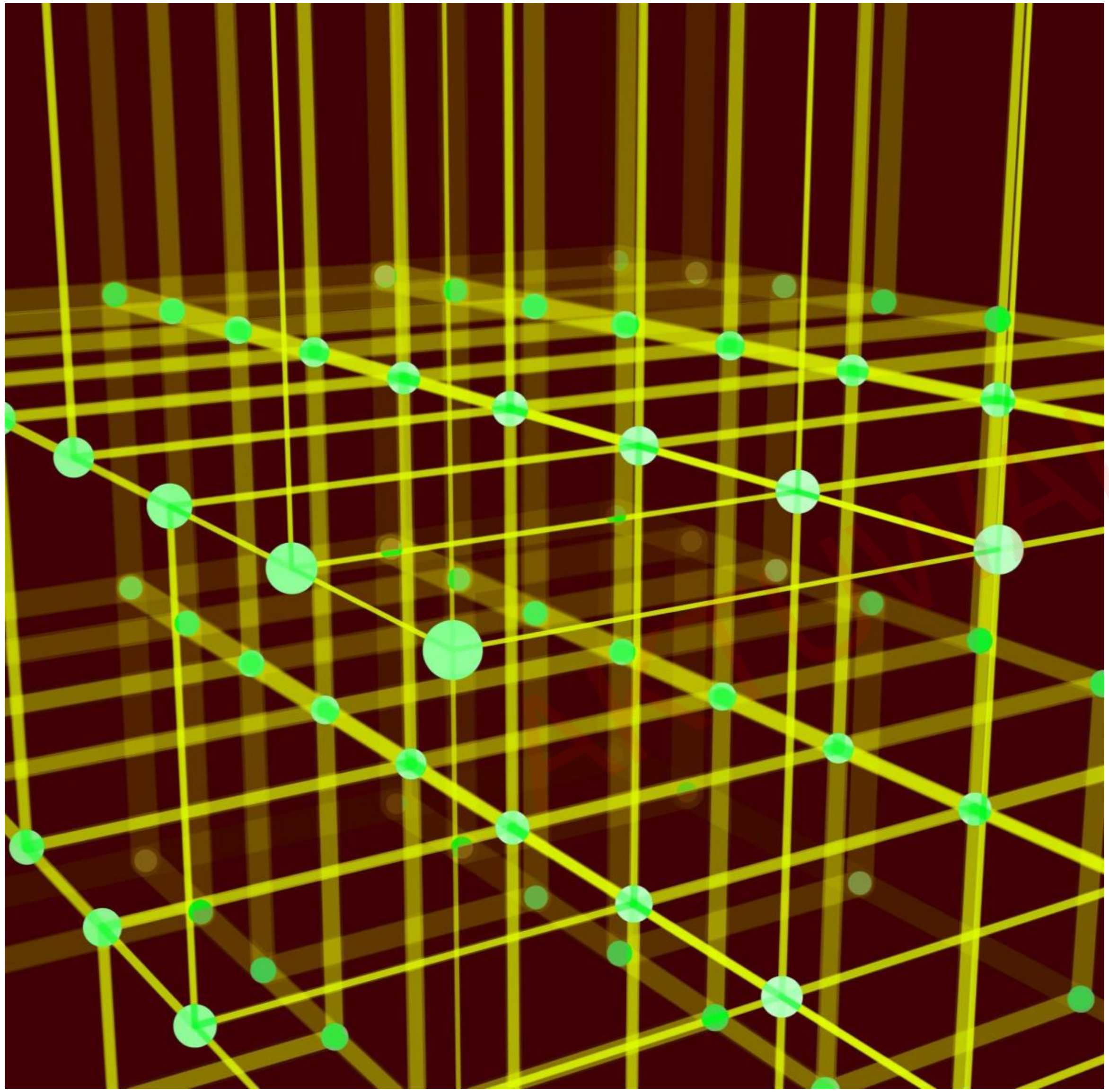
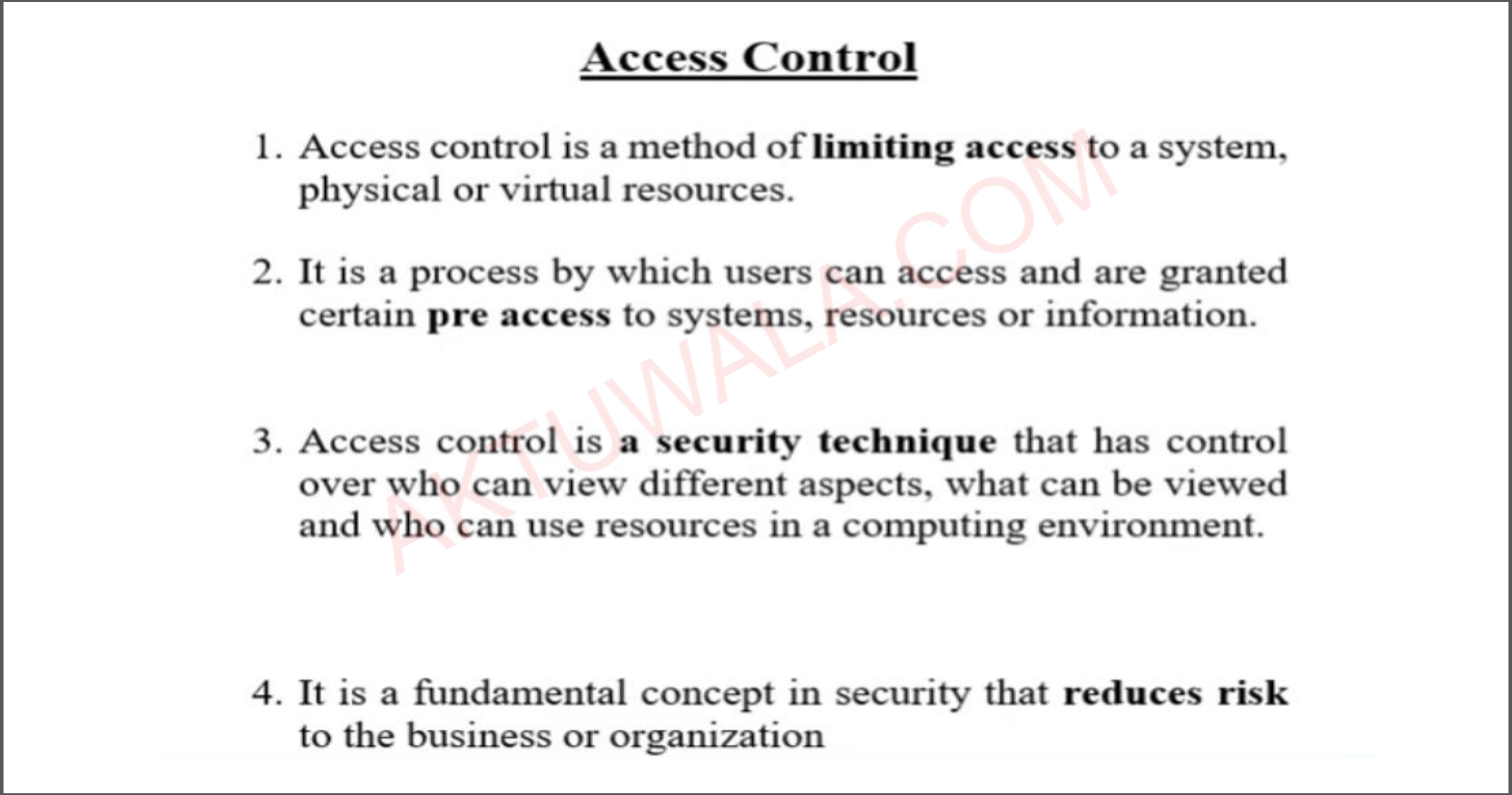


