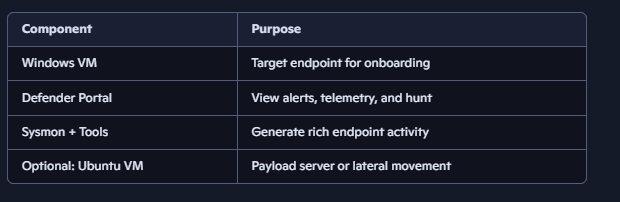
# 🎯 Goal

Simulate a real-world SOC scenario: onboard a Windows VM to Defender for Endpoint, generate telemetry through benign and suspicious activity, and validate detection and hunting capabilities.

# 🛠️ Lab Setup Overview

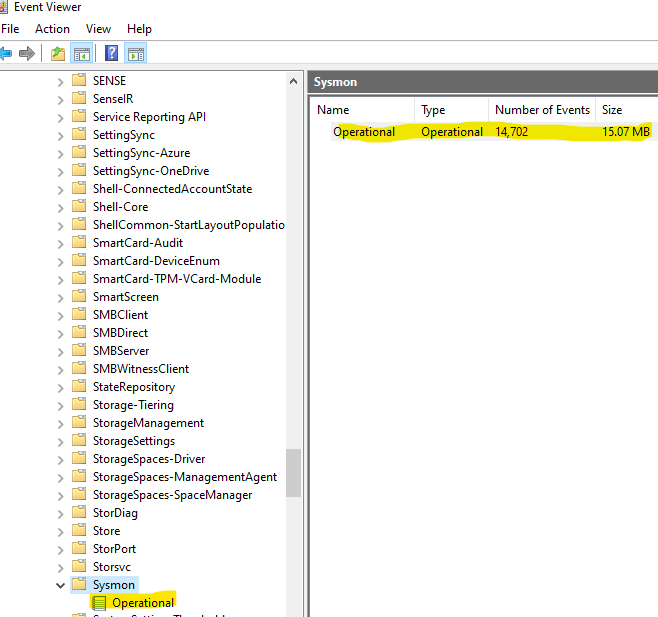


# 🔧 Step-by-Step Setup

## 1️⃣ Prepare Your Windows VM

* Use **Windows 10/11 Pro or Enterprise**
* Ensure internet access and latest updates
* Install **Sysmon** with a community config:

sysmon -accepteula -i sysmonconfig.xml



## 2️⃣ Onboard to Defender for Endpoint

### 🔐 Step 1: Go to the Right Portal

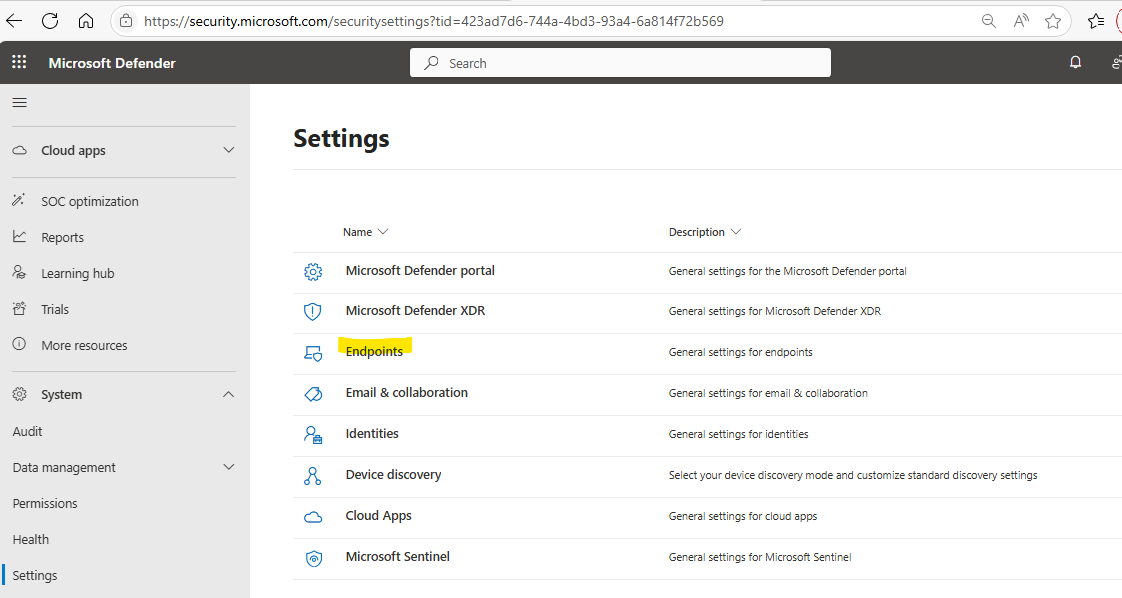
* Go to <https://security.microsoft.com>
* This is now called **Microsoft Defender XDR** (formerly Microsoft 365 Defender)

