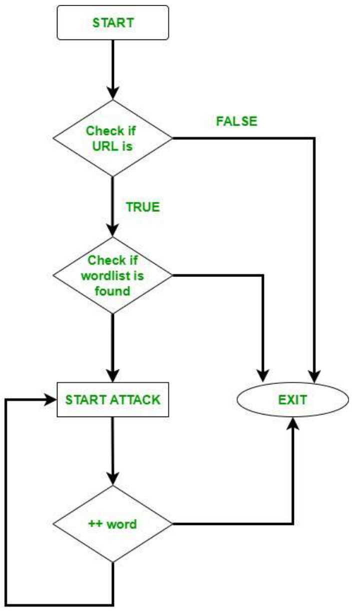
1. Define directory traversal attack.

Properly controlling access to web content is crucial for running a secure web server. Directory traversal or Path Traversal is an HTTP attack that allows attackers to access restricted directories and execute commands outside of the web server's root directory.

Web servers provide two main levels of security mechanisms

- Access Control Lists (ACLs)
- Root directory



An Access Control List is used in the authorization process. It is a list which the web server's administrator uses to indicate which users or groups are able to access, modify or execute particular files on the server, as well as other access rights.

Advantages

1. DirBuster provides a GUI interface, which is obviously very easy to understand and use. DirBuster is often employed by anyone with no hustle.
2. As compared to other Directory Brute-forcing tools, GoBuster is extremely fast. GoBuster has been developed in the Go language & This language is known for speed.

2. How buffer overflow is used to perform malicious activities?

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.

In addition, modern operating systems have runtime protection. Three common protections are:

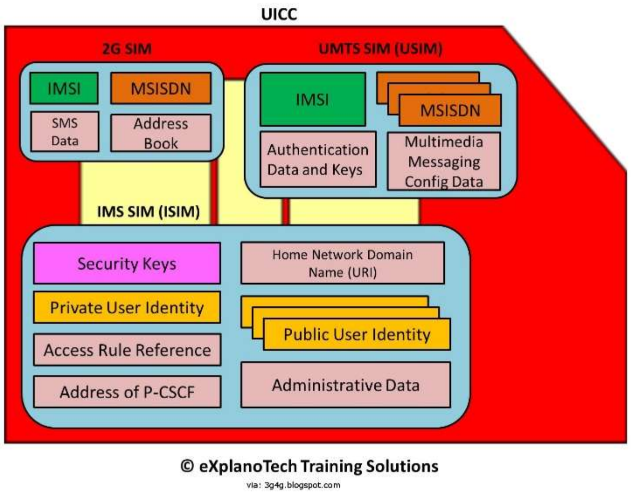
- **Address space randomization (ASLR)**—randomly moves around the address space locations of data regions. Typically, buffer overflow attacks need to know the locality of executable code, and randomizing address spaces makes this virtually impossible.
- **Data execution prevention**—flags certain areas of memory as non-executable or executable, which stops an attack from running code in a non-executable region.
- **Structured exception handler overwrite protection (SEHOP)**—helps stop malicious code from attacking Structured Exception Handling (SEH), a built-in system for managing hardware and software exceptions.

3. Explain SIM/UICC Security.

The Universal Integrated Circuit Card (UICC) is a type of SIM card, a smart card used for mobile terminals/phones utilizing GSM or UMTS networks. The UICC is used to ensure the security and integrity of all kinds of personal data as well as hold information that identifies the user to the wireless operator in order for the latter to know the plans and services associated with the card.

The UICC is a type of smart card technology that has its own processor, software and data storage; so, it is essentially a computer in and of itself. It is essentially an evolution of the subscriber identification module (SIM) card, and, as such, it contains many of the latter's features, such as storing contact details and maintaining a list of preferred networks.

Since the card slot is standardized, a subscriber can easily move their wireless account and phone number from one handset to another. This will also transfer their phone book and text messages. Similarly, usually a subscriber can change carriers by inserting a new carrier's UICC card into their existing handset. However, it is not always possible because some carriers (e.g., in U.S.) SIM-lock the phones that they sell, preventing rival carriers' cards from being used.



4. What is browser exploit?

In cybersecurity, an exploit is a piece of code that utilizes vulnerabilities in computer software or hardware in order to perform malicious actions. These actions may include gaining control of a device, infiltrating a network, or launching some form of cyber attack. A browser exploit is a type of exploit that takes advantage of a web browser vulnerability in order to breach web browser security.

A browser exploit is a form of malicious code that takes advantage of a flaw or vulnerability in an operating system or piece of software with the intent to breach browser security to alter a user's browser settings without their knowledge. Malicious code may exploit ActiveX, HTML, images, Java, JavaScript, and other Web technologies and cause the browser to run arbitrary code.

Prevention

Install firewall software and other security software

Keep all software up to date

Be careful when browsing the web, especially when downloading files

Don’t click on suspicious attachments or links in emails

Use a more secure browser, or remote browser isolation

5. What are canonicalization attacks?

A canonicalization attack is a cyberattack method in which the attacker substitutes various inputs for the canonical name of a path or file.

