

What is a kernel windows_priv

A kernel is a computer program that serves as the core or heart of an operating system. It manages memory management, task management, and disk management.

Kernel Functionality	Device management	A device driver is a computer program that enables the operating system to interact with a hardware device.
	Memory management	The kernel is responsible for deciding which memory each process can use, and determining what to do when not enough memory is available.
	Access Resource Management	I/O devices include such peripherals as keyboards, mice, disk drives, printers, USB devices, network adapters, and display devices.
	Resource management	Kernels also provide methods for synchronization and inter-process communication (IPC).

An operating system has the following separated spaces:

- **Kernel Space:** A kernel is typically maintained and loaded into a distinct memory region referred to as protected Kernel space. It is secured against access by application programs or less critical components of the operating system.
- **User Space:** The operating system (OS) is the software that acts as a bridge between hardware components and the end-user. User-space memory is used by application programs such as a browser, word processor, and audio and video player.

lab_link:- windows 7 build 7600

<https://archive.org/details/build-7600-rtm>

<https://stackoverflow.com/questions/44389963/how-to-install-mingw32-on-ubuntu>

sudo apt-get install gcc-mingw-w64

i686-w64-mingw32-gcc 40564.c -o MS11-046.exe -lws2_32

```
(kali㉿kali)-[~/HTB/devel]
$ i686-w64-mingw32-gcc 40564.c -o MS11-046.exe -lws2_32

(kali㉿kali)-[~/HTB/devel]
$ ls
40564.c  MS11-046.exe  shell.aspx  shell.exe  shell.jsp  test.txt  winPEAS.bat
```

Watson tool

<https://github.com/rasta-mouse/Watson>

<https://www.hackingarticles.in/windows-privilege-escalation-kernel-exploit/>