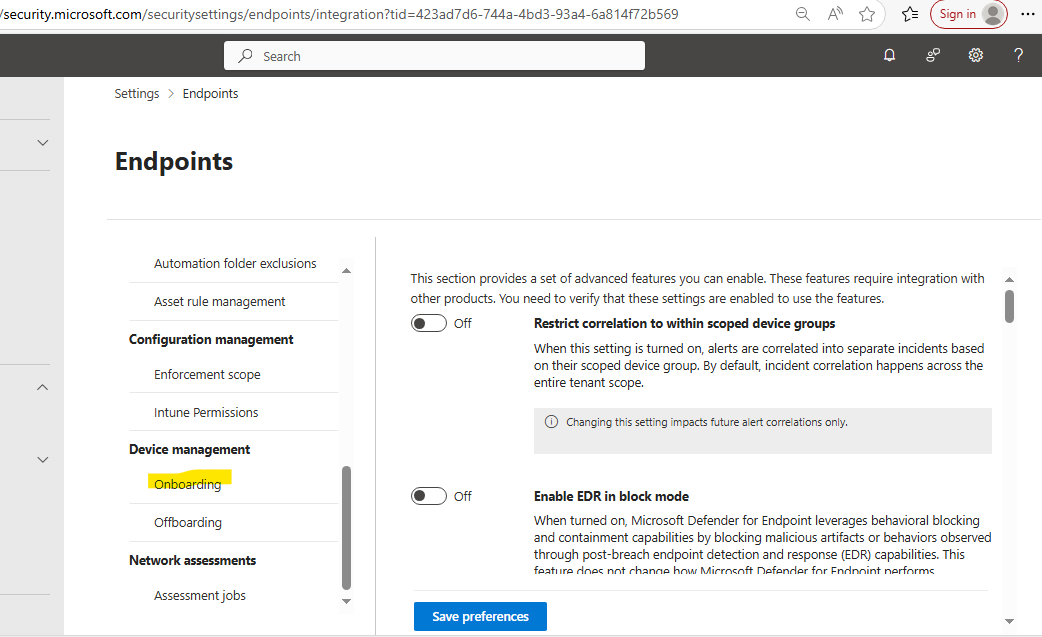
### ⚙️ Step 2: Navigate to Device Onboarding

1. In the left-hand menu, click **Settings** (gear icon at bottom left)
2. Under **Settings**, choose **Endpoints**
3. Then select **Device Onboarding**

You’ll now see onboarding options for:

* **Windows 10/11**
* **Windows Server**
* **macOS**
* **Linux**
* **Mobile (Android/iOS)**





