Every example is related to a Secred Castle.

- Whoami: User
- Whoami /priv : The whoami /priv command in a Windows command prompt or PowerShell session displays the security privileges of the current user. This command provides information about the user's security token, specifically the privileges that are assigned to that user.
- SeShutdownPrivilege (Shutdown):This privilege allows a user to shut down the system. It's like having the ability to turn off the lights in the castle. This is a powerful privilege that should be given only to trusted users.
- SeChangeNotifyPrivilege (Bypass Traverse Checking):This privilege allows a user to bypass certain security checks when accessing files or directories. It's like having a secret shortcut through the castle that lets you move around more freely.
- SeUndockPrivilege (Undock):This privilege is related to mobile computing. It allows a user to undock a laptop or other mobile device from a docking station. It's like being able to detach your knight's shield when they want to move around more easily.
- SeIncreaseWorkingSetPrivilege (Increase a Process Working Set):This privilege allows a user to increase the amount of memory a process can use. It's like being able to give more space to a room in the castle when it needs it.
- SeTimeZonePrivilege (Change the Time Zone):This privilege allows a user to change the time zone of the system. It's like being able to adjust the clocks in the castle to match a different time zone.

Whoami \groups

1. Alias: An alias is a type of security group that is predefined by the operating system to represent a set of users or other groups. Aliases are created for common sets of permissions or roles, making it easier to manage access control. Example: The "BUILTIN\Users" and "BUILTIN\Administrators" groups are examples of aliases. The "Users" group includes all user accounts on the system, while the "Administrators" group grants administrative privileges.
2. Well-known group: Well-known groups are a specific category of security groups that are built into the Windows operating system and have predefined SIDs (Security Identifiers). These groups have consistent SIDs across all Windows systems, making them universally recognizable. Example: The "Everyone" and "INTERACTIVE" groups are well-known groups. The "Everyone" group includes all user accounts, and the "INTERACTIVE" group represents users who are interactively logged on to the system

WinPEAS (Windows Privilege Escalation Awesome Scripts) is a collection of various scripts and binaries for Windows post-exploitation, enumeration, and privilege escalation. It's designed to automate the process of gathering information on a Windows system that may be useful for security assessments or penetration testing.

The "exe" in "WinPEASexe" indicates that it's an executable file (an EXE file). To use WinPEAS, you typically upload or transfer the WinPEAS executable to the target Windows machine and then run it to perform automated enumeration and analysis.

Here are some common use cases for WinPEAS:

Privilege Escalation: WinPEAS helps identify potential paths for privilege escalation by checking misconfigurations, weak permissions, and vulnerabilities on the system.

Enumeration: It collects a wide range of information about the system, including details about user accounts, installed software, network configurations, and more.

Post-Exploitation: After gaining initial access to a system, security professionals and penetration testers can use WinPEAS to gather additional information that may aid in further exploitation or lateral movement.

Scripted Analysis: WinPEAS includes a variety of scripts bundled together, making it a convenient tool for conducting comprehensive Windows security assessments.

It's important to note that while WinPEAS is a powerful tool for security professionals, it should be used responsibly and only in environments where you have explicit permission to conduct security assessments.

To use WinPEAS, you typically download the latest version from the official GitHub repository, transfer it to the target system, and then execute it. The tool will generate a detailed report with information about the system's configuration and potential security issues.

Hotfixes, in the context of Windows operating systems, refer to patches or updates that are released by Microsoft to address specific issues, vulnerabilities, or bugs in the software. These fixes are typically targeted and are released outside of the regular Windows Update schedule