### **Report 4: Suspicious PowerShell Execution**

**Title**: Suspicious PowerShell Execution through Encoded Command  
**Date**: June 1, 2025  
**Platform**: TryHackMe SOC Level 1 Simulator  
**Severity**: High  
**Detection** Tool: Splunk SIEM  
**Category**: Scripting Abuse

**Steps Taken:**

* Queried logs in Splunk for powershell.exe with -EncodedCommand
* Found a suspicious command executed by a user at 10:03 AM
* Command decodes to the execution of Invoke-WebRequest and script download
* Source IP traced to 185.62.57.49 (flagged as malicious on VirusTotal)
* Activity was not consistent with baseline user behavior

**Final Assessment**:  
**True Positive**. This was a likely malware dropper or reconnaissance script being executed using PowerShell obfuscation. Potential compromise of user account.

**Mitigation**:

* Block outbound web access for scripting tools
* Review account activity for further signs of compromise
* Add alerting for any future PowerShell encoded commands
* Do a full malware scan and memory dump analysis