Advanced Security 2 2019

Q1.

Graphical user interface, text, application

Description automatically generated

**Cache** – This is one of Google’s Advanced Operators for searches. If cache:url is placed in the search, it will tell google to find an old version of that Website in Google’s cache. This can be used to find old information about the website that’s already been updated, or even find an old version of a website that has been recently taken down

So saying cache:www.tudublin.ie will return an old version of TU Dublin that’s been stored in Google’s cache.

**Inurl** : Another Advanced Operator. It will return search results where the inputted parameter matches the title. So for example inputting inurl : .ie will return websites that contain the ie in the url of the page, returning only websites in the Irish domain

**Intitle** : Very similar to inurl except it will search the title of the page instead of the url. So the term intitle:healthy will return webpages that contain healthy in the title of the webpage.

**Filetype** : this can specify what filetype the search results will return. So this can be handy for example if someone is researching papers, they can specify filetype:pdf and get only PDFs returned to them. Also using filetype:xls username password email will return Microsoft excel spreadhseets containing the words username, password and email.



Four password selection strategies include the following

**User education** – this is when Users can be told the importance of using hard to guess passwords and can be provided with guidelines for selecting strong passwords. This allows users to told

**Computer Generated Passwords** – some users have trouble remembering their passwords, so passwords can be generated by the computer itself

**Reactive password checking** – this is when the system would run it’s own password cracker and attacks to find easily guessable passwords, and would then select a password that fails to be cracked. Ways to crack passwords can include dictionary attacks, or open source tools such as John the ripper.

**Complex password** policy – this allow users to select their own password, however the system checks to see if the password is allowable and if not rejects it. The goal is to eliminate guessable passwords while allowing the user to select a password that is memorable. There are many sites that tells you with feedback whether your password is weak, average or strong, and will in fact not allow you to put in passwords deemed weak. As well as that there are some sites that force at least upper cases or special characters in passwords to strengthen the password.



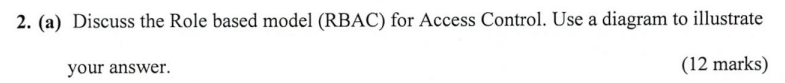
Passwords are suspectable to a number of different attacks that can exploit its vulnerabilities. A list of password vulnerabilities includes the following

Offiline dictionary attack, guessing the password against a single user, workstation hijacking, electronic monitoring, specific account attack, popular password attack, exploiting user mistakes, exploting multiple password use.

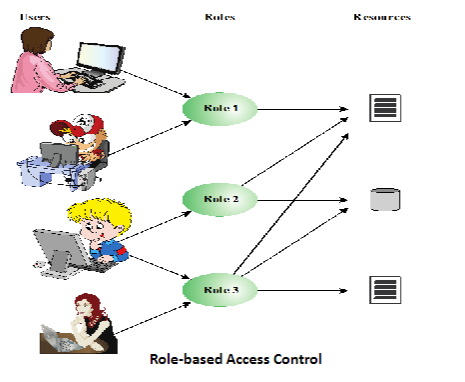
A lot of them involves brute force techniques, such as popular password attack, exploiting multiple passwords use and password guessing against a single user. It takes advantages of commonly used passwords, or short password lengths and simply trial and error until one is found. However, there is a number of techniques that can crack passwords such as dictionary attacks, which is developing a large dictionary of possible passwords, and try each against the password file. Each password must be hashed using each salt value and then compared to stored hash values. There is also tools and password crackers like john the ripper which uses dictionary attacks. There’s also rainbow table attacks, which is pre-compute tables of hash values for all salts. So it has a mammoth table of hash values. And it can be countered using a sufficiently salt value and a sufficiently large hash length