Canonicalization is the process of mapping inputs to their canonical equivalent. It is often used for cryptographic algorithms and data that are intended to be secured from tampering, usually by hashing. In computer security, a Canonicalization attack aims to find or compute the mapping between two different inputs which produce the same output when processed by a given system.

This attack then seeks ways to manipulate input strings so they both result in an undesired output (such as "war" which can be manipulated into each other by changing just one character). With some algorithms such as MD5, even minor changes in input will result in enormous differences in hash values, making this type of attack relatively easy. A Canonicalization attack is a type of specific-pattern attack.

Key Points:

- This technique is used to steal a victim's data from the server.
- The attacker first creates a domain, usually at different TLDs, for example: .com, .co.uk or .info etc. Then registers a website with that domain name, and finally publishes links to the site from various social media or different blogs around the internet so that it will appear on search engines' results pages for certain keywords searched by users.
- The attacker then waits for users who arrive at their fake site and enter their username/password in order to complete an action (e.g., perform a payment).
- In the case of a payment operation, users would be redirected to the real website of cybercriminals, where they would complete the operation and then immediately be redirected back to the fake website through a cryptocurrency mining script.
- A user can visit any malicious site that is using this technique. Such sites may appear in search engines and social media results, but not on legitimate results pages. The only way to know if it's safe to enter information on such websites is to check for certificate errors: If it gives one, then it's fake.

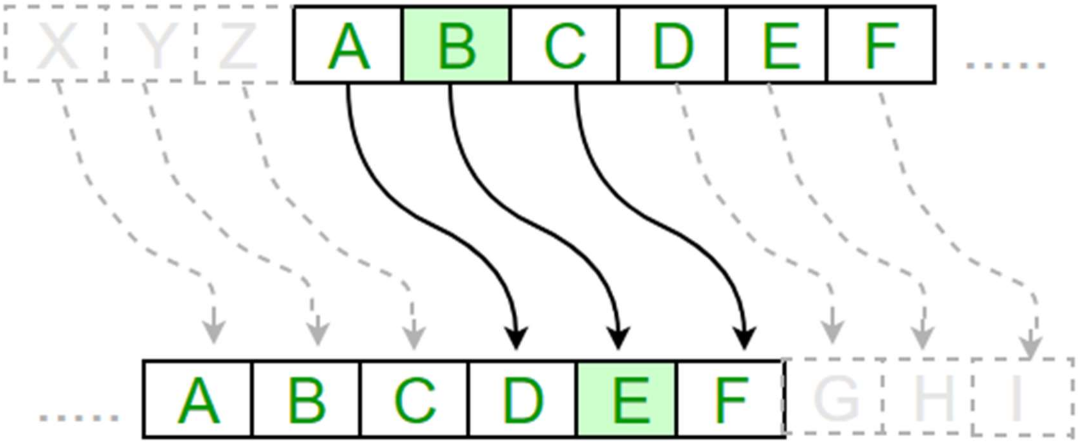
6. Explain Creaser cipher with an example.

The Caesar Cipher technique is one of the earliest and simplest methods of encryption technique. It's simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter with a fixed number of positions down the alphabet.

For example with a shift of 1, A would be replaced by B, B would become C, and so on. The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials.

Thus to cipher a given text we need an integer value, known as a shift which indicates the number of positions each letter of the text has been moved down.

The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,…, Z = 25. Encryption of a letter by a shift n can be described mathematically as.



```
Text : ABCDEFGHIJKLMNOPQRSTUVWXYZ
Shift: 23
Cipher: XYZABCDEFGHIJKLMNOPQRSTUVW

Text : ATTACKATONCE
Shift: 4
Cipher: EXXEGOEXSRGI
```

Algorithm for Caesar Cipher:

Input:

1. A String of lower case letters, called Text.
2. An Integer between 0-25 denoting the required shift.

Procedure:

- Traverse the given text one character at a time .
- For each character, transform the given character as per the rule, depending on whether we’re encrypting or decrypting the text.
- Return the new string generated.

7. Explain encryption and decryption process of Monoalphabetic cipher with an example

Monoalphabetic and Polyalphabetic Cipher

Monoalphabetic cipher is a substitution cipher in which for a given key, the cipher alphabet for each plain alphabet is fixed throughout the encryption process. For example, if ‘A’ is encrypted as ‘D’, for any number of occurrence in that plaintext, ‘A’ will always get encrypted to ‘D’.

All of the substitution ciphers we have discussed earlier in this chapter are monoalphabetic; these ciphers are highly susceptible to cryptanalysis.

Polyalphabetic Cipher is a substitution cipher in which the cipher alphabet for the plain alphabet may be different at different places during the encryption process. The next two examples, **playfair and Vigenere Cipher are polyalphabetic ciphers**.

The substitution cipher is the oldest forms of encryption algorithms according to creates each character of a plaintext message and require a substitution process to restore it with a new character in the ciphertext.

This substitution method is deterministic and reversible, enabling the intended message recipients to reverse-substitute ciphertext characters to retrieve the plaintext.

The specific form of substitution cipher is the Monoalphabetic Substitution Cipher, is known as “Simple Substitution Cipher”. Monoalphabetic Substitution Ciphers based on an individual key mapping function K, which consistently replaces a specific character α with a character from the mapping K (α).

