**Cybersecurity 401**

**Module 6 - Threat Modeling and Analysis**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

## **Lab 26 - Remote Code Execution**

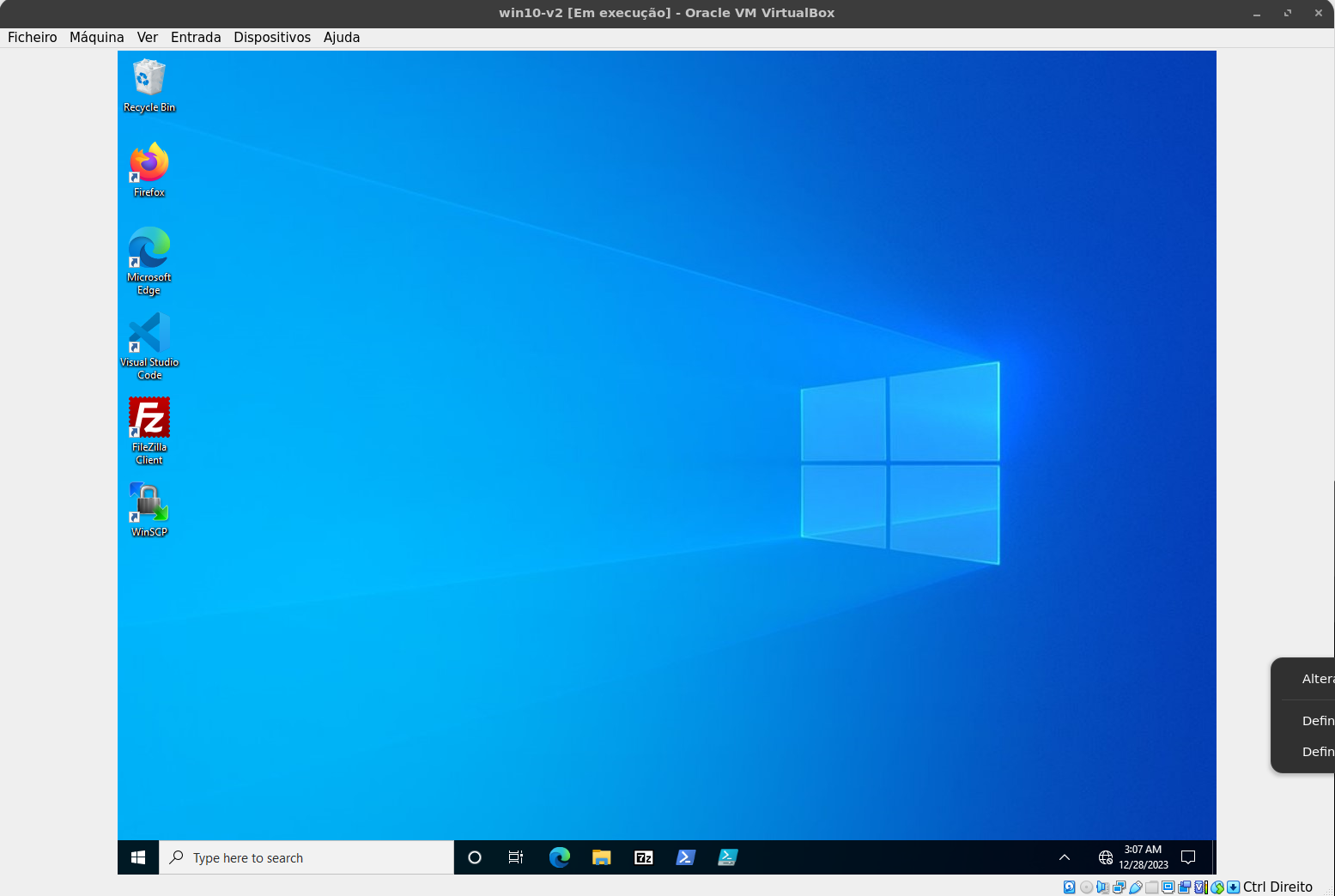
## 

**| Rodrigo Brasil 12/2023 |**

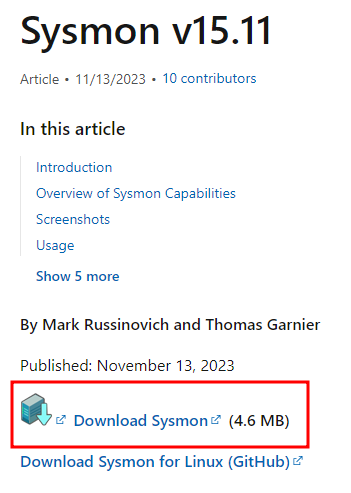
### **Part 1: Staging**

This lab utilizes Splunk Enterprise (Trial), Windows Server 2019, and Windows 10. If you’d like to start term 2 with a working baseline threat detection lab environment in VirtualBox, download and import Term2-baseline-lab-v5.zip. You are welcome to use your own VMs instead, but you may need to manually configure things such as VirtualBox network adapters, etc. If you end up using the provided baseline lab, skip to the final two items in the list below. The remaining labs in this module will be instructing you as if you are using the provided lab environment.

