# 18IT702

**Hall Ticket Number:**

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |

**IV/IV B.Tech (Regular/Supplementary) DEGREE EXAMINATION**

**November,2022** **Information Technology**

**Seventh Semester** **Advanced Cyber Security**

**Time:** Three Hours **Maximum: 5**0 Marks

*Answer Question No. 1 Compulsorily.* (10X1 = 10 Marks)

*Answer **ANY ONE** question from each Unit.* (4X10=40 Marks)

| | | | | |
|---|---|---|---|---|
| 1. | a) | Define Vulnerability? | CO1(BL1) | 1M |
| | b) | Sniffing and eavesdropping are passive or active attack justify it. | CO1(BL3) | 1M |
| | c) | What are the limitations of firewall? | CO2(BL1) | 1M |
| | d) | What is a Malicious software? Give any two examples. | CO2(BL1) | 1M |
| | e) | What is the use of Nmap? | CO2(BL1) | 1M |
| | f) | What are the types of enumerations? | CO1(BL1) | 1M |
| | g) | List out any two password cracking tools. | CO3(BL1) | 1M |
| | h) | Give short notes backdoor. | CO3(BL3) | 1M |
| | i) | When will the broken session occur give examples? | CO4(BL2) | 1M |
| | j) | What is meant by Information disclosure? | CO4(BL1) | 1M |
| | | **Unit - I** | | |
| 2. | a) | Define Pen Test? Explain Penetration Testing strategies. | CO1(BL2) | 5M |
| | b) | Distinguish between threat and exploits. | CO1(BL3) | 5M |
| | | **(OR)** | | |
| 3. | a) | What Information Security? Discuss different Information Security objectives and goals. | CO1(BL2) | 5M |
| | b) | Explain in detail different Hackers Motives and Objectives. | CO1(BL2) | 5M |
| | | **Unit - II** | | |
| 4. | a) | Explain how DNS and ARP poisoning happens. | CO2(BL3) | 5M |
| | b) | Discuss Man-in-the-Middle attack scenario with suitable example. | CO2(BL2) | 5M |
| | | **(OR)** | | |
| 5. | a) | What is a Firewall? Discuss different types of firewalls. | CO2(BL2) | 5M |
| | b) | List different Information gathering tools with examples. | CO2(BL1) | 5M |
| | | **Unit - III** | | |
| 6. | a) | Describe and discuss different type of Denial-of-Service attacks. | CO3(BL2) | 5M |
| | b) | When will use the 'Privilege escalation' explain? | CO3(BL3) | 5M |
| | | **(OR)** | | |
| 7. | a) | List various Backdoor attacks with suitable examples. | CO3(BL2) | 5M |
| | b) | What are the types of Password attacks? Explain types of attacks in detail. | CO3(BL1) | 5M |
| | | **Unit - IV** | | |
| 8. | a) | What is meant by Buffer Overflow attack? Explain Buffer over flow issues. | CO4(BL2) | 5M |
| | b) | What is meant by SQL injection attack? Discuss SQL injection in detail. | CO4(BL3) | 5M |
| | | **(OR)** | | |
| 9. | a) | Discuss in detail Security misconfiguration. | CO4(BL2) | 5M |
| | b) | Give difference between error and exception? Discuss Improper error handling and exception management in cyber world. | CO4(BL3) | 5M |

IV/IV B.Tech (Regular) DEGREE EXAMINATION

Advanced Cyber Security (18IT702)

Scheme of Evaluation

Maximum: 60 Marks

1. Write briefly about the following 1*10= 10 Marks

a) Define Vulnerability?
Ans: Vulnerability is a weakness in design, implementation, operation or internal control.

b) Sniffing and eavesdropping are passive or active attacks justify it.
Ans: Sniffing can do passive and active attacks, as like
Active Sniffing: Active sniffing is used to sniff a switch-based network.
Passive Sniffing: Passive sniffing means sniffing through a hub, on a hub the traffic is sent to all ports.
Eavesdropping can do passive and active attacks, as like with passive eavesdropping, the hacker simply "listens" to data that is passing through the network. With active eavesdropping, hackers disguise themselves. This allows them to impersonate a website where users would normally share their private data.