A mono-alphabetic substitution cipher is a type of substitution ciphers in which the equivalent letters of the plaintext are restored by the same letters of the ciphertext.

Mono, which defines one, it signifies that each letter of the plaintext has a single substitute of the ciphertext.

Caesar cipher is a type of Monoalphabetic cipher. It uses the similar substitution method to receive the cipher text characters for each plain text character. In Caesar cipher, it can see that it is simply for a hacker to crack the key as Caesar cipher supports only 25 keys in all. This pit is covered by utilizing Monoalphabetic cipher.

In Monoalphabetic cipher, the substitute characters symbols supports a random permutation of 26 letters of the alphabet. 26! Permutations of the alphabet go up to 4*10^26. This creates it complex for the hacker to need brute force attack to gain the key.

Mono-alphabetic cipher is a type of substitution where the relationship among a symbol in the plaintext and a symbol in the cipher text is continually one-to-one and it remains fixed throughout the encryption process.

These ciphers are considered largely susceptible to cryptanalysis. For instance, if ‘T’ is encrypted by ‘J’ for any number of appearance in the plain text message, then ‘T’ will continually be encrypted to ‘J’.

If the plaintext is “TREE”, thus the cipher text can be “ADOO” and this showcases that the cipher is possibly mono-alphabetic as both the “O”s in the plaintext are encrypted with “E”s in the cipher text.

Although the hacker will not be capable to need brute force attack, it is applicable for consider the key by using the All- Fearsome Statistical Attack. If the hacker understand the characteristics of plaintext of any substitution cipher, then regardless of the size of the key space, it can simply break the cipher using statistical attack. Statistical attack includes measuring the frequency distribution for characters, comparing those with same statistics for English.

8. Discuss polyalphabetic algorithm with example.

A poly-alphabetic cipher is any cipher based on substitution, using several substitution alphabets. In polyalphabetic substitution ciphers, the plaintext letters are enciphered differently based upon their installation in the text. Rather than being a one-to-one correspondence, there is a one-to-many relationship between each letter and its substitutes.

For example, ‘a’ can be enciphered as ‘d’ in the starting of the text, but as ‘n’ at the middle. The polyalphabetic ciphers have the benefit of hiding the letter frequency of the basic language. Therefore attacker cannot use individual letter frequency static to divide the ciphertext.

The first Polyalphabetic cipher was the Alberti Cipher which was introduced by Leon Battista Alberti in the year 1467. It used a random alphabet to encrypt the plaintext, but at different points and it can change to a different mixed alphabet, denoting the change with an uppercase letter in the cipher text.

It can utilize this cipher, Alberti used a cipher disc to display how plaintext letters are associated to cipher text letters. In this cipher, each ciphertext character based on both the corresponding plaintext character and the position of the plaintext character in the message.

As the name polyalphabetic recommend this is achieved by using multiple keys rather than only one key. This implies that the key should be a stream of subkeys, in which each subkey depends somehow on the position of the plaintext character that needs subkey for encipherment.

In other words, it is required to have s key stream k = (K_1, K_2, K_3 ...) in which K_i is used to encipher the ith character in the plaintext to make the i^{th} character in the ciphertext. The best known and simplest of such algorithm is defined as Vigenere cipher.

Vigenere cipher is one of the simplest and popular algorithms in polyalphabetic cipher. In this approach, the alphabetic text is encrypted using a sequence of multiple Caesar ciphers based on the letters of a keyword.

The Caesar cipher restoring each letter in the plaintext with the letters standing constant position to the right in the alphabet. This shift is implemented modulo 26. For instance, in a Caesar cipher of shift 3, A can become D, B can become E and so on.

The Vigenère cipher includes several simple substitution ciphers in sequence with several shift values. In this cipher, the keyword is repeated just before it connects with the duration of the plaintext.

Encryption is implemented by going to the row in the table correlating to the key, and discover the column heading the corresponding letter of the plaintext character; the letter at the intersection of corresponding row and column of the Vigenere Square create the ciphertext character. The rest of the plaintext is encrypted in the similar method.

9. What types of attacks are performed on Apache server? Explain each with their countermeasures.

How Security Disasters Develop

The scenarios you'll face are the following:

- Intruders gaining simple access

- Denial of service
- Defacement or total system seizure

Let's run through the factors that invite these situations.

Intruders Gaining Simple Access

Simple unauthorized access can happen in several ways:

- Insiders who once had authorized access (former employees or developers, for example) return to haunt you.
- Your users make bad password choices on other networks that fall to hackers. This leads to cross-network unauthorized access.
- Your underlying operating system has holes, and diligent hackers exploit it to gain limited access.
- The tools you use in conjunction with Apache are flawed.

Denial-of-Service (DoS) / Distributed Denial-of-service (DDoS)

- Reduce Attack Surface Area
- Plan for Scale
- Know what is normal and abnormal traffic
- Deploy Firewalls for Sophisticated Application attacks

Web Defacement Attack

- Avoid common web vulnerabilities
- Secure your database
- Secure your source code

SSH Brute Force Attack.