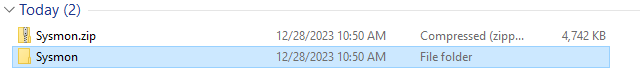
* Prepare a Windows 10 VM

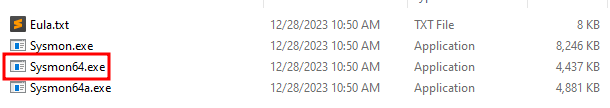


* Install Sysmon on Windows 10 VM

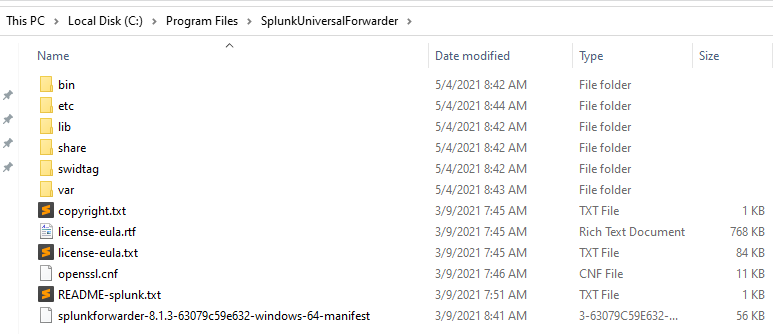


<https://learn.microsoft.com/pt-pt/sysinternals/downloads/sysmon>



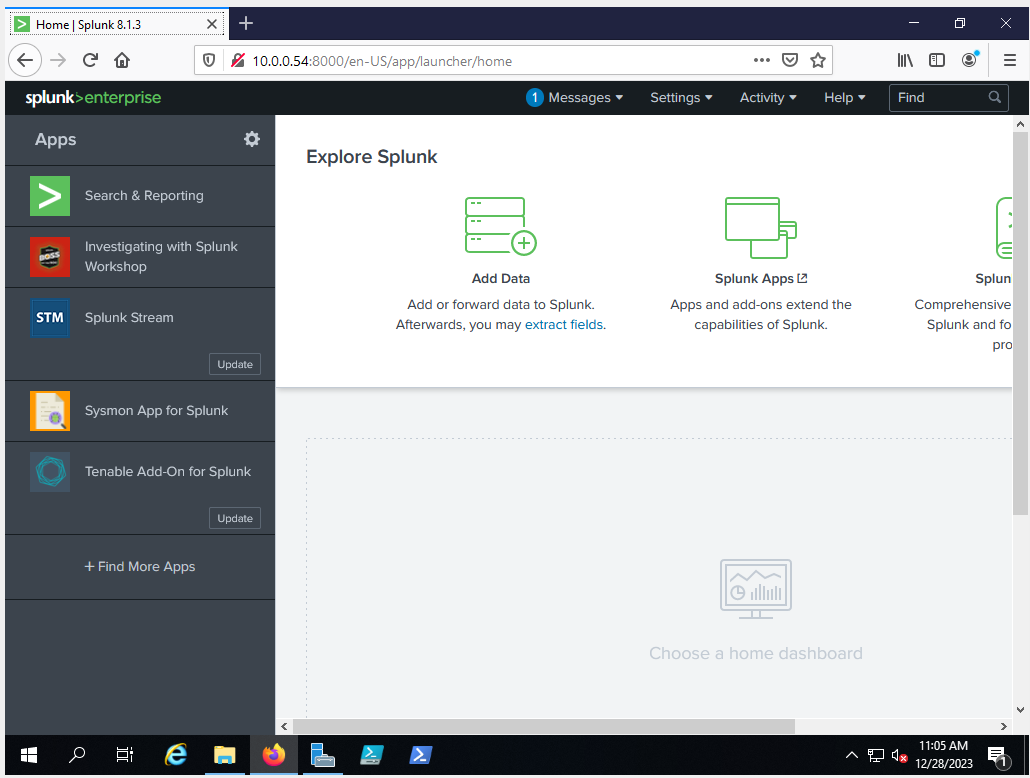


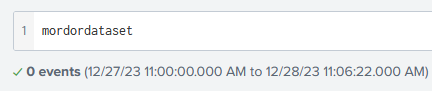
* Install Splunk Universal Forwarder on Windows 10 VM to forward logs in real time to Splunk