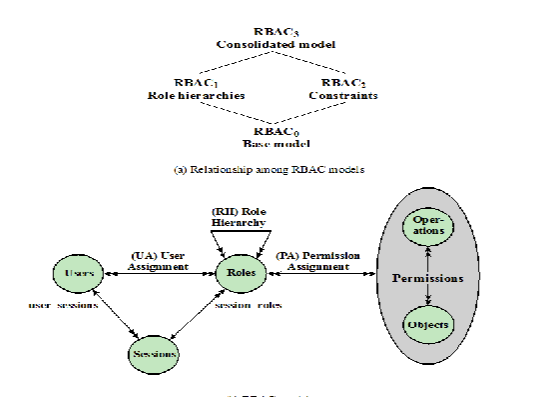
Password file access control can block offline guessing attacks by denying access to encrypted passwords, and are only available to privileged users. However vulnerabilities with the file access control is that it has a weakness in the OS that allows access to a file, there could be accidents with permissions making confidential files readable. Users may be using the same password on other systems, so if discovered a number of systems may be compromised. Access from backup media may be gained as well as passwords maybe be discovered in the network traffic. There may be access to shadow password files as well. A shadow password file, also known as /etc/shadow, is **a system file in Linux that stores encrypted user passwords and is accessible only to the root user**, preventing unauthorized users or malicious actors from breaking into the system.

Q2



Role-based access control is a access control model , in which based on it’s name, will control access to certain areas of the system based on the roles a user would have within the system and the rules stating what accesses are allowed to users that have been assigned a certain role.





RBAC can also have constraints. These provide a means of adapting RBAC to the specifics of administrative and security policies of an organization. These defined the relationships among roles or a condition related to the roles. These constraints come in the form of 3 different types.

Mutually exclusive > A user can only be assigned to one role in the set (either during a session or statically). Any permission or access right can be granted to the only one role in the set.

Cardinality -> This is setting a maximum number with respect to the roles

Prerequisite roles -> this dictates that a user can only be assigned to a particular role if it’s already assigned to some other specified role.

Text

Description automatically generated

An access matrix is a 2-dimensional structure that contains identified subjects that may attempt to access data and resources in one dimension, and the other contains a list of resources or objects that may be accessed by the subject. Each entry in the matrix indicates the access rights of a particular subject for a particular object.

Table

Description automatically generated

capability list is a key, token, or ticket that grants the processor approval to access an object within the computer system. The user is evaluated against a capability list before gaining access to a specific object. In addition, a capability list is wholly transferable regardless of its administrator. Such an arrangement eradicates the need for system authentication

Diagram

Description automatically generated

Environment attributes -> this is one type of attributes used in ABAC which is attribute based access control. These attributes that describe the operational, technical, and sometimes situational environment or context in which the information access occurs. These attributes have so far been largely ignored in most access control policies. Examples of environmental attributes are like time, location of access attempt, communication protocol and subject’s device.

Credential Management -> this is an established form of software that is used for issuing and managing credentials as part of a public key infrastructure. Examples of credential are smart cards, private/public. Credential management encompasses five logical component which are

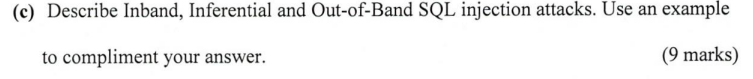
An authorised individual sponsors an individual or entity for a credential to establish the need for the credential.

The sponsored individual enrols for the credential. The process typically consists of identity proofing and the capture of biographic and biometric data. This step may also involve incorporating authoritative attribute data, maintained by the identity management component.

A credential is then produced. Depending on the credential type, the production may involve encryption, the use of a digital signature, the production of a smart card or other functions.

The credential is issued to the individual or NPE.

Finally, a credential must be maintained over it’s life cycle. It might include revocation, reissuance/ replacement, reenrolment, expiration, personal identification number (PIN) reset, suspension or reinstatement.



In-band attacks uses the same communication channel for injecting SQL code and retrieving results. The retrieved data are presented directly in application web page. These include

Tautology -> this form of attack code in one or more conditional statements so that they always evaluate to true

End of line comment -> after injecting code into a particular field, legitimate code that follows are nullified through usage of end of line comments

Piggybacked queries -> the attacker adds additional queries beyond the intended query, piggy-backing the attack on top of a legitimate request.

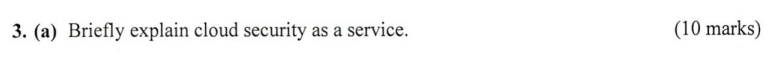
Inferential Attack -> there is no actual transfer of data, but the attack is able to reconstruct the information by the sending particular requests and observing the resulting behaviour of the website or database server.