- Don't allow root to login
- Don't allow ssh passwords (use private key authentication)
- Don't listen on every interface

Cross-site scripting (XSS)

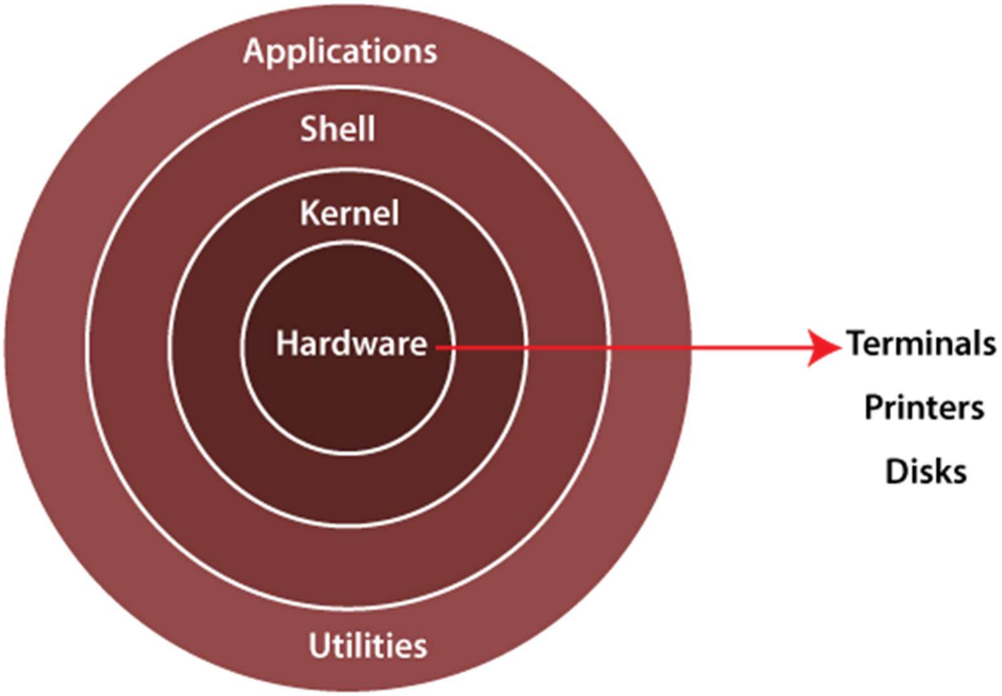
1. Blacklist filtering.
2. Whitelist filtering.
3. Contextual Encoding.
4. Input Validation.
5. Content Security Policy.

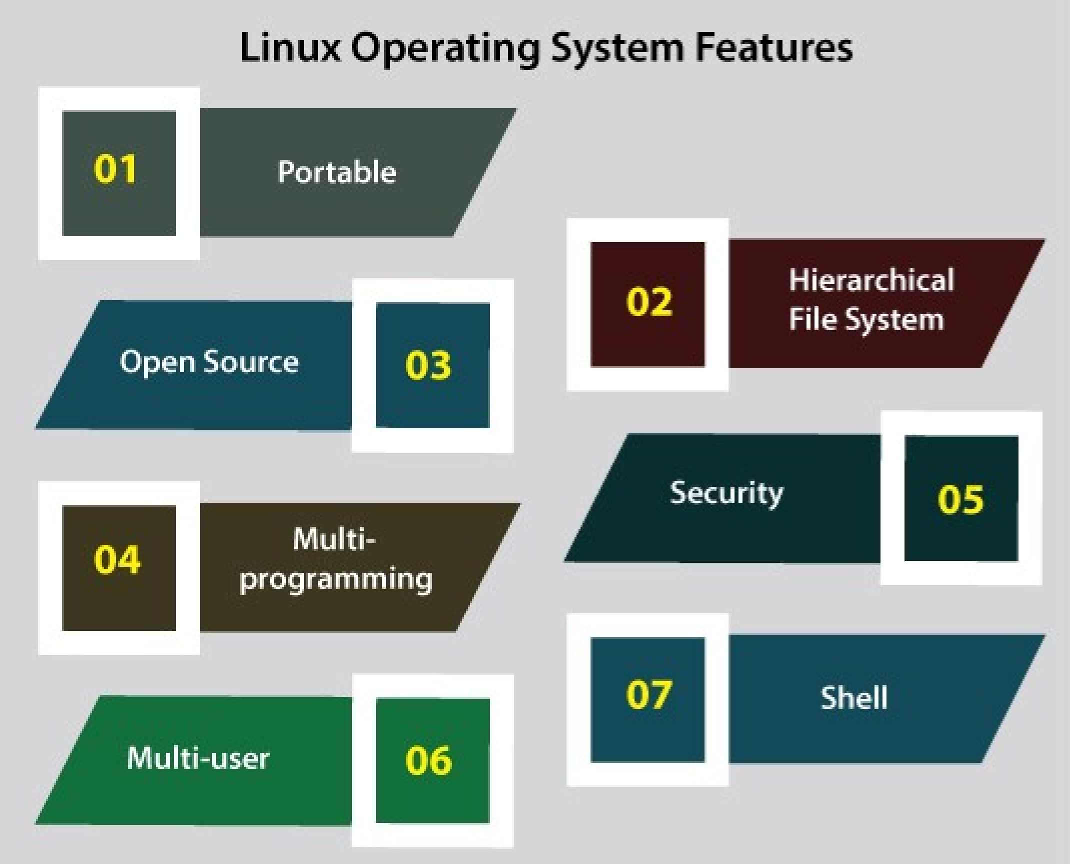
10. Explain features of Window and Linux along with layer architecture. How these platforms are made secure? Explain in detail.