* On Windows Server, download Invoke-PsExec for Powershell







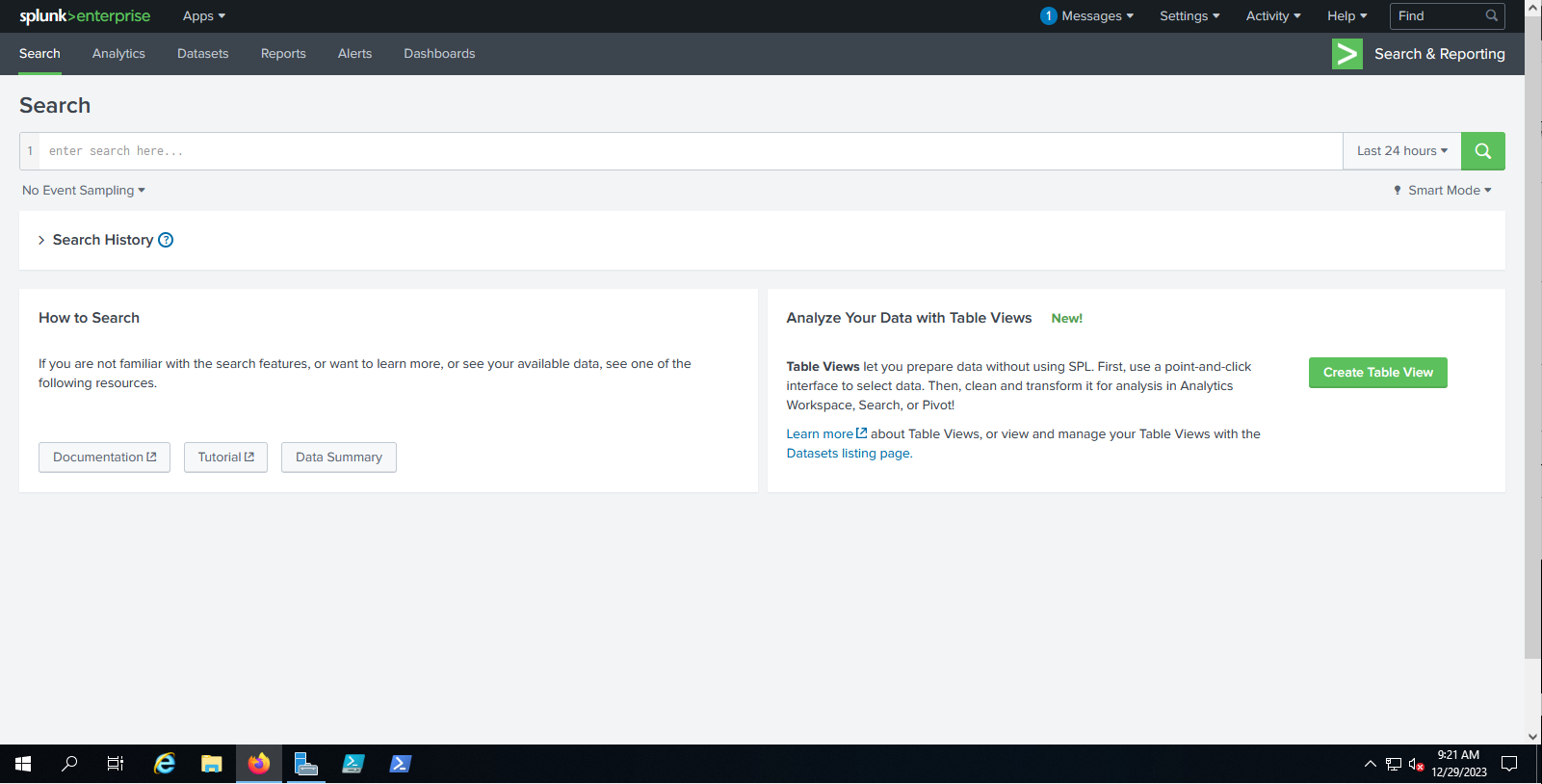
***\*\*Note****\*\*: If your Splunk instance has an expired enterprise license, you will have daily indexing limits (500MB per day). If you need more than that, follow the Staging Instructions for Splunk (provided above). Otherwise, Splunk free will suffice.*

