Windows Fundamentals 2

## **SOC Learning Report – Windows Fundamentals 2**

**Analyst:** Inam Qadeer  
**Tool(s) Used:** Windows 10 VM, TryHackMe Lab Environment

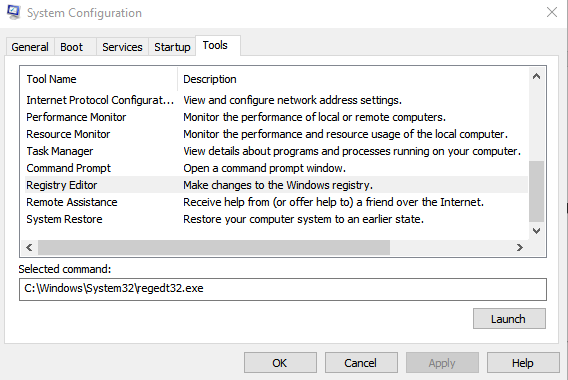
### **1. Executive Summary**

The Windows Fundamentals 2 lab focuses on deeper navigation of the Windows operating system, specifically the Task Manager, User Account Control (UAC), Windows Registry, and Command Prompt/PowerShell.  
These tools are essential for SOC analysts to monitor running processes, control application permissions, and investigate system configurations during incident response.

### **2. Investigation / Learning Steps**

1. **Task Manager**
   * Learned how to view running processes, CPU/memory usage, and network activity.
   * Explored tabs such as Processes, Performance, App history, Startup, Users, and Details.
2. **User Account Control (UAC)**
   * Examined UAC settings and learned how they help prevent unauthorized changes to the system.
3. **Windows Registry**
   * Navigated the Registry Editor (regedit) to view and understand how Windows stores configuration data.
   * Observed key areas like HKEY\_LOCAL\_MACHINE and HKEY\_CURRENT\_USER.
4. **Command Prompt & PowerShell**
   * Learned basic command-line operations such as dir, ipconfig, and PowerShell commands for system information.

### **3. Findings**

* **Task Manager** can help identify suspicious processes (e.g., malware disguising as system processes).
* **UAC** helps block unapproved software from making changes. Lower UAC settings increase the risk of malware infections.
* **Registry** is a common target for persistence techniques in attacks; attackers may add keys to auto-run malicious scripts.
* **Command Prompt / PowerShell** allows powerful system interaction and can be used by attackers for lateral movement if not secured.
* 

### **4. Importance for SOC Work**

* Monitoring **Task Manager** helps detect high CPU/memory processes or unknown executables.
* Checking **UAC settings** can reveal if security controls have been weakened.
* Investigating the **Windows Registry** can uncover malware persistence.
* Knowing basic **CLI commands** helps with quick triage during live response.

### **5. Recommendations**

* Keep UAC at the default or higher setting to block unauthorized changes.
* Regularly review **Startup** entries in Task Manager for suspicious programs.
* Back up the registry before making changes and monitor for unusual keys.
* Limit PowerShell access for standard users to reduce attack surface.

### **6. Conclusion**

Windows Fundamentals 2 provides the operational knowledge to monitor and manage processes, control permissions, and investigate system configurations — all critical skills for SOC analysts responding to Windows-based threats.

