Windows os security assessment essay examples

Business, Company

Windows objects and the file system:

Windows objects are objects that can be identified, accessed and classified by a unique name.

A file system is a data store type that is normally used to store, update and retrieve a given set of files. Computers use specific types of file systems to organize and store data on various media, such as hard drive, CDs, DVDs and flash drives. An example is NTFS used by windows 7. A file system can therefore be viewed as an index to the physical location of every bit of information on a media.

Sessions:

A session is a conversation or a dialogue between communicating devices, or between a computer system and a user.

Security ID, or Security Identifier is a unique, immutable attribute of a given user, user group or security principal (an entity that can be validated and authenticated by a computer or a network). Security ID is commonly abbreviated as SID

Logon rights are rights delegated to a given system user, and stipulate the ways in which the user can log onto the system or network.

Access token is an object that encloses the security descriptor of a given process.

Security Descriptors:

Security descriptors are special data structures that contain security information of securable windows objects. They can be related to any named objects including registry keys, files, folders and shares.

Processes and threads:

A process is an instance of a computer program which is currently in execution. It normally consists of the program code and the current activity. A thread is the smallest succession of programmed instructions that can be independently handled by the scheduler in an operating system

Files access:

These are mechanisms employed by the Operating System to control access to information contained on files. These mechanisms protect files from corruption and modification from unauthorized users.

The registry:

The Registry is a huge batch of files containing information about virtually every activity that occurs on the computer, from an installation of a program to a visit to a particular Web site. The registry is organized in a tree structure, where each top node represents a key.

Key permissions are a set of access rights used to regulate who can modify keys and their constituent values

Key and value squatting is a situation whereby a malicious user or program creates a key and/or values before a legitimate application creates them. Services in the system could store session-related information, thereby allowing malicious applications to squat on key-value pairs.

Windows Inter-Process communication:

Abbreviated as IPC, Inter-Process Communication is a set of mechanisms and techniques provided by the operating system to manage communications

and data sharing among multiple threads within one or more processes. Such mechanisms include Named Pipes, Shared memory, Mapped memory, Message queues and Sockets.

Windows IPC security involves the strategies put in place by the operating system (OS) to ensure secure and safe communication between threads. Such strategies could include memory sharing strategies.

Station Object:

A station object is a securable object that is linked to a process, and contains an atom table, a clipboard, and one or several desktop objects. Station objects are also called window stations.

Desktop Object:

A desktop object is a securable object incorporated in a station object. A desktop usually has an interactive display surface and consists of user interface objects like menus, windows and hooks.

Windows messaging:

Windows messaging is a windows email-client included with Windows 95, windows 98 and Windows NT 4. 0. Windows messaging was initially called Microsoft Exchange

Windows messages:

Windows messages are messages sent to the Operating System for the management of the activities of various windows. For example WM_DESTROY is a message sent to the operating system to indicate that a window is being destroyed.

Shatter attacks:

This is a programming technique applied by malicious system users to circumvent security limitations between processes in a particular session. A shatter attack is made possible due to a design flaw within Windows's message-passing system, where arbitrary codes could be inserted into any service in the same session, which makes use of a message loop

DDE:

DDE, short for Dynamic Data Exchange, is a technique of achieving Inter-Process Communication in Microsoft Windows and/or OS/2. DDE was partially superseded by OLE (Object Linking and Embedding) but is still widely used in simple Inter-Process communication tasks.

Pipes:

A pipe is a method of performing Inter-Process Communication on UNIX or Unix-like systems. A pipe exists anonymously, thus is “ unnamed”, and remains in existence only for as long as the process is still running.
Mail-to: This is a URI (Uniform Resource Identifier) scheme registered by IANA (Internet Assigned Numbers Authority). Mail-to represents the standard scheme for Simple Mail Transfer Protocol (SMTP) email addresses.

Remote procedure calls:

A Remote Procedure Call, abbreviated as RPC, is an inter-process communication that enables a computer program to cause a particular subroutine or procedure to execute in another address space, usually on a different computer within a shared network, without the developer explicitly specifying the details of this remote interaction.

COM:

Component Object Model (COM) is a binary-interface standard for software modules that was introduced by Microsoft in 1993. It enables inter-process communication and dynamic object creation in a wide variety of programming languages. COM forms the basis for most of other Microsoft technologies and frameworks, including ActiveX, OLE (Object Linking and Embedding), DCOM (Distributed Component Object Model), and OLE Automation, DirectX, COM+, the Windows shell and Windows Runtime. Today, Microsoft exposes every new technology by implementing each new module as a COM object. COM is the standard way to interact with subsystems like ADSI (Active Directory Services Interface), DirectX, Shell extensions, ActiveX controls, MTS (Microsoft Transaction Server) and ActiveX scripting.

The major goal of COM is language independence. COM based components can be developed in a wide range of development environments.

References

Russinovich, M. E., Solomon, D. A., & Ionescu, A. (2009). Windows® Internals. New York: O'Reilly Media, Inc.

Dowd, M., & McDonald, J. (2006). The art of software security assessment: Identifying and preventing software vulnerabilities. Harlow: Addison-Wesley.

Russinovich, M. E., & Margosis, A. (2011). Windows sysinternals administrator's reference. Redmond, Wash: Microsoft Press.