# INTRODUCTION TO WINDOWS

It's crucial to be knowledgeable about a wide range of technologies if you want to be a penetration tester. In a variety of evaluation kinds, having a solid grasp of Windows and Linux operating systems is advantageous. These two operating systems will form the foundation of the bulk of the systems we come across during evaluations, whether they are on-premise or in the cloud. It's crucial to comprehend how to protect against attacks on various operating systems as well as how each one might be employed as a platform for more penetration testing operations. The objective of this assignment is to gather specific information about a target workstation. It consists of two practical questions that focus on identifying crucial details about the workstation's build number and the installed Windows NT version.

# TASKS

What is the build number of the target workstation?

Since I am using a Linux machine ill use OpenVPN to connect to the HTB instance. After that I will connect to the rdp using the ‘xfreerdp’ tool together with the given Ip, username and password information. Then use the Get-WmiObject cmdlet to find information about the operating system. This will give you the build number of the working station. This answers the first question 19041.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

Which Windows NT version is installed on the workstation?

From the previous question in the PowerShell we already have the answer for this question. It indicated that we are using Windows 10 version. There are also many other ways to find out.

A screenshot of a computer

Description automatically generated with medium confidence

# OPERATING SYSTEM STRUCTURE

The operating system structure in Windows is built upon a layered architecture, with the kernel at its core. The kernel, known as the Windows Executive, provides essential services like process management, memory management, and I/O operations.

# TASKS

Find the non-standard directory in the C drive. Submit the contents of the flag file saved in this directory.

Using the given hint that the directory starts with A we are going to make use of dir and cd command. Open cmd and move out of the user’s directory to the C directory. Here you’ll find an academy folder. Cd to this folder and you shall find a flag then cat this flag. (c8fe8d977d3a0c655ed7cf81e4d13c75)

A picture containing text, screenshot, font

Description automatically generated

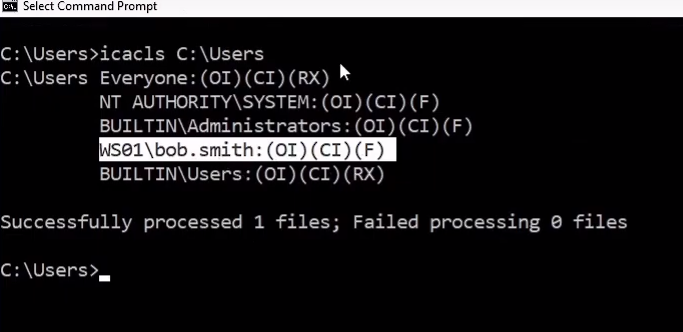
# FILE SYSTEM

Managing and arranging data on storage devices is the responsibility of the file system in Windows, which is essentially NTFS. To ensure dependability and security, NTFS provides cutting-edge features including file and folder permissions, encryption, compression, and journaling. The Master File Table (MFT) is a fundamental component and holds data about files and directories, including metadata like size, permissions, and timestamps. Long file names, technologies like compression and encryption, and Windows' hierarchical directory structure enable for orderly data storage while enhancing file management capabilities.

# TASKS

What system user has full control over the c:\users directory?

So now we need to check the permissions for users in that users directory. Cd users and hit dir command. Next utilize the icacls tool followed by the directory path and you will get the permissions information there. bob.smith is the answer.



# NTFS VS SHARE PERMISSIONS

NTFS permissions and Share Permissions are two distinct access control mechanisms in Windows. NTFS permissions are applied at the file and folder level on NTFS-formatted drives, allowing for precise control over access rights for individual users and groups. With NTFS permissions, administrators can assign permissions such as read, write, modify, and full control to regulate local and remote access. In contrast, Share Permissions are set on shared folders to control remote access over a network. While Share Permissions provide a broader level of access control, they are less granular than NTFS permissions, as they apply to the entire shared folder rather than specific files or folders within it. It is common practice to configure both NTFS and Share Permissions together to establish comprehensive security measures for shared resources in Windows.