### 

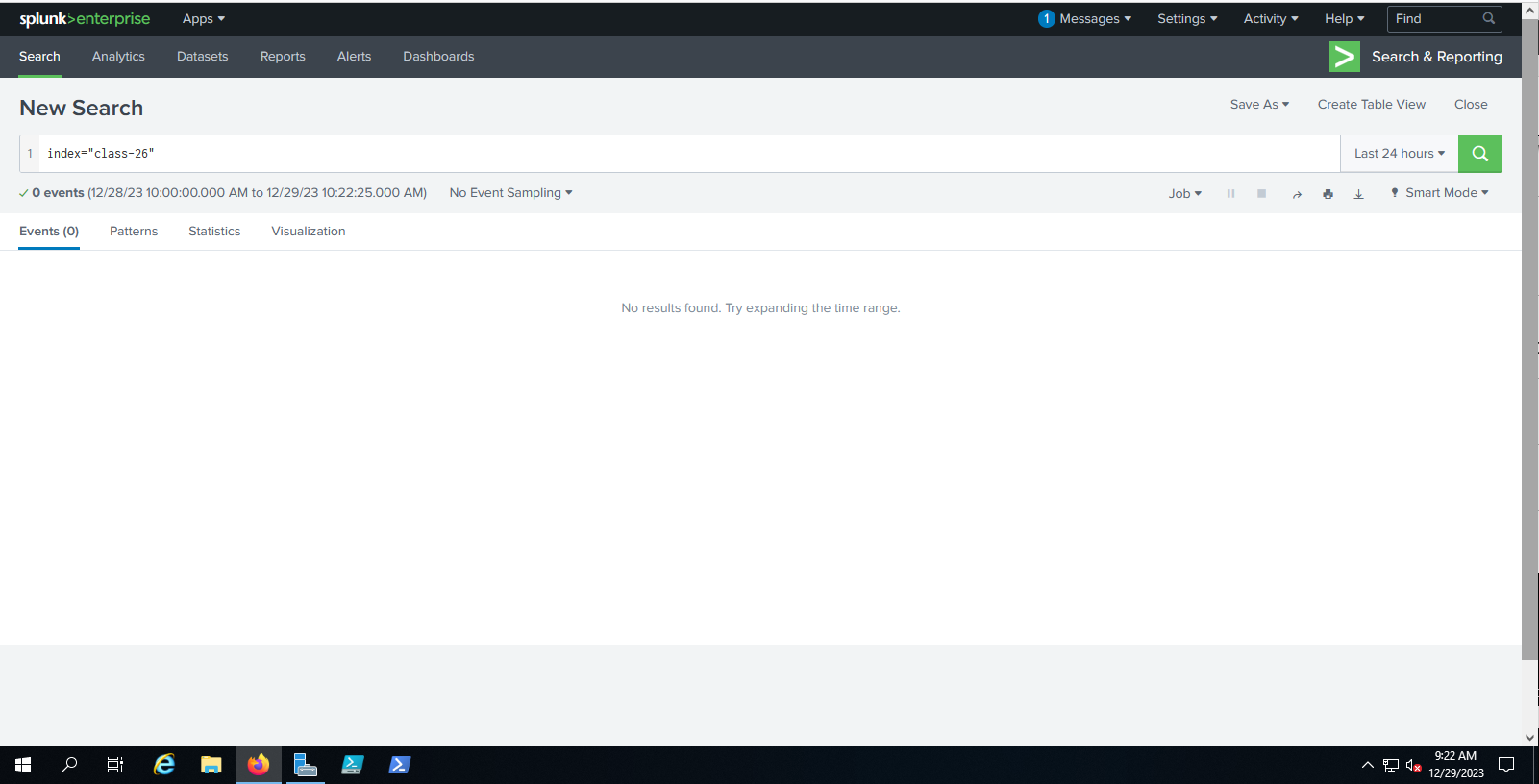
### **Part 2: Analysis of a Sample Data Set**

In this part of the lab, we will investigate the data set by consulting the PsExec Artifacts Reference as a guide for obtaining critical information from our sample data set. Get ready to practice your SPL querying skills as we comb through a sizable data set.

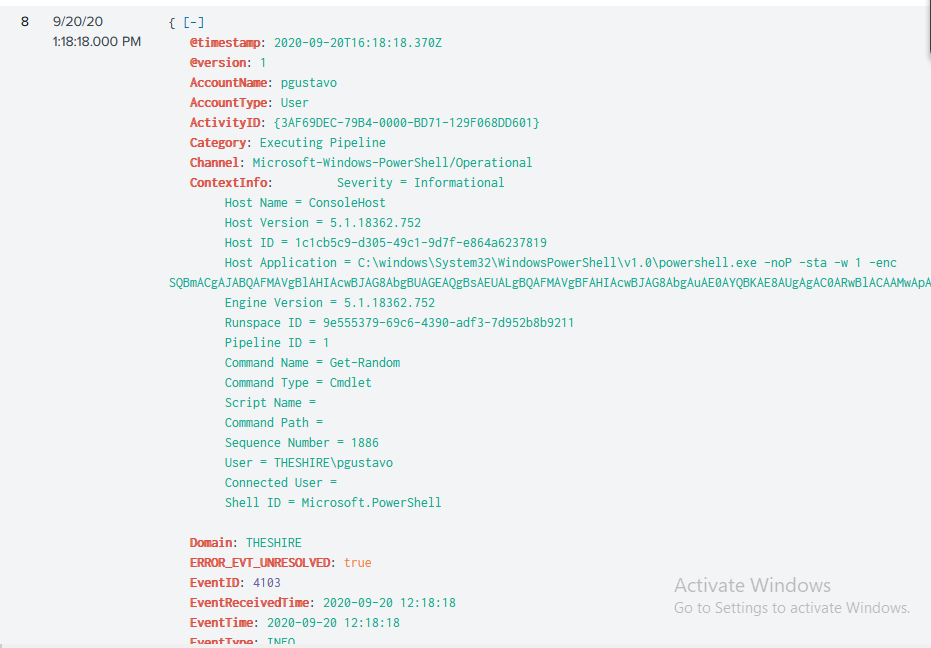
* In Windows Server VM, access Splunk at **http://10.0.0.5:8000/en-US/app/launcher/home** and login with **splunkadmin** / **splunkadmin**.