Secure Architecture Principles Isolation And Leas

UNIT - 3



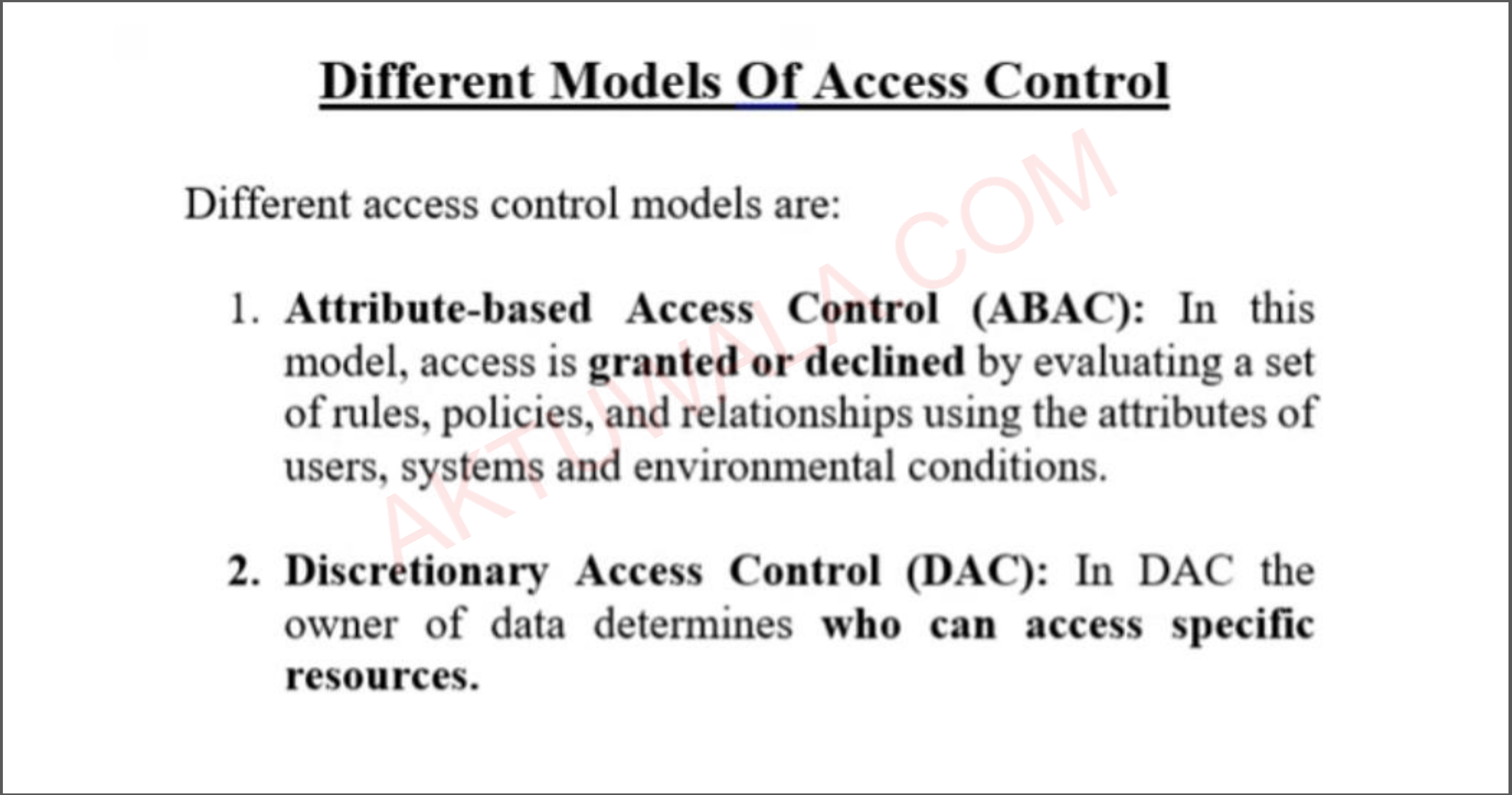
Access Control

1. Access control is a method of **limiting access** to a system, physical or virtual resources.

2. It is a process by which users can access and are granted certain **pre access** to systems, resources or information.

3. Access control is **a security technique** that has control over who can view different aspects, what can be viewed and who can use resources in a computing environment.

4. It is a fundamental concept in security that **reduces risk** to the business or organization



Different Models Of Access Control

Different access control models are:

1. **Attribute-based Access Control (ABAC):** In this model, access is **granted or declined** by evaluating a set of rules, policies, and relationships using the attributes of users, systems and environmental conditions.

2. **Discretionary Access Control (DAC):** In DAC the owner of data determines **who can access specific resources.**

3. **History-Based Access Control (HBAC):** In this model, access is **granted or declined by evaluating the history of activities** of the inquiring party that includes behaviour, the time between requests and content of requests.

4. **Identity-Based Access Control (IBAC):** By using this model Network administrators can more effectively manage activity and access, based on **individual requirements.**

5. **Mandatory Access Control (MAC):** A control model in which access rights are regulated by a central authority based on multiple levels of security. Security Enhanced Linux is implemented using MAC on the Linux operating system.

