***1 (A)***



Google hacking is the term used when a hacker tries to find  
vulnerable targets or sensitive data by using the Google search  
engine.

Operators are used to refining the results and maximize the search value. They are your tools as well as hackers’ weapons.

Google can search many different types of files, including PDF and Microsoft Office documents. In this example we will search for confidential files in web pages:

"not for distribution" confidential,

Finds Login Pages of CentOS,

inurl:/login/index.php intitle:CentOS

cache:tudublin.ie

Microsoft Excel spreadsheets containing the words username, password, and email.:

filetype:xls username password email

Access SAP Crystal report, crystal reports help analyse data by creating richly formatted reports. These reports can be a major

Inurl: apspassword

***(B)***



**Authentic Process**

Fundamental building block and primary line of defence. The basis for access control and user accountability.  
Identification presents an identifier to the security system. Verification is the presenting or generating of authentication information that corroborates the binding between the entity and the identifier.

Authenticating user identity through 4 functions.

1. Something the individual knows: password, pin, prearranged questions.
2. Something the individual possesses (token): smartcard, physical key, electronic key card
3. Static Biometrics: fingerprint, retina, face

Dynamic biometrics: voice pattern, handwriting, typing rhythm

**Password Authentication:**

Widely used line of defence against intruders  
• User provides name/login and password  
• System compares password with the one stored for that specified login

The user ID:  
• Determines that the user is authorized to access the system  
• Determines the user’s privileges  
• Is used in discretionary access control

Offline dictionary attack

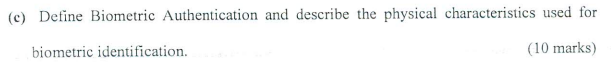
Popular password attack

Password guessing against single user

Workstation Hijacking

Exploiting user mistakes

***(C)***



***Biometric Authentication***

Attempts to authenticate an individual based on unique physical  
characteristics  
• Based on pattern recognition  
• Is technically complex and expensive when compared to passwords and  
tokens  
• Physical characteristics used include:  
o Facial characteristics  
o Fingerprints  
o Hand geometry  
o Retinal pattern  
o Iris  
o Signature  
o Voice

Diagram

Description automatically generated

Diagram

Description automatically generated

***2 (A)***

******

Text, application, email

Description automatically generated

Table

Description automatically generated

***(B)***



DAC

Discretionary access control (DAC)  
• Controls access based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do.

Table

Description automatically generated

Diagram

Description automatically generated

***(C)***



Prepared Statements: pre-compiled SQL commands created inside a program that can be used many times over the course of the application’s lifecycle. By default, PS input parameters are bound. Bound parameters are treated as plain text values, which prevents any command alteration during an SQL injection attack.

Least Privilege: A program requires user credentials to run SQL commands, such as insert, update, search, delete, and drop, to communicate with a database. he program user should only have the required database privileges. Additional privileges should be granted on an as-needed basis. With minimal database privileges, the potential damage of an SQL injection attack is reduced.

Input Validation: Suspicious inputs are filtered prior to submission or processing by the server when validated. An example of input validation is an email validator. Passing an SQL injection query would not work, since the input field only accepts a valid email address based on a regular expression

Diagram

Description automatically generated

Graphical user interface, text

Description automatically generated

The type of different cloud security attacks that occur are the following attacks which are:

Denial of Service (DoS) attacks -> this is an action that prevents or impairs the authorized use of network systems, or applications by exhausting resources such as CPU, memory, bandwidth, and disk space. This is a form of attack on the availability of some service such as resources like network bandwidth, system, and application resources.

Malware Injection Attack -> this is when malware and malicious code is injected in the network. Malware can be defined as a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating systems or otherwise annoying or disrupting the victim.

Authentication attacks -> authentication is the process of verifying an identity claimed by or for a system entity. Attacks may pose themselves as someone else, going by fake identities and use phishing and social engineering attacks. If they bypass authentication and gain access, they might be able to access confidential information and perform actions that they normally not be authorized to, such as admin privileges.