* Perform the search **index="class-26"** to view today’s sample data set that has been imported from Mordor Data Sets.

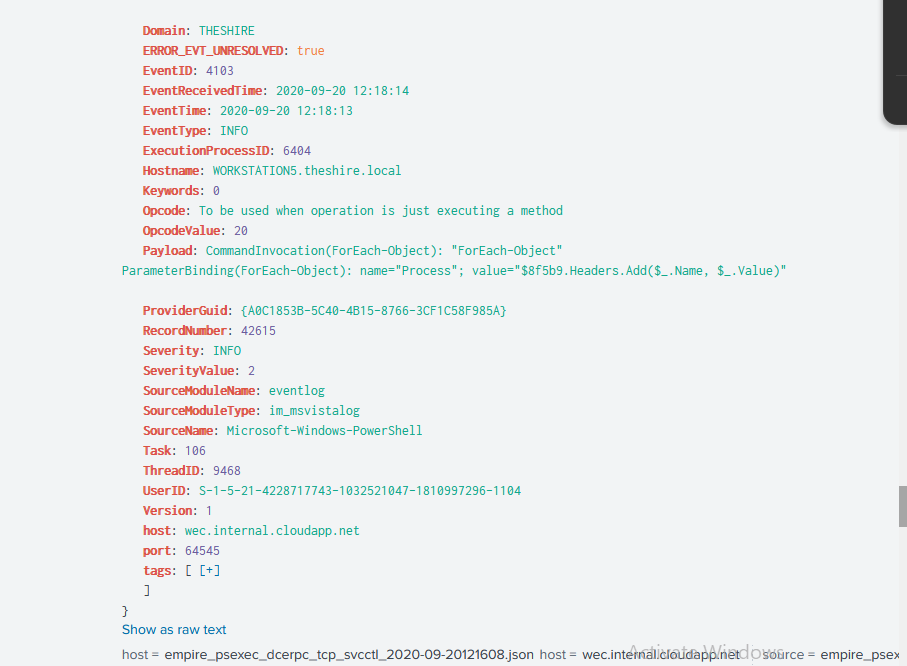


* Identify the three event logs where a network connection was established using powershell.exe
  + Include a screenshot of Splunk indicating the SPL query you used to exclusively display these three logs according to the stated attributes









* What port was used throughout the attack?



* What is the domain prefix and account name that invoked PsExec (e.g. RIVENDELL\Elessar)?



* + When did this invocation take place?



* + What is the location of the executable that this process used?

Note: The encoded code is encoded in base-64 and after unencoding it, I can say it is harmless. here it is uncoded: Invoke-Expression 'Add-Type -AssemblyName "System.Windows.Forms"; [System.Windows.Forms.MessageBox]::Show("A message from PowerShell")'

all it does is display a message box saying “A message from PowerShell”

* What TTPs were used in this attack?

Exploitation of Software Vulnerabilities

* What part of the kill chain is this?