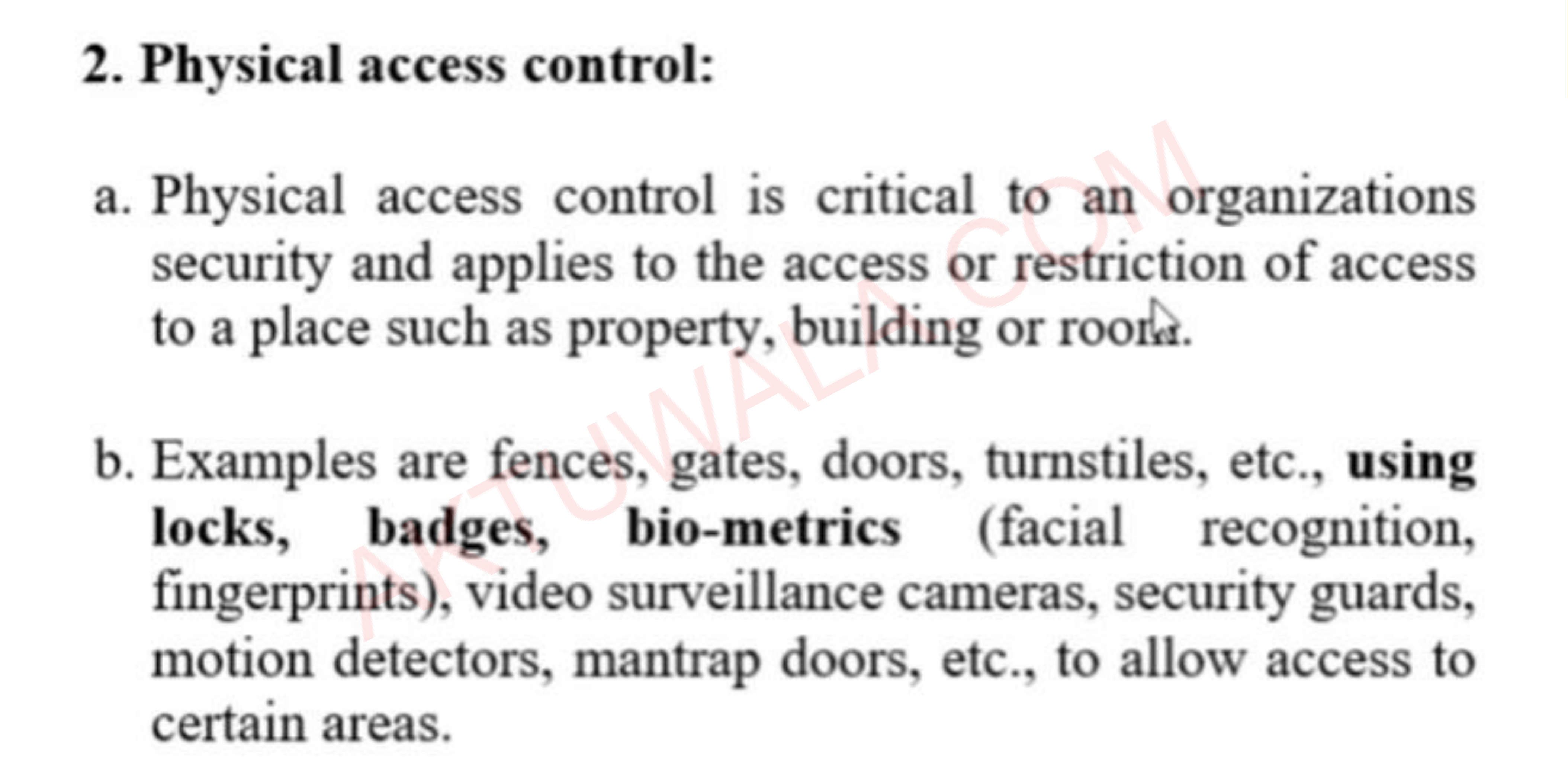
Implementation Of Access Control

Implementation of access control:

1. Administrative access control:

a. Administrative access control **sets the access control policies and procedures for the whole organization,** defines the implementation requirements of both physical and technical access control, and what the consequences of non-compliance will be.

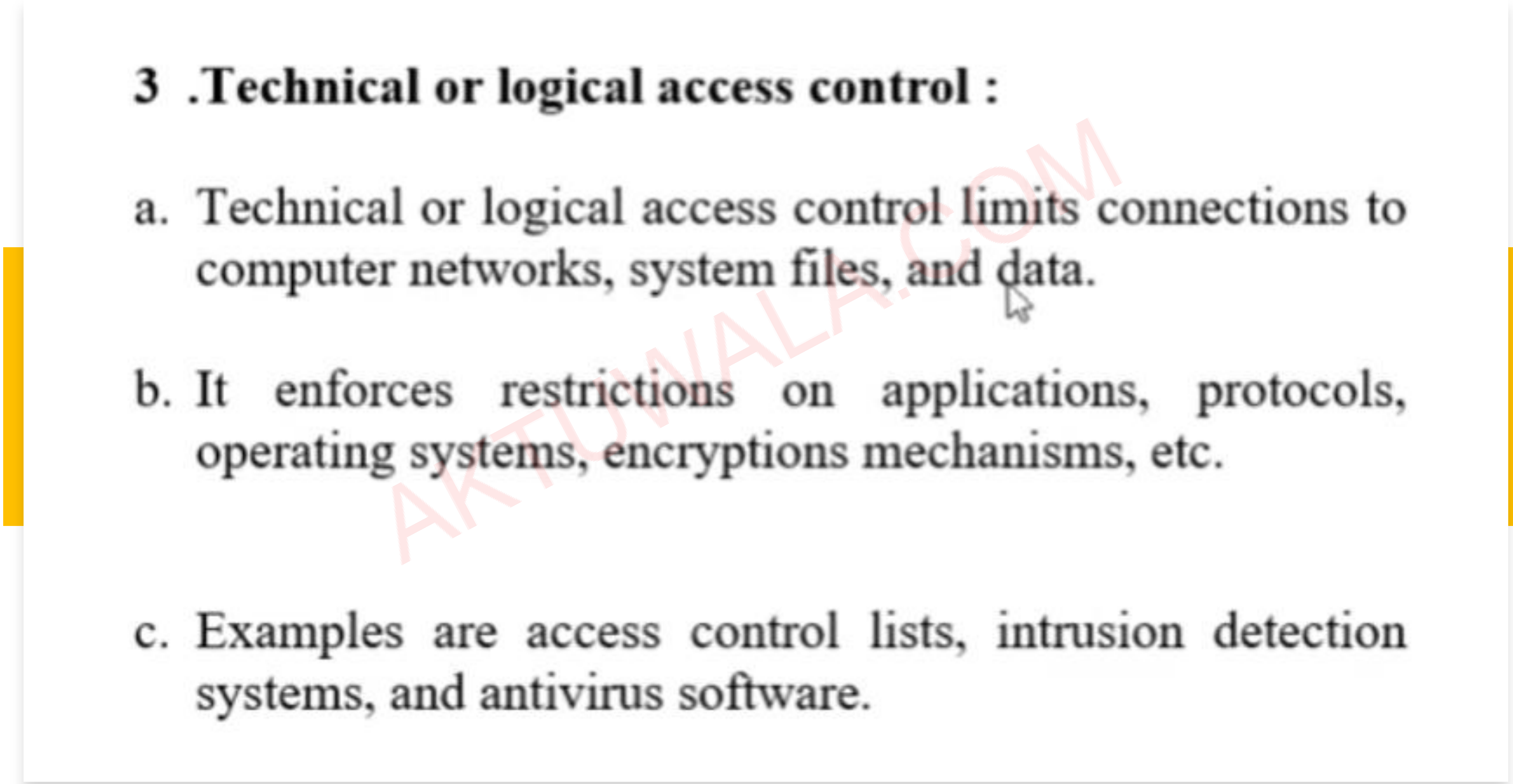
b. Examples are supervisory structure, staff and contractor controls, information classification, and training, auditing, and testing.



2. Physical access control:

a. Physical access control is critical to an organizations security and applies to the access or restriction of access to a place such as property, building or room.

b. Examples are fences, gates, doors, turnstiles, etc., **using locks, badges, bio-metrics** (facial recognition, fingerprints), video surveillance cameras, security guards, motion detectors, mantrap doors, etc., to allow access to certain areas.

