Incident Response Report

Title: PowerShell Activity Simulation & Response – Hosts File Access and Firewall Rule Addition
Date and Time: 13 May 2025, 11:30 PM (IST)
Reported by: Karthik S Arkasali

---

1. Incident Overview

This report documents a simulated suspicious activity using PowerShell. The activity involved accessing the system's hosts file and adding a firewall rule to block outbound network connections. This simulation demonstrates the detection and incident response workflow.

---

2. Simulation Details

2.1 Suspicious Command Execution

Start-Process "notepad.exe" -ArgumentList "C:\Windows\System32\drivers\etc\hosts"

- **Purpose:** Opens the system hosts file in Notepad.
- **Executed By:** User account running PowerShell (retrieved from logs).
- **Timestamp:** Captured via Event ID 4103 in Event Viewer.
- **Log Path:**
  Event Viewer > Applications and Services Logs > Microsoft > Windows > PowerShell > Operational

2.2 Firewall Modification Simulation

New-NetFirewallRule -DisplayName "Block Network Access" -Direction Outbound -Action Block -Enabled True -Profile Any

- **Purpose:** Simulates blocking outbound connections for containment.
- **Risk:** Can be used by attackers to isolate a system or prevent updates.

---

3. Detection and Analysis

- **Tool Used:** Event Viewer
- **Log Type:** PowerShell Operational Logs
- **Event ID:** 4103 (Script Block Logging)

- **Findings:**
    - Detected command to open hosts file.
    - User and timestamp captured.
    - No signs of real malware or persistence.

---

4. Incident Response

4.1 Containment

- **Command Executed:**

New-NetFirewallRule -DisplayName "Block Network Access" -Direction Outbound -Action Block -Enabled True -Profile Any

- **Impact:** Temporarily blocked outbound connections.

4.2 Eradication

- **Restored hosts file from backup (if needed):**

Copy-Item "C:\Backup\hosts" -Destination "C:\Windows\System32\drivers\etc\hosts" -Force

- **Removed Suspicious File (if any):**

Remove-Item "C:\Path\To\SuspiciousFile.exe" -Force

4.3 Recovery

- **Restored System (if needed):**

Restore-Computer -RestorePoint 1

- **Re-enabled Network Access:**

Set-NetFirewallRule -DisplayName "Block Network Access" -Enabled False

---

5. Recommendations

- Enable PowerShell Logging (Event IDs 4103, 4104) in Group Policy.
- Apply file integrity monitoring using AIDE or Windows tools.
- Restrict access to C:\Windows\System32\drivers\etc\hosts to administrators only.
- Monitor for unusual firewall rule changes using audit policies.
- Educate users on avoiding unknown scripts or PowerShell misuse.

- Use Endpoint Detection and Response (EDR) tools to track execution and isolate systems quickly.

---

6. Evidence Screenshots (Attached)

- PowerShell Operational Log – Event ID 4103
- Hosts file opened in Notepad
- Confirmation of new firewall rule
- Removal of suspicious file
- Restoration and recovery actions