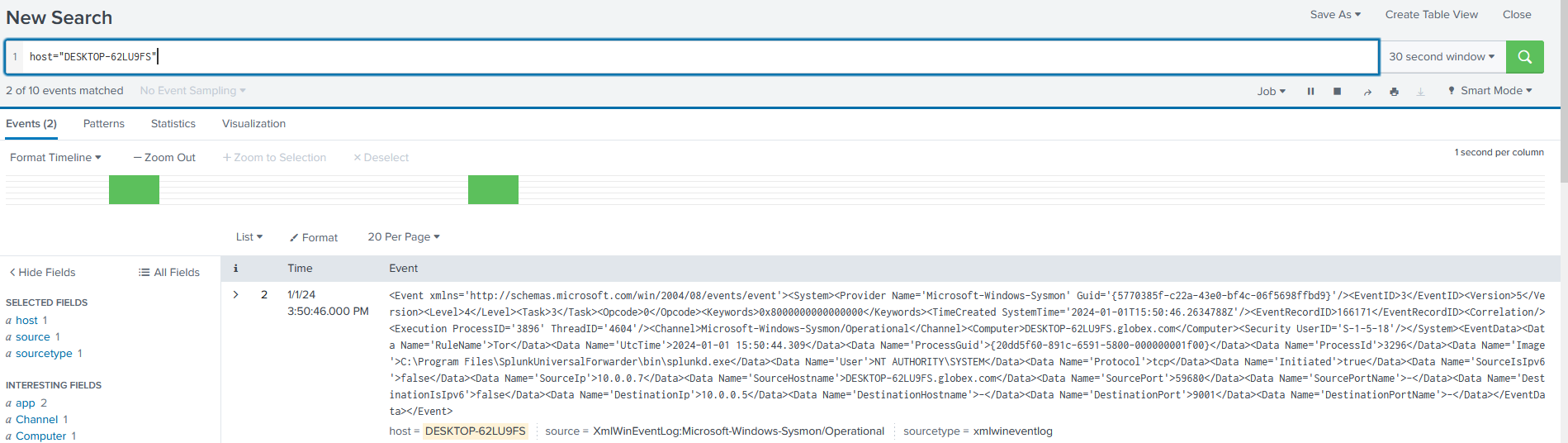
Exploitation

### 

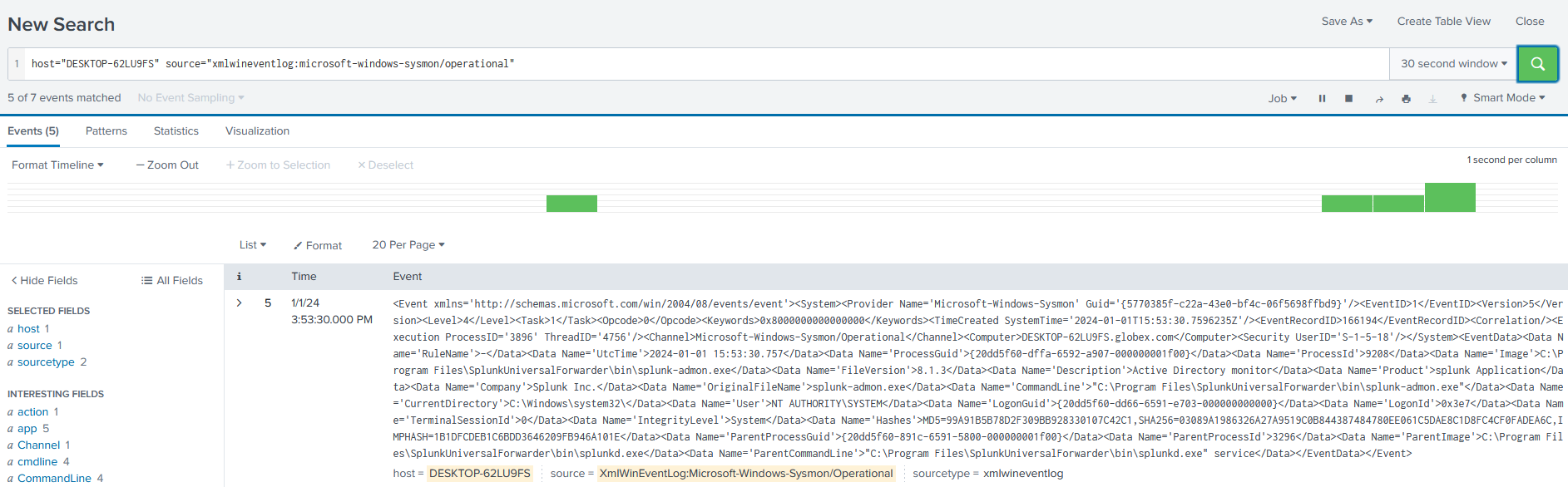
### **Part 3: Simulation of this**

Now that we have an idea of what this attack might look like, let’s reproduce the remote code execution in our own lab environment. For this simulation we won’t be using Empire, but instead be using Invoke-PsExec as a standalone tool from our Windows Server VM. The required components of this activity have been pre-staged for you in the provided baseline lab package. However, feel free to experiment. For example, if **Invoke-PsExec** isn’t getting the job done for you, try **PsExec** from Microsoft Sysinternals instead.

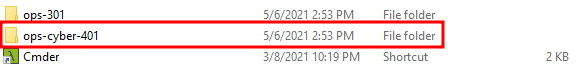
* In Windows Server VM, access Splunk at **http://10.0.0.5:8000/en-US/app/launcher/home**
* Check that regular event logs are being correctly forwarded from Win10 by querying **host="DESKTOP-XXXXX"**. Note: Replace the host name with the name of your Win10 VM.



