## Introduction

You have been hired as a security analyst. You were tasked to determine any malicious activity associated with a malware attack.

You will have access to the internet to learn more about the events. You can use websites, such as VirusTotal, to upload and verify threat existence.

The tasks below are designed to provide some guidance through the analysis process.

You will practice and be assessed on the following skills:

* Evaluate event alerts using Squil.
* Use Google search as a tool to obtain intelligence on a potential exploit.
* Use VirusTotal to upload and verify threat existence.

# Instructions

## Gather the Basic Information

In this part, you will review the alerts listed in Security Onion VM and gather basic information for the interested time frame.

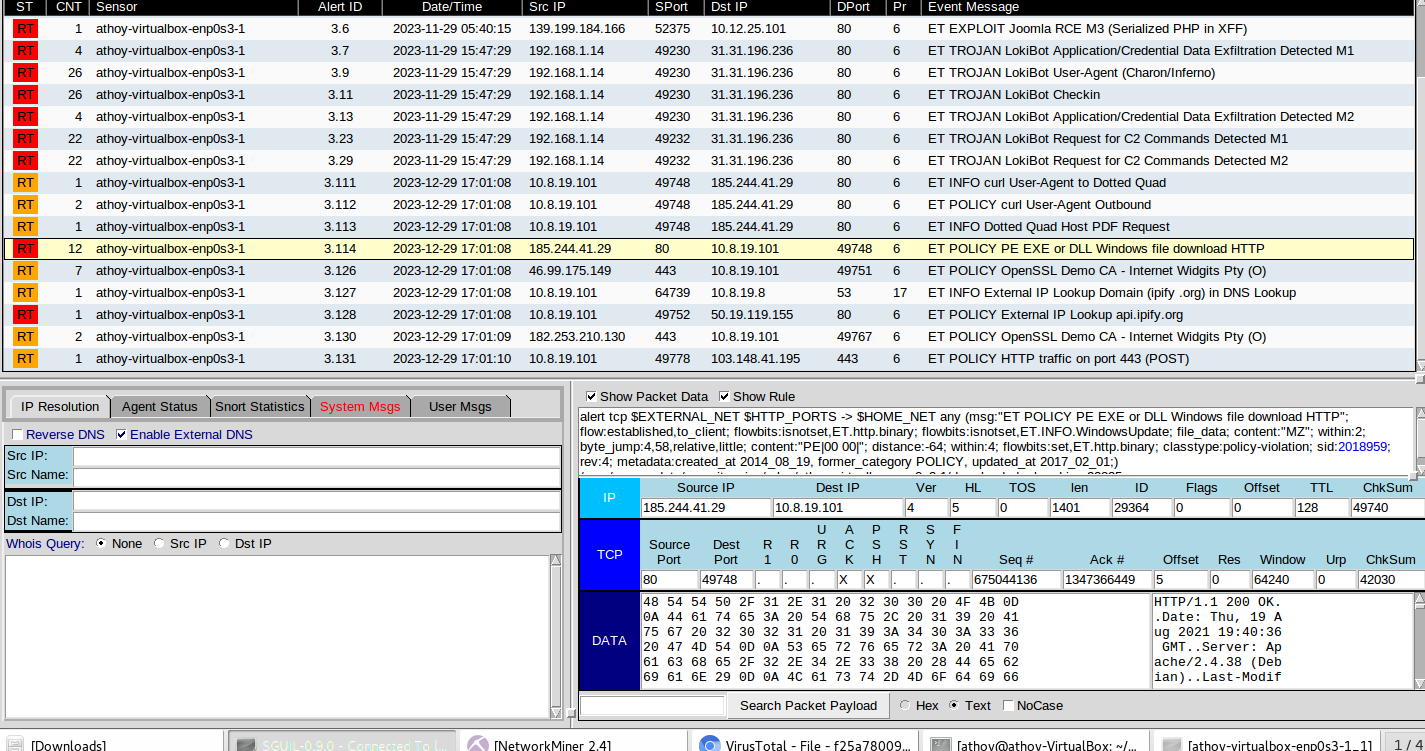
### Verify the status of services

* + - 1. Log into Security Onion VM.
      2. Open a terminal window. Enter the **sudo so-status** command to verify that all the services are ready.
      3. When the nsm service is ready, log into Sguil.sud
      4. Download the .pcap file of yours and replay the malware packet capture. Before replaying the packet capture, update IDS rules using the command **sudo rule-update**.