c) What are the limitations of firewall?
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

d) What is a malicious software? Give any two examples.
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. Worms and Trojans.

e) What is the use of Nmap?
Ans: Network administrators can use Nmap for network inventory, managing service upgrade schedules, and monitoring host or service uptime. Attacker uses Nmap to extract information such as live hosts on the network, services, type of packet filters/firewalls, operating systems and OS versions.

f) What are the types of enumerations?
Ans: NetBIOS Enumeration, SNMP enumeration, Lightweight Directory Access Protocol (LDAP) enumeration and Network Time Protocol enumeration.

g) List out any two password cracking tools.
Ans: Medusa, Thuc-Hydra, Cain and Able and Rainbowcrack.

h) Give short notes backdoor.
Ans: The backdoor attack is a type of malware that is used to get unauthorized access to a website by the cybercriminals. The cybercriminals spread the malware in the system through unsecured points of entry, such as outdated plug-ins or input fields.

i) When will the broken session occur give examples?
Ans:

- User authentication credentials are not protected when stored.
- Predictable login credentials.
- Session IDs are exposed in the URL

j) What is meant by Information disclosure?
Ans: Information disclosure, also known as information leakage, is when a website unintentionally reveals sensitive information to its users.

**UNIT- I**

2. a) Define Pen Test? Explain Penetration Testing strategies.
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. **----1 Mark**

**Penetration Testing Phases**

A penetration test typically involves the following phases. Since different types of penetration tests have distinct purposes and scopes, a specific penetration test may focus more heavily on some of these phases or omit others.

**1. Pre-engagement**

In the pre-engagement penetration testing phase, the tester and client define the scope of the penetration test, such as what systems will be tested, what methods the tester will use, and any additional goals and legal implications.

**2. Reconnaissance**

Reconnaissance requires the tester to collect as much information on the testing subject as possible, including personnel, technology, and systems information.

**3. Threat Modeling**

After collecting sufficient information on the client's system, testers then begin modeling realistic threats that the client will face before scanning for the relevant vulnerabilities in the system that those attacks would normally target.

**4. Exploitation**

All identified vulnerabilities are exploited at this stage in accordance with the scope outlined in the pre-engagement phase.

**5. Post-exploitation**

Once the testing time has run out or all relevant systems have been exploited, all testing methods and vulnerabilities—including associated devices, ports, or personnel—are recorded.

**6. Reporting**

The tester generates a penetration testing report for the client that describes the methods that were used, what vulnerabilities were exploited, what remedial actions should be undertaken, and any other relevant information.

**7. Re-testing**

After the client has had time to resolve the vulnerability issues outlined in the initial report, the tester can return to run the same penetration tests on the client's system to verify that the vulnerabilities have been resolved. This phase is not as common but may be requested by the client. **----4 Marks**

2. b) Distinguish between threat and exploits. 5 Marks

Ans:

**Exploit:**

Exploitation is the next step in an attacker's playbook after finding a vulnerability. Exploits are the means through which a vulnerability can be leveraged for malicious activity by hackers; these include pieces of software, sequences of commands, or even open-source exploit kits.

Exploit code for many vulnerabilities is readily available publicly (on the open Internet on sites such as exploit-db.com as well as on the dark web) to be purchased, shared, or used by attackers. (Organized attack groups and nations state actors write their own exploit code and keep it to themselves.) It's important to note that exploit code does not exist for every known vulnerability. Attackers generally take the time to develop exploits for vulnerabilities in widely used products and those that have the greatest potential to result in a successful attack.

**Threat:**

A threat refers to the hypothetical event wherein an attacker uses the vulnerability. The threat itself will normally have an exploit involved, as it's a common way hackers will make their move. A hacker may use multiple exploits at the same time after assessing what will bring the most reward.

There are three categories.

- **Intentional threats:** Things like malware, ransomware, phishing, malicious code, and wrongfully accessing user login credentials are all examples of intentional threats. They are activities or methods bad actors use to compromise a security or software system.
- **Unintentional threats:** Unintentional threats are often attributed to human error. For example, let's say you forgot to lock the back door before leaving for work.
- **Natural threats:** While acts of nature (floods, hurricanes, tornadoes, earthquakes, etc.) aren't typically associated with cybersecurity, they are unpredictable and have the potential to damage your assets.