* Check that Sysmon logs are being correctly forwarded from Win10 by querying **source="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"**.

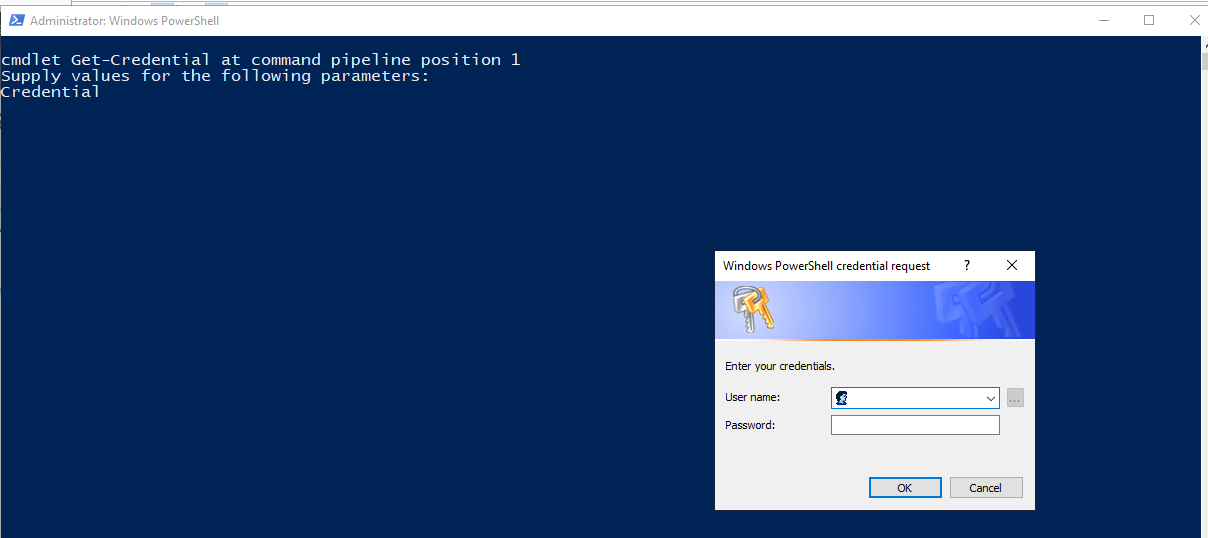


* From Windows Server, access **C:\Users\Administrator\Desktop\ops-cyber-401\Invoke-PsExec.ps1** using PowerShell IDE running as Administrator.



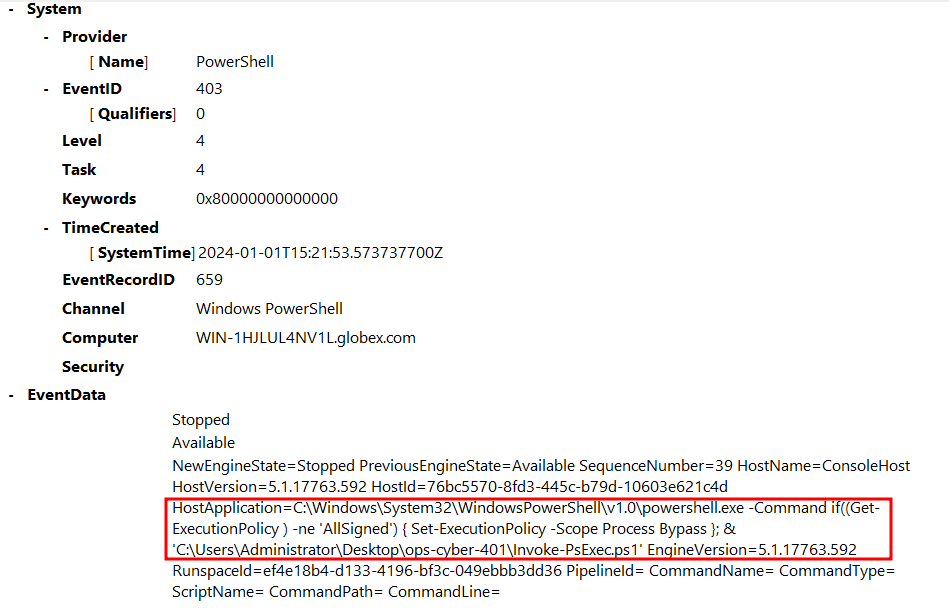


* Execute this script a few times.

