

How to Perform Microsoft Windows Post Exploitation on a Security Test



On a security test once you have compromised a Microsoft Windows machine there are a number of actions that you are going to want to perform to profile the target system. These are listed as follows:

- Operating System Profiling
 - C:\> **ver**
 - Display version information about the operating system.
 - C:\> **systeminfo**
 - Displays detailed system information about the target system.
 - C:\> **hostname**
 - Displays the target system current host name.
- Network Profiling
 - C:\> **ipconfig /all**
 - This displays information on the status, and configuration, of the network adaptors. It will also display information about the domain configuration of the target system.
 - C:\> **netstat -ano**
 - Display information about the process with open TCP/UDP ports.
 - C:\> **route print**
 - This displays routing information and can be used to help map out network topology.
 - C:\> **netsh advfirewall show allprofiles**
 - This displays the firewall profiles and state.
- User Profiling
 - C:\> **whoami /all**
 - Displays information about the current users and its associated privileges.
 - C:\> **echo %username%**
 - Displays the name of the current user.
 - C:\> **net users**
 - Produces a list of users on target machine. We can then further analyse each user in this list via the C:\> **net users <username>** command.
 - C:\> **net localgroup**
 - Produces a list of local groups on target machine.
 - C:\> **net group /domain**
 -
- Service Profiling
 - C:\> **tasklist /svc**
 - Display a list of processes/tasks running on the target system
 - C:\> **net start**
 - Display a list of all services running on the target system
 - C:\> **sc query**
 - Enumerates status of active services and drivers. A more detailed description of the service can be obtained via the C:\> **sc qc <service name>** command.
- File System Profiling
 - C:\> **icacls <filename>**
 - Displays access permissions on a specified filename. The goal is to identify files that we have Write permission to.

There are a number of automated tools that can help you profile a target system these include:

- BeRoot - <https://github.com/AlessandroZ/BeRoot/tree/master/Windows>
- WindowsEnum - <https://github.com/absolomb/WindowsEnum>
- PowerUp - <https://github.com/PowerShellMafia/PowerSploit/tree/master/Privesc>
- Metasploit - <https://www.offensive-security.com/metasploit-unleashed/privilege-escalation/>