An operating system can be described as an interface among the computer hardware and the user of any computer. It is a group of software that handles the resources of the computer hardware and facilitates basic services for computer programs.

An operating system is an essential component of system software within a computer system. The primary aim of an operating system is to provide a platform where a user can run any program conveniently or efficiently.

On the other hand, Linux OS is one of the famous versions of the UNIX OS. It is developed to provide a low-cost or free OS for several personal computer system users. Remarkably, it is a complete OS Including an **X Window System, Emacs editor, IP/TCP, GUI** (graphical user interface), etc.





Linux Operating System Features

01 Portable

02 Hierarchical File System

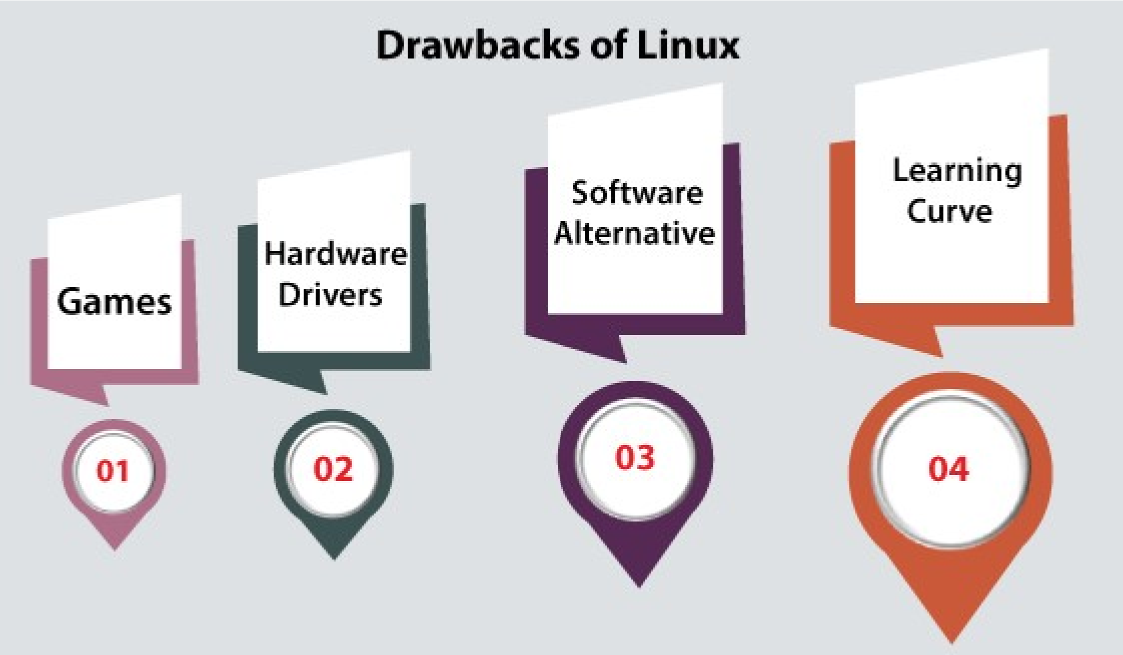
03 Open Source

04 Multi-programming

05 Security

06 Multi-user

07 Shell



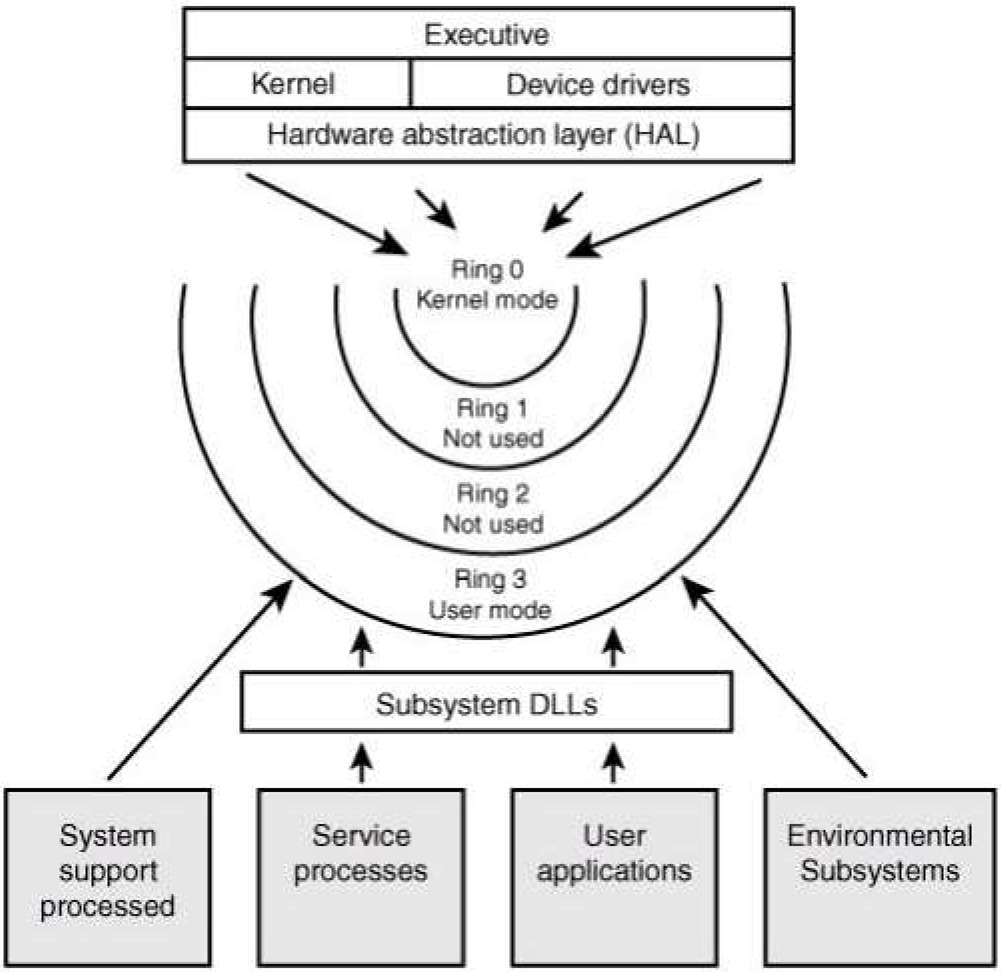
Drawbacks of Linux

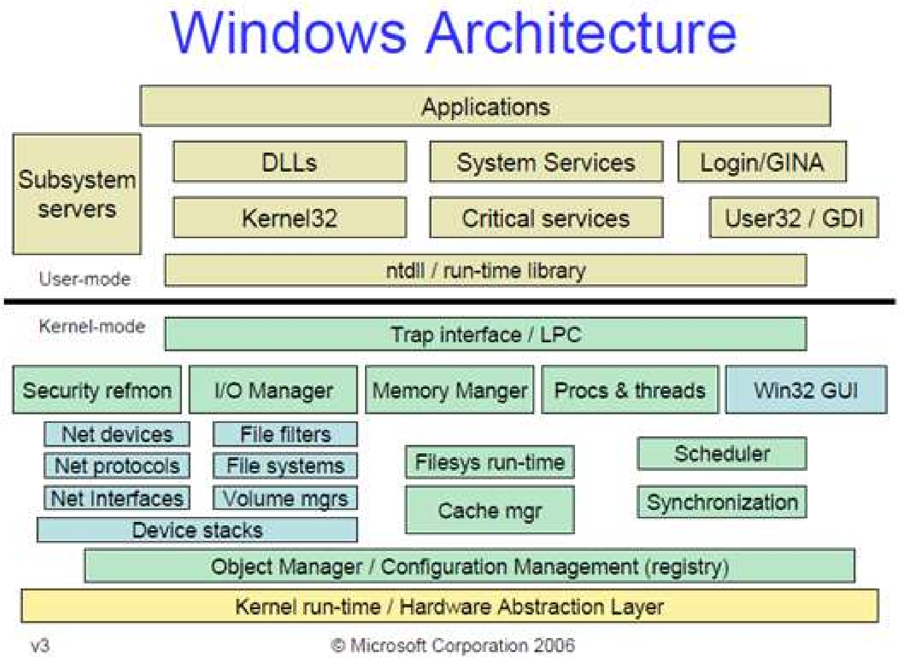
01 Games

02 Hardware Drivers

03 Software Alternative

04 Learning Curve





Windows Architecture

Applications

Subsystem servers

DLLs | System Services | Login/GINA

Kernel32 | Critical services | User32 / GDI

User-mode

ntdll / run-time library

Kernel-mode

Trap interface / LPC

Security refmon | I/O Manager | Memory Manger | Procs & threads | Win32 GUI

Net devices | File filters

Net protocols | File systems | Filesys run-time | Scheduler

Net Interfaces | Volume mgrs | Cache mgr | Synchronization

Device stacks

Object Manager / Configuration Management (registry)

Kernel run-time / Hardware Abstraction Layer

v3

11. Explain security attacks and measures of WI-FI attacks.

What are the risks to your wireless network?

Whether it’s a home or business network, the risks to an unsecured wireless network are the same. Some of the risks include:

Piggybacking

If you fail to secure your wireless network, anyone with a wireless-enabled computer in range of your access point can use your connection. The typical indoor broadcast range of an access point is 150–300 feet. Outdoors, this range may extend as far as 1,000 feet. So, if your neighborhood is closely settled, or if you live in an apartment or condominium, failure to secure your wireless network could open your internet connection to many unintended users. These users may be able to conduct illegal activity, monitor and capture your web traffic, or steal personal files.