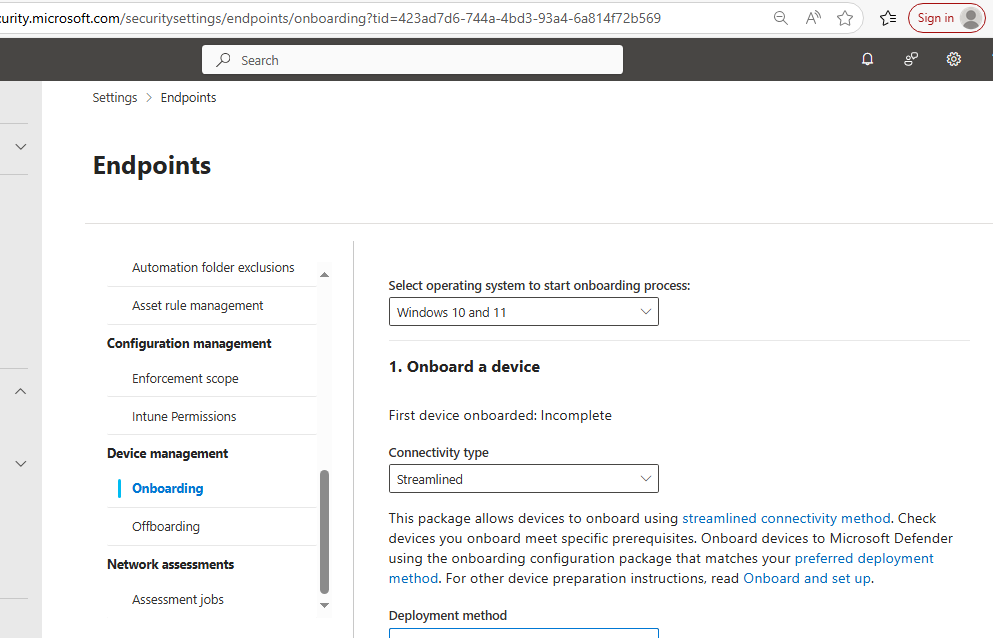
### 📦 Step 3: Choose Your Platform & Onboarding Method

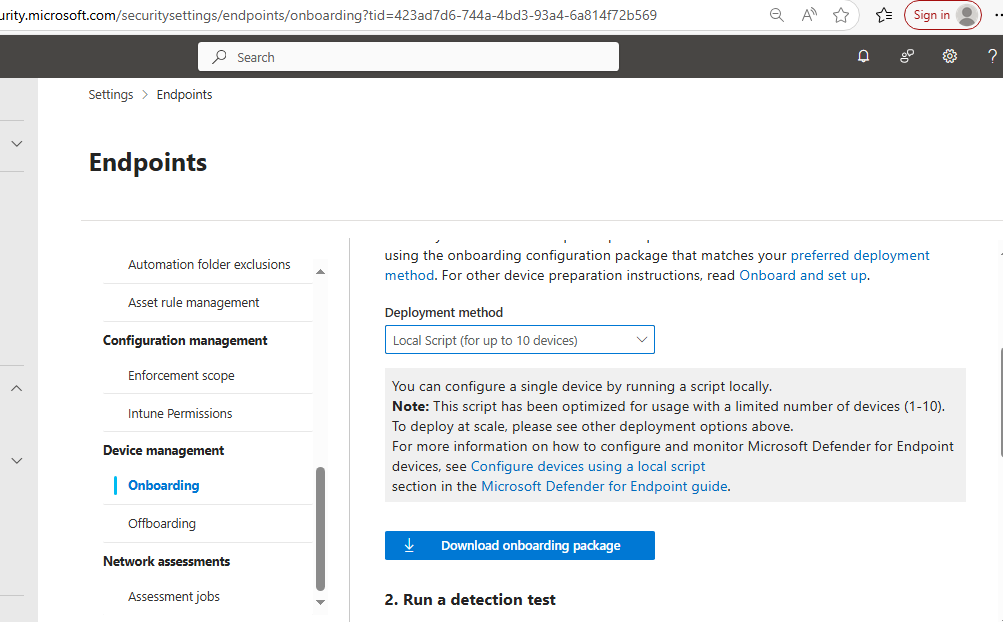
For your **Windows VM**:

