DefenderC2> send_command agent-name command

🔐 USER & SYSTEM AUTH

DefenderC2> send_command agent-1 whoami

DefenderC2> send_command agent-1 hostname

DefenderC2> send_command agent-1 echo %username%

DefenderC2> send_command agent-1 id

DefenderC2> send_command agent-1 query user

DefenderC2> send_command agent-1 net user

DefenderC2> send_command agent-1 net user USERNAME

DefenderC2> send_command agent-1 net localgroup administrators

DefenderC2> send_command agent-1 getent passwd

DefenderC2> send_command agent-1 wmic useraccount get name,sid

💻 SYSTEM INFORMATION

DefenderC2> send_command agent-1 systeminfo

DefenderC2> send_command agent-1 uname -a

DefenderC2> send_command agent-1 lscpu

DefenderC2> send_command agent-1 hostnamectl

DefenderC2> send_command agent-1 wmic computersystem get model,name,manufacturer

DefenderC2> send_command agent-1 wmic os get Caption,CSDVersion,OSArchitecture,Version

🌐 NETWORK INFO

DefenderC2> send_command agent-1 ipconfig /all

DefenderC2> send_command agent-1 ifconfig

DefenderC2> send_command agent-1 netstat -ano

DefenderC2> send_command agent-1 ss -tulnp

DefenderC2> send_command agent-1 route print

DefenderC2> send_command agent-1 ip a

DefenderC2> send_command agent-1 arp -a

DefenderC2> send_command agent-1 netsh wlan show profile

DefenderC2> send_command agent-1 ip r

DefenderC2> send_command agent-1 ip n

🧠 ACTIVE PROCESSES

DefenderC2> send_command agent-1 tasklist

DefenderC2> send_command agent-1 ps aux

DefenderC2> send_command agent-1 top -n 1

DefenderC2> send_command agent-1 Get-Process

DefenderC2> send_command agent-1 wmic process list brief

🔧 SERVICES

DefenderC2> send_command agent-1 sc query

DefenderC2> send_command agent-1 systemctl list-units --type=service

DefenderC2> send_command agent-1 Get-Service

DefenderC2> send_command agent-1 service --status-all

🧱 FIREWALL & PORTS

DefenderC2> send_command agent-1 netsh advfirewall show allprofiles

DefenderC2> send_command agent-1 ufw status verbose

DefenderC2> send_command agent-1 firewall-cmd --list-all

DefenderC2> send_command agent-1 iptables -L

📂 FILE SYSTEM & STORAGE

DefenderC2> send_command agent-1 dir C:\

DefenderC2> send_command agent-1 ls -la /

DefenderC2> send_command agent-1 tree /f

DefenderC2> send_command agent-1 wmic logicaldisk get name,size,freespace

DefenderC2> send_command agent-1 df -h

DefenderC2> send_command agent-1 mount

🧭 DIRECTORY NAVIGATION

DefenderC2> send_command agent-1 cd \

DefenderC2> send_command agent-1 pwd

DefenderC2> send_command agent-1 ls

DefenderC2> send_command agent-1 dir

📜 ENVIRONMENT VARIABLES

DefenderC2> send_command agent-1 set

DefenderC2> send_command agent-1 env

DefenderC2> send_command agent-1 printenv

⏱️ SYSTEM UPTIME

DefenderC2> send_command agent-1 uptime

DefenderC2> send_command agent-1 net statistics workstation

🧩 INSTALLED SOFTWARE

DefenderC2> send_command agent-1 wmic product get name,version

DefenderC2> send_command agent-1 powershell "Get-WmiObject -Class Win32_Product"

DefenderC2> send_command agent-1 dpkg -l

DefenderC2> send_command agent-1 rpm -qa

DefenderC2> send_command agent-1 flatpak list

🛡️ SECURITY EVENTS (Windows)

DefenderC2> send_command agent-1 wevtutil qe Security /f:text /c:10

DefenderC2> send_command agent-1 auditpol /get /category:*

🦹 USB & DEVICES

DefenderC2> send_command agent-1 wmic logicaldisk where drivetype=2 get deviceid, volumename, description

DefenderC2> send_command agent-1 lsusb

DefenderC2> send_command agent-1 lspci

💬 NETWORK SHARES

DefenderC2> send_command agent-1 net share

DefenderC2> send_command agent-1 smbclient -L //localhost

⚙️ SCHEDULED TASKS

DefenderC2> send_command agent-1 schtasks /query /fo LIST /v

DefenderC2> send_command agent-1 crontab -l

📦 INSTALLED DRIVERS

DefenderC2> send_command agent-1 driverquery

DefenderC2> send_command agent-1 lsmod

🗑️ DELETION / FILE ACTIONS (Use With Care ⚠️)

DefenderC2> send_command agent-1 del C:\example.txt

DefenderC2> send_command agent-1 rm /home/user/file.txt

DefenderC2> send_command agent-1 copy C:\source.txt D:\dest.txt

📂 LOG FILES

DefenderC2> send_command agent-1 type C:\Windows\WindowsUpdate.log

DefenderC2> send_command agent-1 cat /var/log/syslog

DefenderC2> send_command agent-1 tail -n 50 /var/log/auth.log

This gives you extensive control over agent machines for:

🕵️ Forensics

🔐 Threat Hunting

📡 Live Monitoring

📘 Report generation