Wardriving

Wardriving is a specific kind of piggybacking. The broadcast range of a wireless access point can make internet connections available outside your home, even as far away as your street. Savvy computer users know this, and some have made a hobby out of driving through cities and neighborhoods with a wireless-equipped computer—sometimes with a powerful antenna—searching for unsecured wireless networks. This practice is known as “wardriving.”

Evil Twin Attacks

In an evil twin attack, an adversary gathers information about a public network access point, then sets up their system to impersonate it. The adversary uses a broadcast signal stronger than the one generated by the legitimate access point; then, unsuspecting users connect using the stronger signal. Because the victim is connecting to the internet through the attacker’s system, it’s easy for the attacker to use specialized tools to read any data the victim sends over the internet. This data may include credit card numbers, username and password combinations, and other personal information. Always confirm the name and password of a public Wi-Fi hotspot prior to use. This will ensure you are connecting to a trusted access point.

Wireless Sniffing

Many public access points are not secured and the traffic they carry is not encrypted. This can put your sensitive communications or transactions at risk. Because your connection is being transmitted “in the clear,” malicious actors could use sniffing tools to obtain sensitive information such as passwords or credit card numbers. Ensure that all the access points you connect to use at least WPA2 encryption.

Unauthorized Computer Access

An unsecured public wireless network combined with unsecured file sharing could allow a malicious user to access any directories and files you have unintentionally made available for sharing. Ensure that when you connect your devices to public networks, you deny sharing files and folders. Only allow sharing on recognized home networks and only while it is necessary to share items. When not needed, ensure that file sharing is disabled. This will help prevent an unknown attacker from accessing your device's files.

Shoulder Surfing

In public areas malicious actors can simply glance over your shoulder as you type. By simply watching you, they can steal sensitive or personal information. Screen protectors that prevent shoulder-surfers from seeing your device screen can be purchased for little money. For smaller devices, such as phones, be cognizant of your surroundings while viewing sensitive information or entering passwords.

Theft of Mobile Devices

Not all attackers rely on gaining access to your data via wireless means. By physically stealing your device, attackers could have unrestricted access to all of its data, as well as any connected cloud accounts. Taking measures to protect your devices from loss or theft is important, but should the worst happen, a little preparation may protect the data inside. Most mobile devices, including laptop computers, now have the ability to fully encrypt their stored data—making devices useless to attackers who cannot provide the proper password or personal identification number (PIN). In addition to encrypting device content, it is also advisable to configure your device's applications to request login information before allowing access to any cloud-based information. Last, individually encrypt or password-protect files that contain personal or sensitive information. This will afford yet another layer of protection in the event an attacker is able to gain access to your device.

What can you do to minimize the risks to your wireless network?

Change default passwords. Most network devices, including wireless access points, are pre-configured with default administrator passwords to simplify setup. These default passwords are easily available to obtain online, and so provide only marginal protection. Changing default passwords makes it harder for attackers to access a device. Use and periodic changing of complex passwords is your first line of defense in protecting your device. (See Choosing and Protecting Passwords.)

Restrict access. Only allow authorized users to access your network. Each piece of hardware connected to a network has a media access control (MAC) address. You can restrict access to your network by filtering these MAC addresses. Consult your user documentation for specific information about enabling these features. You can also utilize the "guest" account, which is a widely used feature on many wireless routers. This feature allows you to grant wireless access to guests on a separate wireless channel with a separate password, while maintaining the privacy of your primary credentials.

Encrypt the data on your network. Encrypting your wireless data prevents anyone who might be able to access your network from viewing it. There are several encryption protocols available to provide this protection. Wi-Fi Protected Access (WPA), WPA2, and WPA3 encrypt information being transmitted between wireless routers and wireless devices. WPA3 is currently the strongest encryption. WPA and WPA2 are still available; however, it is advisable to use equipment that specifically supports WPA3, as using the other protocols could leave your network open to exploitation.

Protect your Service Set Identifier (SSID). To prevent outsiders from easily accessing your network, avoid publicizing your SSID. All Wi-Fi routers allow users to protect their device's SSID, which makes it more difficult for attackers to find a network. At the very least, change your SSID to something unique. Leaving it as the manufacturer's default could allow a potential attacker to identify the type of router and possibly exploit any known vulnerabilities.

Install a firewall. Consider installing a firewall directly on your wireless devices (a host-based firewall), as well as on your home network (a router- or modem-based firewall). Attackers who can directly tap into your wireless network may be able to circumvent your network firewall—a host-based firewall will add a layer of protection to the data on your computer (see Understanding Firewalls for Home and Small Office Use).

Maintain antivirus software. Install antivirus software and keep your virus definitions up to date. Many antivirus programs also have additional features that detect or protect against spyware and adware (see Protecting Against Malicious Code and What is Cybersecurity?).

Use file sharing with caution. File sharing between devices should be disabled when not needed. You should always choose to only allow file sharing over home or work networks, never on public networks. You may want to consider creating a dedicated directory for file sharing and restrict access to all other directories. In addition, you should password protect anything you share. Never open an entire hard drive for file sharing (see Choosing and Protecting Passwords).