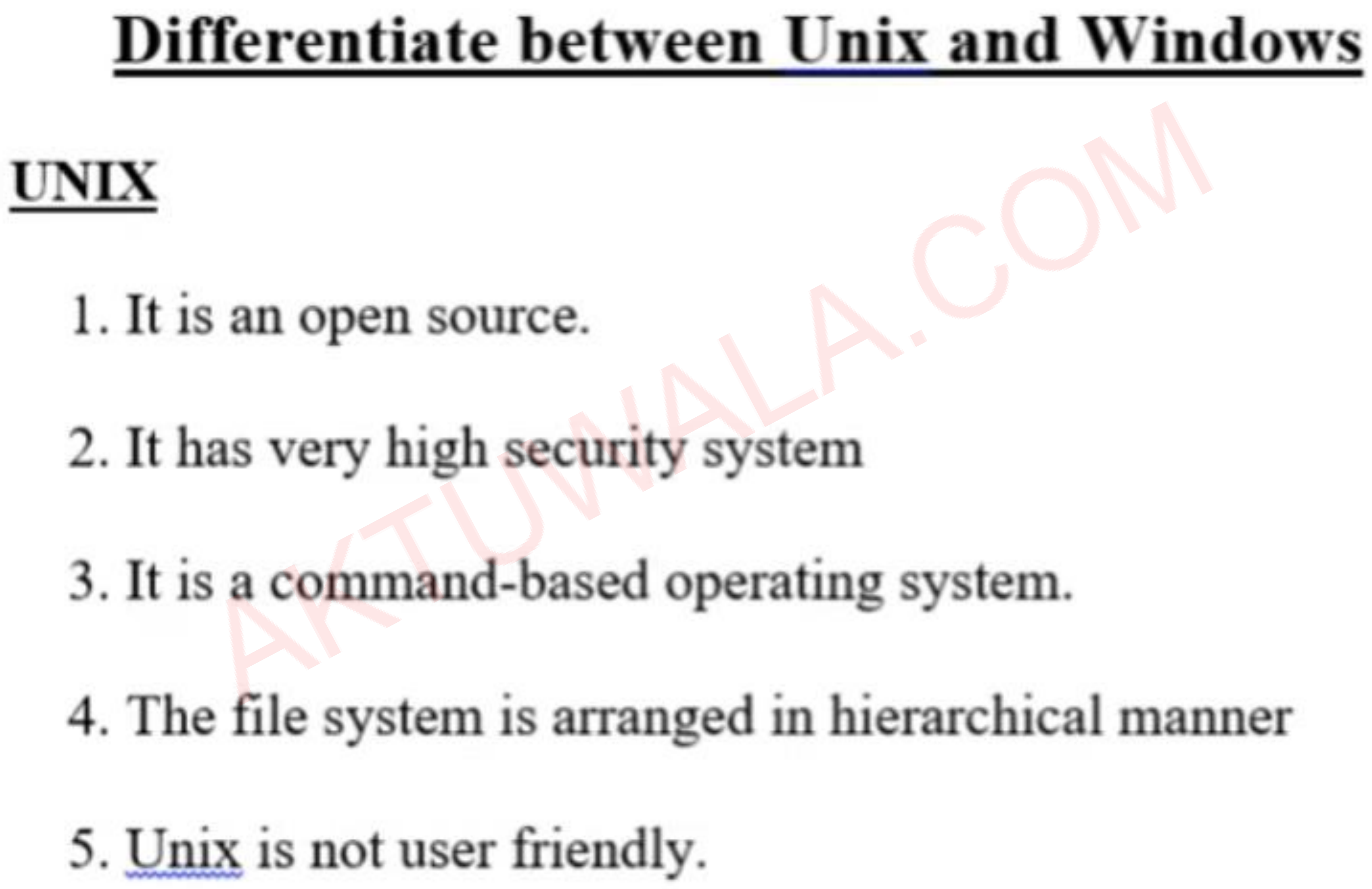


3 .Technical or logical access control :

a. Technical or logical access control limits connections to computer networks, system files, and data.

b. It enforces restrictions on applications, protocols, operating systems, encryptions mechanisms, etc.

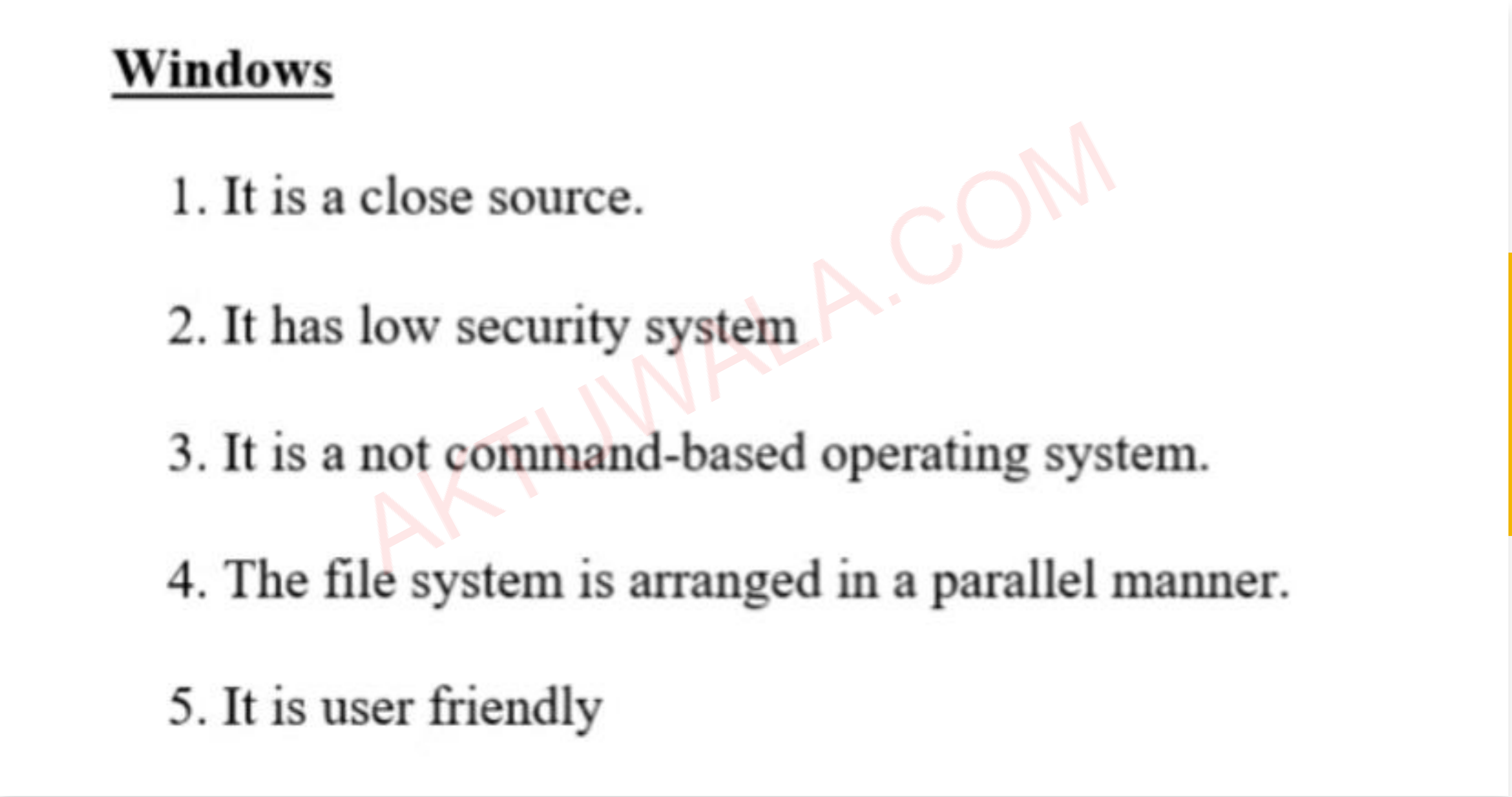
c. Examples are access control lists, intrusion detection systems, and antivirus software.