# TASKS

What protocol discussed in this section is used to share resources on the network?

SMB

What is the utility that can be used to view logs made by a Windows system?

Event Viewer

What is the full directory path to the Company Data share we created?

Copy paste from the tutorial(C:\Users\htb-student\Desktop\Company Data)

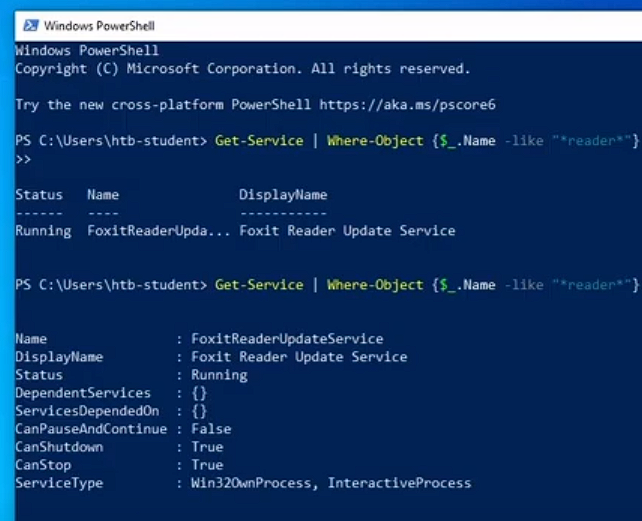
# WINDOWS SERVICES & PROCESSES

Windows Services and Processes play crucial roles in the functioning of the Windows operating system. Services are background programs that run independently of user interaction and provide system-level functionality, such as networking, printing, or security. They start automatically during system boot and continue running until shutdown. On the other hand, Processes are instances of executing programs and applications.

# TASK

Identify one of the non-standard update services running on the host. Submit the full name of the service executable.

We use the Get-Service command in PowerShell and then simplify the output to only outputs that their $\_.Name is -like “\*reader\*”. This is because we were given a hint that the service is related to pdf e.g., an adobe reader. Ans FoxitReaderUpdateService.exe



# SERVICE PERMISSIONS

Service permissions in Windows determine the access rights and privileges assigned to services, which are background programs that provide system-level functionality. Service permissions regulate the ability of users, groups, or processes to interact with and control specific services. These permissions allow administrators to define who can start, stop, pause, or modify the configuration of a service. By configuring service permissions, administrators can enhance security, limit access to sensitive services, and ensure that only authorized entities can manage or manipulate the behaviour of services. Service permissions play a crucial role in maintaining the integrity, availability, and reliability of the Windows operating system by providing fine-grained control over service management and access.

# WINDOWS SESSIONS

In Windows, a session refers to a user's interactive or remote interaction with the operating system. A session begins when a user logs in to the system and ends when the user logs out or the session is disconnected. Each session is independent and maintains its own set of resources, including a unique session identifier, user-specific settings, and running applications. Windows supports multiple concurrent sessions, allowing multiple users to interact with the system simultaneously. Remote desktop sessions enable users to access the system remotely and interact with their own separate sessions. Windows Sessions play a vital role in facilitating user interactions, managing resources, and maintaining a secure and personalized computing experience for each user in a multi-user environment.

# INTERACTING WITH WINDOWS OS

The graphical user interface (GUI) was introduced to improve the usability of operating systems and make them more accessible to everyday users. It provides an interactive point-and-click interface for users to navigate through the system and applications without relying on the command line. RDP (Remote Desktop Protocol) is a Microsoft protocol that enables users to remotely connect to a system and access its GUI as if they were physically present. System administrators often use RDP for remote administration, while users can utilize it to access their work computers from home through a VPN. Command-line interfaces, such as the Command Prompt (CMD) and PowerShell, offer users greater control over their systems and the ability to perform various administrative and troubleshooting tasks. Command-line interfaces allow for automation and efficient execution of tasks, such as adding multiple users to a domain simultaneously. While GUIs provide a user-friendly experience, command-line interfaces offer flexibility and power in managing Windows operating systems.