### Gather basic information.

#### Questions:

* + - 1. What is the name of the trojan? Identify the time frame of the attack, including the date and approximate time.

Type your answers here.

* + - 1. List the alerts noted during this time frame associated with the trojan.

ET CURRENT\_EVENTS WinHttpRequest Downloading EXE

ET POLICY PE EXE or DLL Windows file download HTTP

ET POLICY PE EXE or DLL Windows file download HTTP

ET CURRENT\_EVENTS Terse alphanumeric executable downloader high likelihood of being hostile

ET POLICY PE EXE or DLL Windows file download HTTP

ET POLICY External IP Lookup Domain (myip.opendns .com in DNS lookup)

ET TROJAN Backdoor.Win32.Pushdo.s Checkin

ET TROJAN Pushdo.S CnC response

ET POLICY TLS possible TOR SSL traffic

Type your answers here.

* + - 1. List the internal IP addresses and external IP addresses involve

**Internal IP address:**

* 192.168.1.96
* 10.8.19.101

**External IP addresses:**

* 31.31.196.236
* 185.244.41.29
* 145.131.10.21

Type your answers here.

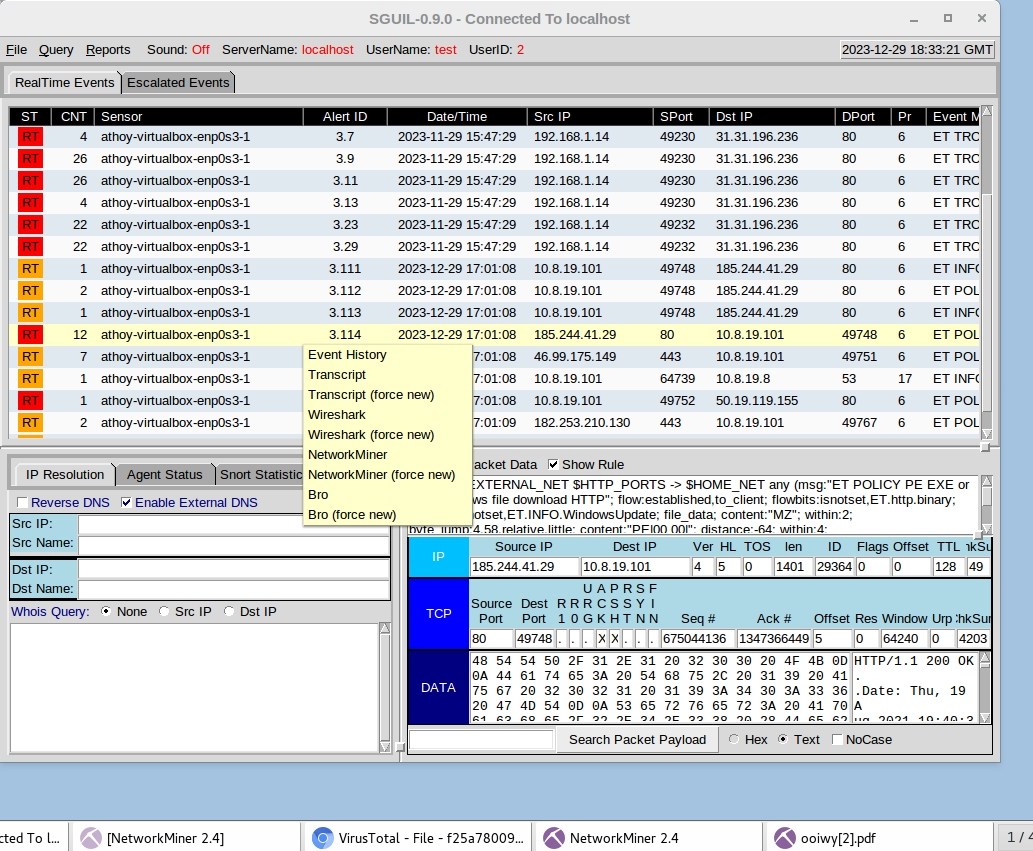
## Learn about the Exploit

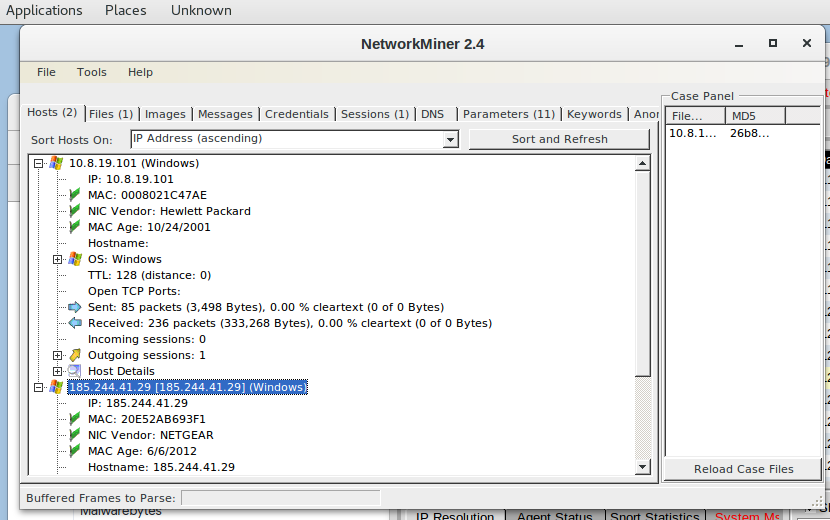
In this part, you will learn more about the exploit.

### Infected host

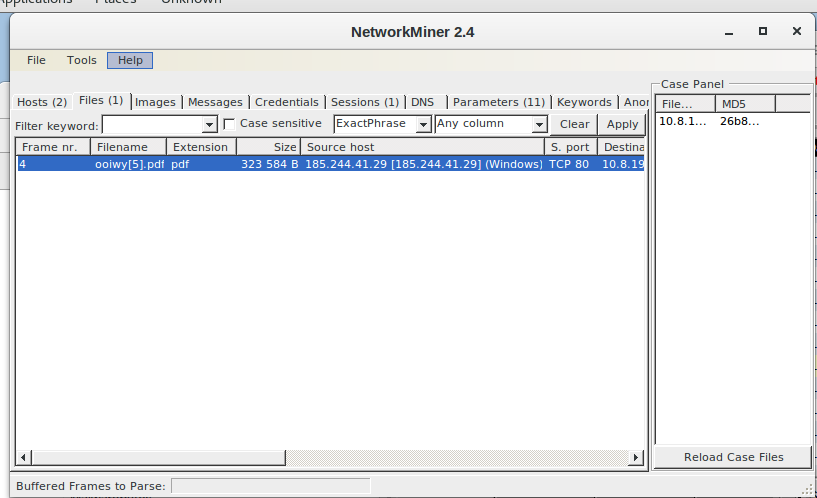
#### Questions:

* + - 1. Based on the alerts, what is the IP and MAC addresses of the infected computer? Based on the MAC address, what is the vendor of the NIC chipset? (**Hint**: NetworkMiner or internet search



T ype your answers heggre

* + - 1. Based on the alerts, when (date and time in UTC) and how was the PC infected? (**Hint**: Enter the command **date** in the terminal to determine the time zone for the displayed time



Type your answers here.