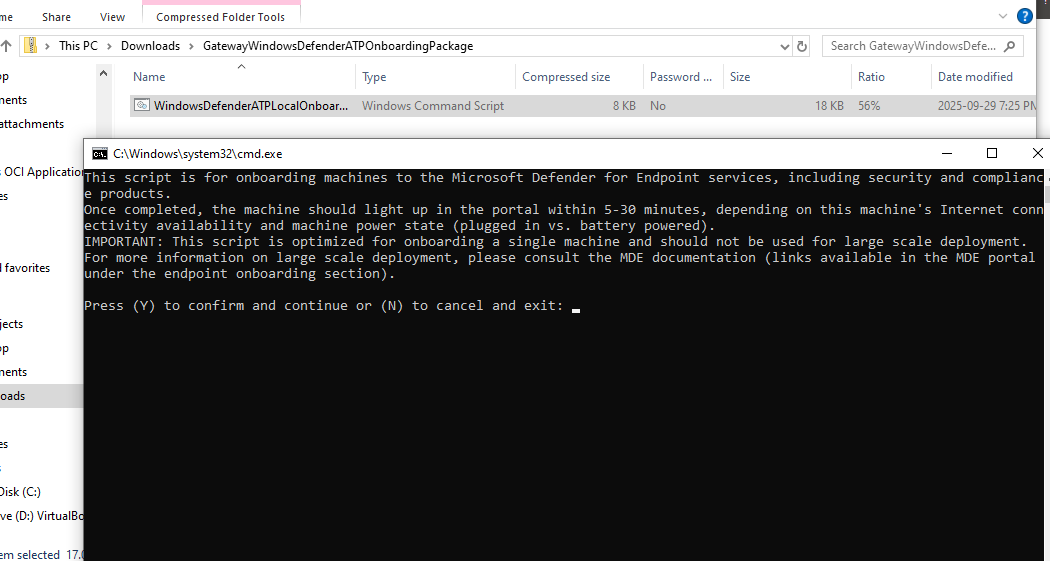
* Select **Windows 10/11**
* Choose **Local Script** (ideal for home lab)
* Download the onboarding package
* Run the script inside your VM

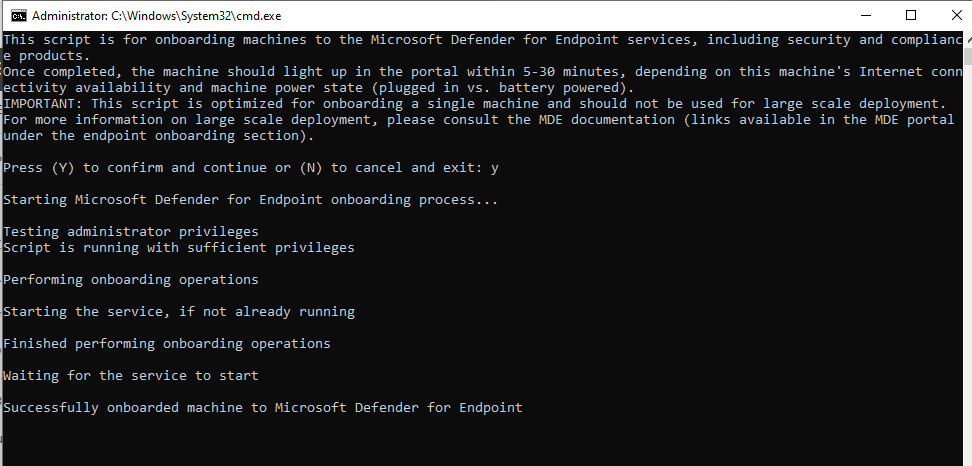
For **Ubuntu VM**:

* Select **Linux**
* Follow the instructions to install the MDE Linux agent
* Run the onboarding script via terminal