Include : Illegal/logically incorrect queries

This attack lets an attacker gather important information about the type and structure of the backend database of a web application. The attack is considered a preliminary, information-gathering step for other attacks.

& blind SQL injection which allows attackers to infer the data present in a database system even when the system is sufficiently secure to not display any erroneous information back to the attacker.

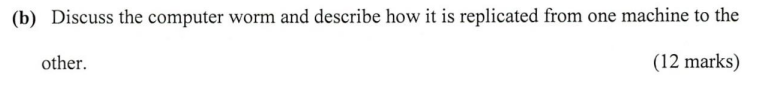
Out of band attack -> data is retrieved using a different channel. This can be used when there are limitations on information retrieval, but outbound connectivity from the database server is lax



The NIST SP-800-145 defines cloud computing as: “A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g, networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of 5 essential characteristics (Broad Network access, rapid flexibility, measured service, on demand self-service, resource), 3 service models (software as a service, platform as a service, infrastructure as a service) and 4 deployment models (public, private, hybrid, community).

The cloud has a number of security threats, and the cloud security alliance, lists the following as the top cloud specific security threats which are: the abuse and nefarious use of cloud computing, insecure interfaces and APIs, malicious insiders, shared technology issues, data loss or leakage, account or service hijacking.

SECaaS , also known as Security as a Service, is a segment of Software as a service. SECaaS is an outsourced service where a outside company handles and manages the security of your cloud application. An example of a security as a service would be anti-virus software over the internet protecting your cloud application from malware. The cloud security alliance defines this as the provision of security applications via the cloud to either cloud-based infrastructure or from the cloud to the customer’s on-premises systems.



A computer worm is a classification of malware. The NIST defines malware 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 system or otherwise annoying or disrupting the system. it is a type of malware that implements the propagation mechanism. This means that the malware infects existing content and is then subsequently spreading to other systems. The propagation mechanism exploits software vulnerabilities to allow malware to replicate.

A computer worm duplicates itself to spread to uninfected computers. It often does this **by exploiting parts of an operating system that are automatic and invisible to the user**. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks.

Worms can be transmitted **via software vulnerabilities**. Or computer worms could arrive as attachments in spam emails or instant messages (IMs). Once opened, these files could provide a link to a malicious website or automatically download the computer worm.

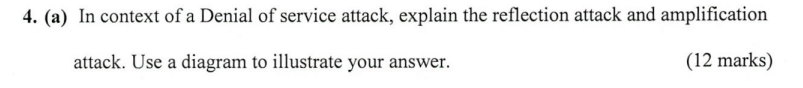
Once a worm has entered your system, usually **via a network connection or as a downloaded file**, it can then run, self-replicate and propagate without a triggering event. A worm makes multiple copies of itself which then spread across the network or through an internet connection.



Viruses are pieces of software that infects programs. They modify programs to include a copy of the virus, as well as similar to worms, replicates itself and goes on to infect other content, and they can easily spread through other network environments. When it is attached to an executable program, a virus can do anything that the program is permitted to do. It executes secretly when the host program is run. A virus is specific to operating system and hardware, and it takes advantage of their details and weaknesses.

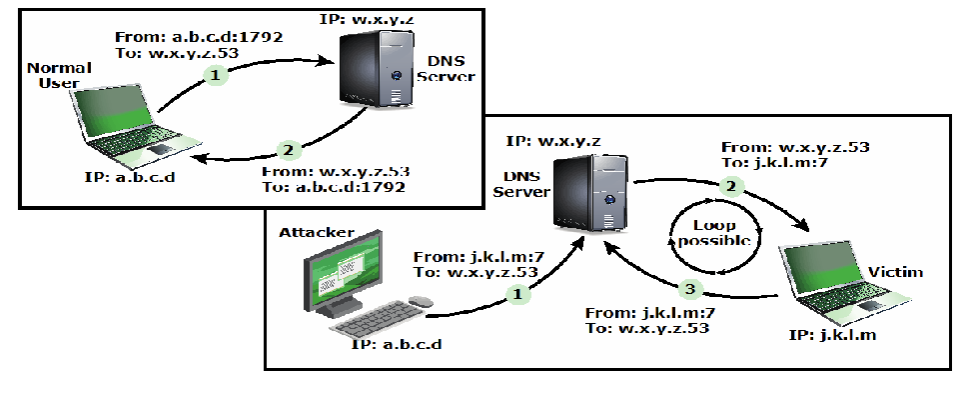
A virus would normally consist of 3 components, which are the infection mechanism which is the means by which a virus spreads or propagates and is also referred to as the infection vector. The trigger is an event or condition that determines when the payload is activated or delivered and is sometimes known as a logic bomb. The final component is the payload, in which it’s what the virus does before spreading and may involve damage or begin noticeable activity.