Differentiate between Unix and Windows

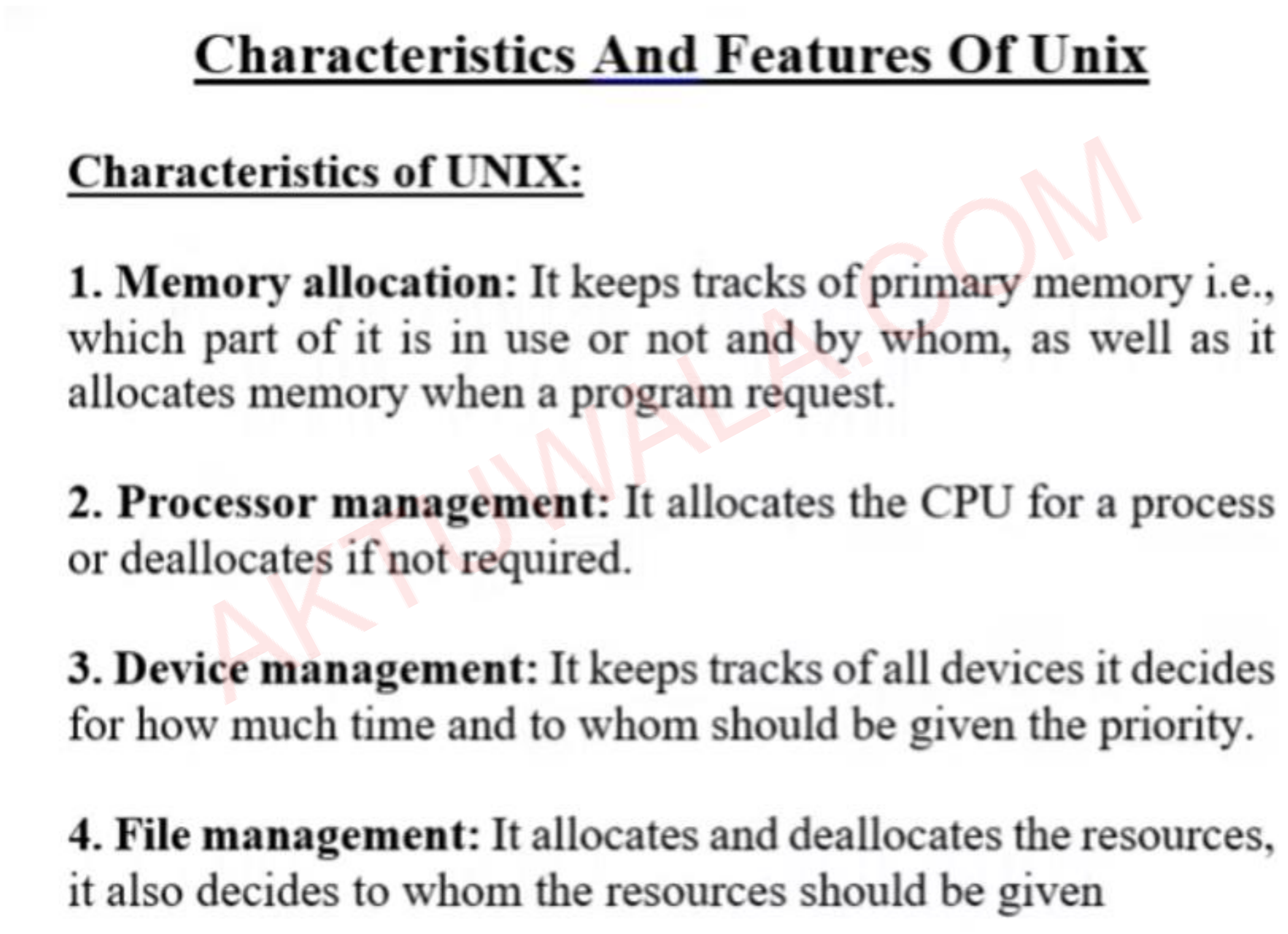
UNIX

1. It is an open source.
2. It has very high security system
3. It is a command-based operating system.
4. The file system is arranged in hierarchical manner
5. Unix is not user friendly.



Windows

1. It is a close source.
2. It has low security system
3. It is a not command-based operating system.
4. The file system is arranged in a parallel manner.
5. It is user friendly



Characteristics And Features Of Unix

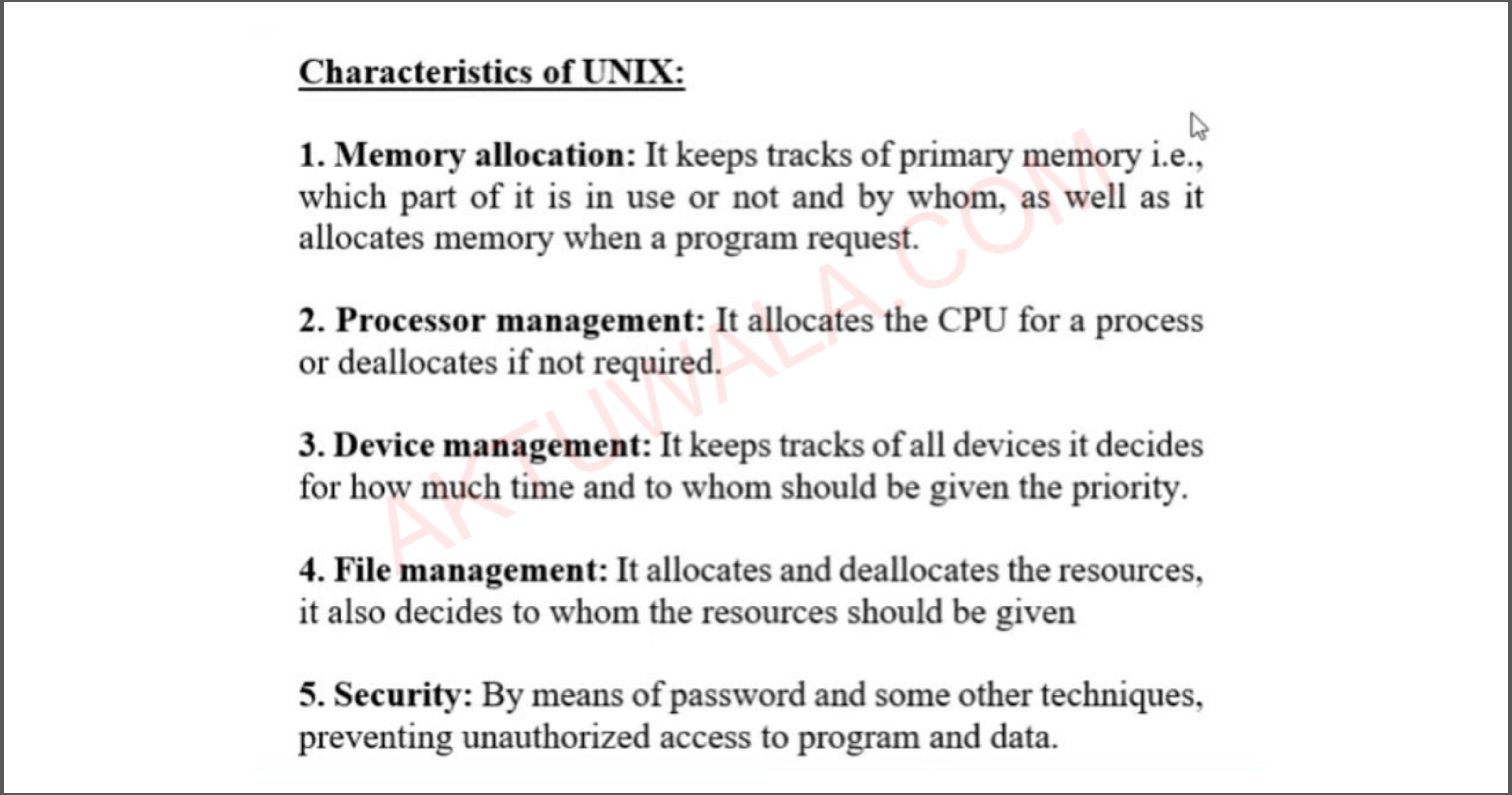
Characteristics of UNIX:

1. Memory allocation: It keeps tracks of primary memory i.e., which part of it is in use or not and by whom, as well as it allocates memory when a program request.