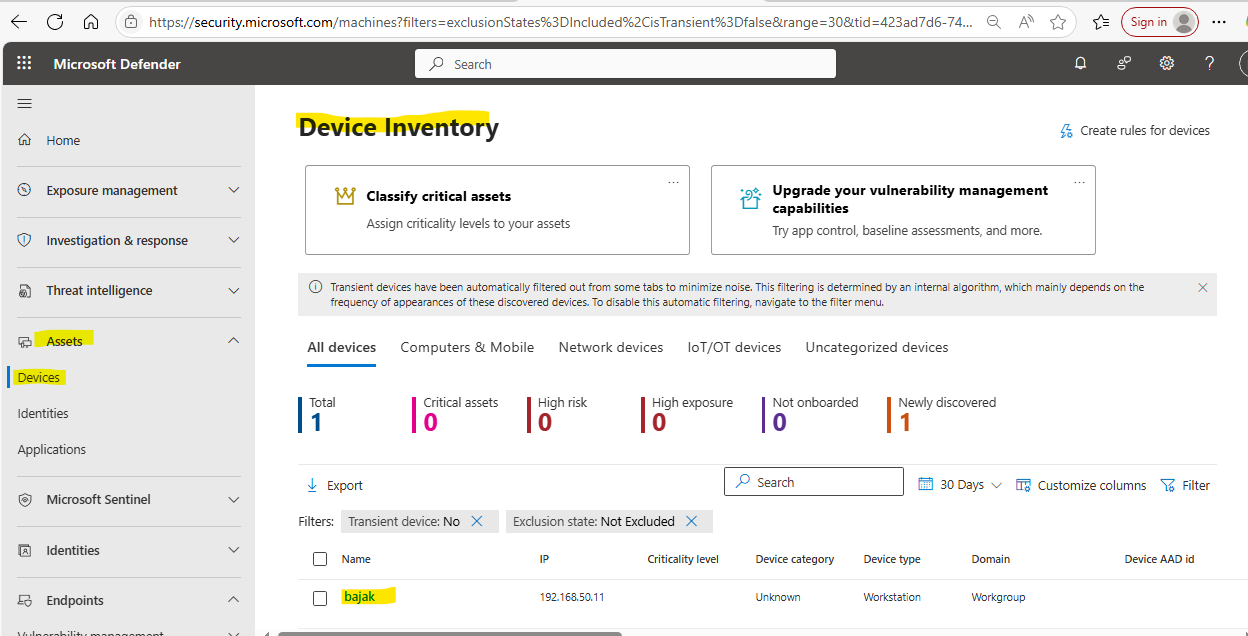




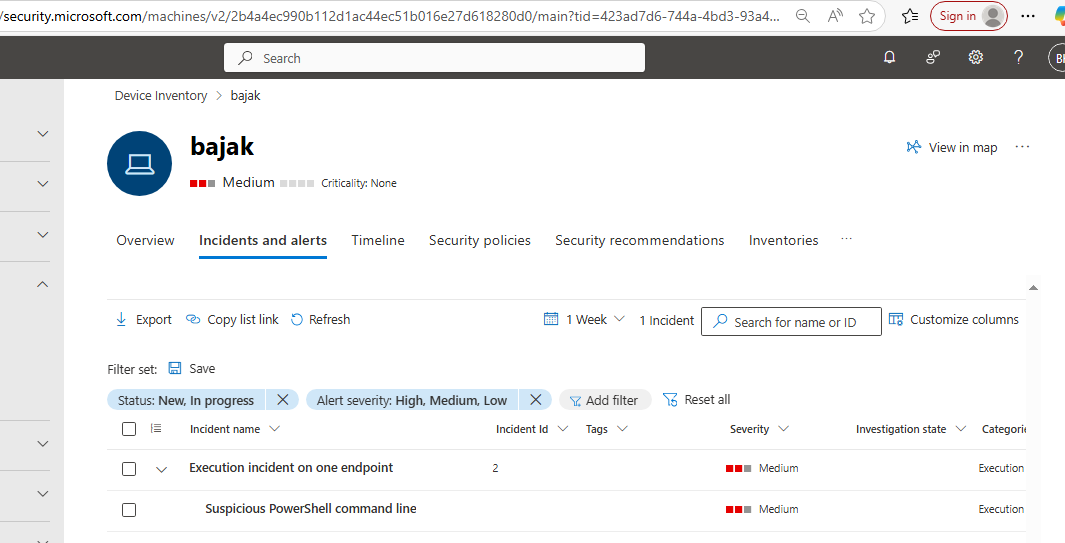


### 🧪 Step 4: Validate Onboarding

* Go to **Devices > Device Inventory**
* Your VM should appear within 30–60 minutes
* You can now simulate activity and use **Advanced Hunting** to query telemetry



