Ref. No.	Tipo de análisis		
A	**Authentication**		The authentication components of the application will be assessed to identify ways in which these may be bypassed by an attacker. Automated testing such as brute-force password guessing attacks will be attempted against the authentication prompt, while manual code injection testing will be conducted to identify ways in which the authentication may be bypassed altogether through parameter tampering and injecting malicious code into the application
B	**Role Based Access Control (RBAC)**		If multiple user roles are present in the application, testing will be conducted to ensure that users are unable to escalate their privileges either “horizontally” or “vertically”. Horizontal privilege escalation vulnerabilities could allow a user to access the data of other users, whereas a vertical privilege escalation vulnerability could allow a lower-privileged user to access functionality that should only be available to an administrator.
C	**Binary Executable Decompilation**		During the assessment, an attempt will be made to decompile all executable files with the intention of identifying ways in which the underlying code may be circumvented or to identify sensitive information that may be hard-coded. Checks will be made to identify sensitive information that may be hard-coded in the application source code. Typical hard-coded information which may be considered sensitive, includes passwords, database connection strings and PKI certificates – all of which could be useful to an attacker. Specific tests will be conducted to identify ways in which the underlying code may be modified to benefit an attacker, this could include enabling functionality which should not normally be available (for example enabling an “engineering mode”) or enabling features that are protected by a software license restriction.
D	**Network Traffic Analysis**		The network traffic that is sent between the application and server will be closely examined to ensure that it cannot be intercepted or modified in transit. Checks will be made to ensure that the network data is securely-encrypted and that it is not possible to obtain sensitive information from the network traffic or inject malicious code into it to modify the applications behaviour.
E	**Code Injection**		Code injection testing will be performed on all entry points to the application to identify ways in which an attacker could inject malicious code. Depending on the application architecture, this could include SQL injection testing if the application relies on a back-end database or command injection testing in an attempt to execute operating system-level commands on the application server on which the application resides.
F	**Local Data Caching**		The application behaviour will be closely monitored during runtime to identify if sensitive data is being cached locally or logged on the hard drive of the end user’s workstation. If data is being cached, the data will be examined to ensure that it has been encrypted or anonymised to the point where it is not useful to an attacker who has been able to obtain local access to an end user’s workstation.
G	**Application & Service Permissions**		The application and any associated services will be examined to identify the permissions that they have within the operating system. Specific checks will be made to identify the level of access that an attacker would have to the operating system if they have been able to compromise the application.
H	**File Permissions**		The file permissions of all files associated with the application will be examined. The purpose of this examination is to identify if an attacker would be able to tamper with the application executable, log files or library files that may allow them to modify the behaviour of the application.
I	**Digital Code Signing**		The application executable and all associated plugins and Dynamically Linked Libraries (DLL) files will be examined to ensure they have been digitally-signed to ensure that they cannot be tampered with by a malicious user.
J	**Certificate & Key Management**		If the application uses encryption for data or network traffic, specific checks will be made around how the encryption keys and certificates are stored and managed by the application. This is to ensure that the keys or certificates cannot be stolen or forged by a malicious user and then used to circumvent the encryption that is in use by the application.
K	**3rd Party Libraries & Plugins**		An assessment will be conducted on all visible 3rd party plugins and libraries that are used by the application. Checks will be made to ensure that these 3rd party plugins and libraries are up-to-date, and that no publicly-available exploit code exists for them that may impact the overall security of the application.
L	**Source code analysis**		If the source code for the application is available, we can also perform automated analysis in order to identify vulnerabilities that could be exploited.
Según aplique cada característica de la Pentest se aplica en el estudio… Esfuerzo a realizar en 2 semans			