3. a) What Information Security? Discuss different Information Security objectives and goals.

Ans: Information security refers to the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption. **----1 Mark**

**Objectives and goals:**

- **Confidentiality:** Assurance that the information is accessible only to those authorized to have access. To ensure confidentiality one needs to use all the techniques designed for security like strong password, encryption, authentication and defense against penetration attacks.
- **Integrity:** The trustworthiness of data or resources in terms of preventing improper and unauthorized changes.
- **Availability:** Assurance that the systems responsible for delivering, storing, and processing information are accessible when required by the authorized users. Availability in information security means matching network and computing resources to compute data access and implement a better policy for disaster recovery purposes.

- **Authenticity:** Authenticity refers to the characteristic of a communication, document or any data that ensures the quality of being genuine
- **Non-Repudiation:** Guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message. **----4 Marks**

3. b) Explain in detail different Hackers Motives and Objectives

Ans: [Motives-2 M, Objectives-3 M]

Motives: A motive originates out of the notion that the target system stores or processes something valuable and this leads to threat of an attack on the system.

**Motives Behind Information Security Attacks:**

- Disrupting business continuity
- Information theft
- Manipulating data
- Creating fear and chaos by disrupting critical infrastructures
- Propagating religious or political beliefs
- Achieving state's military objectives
- Damaging reputation of the target
- Taking revenge

**Objectives**

Malware is created with an objective in mind. While it could be said that the objective is "limited only to the imagination of its creator," this will focus on some of the most common objectives observed in malware.

**Exfiltrate Information**

- Stealing data, credentials, payment information, etc. is a recurring theme in the realm of cybercrime. Malware focused on this type of theft can be extremely costly to a person, company, or government target that falls victim.

**Disrupt Operations**

- Actively working to "cause problems" for a target's operation is another objective seen in malware. From a virus on a single computer corrupting critical OS files (making that one system unusable) to an orchestrated, physical self-destruction of many systems in an installation, the level of "disruption" can vary. And there's also the scenario where infected systems are directed to carry out large-scale distributed denial of service attacks

## UNIT - II

4. a) Explain how DNS and ARP poisoning happens.

Ans:

DNS Poisoning: DNS cache poisoning, also known as DNS spoofing, is a type of attack that exploits vulnerabilities in the domain name system (DNS) to divert Internet traffic away from legitimate servers and towards fake ones. One of the reasons DNS poisoning is so dangerous is because it can spread from DNS server to DNS server. **----1 Mark**

DNS spoofing is the resulting threat which mimics legitimate server destinations to redirect a domain's traffic. Unsuspecting victims end up on malicious websites, which is the goal that results from various methods of DNS spoofing attacks.

DNS cache poisoning is a user-end method of DNS spoofing, in which your system logs the fraudulent IP address in your local memory cache. This leads the DNS to recall the bad site specifically for you, even if the issue gets resolved or never existed on the server-end.

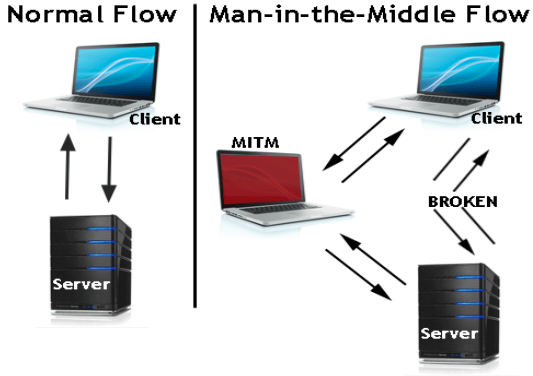
Man-in-the-middle duping: Where an attacker steps between your web browser and the DNS server to infect both. A tool is used for a simultaneous cache poisoning on your local device, and server poisoning on the DNS server. The result is a redirect to a malicious site hosted on the attacker's own local server.

