UNIT 4: Cyber Security Attacks and Vulnerabilities

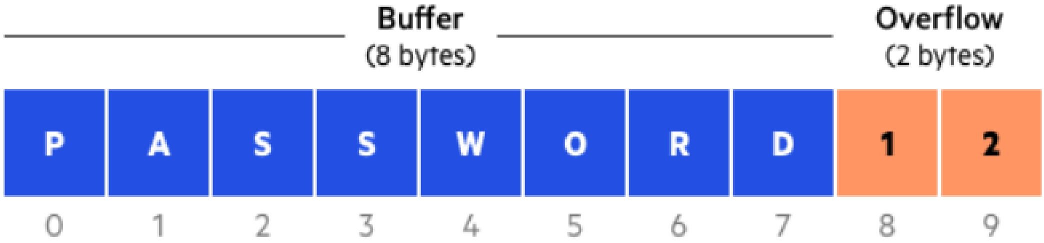
1. What is buffer overflow, explain with a diagram? What are the types of buffer overflow attacks?

Buffer Overflow

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 example

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-based buffer overflows are more common, and leverage stack memory that only exists during the execution time of a function.
- Heap-based attacks are harder to carry out and involve flooding the memory space allocated for a program beyond memory used for current runtime operations.

2. What is system hacking? Explain Linux and Windows Hacking.

System Hacking

System hacking is a vast subject that consists of hacking the different software-based technological systems such as laptops, desktops, etc. System hacking is defined as the compromise of computer systems and software to access the target computer and steal or misuse their sensitive information. Here the malicious hacker exploits the weaknesses in a computer system or network to gain unauthorized access to its data or take illegal advantage.

Linux Hacking

As we all know, Linux is an Operating System (OS) assembled user the model of open-source software development and distribution and is based on Unix OS created by Linus Torvalds.
Now to hack a Linux-based computer system and get access to a password protected Linux system, we have to know Linux's basic file structure. As we know,

Linux is considered to be the most secure OS to be hacked or cracked, but in the world of Hacking, nothing is 100% secured.
Hackers usually use the following techniques to hack the Windows system.

- Hack Linux using the SHADOW file.
- Another technique commonly used by hackers is to bypass the user password option in Linux.
- In another technique, the hacker detects the bug on Linux distribution and tries to take advantage of it.

Windows Hacking

The user password of Windows OS, which appears after the Windows starts logging in, lets users protect the computer from getting unauthorized access. Choosing a strong password of more than eight digits is an excellent practice. Henceforth you can protect your files and folders from the hands of malicious users. There are several tricks and techniques to crack a windows password. But, from the hacker's point of view, if you can use social engineer your victim and find a Windows computer open, you can easily modify the existing password and give a new password that will be unaware of the victim or the owner of the computer.

3. What can the attackers do after compromising the system?

- Ruin the victim's data by deleting the files.
- Steal files and folders.
- Hijack victim's username and password.
- Steal money and credit card details while the victim is doing e-marketing or online transaction.
- Sell victim's information to third parties who may use this information for illicit purposes.
- Create traffic to shut down your website.
- Get access to the servers and manipulate the files, programs, etc.

4. **What is Eavesdropping and Explain any two Eavesdropping methods.**

Eavesdropping

An eavesdropping attack occurs when a hacker intercepts, deletes, or modifies data that is transmitted between two devices. Eavesdropping, also known as sniffing or snooping, relies on unsecured network communications to access data in transit between devices.

Eavesdropping Methods are:

Pickup Device

Attackers can use devices that pick-up sound or images, such as microphones and video cameras, and convert them into an electrical format to eavesdrop on targets. Ideally, it will be an electrical device that uses power sources in the target room, which eliminates the need for the attacker to access the room to recharge the device or replace its batteries.

Some listening devices are capable of storing digital information and transmitting it to a listening post. Attackers may also use mini amplifiers that enable them to remove background noise.

Transmission Link

A transmission link between a pickup device and the attacker’s receiver can be tapped for eavesdropping purposes. This can be done in the form of a radiofrequency transmission or a wire, which includes active or unused telephone lines, electrical wires, or ungrounded electrical conduits. Some transmitters can operate continuously, but a more sophisticated approach involves remote activation.

Listening Post

A listening post is used to transmit conversations intercepted by bugs on telephones. When a telephone is picked up to make or take a call, it triggers a recorder that is automatically turned off when the call is ended.

Listening posts are secure areas in which signals can be monitored, recorded, or retransmitted by the attacker for processing purposes. It can be located anywhere from the next room to the telephone up to a few blocks away. The listening post will have voice-activated equipment available to eavesdrop on and record any activity.

Weak Passwords

Weak passwords make it easier for attackers to gain unauthorized access to user accounts, which gives them a route into corporate systems and networks. This includes hackers being able to compromise confidential communication channels, intercept activity and conversations between colleagues, and steal sensitive or valuable business data.