A virus has 4 lifetime phases, which is first the dormant phase in which the virus is idle and will eventually be activated by some event. Important to note that not all viruses have this stage. The next phase is the triggering phase where the event to trigger the payload occurs and begins to attack. Next phase is the propagation phase where the virus begins to spread into other systems. Finally, the execution phase is the final phase of a virus.



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.

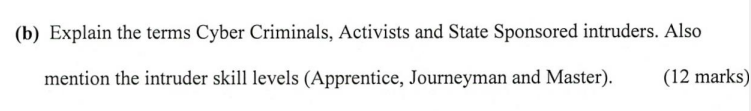
There are several types of DOS attacks, such attacks are the reflection attack and amplification attack. The reflection attack is when the attacker sends packets to a known service on the intermediary with a spoofed source address of the actual target system. when the intermediary responds, the response 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.



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



Cyber criminals are individuals or members of an organized crime group, with a goal of financial reward and may perform activities, such as identity theft, theft of financial credentials, corporate espionage, data theft and data ransoming. They are typically young eastern European, Russian or southeast Asian hackers who do business on the web and meet in underground forums to trade tips and data and coordinate attack.

Intruders can be identified by a number of classes. One of these classes are called Activists, which are individuals, usually working as insiders or members of a larger group of outsider attackers, who are motivated by social or political causes. They are also known as hacktivists whose skill level is often quite low. The aim of their attacks is often to promote and publicize their cause typically through website defacement, DOS attacks or theft and distribution of data that results in negative publicity or compromise of their targets.

Another class is state-sponsored organizations, which are groups of hackers sponsored by the governments to conduct espionage or sabotage activities. Also known as Advanced Persistent threats (APTs) due to the covert nature and persistence over extended periods involved with any attacks in this class. Wipespead nature and scope of these activities by a wide range of countries from China to the USA, UK, and their intelligence allies

Intruder of skills can very into 3 different levels which are

Apprentice -> hackers with minimal technical skill who primarily use existing attack toolkits. They likely comprise the largest number of attackers, including many criminal and activist attackers. Given their use of existing known tools, these attackers are the easiest to defend against. Also known as script-kiddies due to their use of existing scripts (tools)

Journeyman -> hackers with sufficient technical skills to modify and extend attack toolkits to use newly discovered or purchased vulnerabilities. There may be able to locate new vulnerabilities to exploit that are similar to some already known. Hackers with such skills are likely found in all intruder classes. They can adapt tools for use by others.

Master -> Hackers with high-level technical skills capable of discovering brand new categories of vulnerabilities. They can write new powerful attack toolkits. Some of the better-known classical hackers are of this level. Some are employed by state-sponsored organizations. Defending against these attacks is of the highest difficulty.

Text, letter

Description automatically generated

Packet filtering firewalls applies rules to each incoming and outgoing IP packet. It typically a list of rules based on matches in the IP or TCP header. It forwards or discards the packet based on rules match. The filtering rules are based on information contained in a network packet, such as source IP address, destination IP address, source and destination transport-level address, IP protocol field and interface. There is two default policies which are discard – prohibit unless expressly permitted. This policy is more conservative, controlled, visible to users. The second policy is forward which permits unless expressly prohibited. It’s easier to manage and use but less secure.

Advantages is simplicity, typically transparent to users and are very fast. Weaknesses are they cannot prevent attacks that employ application specific vulnerabilities or functions. It has limited logging functionality. Do not support advanced user authentication. Vulnerable to attacks on TCP/IP protocol bugs, improper configuration can lead to breaches.