

SOC lab – Malicious PowerShell Incident Report

Emma

August 20th, 2026

Incident Report

Date of Incident: August 19th, 2026

Type of Incident: Malicious Network Connection, Insider Threat

Description of Event: At 6:04pm CST we identified an unauthorized PowerShell session execution on Workstation A using Lab Admin's Account to connect to 192.168.122.117; from this IP two PowerShell Scripts were downloaded onto Lab User's A desktop and executed. The logs recorded a single PowerShell Session using Lab Admins Credentials which both scripts were downloaded and executed.

Initial discovery on the workstation shows an empty folder on Workstation A, C: drive named HACKER, and two unknown scripts on the default desktop. Folder-Creation.ps1 and Process-Network.ps1 both appear non-malicious. The risk of an Insider Threat from Lab Admin and Lab User A are visible due to this event.

Detection: Wazuh SIEM System, Windows Event Logs, Physical Discovery

Action Taken: Blocked external device IP 192.168.122.117. This IP was identified as an unauthorized device on our network. This IP was connected to, and both files were downloaded from it. Lab User A, and Lab Admin were given formal warnings, and the created folder, and downloaded files were removed. Both users were required to change their passwords.