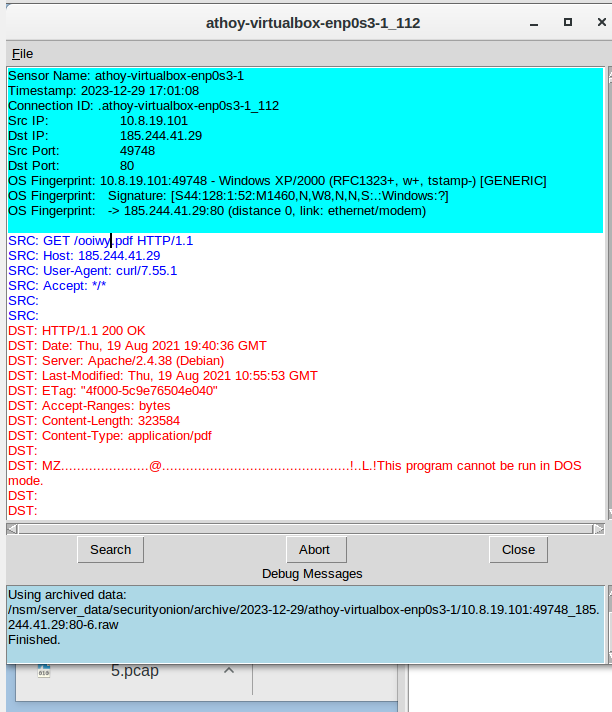
c. How did the malware infect the PC? Use an internet search as necessary.

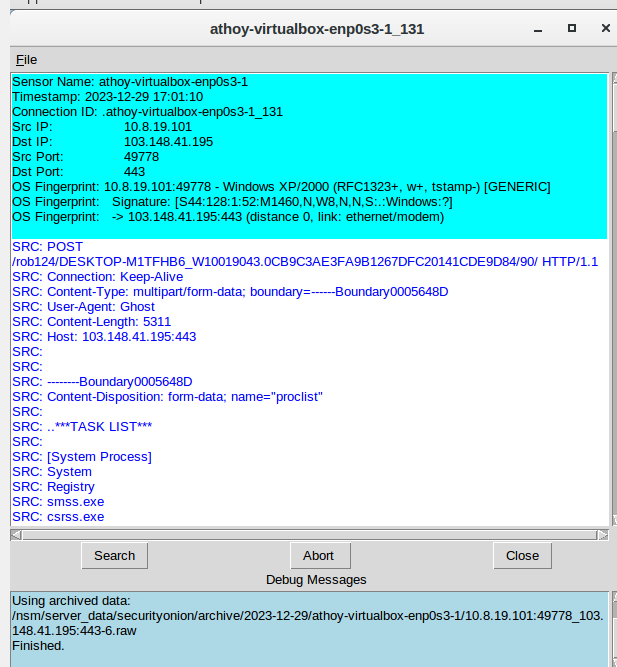
Type your answers here.

### Examine the exploit.

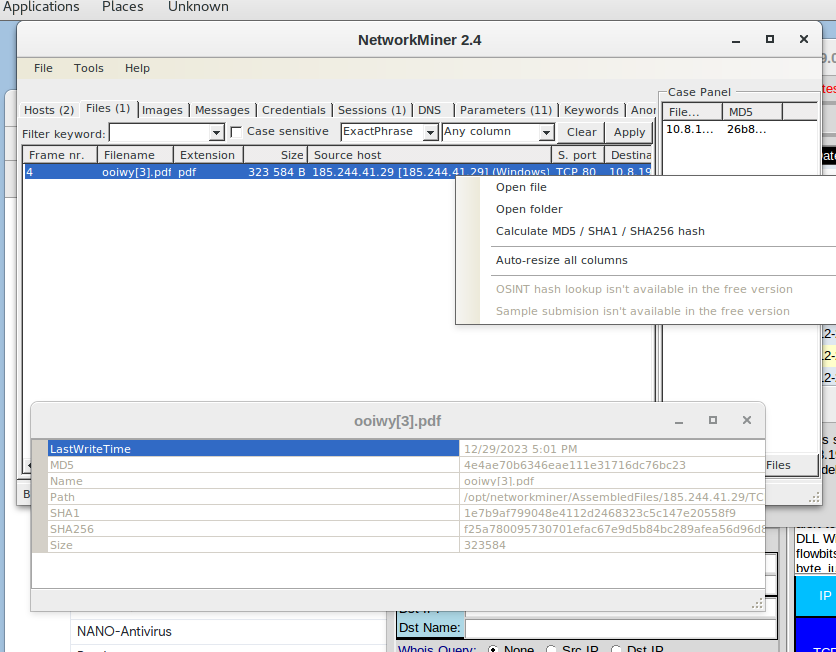
#### Questions:

* + - 1. Based on the alerts associated with HTTP GET request, what files were downloaded? List the malicious domains observed and the files downloaded.