2. Processor management: It allocates the CPU for a process or deallocates if not required.

3. Device management: It keeps tracks of all devices it decides for how much time and to whom should be given the priority.

4. File management: It allocates and deallocates the resources, it also decides to whom the resources should be given



Characteristics of UNIX:

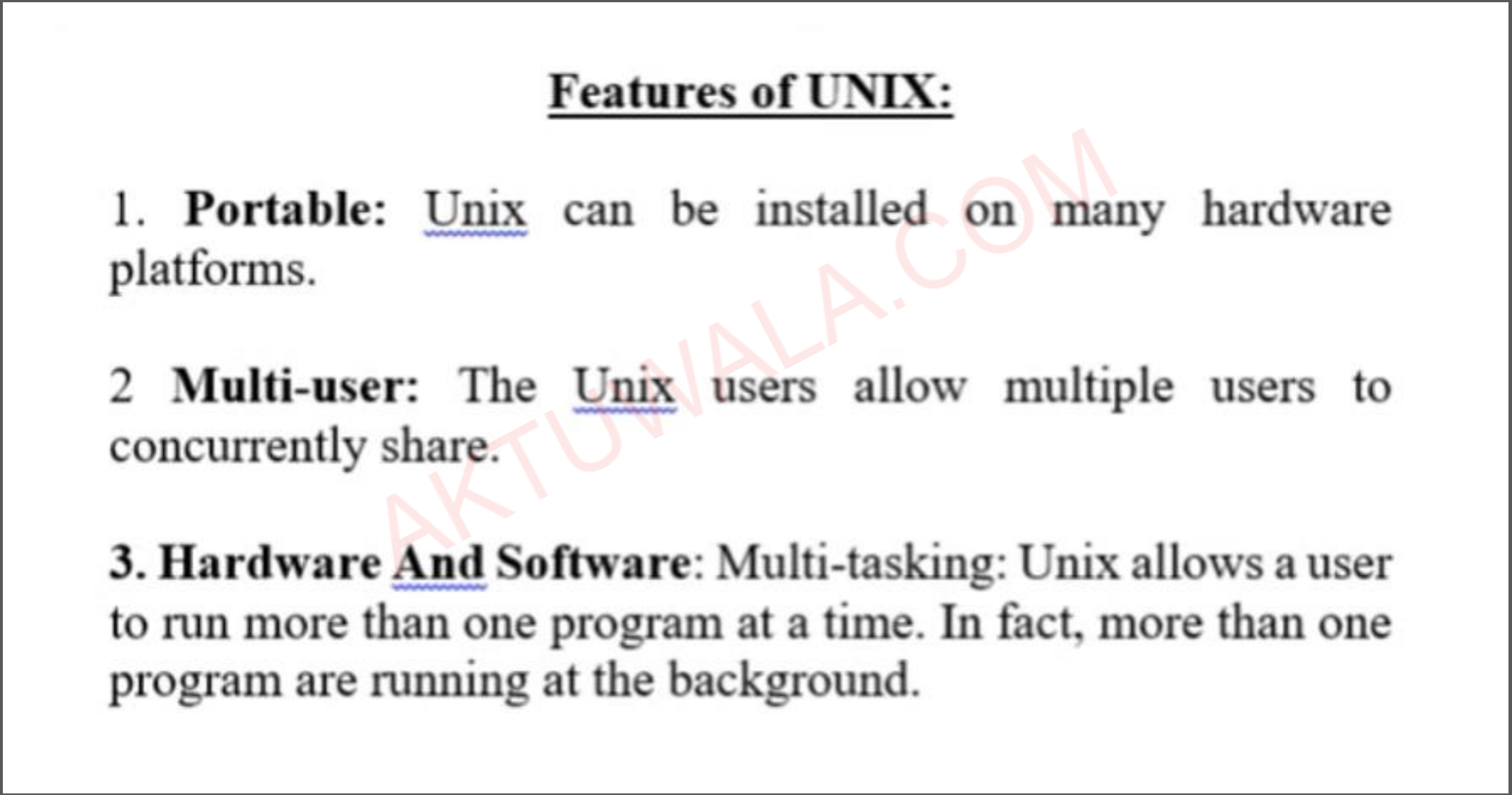
1. Memory allocation: It keeps tracks of primary memory i.e., which part of it is in use or not and by whom, as well as it allocates memory when a program request.

2. Processor management: It allocates the CPU for a process or deallocates if not required.

3. Device management: It keeps tracks of all devices it decides for how much time and to whom should be given the priority.