Man-in-the-Middle attacks -> A man in the middle (MITM) attack is **a general term for when a perpetrator positions himself in a conversation between a user and an application**—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway.

There are several cloud security mechanisms, out there to defend against these types of attacks. Such as a secure Operating system, that can resist against DOS attacks. Strong authentication, such as secure password validation can defend against authentication attacks and a strong password can defend against brute force dictionary attacks. Encrypt store data can also aid, as encrypted data will be protected against attacks who bypass the system security. Intrusion detection can defend against man in the middle attack and any intruders. The use of intrusion detection systems like host-based IDS, or Network based IDS can monitor network traffic or characteristics of hosts to detect intruders like the man in the middle.

HIDS --- detection and filtering

NIDS --- Prevention & detection

Graphical user interface, application

Description automatically generated with medium confidence

Denial of Service (DoS) attacks -> this is an action that prevents or impairs the authorized use of network systems, or applications by exhausting resources such as CPU, memory, bandwidth, and disk space. This is a form of attack on the availability of some service such as resources like network bandwidth, system, and application resources.

Classic DoS attacks include flooding ping command -> the aim of this attack is to overwhelm the capacity of the network connection to the target organization. Traffic can be handled by higher capacity links on the path, but the packets are discarded as capacity decreases. The source of the attack is clearly identified unless a spoofed address is used, network performance is noticeably affected

There are ways to defend against a Denial-of-Service attack. There are four lines of defence against a DoS attack, and these are attack prevention and pre-emption which generally happens before the attack. During the attack, the defences are attack detection and filtering. During and after the attack, the defence mechanism is to identify and attempt to traceback the attack source. After the attack, the defence mechanism is to react to the attack.

Ways of DoS attack prevention is blocking spoofed source addresses on routers as close to the source as possible. Filters may be used to ensure path back to the claimed source address is the one being used by the current packet. Filters must be applied to traffic before it leaves the ISP’s network or at the point of entry to their network.

Use modified TCP connection handling code. Cryptographically encode critical information in a cookie that is sent as the server’s initial sequence number. Legitimate client responds with an ACK packet containing the incremented sequence number cookie. Drop an entry for an incomplete connection from the TCP connections table when it overflows.

Other ways of attack prevention is block IP directed broadcasts, block suspicious services and combinations, manage application attacks with a form of graphical puzzle (captcha) to distinguish legitimate human request, good security practices and use mirrored and replicated servers when high performance and reliability is required

Graphical user interface, text, application

Description automatically generated

The NIST computers security incident handling guide defines a Denial-of-Service Attack as an action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, & disk space.

There are several types of DOS attacks, such attacks are the reflection attack and amplification attack. The reflection attack is when the attacker sends packets to a known service on the intermediary with a spoofed source address of the actual target system. when the intermediary responds, the response is sent to the target, and it reflects the attack off the intermediary (reflector). The goal is to generate enough volumes of packets to flood the link to the target system without altering the intermediary. The basic defence against these attacks is blocking spoofed-source packets.

Diagram

Description automatically generated

DNS Amplification attacks use packets directed at a legitimate DNS server as the intermediary system. Attackers create a series of DNS requests containing the spoofed source address of the target system. it exploits the DNS behaviour to convert a small request to a much larger response (amplification). The target is then flooded with responses. A basic defence against this attack is to prevent the use of spoofed source addresses.

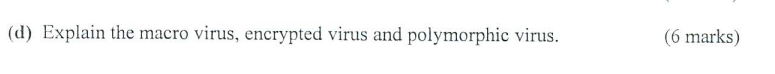
Diagram, engineering drawing

Description automatically generated

ALTERNATIVE ANSWER

Text

Description automatically generated



The macro virus is a type of classification by target virus. Macro viruses infects files with macro or scripting code that is interpreted by an application. It was very common in the mid 1990s and were platform independent, and infected documents (not executable portions of code) and spread easily.

Encrypted virus and polymorphic viruses are classification by concealment. Encrypted viruses are a portion of the virus creates a random encryption key and encrypts the remainder of the virus. Polymorphic viruses are viruses that mutates and changes with every infection.