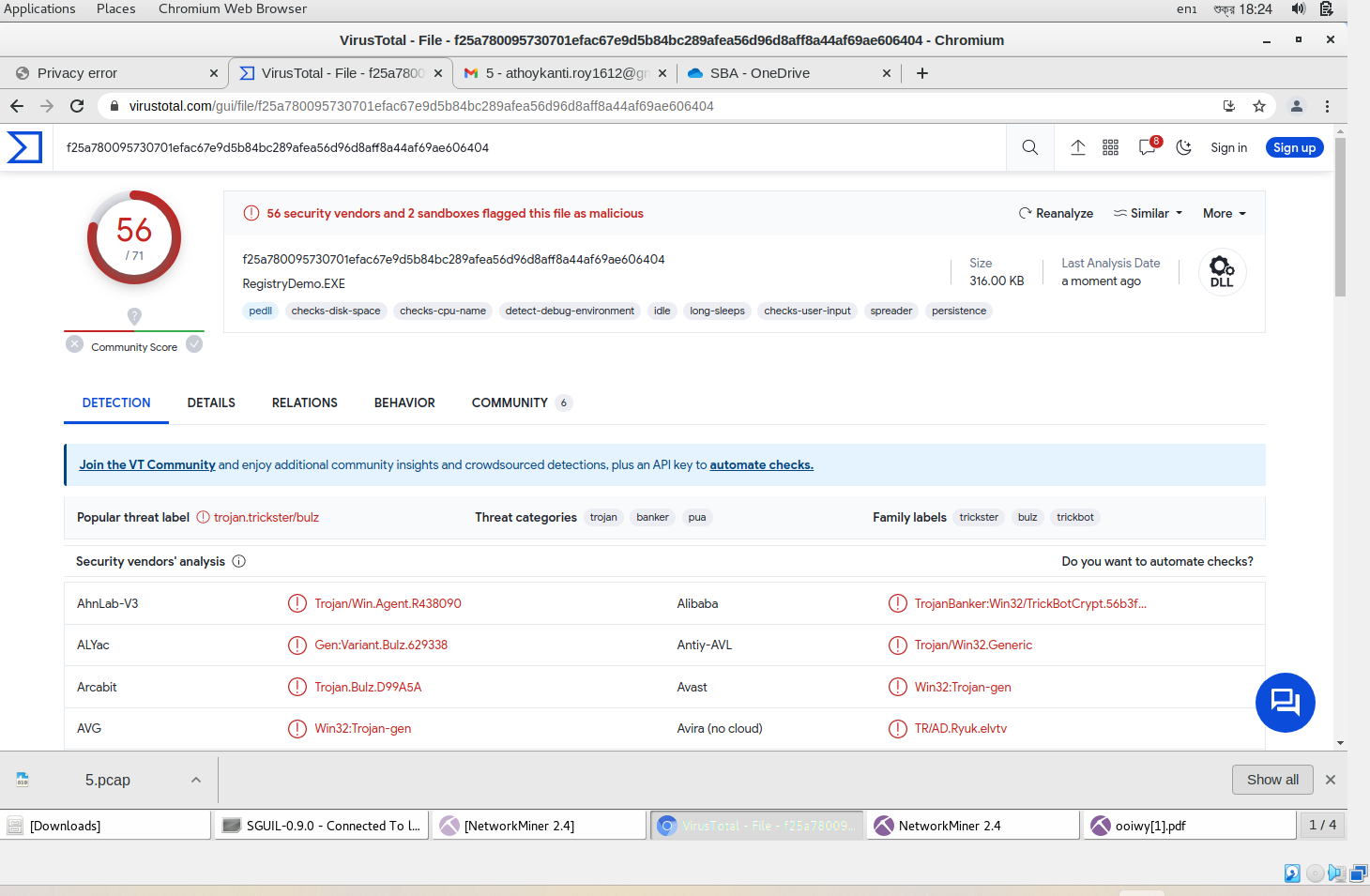
Type  your answers here.