4. File management: It allocates and deallocates the resources, it also decides to whom the resources should be given

5. Security: By means of password and some other techniques, preventing unauthorized access to program and data.

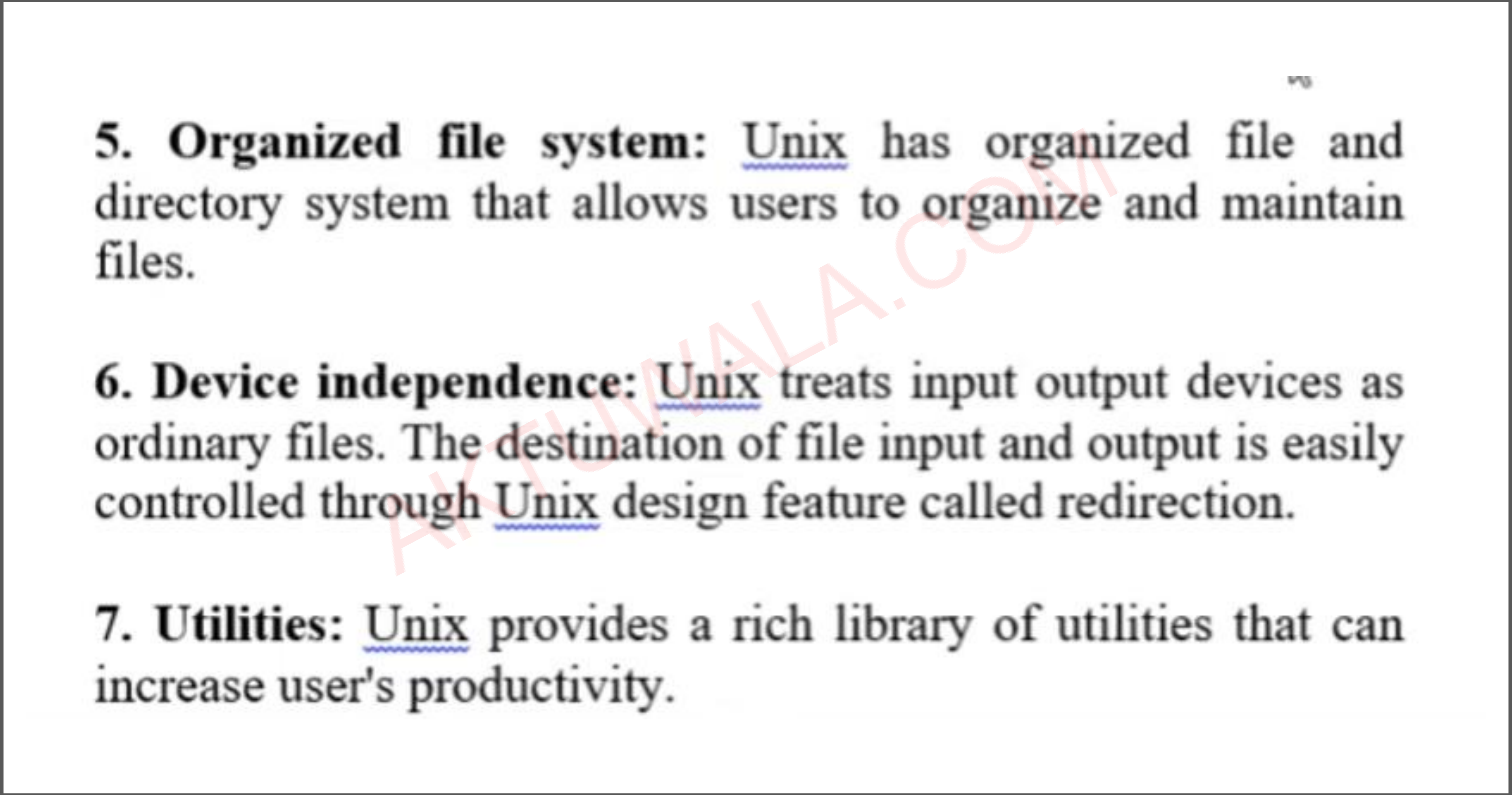


Features of UNIX:

1. **Portable:** Unix can be installed on many hardware platforms.

2 **Multi-user:** The Unix users allow multiple users to concurrently share.

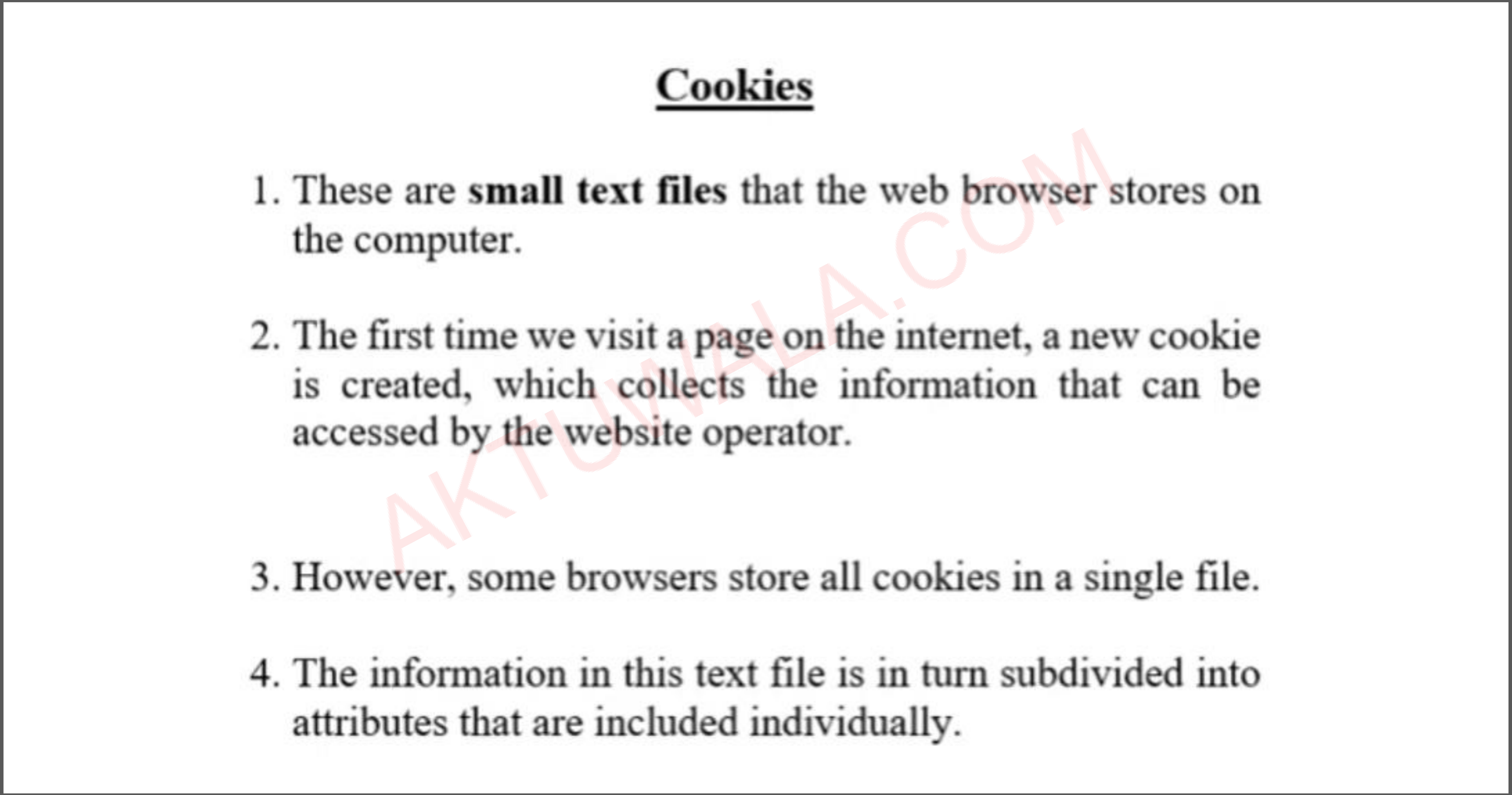
3. Hardware And Software: Multi-tasking: Unix allows a user to run more than one program at a time. In fact, more than one program are running at the background.



5. Organized file system: Unix has organized file and directory system that allows users to organize and maintain files.

6. Device independence: Unix treats input output devices as ordinary files. The destination of file input and output is easily controlled through Unix design feature called redirection.