The detection test I ran showed up under incidents and alerts tab as seen in the screen shot below

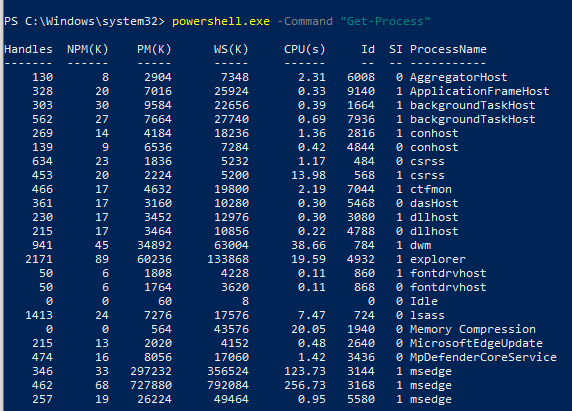


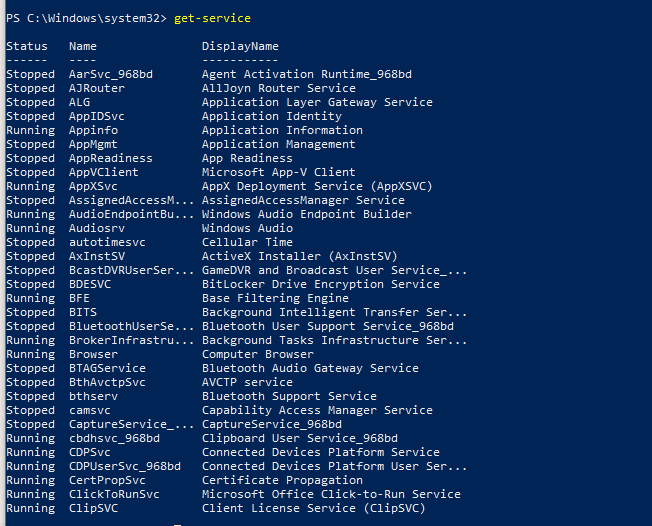
## 3️⃣ Simulate Suspicious Activity

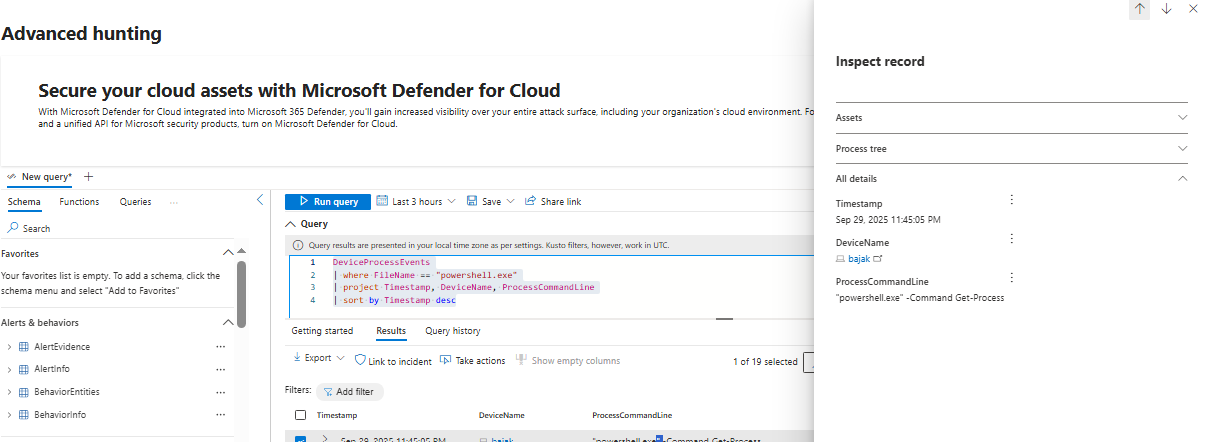
#### 🔹 PowerShell Enumeration

Get-Process

Get-Service

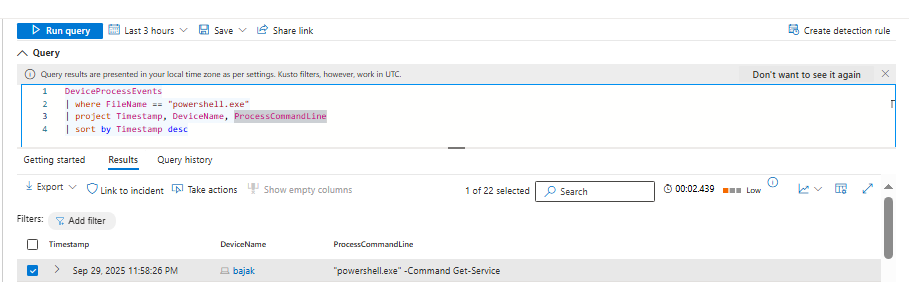






What I just proved is that:

* 1. Command line auditing is enabled.
  2. Telemetry is flowing to MDE.
  3. I can detect real threats.

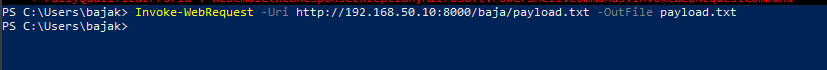


#### 🔹 LOLBin (Living off the land binary) Execution

LOLBins are legitimate windows binaries often abused by attackers.

