any other internal functions.

Exception management:

Exceptions to any information security policies or procedures should be reviewed and approved by the senior management. Exceptions should be managed accordingly. In most cases, exceptions could be provided for the following:

- Legacy systems
- Third party applications
- Proprietary systems
- Physical security
- Emergencies
- Legal situations

Examples of exceptions:

- A specialized application may be configured to require passwords that do not meet password policy requirements.
- A proprietary business system only allows for one administrator ID; however, multiple individuals support this system. Administrators must share this ID to manage the system.
- Some mobile device operating systems do not have the ability to meet the network device attachment requirements.
- A legacy system that does not meet the technical requirements.
- A lawsuit requires retaining information above and beyond the retention procedure.
- An emergency situation takes place that requires a workforce member to use the credentials of another workforce member to cover a time-critical business operation.

9. a) Explain in – detail SQL injection attack with example. ----6 Marks

Ans:

SQL injection is a technique used to take advantage of non-validated input vulnerabilities to pass SQL commands through a web application for execution by a backend database. SQL injection is a basic attack used to either gain unauthorized access to a database or to retrieve information directly from the database. It is a flaw in web applications and not a database or web server issue.

Types of SQL Injection:

Error Based SQL Injection:

UNION SQL Injection
System Stored Procedure
Tautology
End of Line Comment
Illegal/Logically Incorrect Query

Blind SQL Injection:

Time Delay
Boolean Exploitation

Error-Based SQL Injection:

Attackers intentionally insert bad input into an application, causing it to throw database errors. The attacker reads the database-level error messages that result in order to find an SQL injection vulnerability in the application. Based on this, the attacker then injects SQL queries that are specifically designed to compromise the data security of the application.

Blind SQL Injection:

The attacker has no error messages from the system with which to work.Instead, the attacker simply sends a malicious SQL query to the database.

Example:

The user is then authenticated and redirected to the requested page.

When the attacker enters blah' or 1=1 -- then the SQL query will look like: SELECT Count(*) FROM Users WHERE UserName='blah' Or 1=1 --' AND Password='' Because a pair of hyphens designate the beginning of a comment in SQL, the query simply becomes: SELECT Count(*) FROM Users WHERE UserName='blah' Or 1=1 string strQry = "DELCET Count(*) FROM Users WHERE UserName='" + txtUser.Text + "' AND Password='" + txtPassword.Text + "'";

Attacker Launching SQL Injection:

blah'; DROP TABLE Creditcard; --

SQL Query Executed:

SELECT jb-email, jb-passwd, jb-login_id, jb-last_name FROM members WHERE jb-email = ' blah'; DROP TABLE Creditcard; --

9. b) Describe and discuss different Security misconfigurations in different applications. 6 Marks

Ans: Security misconfiguration is the implementation of improper security controls, such as for servers or application configurations, network devices, etc. that may lead to security vulnerabilities.

For example, insecure configuration of web applications could lead to numerous security flaws including:

- Incorrect folder permissions
- Default passwords or username
- Setup/Configuration pages enabled
- Debugging enabled

A security misconfiguration could range from forgetting to disable default platform functionality that could grant access to unauthorized users such as an attacker to failing to establish a security header on a web server. Security misconfiguration can happen at any level of an application, including the web server, database, application server, platform, custom code, and framework. The impact of a security misconfiguration in your web application can be far reaching and devastating. According to Microsoft, cyber security breaches can now globally cost up to $500 billion per year, with an average breach costing a business $3.8 million.

Security Misconfiguration Examples:

- To give you a better understanding of potential security misconfigurations in your web application, here are some of the best examples:

Example #1: Default Configuration Has Not Been Modified / Updated

- If you have not changed the configuration of your web application, an attacker might discover the standard admin page on your server and log in using the default credentials and perform malicious actions.

Example #2: Directory Listing is Not Disabled on Your Server

In such cases, if an attacker discovers your directory listing, they can find any file. Hackers can find and download all your compiled Java classes, which they can reverse engineer to get your custom code. They can then exploit this security control flaw in your application and carry out malicious attacks.

Example #3: Insecure Server Configuration Can Lead Back to the Users, Exposing Their Personal Information

Applications with security misconfigurations often display sensitive information in error messages that could lead back to the users. This could allow attackers to compromise the sensitive data of your users and gain access to their accounts or personal information

Example #4: Sample Applications Are Not Removed From the Production Server of the Application

Many times these sample applications have security vulnerabilities that an attacker might exploit to access your server.

Example #5: Default Configuration of Operating System (OS)

The default configuration of most operating systems is focused on functionality, communications, and usability. If you have not updated or modified the default configuration of your OS, it might lead to insecure servers.

Scheme prepared by Signature of the HOD, IT Dept.

Paper Evaluators:

S.No	Name Of the College	Name of the Faculty	Signature