HACKTHEBOX

WINDOWS FUNDAMENTALS

CHEAT SHEET

RDP to lab target:

```
xfreerdp /v:<target IP address>
/u:htb-student /p:<password>
```

Get information about the operating system:

```
Get-WmiObject -Class win32_OperatingSystem
```

View all files and directories in the c:\ root directory:

```
dir c:\ /a
```

Graphically displaying the directory structure of a path:

```
tree <directory>
```

Walk through results of the tree command page by page:

```
tree c:\ /f | more
```

View the permissions set on a directory:

```
icacls <directory>
```

HTB ACADEMY CHEATSHEET

HTB ACADEMY CHEATSHEET

WINDOWS FUNDAMENTALS

CHEAT SHEET

Grant a user full permissions to a directory:

```
icacls c:\users /grant joe:f
```

Remove a users' permissions on a directory:

```
icacls c:\users /remove joe
```

PowerShell cmdlet to view running services:

```
Get-Service
```

Display the help menu for a specific command:

```
help <command>
```

List PowerShell aliases:

```
get-alias
```

Create a new PowerShell alias:

```
New-Alias -Name "Show-Files" Get-ChildItem
```

View imported PowerShell modules and their associated commands:

```
Get-Module | select Name,ExportedCommands | fl
```

View the PowerShell execution policy:

```
Get-ExecutionPolicy -List
```

HACKTHEBOX

WINDOWS FUNDAMENTALS

CHEAT SHEET

Set the PowerShell execution policy to bypass for the current session:

```
Set-ExecutionPolicy Bypass -Scope Process
```

Get information about the operating system with wmic:

```
wmic os list brief
```

Call methods of WMI objects:

```
Invoke-WmiMethod
```

View the current users' SID:

```
whoami /user
```

View information about a registry key:

```
reg query <key>
```

Check which Defender protection settings are enabled:

```
Get-MpComputerStatus
```

Load Server Configuration menu in Windows Server Core:

```
sconfig
```