# TASKS

What is the alias set for the ipconfig.exe command?

We can do this using the get-alias. It will give us a list of all aliases. Ans ifconfig

Find the Execution Policy set for the LocalMachine scope.

Use the Get-ExecutionPolicy command to get the list. Ans is Unrestricted

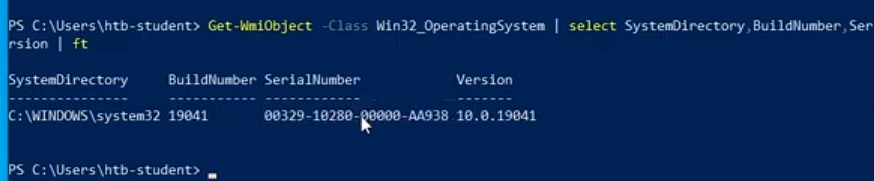
# WINDOWS MANAGEMENT INSTRUMENTATION (WMI)

System administrators have access to effective tools for system monitoring using the PowerShell subsystem WMI. Consolidating device and application administration across corporate networks is the aim of WMI. Since Windows 2000, WMI has been pre-installed and is an essential component of the Windows operating system. It consists of the following elements:

# TASKS

Use WMI to find the serial number of the system.

Again, we make use of the WmiObject tool for this to get details about the os then we can see our serial number. Ans 00329-10280-00000-AA938



# Microsoft Management Console (MMC)

To control hardware, software, and network components on a Windows host, snap-ins, or administrative tools, can be grouped in the MMC. It is supported by all Windows versions and has been around since Windows Server 2000.

# Windows Subsystem for Linux (WSL)

Linux binaries may now be executed natively on Windows 10 and Windows Server 2019 thanks to a technology called WSL. It was first created for programmers who need direct access to native Linux command-line tools like sed, awk, grep, and bash on their Windows workstations. A program called Bash.exe is installed by WSL, and it may be launched by simply entering bash into a Windows terminal to launch a Bash shell. From this shell, we can see the entire appearance and feel of a Linux server, including the default Linux directory structure.

# Desktop Experience vs. Server Core

When Windows Server Core was initially introduced, it was a basic server environment with only the most essential server features. As a consequence, Server Core utilizes less memory and disk space than Desktop Experience (GUI) and has less maintenance needs. It also offers a reduced attack surface. All configuration and upkeep procedures in Server Core are carried out via the command line, PowerShell, remote administration using MMC, or Remote Server Administration Tools (RSAT). Although Server Core doesn't have a graphical user interface (GUI), it still supports several graphical applications including PowerShell, Registry Editor, Notepad, System Information, Windows Installer, and Task Manager. Additionally, it supports parts of the Sysinternals suite's features, including TCPView, Active Directory Explorer, Process Explorer, and Process Monitor.

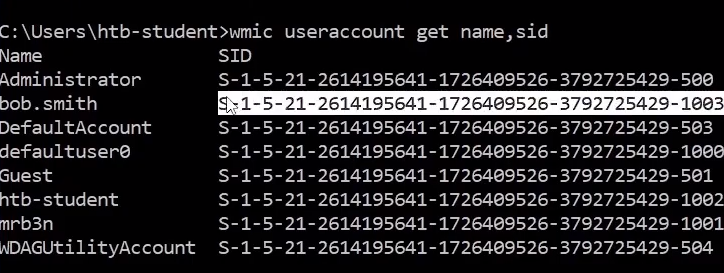
# Windows Security

Windows Security plays a vital role in safeguarding the operating system and user data from various threats. Windows OS incorporates multiple layers of security features and mechanisms to protect against malware, unauthorized access, and data breaches. These security measures include built-in firewall protection, regular security updates and patches, and robust user authentication protocols. Windows Defender, the built-in antivirus and anti-malware solution, provides real-time protection against known and emerging threats.