DNS server hijack: The criminal directly reconfigures the server to direct all requesting users to the malicious website. Once a fraudulent DNS entry is injected onto the DNS server, any IP request for the spoofed domain will result in the fake site.**----1.5 Marks**

ARP Poisoning: 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**

ARP Poisoning (also known as ARP Spoofing) is a type of cyber attack carried out over a Local Area Network (LAN) that involves sending malicious ARP packets to a default gateway on a LAN in order to change the pairings in its IP to MAC address table. ARP Protocol translates IP addresses into MAC addresses. Because the ARP protocol was designed purely for efficiency and not for security, ARP Poisoning attacks are extremely easy to carry out as long as the attacker has control of a machine within the target LAN or is directly connected to it.
The attack itself consists of an attacker sending a false ARP reply message to the default network gateway, informing it that his or her MAC address should be associated with his or her target's IP address (and vice-versa, so his or her target's MAC is now associated with the attacker's IP address).
Once the default gateway has received this message and broadcasts its changes to all other devices on the network, all of the target's traffic to any other device on the network travels through the attacker's computer, allowing the attacker to inspect or modify it before forwarding it to its real destination. Because ARP Poisoning attacks occur on such a low level, users targeted by ARP Poisoning rarely realize that their traffic is being inspected or modified. Besides Man-in-the-Middle Attacks, ARP Poisoning can be used to cause a denial-of-service condition over a LAN by simply intercepting or dropping and not forwarding the target's packets. **---1.5 Marks**

4. b) Discuss Man-in-the-Middle attack scenario with suitable example.
Ans: A man-in-the-middle attack is a type of cyber attack where a malicious actor inserts him/herself into a conversation between two parties, impersonates both parties and gains access to information that the two parties were trying to send to each other. A man-in-the-middle attack allows a malicious actor to intercept, send and receive data meant for someone else, or not meant to be sent at all, without either outside party knowing until it is too late.



Key Concepts of a Man-in-the-Middle Attack:

Man-in-the-middle is a type of eavesdropping attack that occurs when a malicious actor inserts himself as a relay/proxy into a communication session between people or systems. A MITM attack exploits the real-time processing of transactions, conversations or transfer of other data. **----3 Marks**

**Example:**

Man-in-the-middle attack in DNS: Where an attacker steps between your web browser and the DNS server to infect both. A tool is used for a simultaneous cache poisoning on your local device, and server poisoning on the DNS server. The result is a redirect to a malicious site hosted on the attacker's own local server.

Man-in-the- Middle Attack in Session Hijacking:

The man-in-the-middle attack is used to intrude into an existing connection between systems and to intercept messages being exchanged. Attackers use different techniques and split the TCP connection into two connections.

1. Client-to-attacker connection
2. Attacker-to-server connection

After the successful interception of TCP connection, an attacker can read, modify, and insert fraudulent data into the intercepted communication. In the case of an http transaction, the TCP connection between the client and the server becomes the target. **----2 Marks**

5. a) What is a Firewall? Discuss different types of firewalls.

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. Firewalls examine all messages entering or leaving the Intranet and block those that do not meet the specified security criteria. Firewalls may be concerned with the type of traffic or with the source or destination addresses and ports. **-----1 Mark**

Types of Firewall:

Packet Filters

Circuit Level Gateways

Application Gateways

Stateful Multilayer Inspection Firewalls

**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.

**Circuit-Level Gateway Firewall:** Circuit-level gateways work at the session layer of the OSI model (or the TCP layer of TCP/IP) Information passed to a remote computer through a circuit-level gateway appears to have originated from the gateway. They monitor requests to create sessions, and determine if those sessions will be allowed. Circuit proxy firewalls allow or prevent data streams, they do not filter individual packets.

**Application-Level Firewall:** Application-level gateways (proxies) can filter packets at the application layer of the OSI model (or the application layer of TCP/IP). Incoming and outgoing traffic is restricted to services supported by proxy; all other service requests are denied. Application-level gateways configured

as a web proxy prohibit FTP, gopher, telnet, or other traffic. Application-level gateways examine traffic and filter on application-specific commands such as http:post and get.

**Stateful Multilayer Inspection Firewall:** Stateful multilayer inspection firewalls combine the aspects of the other three types of firewalls. They filter packets at the network layer of the OSI model (or the IP layer of TCP/IP), to determine whether session packets are legitimate, and they evaluate the contents of packets at the application layer. **------- 4 Marks (any Two)**

5. b) List different Information gathering tools with examples.