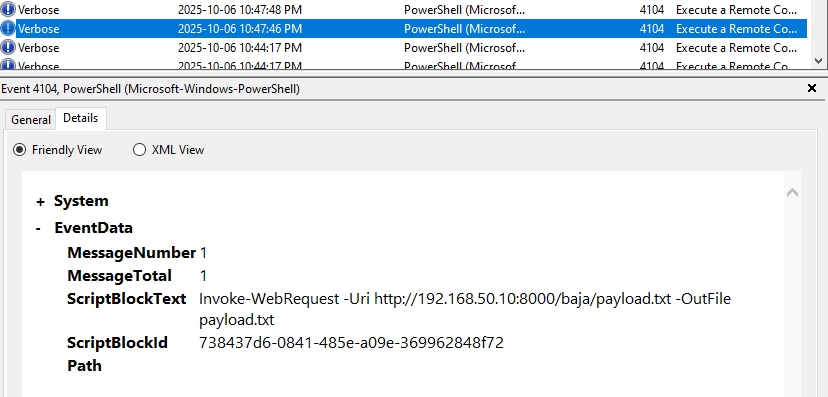
Invoke-WebRequest -Uri [http://your-ubuntu-vm-ip/payload.txt -OutFile payload.txt](http://your-ubuntu-vm-ip/payload.txt%20-OutFile%20payload.txt)

* 1. Powershell initiates a webrequest
  2. Powershell downloads the file
  3. The file is saved locally

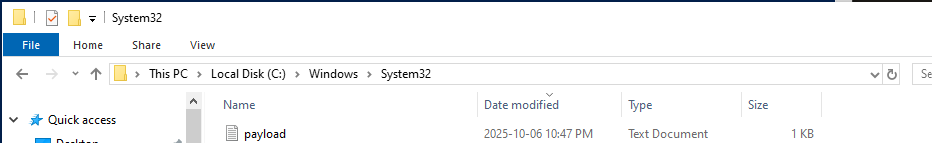




Script block logged event id 4104 captured the command as script block logging is enabled.



The payload file from ubuntu got successfully downloaded to windows vm as seen in the path below



As seen in the screen shots below Microsoft Defender for Endpoint

Device Network Events logged the outbound connections