7. Utilities: Unix provides a rich library of utilities that can increase user's productivity.



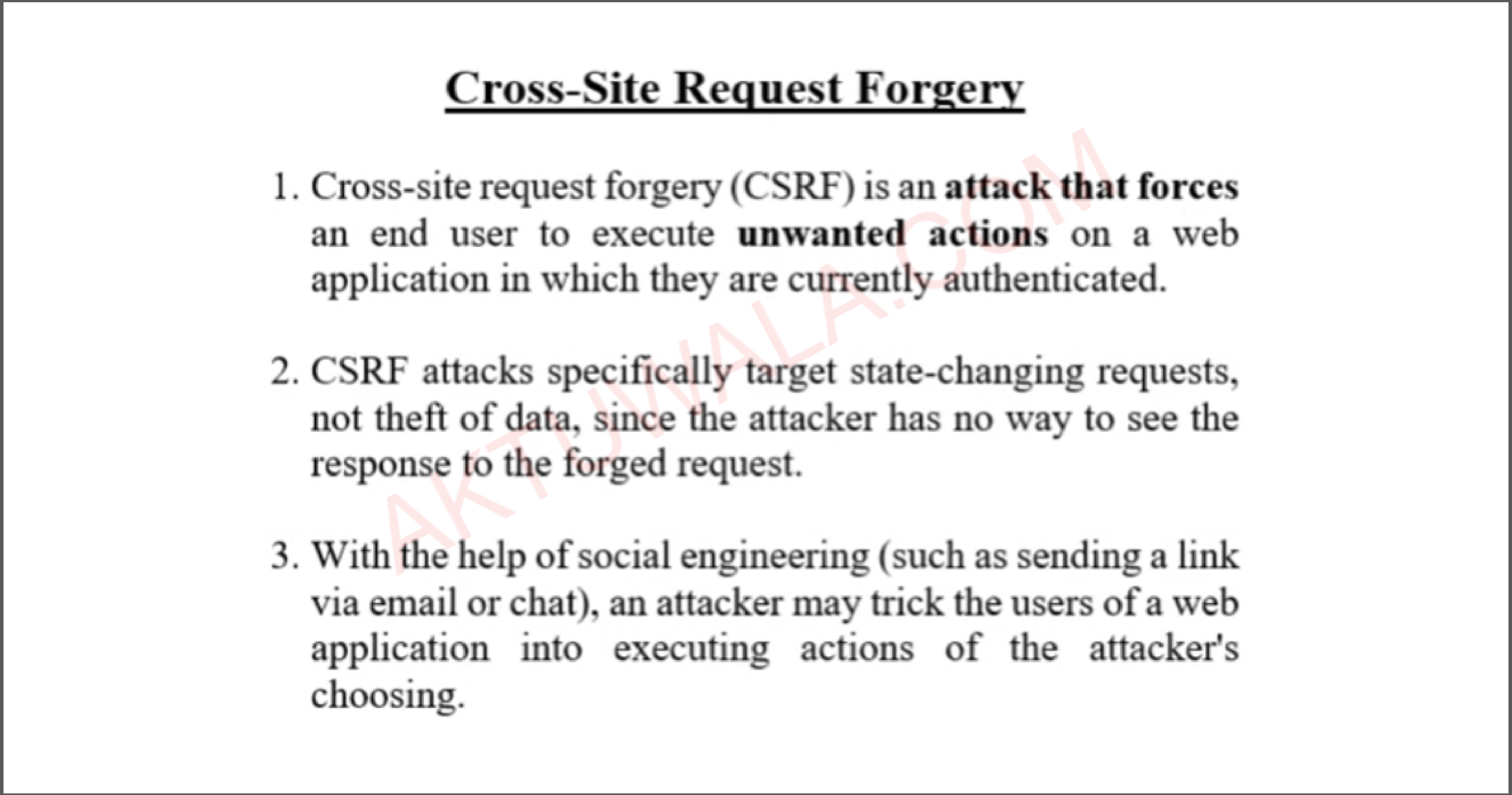
Cookies

1. These are **small text files** that the web browser stores on the computer.

2. The first time we visit a page on the internet, a new cookie is created, which collects the information that can be accessed by the website operator.

3. However, some browsers store all cookies in a single file.

4. The information in this text file is in turn subdivided into attributes that are included individually.

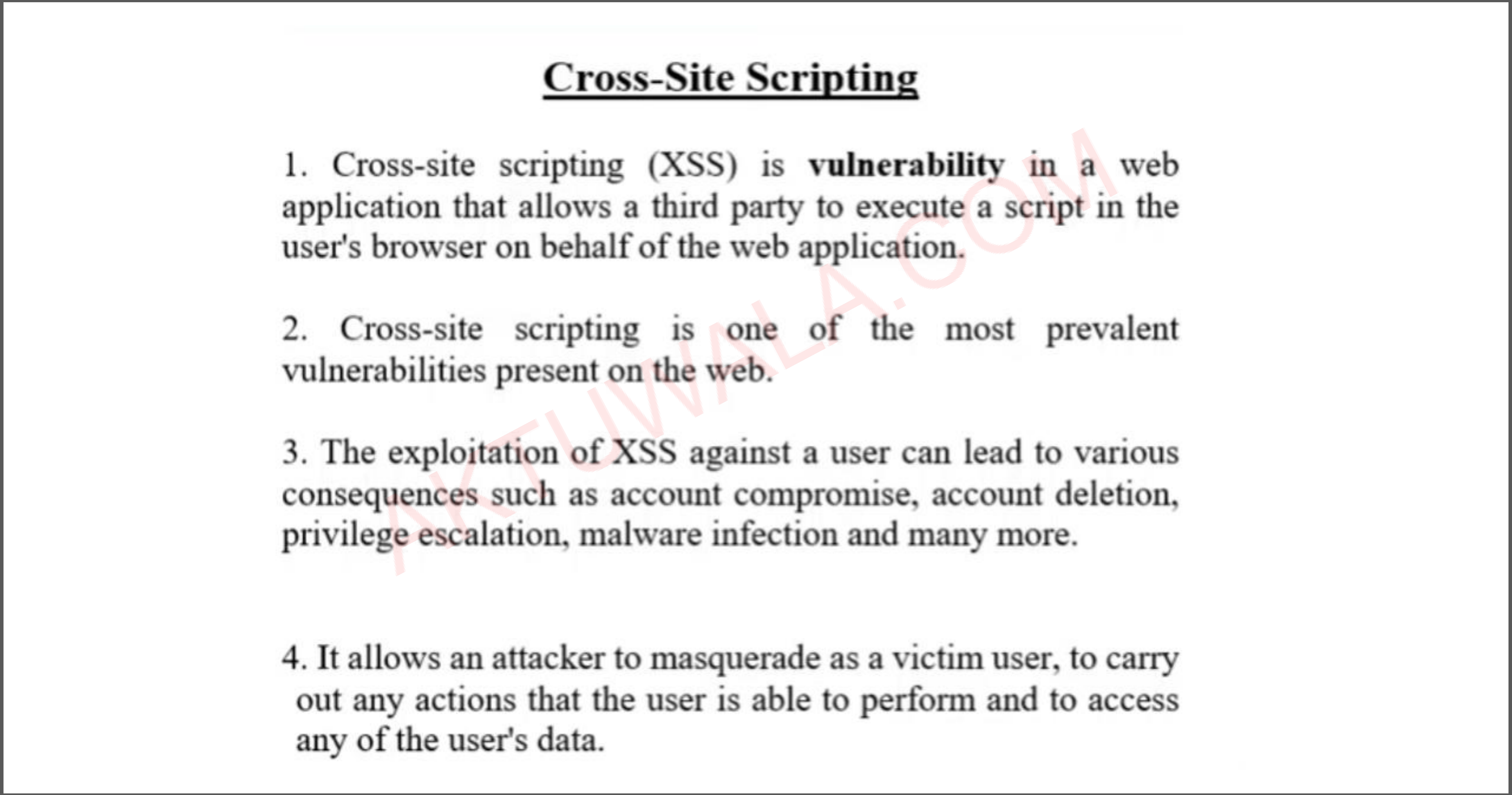


Cross-Site Request Forgery

1. Cross-site request forgery (CSRF) is an **attack that forces** an end user to execute **unwanted actions** on a web application in which they are currently authenticated.

2. CSRF attacks specifically target state-changing requests, not theft of data, since the attacker has no way to see the response to the forged request.

3. With the help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing.



Cross-Site Scripting

1. Cross-site scripting (XSS) is **vulnerability** in a web application that allows a third party to execute a script in the user's browser on behalf of the web application.

2. Cross-site scripting is one of the most prevalent vulnerabilities present on the web.

3. The exploitation of XSS against a user can lead to various consequences such as account compromise, account deletion, privilege escalation, malware infection and many more.

4. It allows an attacker to masquerade as a victim user, to carry out any actions that the user is able to perform and to access any of the user's data.

Made By :- AKTU WALA (Satyam Sahu)

AKTU
WALA

YouTube