



## WINDOWS FUNDAMENTALS CHEAT SHEET

Command	Description
<code>xfreerdp /v:&lt;target IP address&gt; /u:htb-student /p:&lt;password&gt;</code>	RDP to lab target
<code>Get-WmiObject -Class win32_OperatingSystem</code>	Get information about the operating system
<code>dir c:\ /a</code>	View all files and directories in the c:\ root directory
<code>tree &lt;directory&gt;</code>	Graphically displaying the directory structure of a path
<code>tree c:\ /f   more</code>	Walk through results of the <code>tree</code> command page by page
<code>icacls &lt;directory&gt;</code>	View the permissions set on a directory
<code>icacls c:\users /grant joe:f</code>	Grant a user full permissions to a directory
<code>icacls c:\users /remove joe</code>	Remove a users' permissions on a directory
<code>Get-Service</code>	<b>PowerShell</b> cmdlet to view running services
<code>help &lt;command&gt;</code>	Display the help menu for a specific command
<code>get-alias</code>	List <b>PowerShell</b> aliases

Command	Description
<code>New-Alias -Name "Show-Files" Get-ChildItem</code>	Create a new <b>PowerShell</b> alias
<code>Get-Module   select Name,ExportedCommands   fl</code>	View imported <b>PowerShell</b> modules and their associated commands
<code>Get-ExecutionPolicy -List</code>	View the <b>PowerShell</b> execution policy
<code>Set-ExecutionPolicy Bypass -Scope Process</code>	Set the <b>PowerShell</b> execution policy to bypass for the current session
<code>wmic os list brief</code>	Get information about the operating system with <b>wmic</b>
<code>Invoke-WmiMethod</code>	Call methods of <b>WMI</b> objects
<code>whoami /user</code>	View the current users' SID
<code>reg query &lt;key&gt;</code>	View information about a registry key
<code>Get-MpComputerStatus</code>	Check which <b>Defender</b> protection settings are enabled
<code>sconfig</code>	Load Server Configuration menu in Windows Server Core