Open Networks

Users who connect to open networks that do not require passwords and do not use encryption to transmit data provide an ideal situation for attackers to eavesdrop. Hackers can monitor user activity and snoop on communications that take place on the network.

5. **Explain DoS, DDoS and PoD attacks.**

DOS and DDOS

A DoS attack tries to make a web resource unavailable to its users by flooding the target URL with more requests than the server can handle. That means that during the attack period, regular traffic on the website will be either slowed down or completely interrupted.

A Distributed Denial of Service (DDoS) attack is a DoS attack that comes from more than one source at the same time. A DDoS attack is typically generated using thousands (potentially hundreds of thousands) of unsuspecting zombie machines. The machines used in such attacks are collectively known as “botnets” and will have previously been infected with malicious software, so they can be remotely controlled by the attacker. According to research, tens of millions of computers are likely to be infected with botnet programs worldwide.

Ping of Death

Ping of Death (a.k.a. PoD) is a type of Denial of Service (DoS) attack in which an attacker attempts to crash, destabilize, or freeze the targeted computer or service by sending malformed or oversized packets using a simple ping command.

While PoD attacks exploit legacy weaknesses, which may have been patched in target systems. However, in an unpatched system, the attack is still relevant and dangerous. Recently, a new type of PoD attack has become popular. This attack, commonly known as a Ping flood, the targeted system is hit with ICMP packets sent rapidly via ping without waiting for replies

6. What is password cracking and Explain any 3 Malware Attack types.

Password Cracking

Password cracking refers to various measures used to discover computer passwords. This is usually accomplished by recovering passwords from data stored in, or transported from, a computer system. Password cracking is done by either repeatedly guessing the password, usually through a computer algorithm in which the computer tries numerous combinations until the password is successfully discovered.

- Password cracking can be done for several reasons, but the most malicious reason is in order to gain unauthorized access to a computer without the computer owner’s awareness. This results in cybercrime such as stealing passwords for the purpose of accessing banking information.

- Other, nonmalicious, reasons for password cracking occur when someone has misplaced or forgotten a password. Another example of nonmalicious password cracking may take place if a system administrator is conducting tests on password strength as a form of security so that hackers cannot easily access protected systems.

Malware Attacks Types

1. Virus
We tend to refer to all malware as viruses, but it’s not so. A virus modifies other legitimate host files in such a way that when you execute a file in the victim’s system, you also execute the virus. Today, with different kinds of malware infecting the cyber world, computer viruses have become rather uncommon; they comprise less than 10% of all malware.

Remember, viruses infect other files, they are the only malware that infect other files and hence it's really hard to clean them up. Even the best among antivirus programs struggle with this; most of the time they either delete or quarantine the infected file and don't get rid of the virus itself.

2. Worm

A worm is self-replicating and spreads without end-user action, causing real devastation. Viruses need end users to kick them off so that they can go on and infect other files and systems. On the other hand, worms don't need any such end-user action. They'd simply spread by themselves, self-replicating in the process and destroying systems, devices, networks and connected infrastructure as well. Worms spread by exploiting other files and programs to do the spreading work. When one person in an organization opens an email that contains a worm, the entire network in the organization could get infected in just a few minutes.

3. Trojan

Trojans, reminding you of what happened during the Trojan war, masquerade as legitimate programs. However, they contain malicious instructions. Trojans mostly arrive via email or spread from infected websites that users visit. They only work when the victim executes it. A user may find a pop up that tells him his system was infected. The pop up would instruct him to run a program to clean his system. He takes the bait, without knowing that it is a Trojan. Trojans are very common, especially because it is easy to write Trojans. Additionally, they are easy because Trojans spread by tricking end-users to execute them. This effectively renders security software useless.

4. Ransomware

Ransomware, as the name suggests, demands a ransom from you to get things back on track. The main issue with ransomware, which would spread tremendously fast across organizations, networks, and countries, is that they encrypt all files in a system or network, rendering them inaccessible. A ransom note pops up, demanding payment in cryptocurrency, for decrypting the files . If the ransom is not paid, the encrypted files could eventually get destroyed and hence ransomware should be seen as one of the most devastating forms of malware. Most ransomware are Trojans and spread through social engineering. Unfortunately, in some cases, hackers refuse to decry-pt files even after you pay the ransom.

5. Adware

Adware is nothing but attempting to expose users to unwanted, potentially malicious advertising. These ads most likely end up infecting a user's device. There are adware programs that redirect a user, during browser searches, to look-alike web pages that have promotions of other products. Removing adware is easier. You just need to find the malicious executable and remove it.

6. Spyware

Spyware, as the name suggests, helps hackers spy on systems and their users. This kind of malware can be used for key-logging and similar activities, thereby helping hackers gain access to personal data (including login credentials) and intellectual property. Spyware is also used by people who want to keep a check on the computer activities of people personally known to them. Spyware, like adware, is easy to remove.