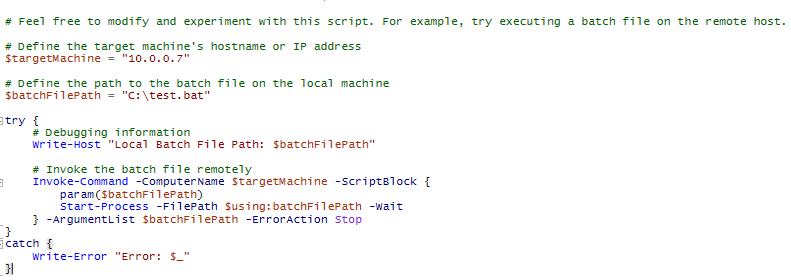


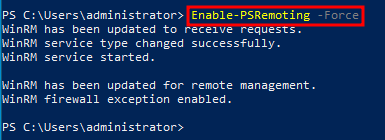
* Review your event logs and Sysmon logs. Did this activity generate new logs? Include a screenshot of them.

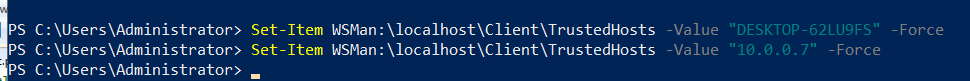


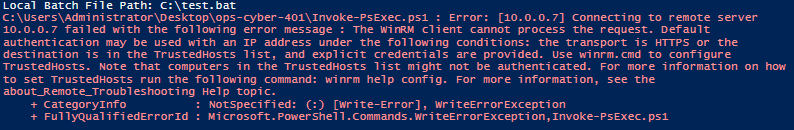


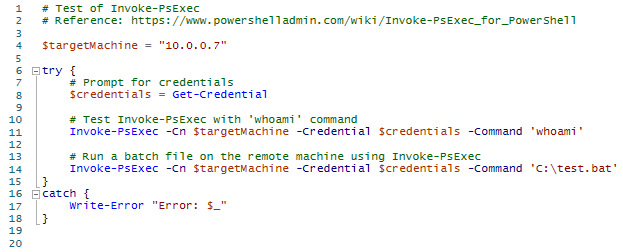
* Modify the PowerShell script to execute a simple batch script file on the Win10 box instead of a command.

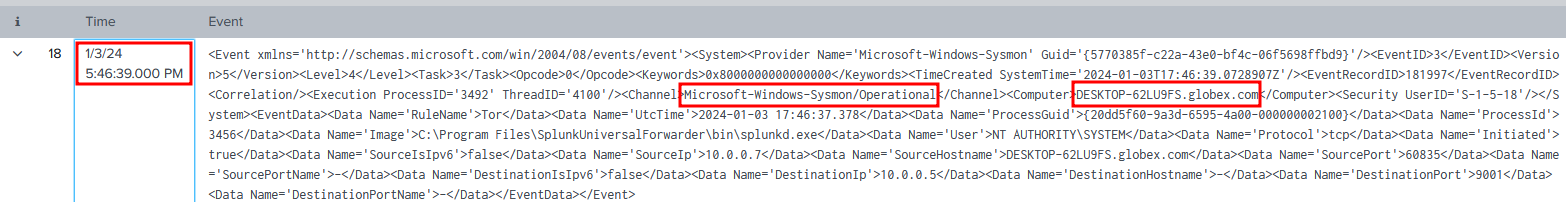












* + Does this affect the type of event logs coming into Splunk?
  + Does this affect alerting configured to detect this activity?

### 

### **Part 4: Reporting**

Explain:

* Summarize what you’ve done and learned today. What are your key takeaways?
  + I inspected previous logs to see what a psexec attack looks like, how to analyze it
* How do Sysmon logs differ from regular event logs?
  + Sysmon logs are more detailed compared to regular event logs
  + Which type was more useful in this scenario?
    - Sysmon was more useful
* How can a Windows system be vulnerable to RCE?
  + There are multiple ways a windows system can be vulnerable to remote code execution, some of them are Service and Network Vulnerabilities like RDP or SSH protocols, Social Engineering like a phishing attack, Third-Party Software that can be outdated and no longer receives security updates, and Scripting and Automation like Powershell and other scripting languages.
* Referencing MITRE ATT&CK, what are some other tools and techniques besides **Invoke-PsExec** that can be used to perform RCE?
  + [T1210](https://attack.mitre.org/techniques/T1210/) Exploitation of remote services: exploiting remote services like [APT28 SMB vuln attack](https://attack.mitre.org/groups/G0007/)
  + [T1059](https://attack.mitre.org/techniques/T1059/) Scripting: Ruby scripting to execute payloads by [APT37](https://attack.mitre.org/groups/G0067/)
  + [T1021](https://attack.mitre.org/techniques/T1021/) Remote Services: [Sandworm](https://attack.mitre.org/groups/G0034/) APT a malware to [attack ukraine electric power in 2016](https://attack.mitre.org/campaigns/C0025/)
* What are some countermeasures against RCE?
  + Software Restriction Policies (SRP)
  + Application Whitelisting
  + Patch and Update Systems
  + Firewall and Intrusion Prevention Systems (IPS)