# TASKS

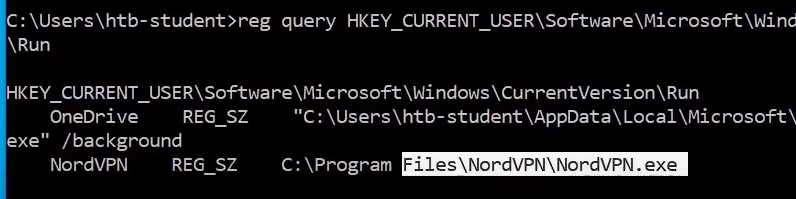
Find the SID of the bob.smith user.

Using cmd and using wmic get names and sid. Ans S-1-5-21-2614195641-1726409526-3792725429-1003



What 3rd party security application is disabled at startup for the current user?

Use registry keys HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run



# **SKILLS ASSESSMENT - WINDOWS FUNDAMENTALS**

Do this process: Creating a shared folder called Company Data. Creating a subfolder called HR inside of the Company Data folder. Creating a user called Jim, Uncheck: User must change password at log. Creating a security group called HR. Adding Jim to the HR security group. Adding the HR security group to the shared Company Data folder and NTFS permissions list, Remove the default group that is present, Share Permissions: Allow Change & Read, Disable Inheritance before issuing specific NTFS permissions, NTFS permissions: Modify, Read & Execute, List folder contents, Read, Write. Adding the HR security group to the NTFS permissions list of the HR subfolder, Remove the default group that is present, Disable Inheritance before issuing specific NTFS permissions, NTFS permissions: Modify, Read & Execute, List folder contents, Read, and Write. Using PowerShell to list details about a service

# QUESTIONS

What is the name of the group that is present in the Company Data Share Permissions ACL by default?

everyone

What is the name of the tab that allows you to configure NTFS permissions?

security

What is the name of the service associated with Windows Update?

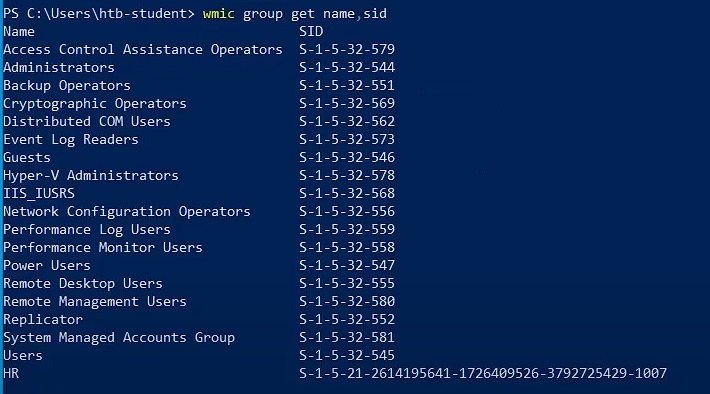
wuauserv

List the SID associated with the user account Jim you created.

S-1-5-21-2614195641-1726409526-3792725429-1006

List the SID associated with the HR security group you created.

Remember to change from name to group S-1-5-21-2614195641-1726409526-3792725429-1007



# CONCLUSION

In conclusion, the Windows operating system provides a robust computing environment with various components and functionalities. The operating system structure in Windows follows a layered architecture, with the kernel at its core, supported by subsystems and a graphical user interface (GUI) shell. The file system in Windows, primarily NTFS, offers advanced features for managing data on storage devices, while service permissions enable fine-grained control over access to services. Windows Sessions allow for user interactions and resource management, supporting multiple concurrent sessions and remote access. Additionally, Windows Security features provide protection against malware, unauthorized access, and data breaches. These features include firewall protection, regular security updates, antivirus software, encryption, and secure authentication. Overall, Windows operating system excels in providing a user-friendly GUI, efficient resource management, secure file systems, and robust security measures. Its combination of graphical interfaces, remote access capabilities, and comprehensive security features make it suitable for both everyday users and system administrators, ensuring a reliable and secure computing experience. [**LINK**](https://academy.hackthebox.com/achievement/643478/49)