Ans: [any 2: 2.5 Marks]

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

Sample Examples.

**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)

Sample Examples.

**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]

Sample Examples.

**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) Describe and discuss different type of Denial-of-Service attacks. 5 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.

6. b) When will use the 'Privilege escalation' explain? 5 Marks

Ans: 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

**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.

7. a) List various Backdoor attacks with suitable examples.

Ans: The backdoor attack is a type of malware that is used to get unauthorized access to a website by the cybercriminals. The cybercriminals spread the malware in the system through unsecured points of entry, such as outdated plug-ins or input fields.

Web server backdoors are used for a number of malicious activities, including:

- Data theft
- Website defacing
- Server hijacking
- The launching of distributed denial of service (DDoS) attacks
- Infecting website visitors (watering hole attacks)
- Advanced persistent threat (APT) assaults

**How to protect:** Good news bad news. The bad news is that it's difficult to identify and protect yourself against built-in backdoors. More often than not, the manufacturers don't even know the backdoor is there. The good news is that there are things you can do to protect yourself from the other kinds of backdoors.

1. Change your default passwords
2. Monitor network activity

3. Choose applications and plug-ins carefully
4. Use a good cyber security solutions **-----5 Marks**

7. b) What are the types of Password attacks? Explain types of attacks in detail. 5 Marks

Ans: Most widely used types of attacks are

**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.

Password sniffing:

Some password crackers can sniff authentication traffic between a client and server and extract password hashes or enough authentication information to begin the cracking process.

**Password Capturing:**

Many attackers capture passwords simply by installing a keyboard-sniffing Trojan horse or one of the many physical keyboard-logging hardware devices for sale on the Internet. Symantec reports that 82 percent of the most commonly used malware programs steal confidential information.

**Password Cracking:**

It is the process of recovering passwords from data that has been stored in or transmitted by a computer system. A common approach (brute-force attack) is to repeatedly try guesses for the password and to check them against an available cryptographic hash of the password. The purpose of password cracking might be to help a user recover a forgotten password (installing an entirely new password is less of a security risk, but it involves System Administration privileges), to gain unauthorized access to a system, or to act as a preventive measure whereby system administrators check for easily crackable passwords.

Additional Types:

**1. Brute Force Attack**

- One of the most common forms of password attack methods, and the easiest for hackers to perform. In fact, inexperienced hackers favor this method precisely because of this.
- In a brute force attack, a hacker uses a computer program to login to a user's account with all possible password combinations. Moreover, brute force accounts don't start at random; instead, they start with the easiest-to-guess passwords.

**2. Dictionary Attack**

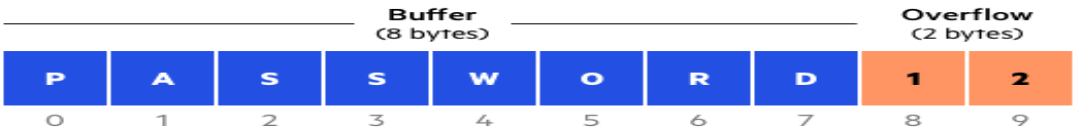
- Conversely, a dictionary attack allows hackers to employ a program which cycles through common words. A brute force attack goes letter by letter, whereas a dictionary attack only tries possibilities most likely to succeed.
- Also, dictionary attacks rely on a few key factors of users' psychology. For example, users tend to pick short passwords and base their passwords off common words. So a dictionary attack starts with those words and variations (adding numbers at the end, replacing letters with numbers, etc.).

## UNIT - IV

8. a) What is meant by Buffer Overflow attack? Explain Buffer over flow issues. 5 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.

8. b) What is meant by SQL injection attack? Discuss SQL injection in detail. 5 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. a) Discuss in detail Security misconfiguration. ----5 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.

9. b) Give difference between error and exception? Discuss Improper error handling and exception management in cyber world. ----5 Marks

Ans: Difference between error and exception is error can occur based on statement either syntax or semantic and exception can occur based on input of data

**Improper error handling:**

- 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. **-----4 Marks**

Scheme prepared by Signature of the HOD, IT Dept.

Paper Evaluators:

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