Keep your access point software patched and up to date. The manufacturer of your wireless access point will periodically release updates to and patches for a device's software and firmware. Be sure to check the manufacturer's website regularly for any updates or patches for your device.

Check your internet provider's or router manufacturer's wireless security options. Your internet service provider and router manufacturer may provide information or resources to assist in securing your wireless network. Check the customer support area of their websites for specific suggestions or instructions.

Connect using a Virtual Private Network (VPN). Many companies and organizations have a VPN. VPNs allow employees to connect securely to their network when away from the office. VPNs encrypt connections at the sending and receiving ends and keep out traffic that is not properly encrypted. If a VPN is available to you, make sure you log onto it any time you need to use a public wireless access point.

12. How SQL injection is performed? Explain methods, types and solutions.

SQL Injection (SQLi) is a type of an injection attack that makes it possible to execute malicious SQL statements. These statements control a database server behind a web application. Attackers can use SQL Injection vulnerabilities to bypass application security measures. They can go around authentication and authorization of a web page or web application and retrieve the content of the entire SQL database. They can also use SQL Injection to add, modify, and delete records in the database.

An SQL Injection vulnerability may affect any website or web application that uses an SQL database such as MySQL, Oracle, SQL Server, or others. Criminals may use it to gain unauthorized access to your sensitive data: customer information, personal data, trade secrets, intellectual property, and more. SQL Injection attacks are one of the oldest, most prevalent, and most dangerous web application vulnerabilities.

- Attackers can use SQL Injections to find the credentials of other users in the database. They can then impersonate these users. The impersonated user may be a database administrator with all database privileges.
- SQL lets you select and output data from the database. An SQL Injection vulnerability could allow the attacker to gain complete access to all data in a database server.
- SQL also lets you alter data in a database and add new data. For example, in a financial application, an attacker could use SQL Injection to alter balances, void transactions, or transfer money to their account.
- You can use SQL to delete records from a database, even drop tables. Even if the administrator makes database backups, deletion of data could affect

application availability until the database is restored. Also, backups may not cover the most recent data.

- In some database servers, you can access the operating system using the database server. This may be intentional or accidental. In such case, an attacker could use an SQL Injection as the initial vector and then attack the internal network behind a firewall.

SQL injections typically fall under three categories: In-band SQLi (Classic), Inferential SQLi (Blind) and Out-of-band SQLi. You can classify SQL injections types based on the methods they use to access backend data and their damage potential.

Types of SQL Injections

SQL injections typically fall under three categories: In-band SQLi (Classic), Inferential SQLi (Blind) and Out-of-band SQLi. You can classify SQL injections types based on the methods they use to access backend data and their damage potential.

In-band SQLi

The attacker uses the same channel of communication to launch their attacks and to gather their results. In-band SQLi's simplicity and efficiency make it one of the most common types of SQLi attack. There are two sub-variations of this method:

- **Error-based SQLi**—the attacker performs actions that cause the database to produce error messages. The attacker can potentially use the data provided by these error messages to gather information about the structure of the database.
- **Union-based SQLi**—this technique takes advantage of the UNION SQL operator, which fuses multiple select statements generated by the database to get a single HTTP response. This response may contain data that can be leveraged by the attacker.

Inferential (Blind) SQLi

The attacker sends data payloads to the server and observes the response and behavior of the server to learn more about its structure. This method is called blind SQLi because the data is not transferred from the website database to the attacker, thus the attacker cannot see information about the attack in-band.

Blind SQL injections rely on the response and behavioral patterns of the server so they are typically slower to execute but may be just as harmful. Blind SQL injections can be classified as follows:

- **Boolean**—that attacker sends a SQL query to the database prompting the application to return a result. The result will vary depending on whether the query is true or false. Based on the result, the information within the HTTP response will modify or stay unchanged. The attacker can then work out if the message generated a true or false result.
- **Time-based**—attacker sends a SQL query to the database, which makes the database wait (for a period in seconds) before it can react. The attacker can see from the time the database takes to respond, whether a query is true or false. Based on the result, an HTTP response will be generated instantly or after a waiting period. The attacker can thus work out if the message they used returned true or false, without relying on data from the database.

Out-of-band SQLi

The attacker can only carry out this form of attack when certain features are enabled on the database server used by the web application. This form of attack is primarily used as an alternative to the in-band and inferential SQLi techniques.

Out-of-band SQLi is performed when the attacker can’t use the same channel to launch the attack and gather information, or when a server is too slow or unstable for these actions to be performed. These techniques count on the capacity of the server to create DNS or HTTP requests to transfer data to an attacker.

Primary Defenses:

- **Option 1: Use of Prepared Statements (with Parameterized Queries)**
- **Option 2: Use of Properly Constructed Stored Procedures**
- **Option 3: Allow-list Input Validation**
- **Option 4: Escaping All User Supplied Input**

Additional Defenses:

- **Also: Enforcing Least Privilege**
- **Also: Performing Allow-list Input Validation as a Secondary Defense**

1) Continuous Scanning and Penetration Testing
2) Restrict Privileges
3) Use Query Parameters
4) Instant Protection