Use any available tools in Security Onion VM, determine and record the SHA256 hash for the downloaded files that probably infected the computer?



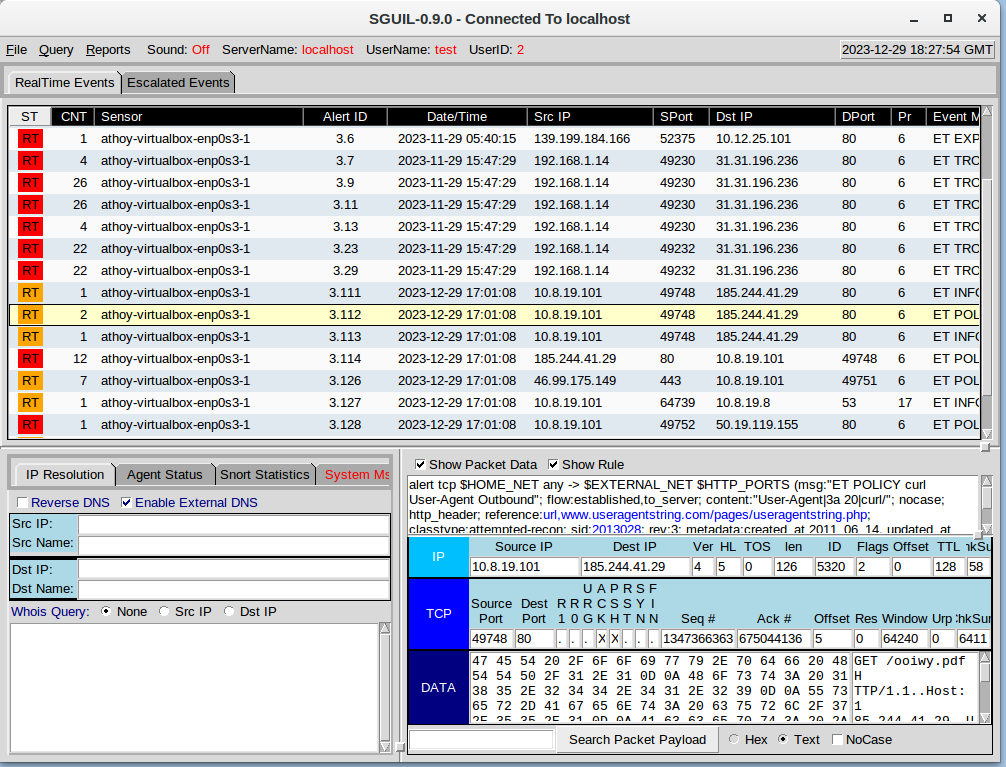
Type your answers here.

* + - 1. Navigate to [www.virustotal.com](http://www.virustotal.com) input the SHA256 hash to determine if these were detected as malicious files. Record your findings, such as file type and size, other names, and target machine. You can also include any information that is provided by the community posted in VirusTotal.



Type your answers here.

* + - 1. Examine other alerts associated with the infected host during this timeframe and record your findings



Type your answers here.

### Report Your Findings

Summarizes your findings based on the information you have gathered from the previous parts, summarize your findings.

Type your The host with IP is a PC running Windows, accessed a malicious domain for a DNS query, and was infected with the Pushdo trojan. The Pushdo trojan pretends to be an Apache webserver, listening on port 80. After infection, the Pushdo trojan downloads various malware. In the examined PC, three malwares were downloaded and installed – gerv.gun, trow.exe and wp.exe. These files were checked in virustotal.com, using their SHA256 hash, and verified as malware by most source.

End of document