## 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.

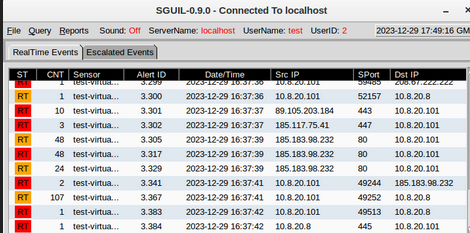
#### Questions:

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

Trojan.trickbot/mint. Tue, 20 Aug 2019 19:49:49 GMT

Type your answers here.

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



Type your answers here.

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

Internal IP Address: 10.8.20.101

External IP Address: 10.8.20.8 , 185.183.98.232

Type your answers here.

## Learn about the Exploit

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

### Infected host

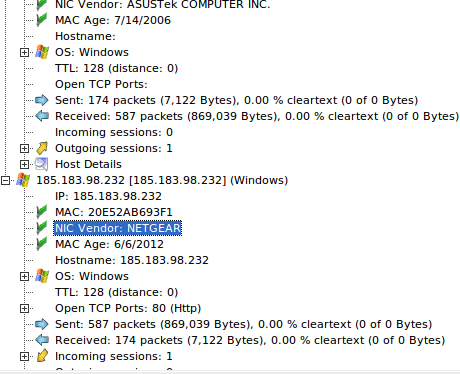
#### Questions:

* + - 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

IP: 10.8.20.101

MAC: 0018F3A60192

NIC Vendor: ASUSTek COMPUTER INC.



Type 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

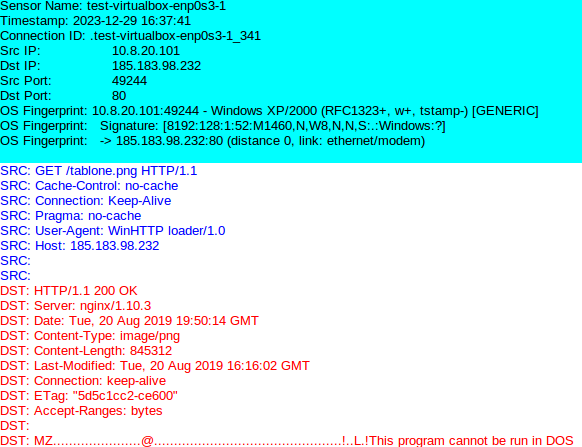
TTTvjhvjhvhbkjb

Time: 20 Aug 2019 19:49:49 GMT

Type your answers here.

* + - 1. How did the malware infect the PC? Use an internet search as necessary.

The endpoint user won't experience any Trickbot infection symptoms. However, since the malware will interact with Trickbot's command and control infrastructure to exfiltrate data and accept tasks, a network administrator is likely to notice variations in traffic or attempts to contact banned IPs and domains.



Type your answers here.

### Examine the exploit.

#### Questions:

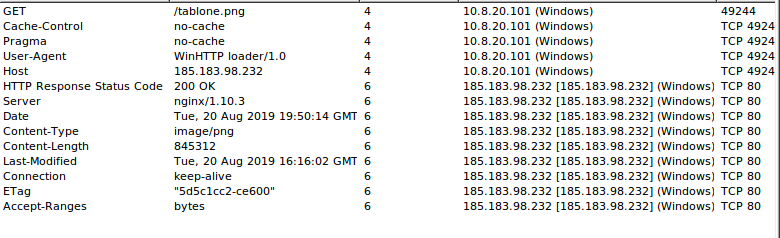
* + - 1. Based on the alerts associated with HTTP GET request, what files were downloaded? List the malicious domains observed and the files downloaded.

GET/tablote.png HTTP/1.1

Tablone4.png

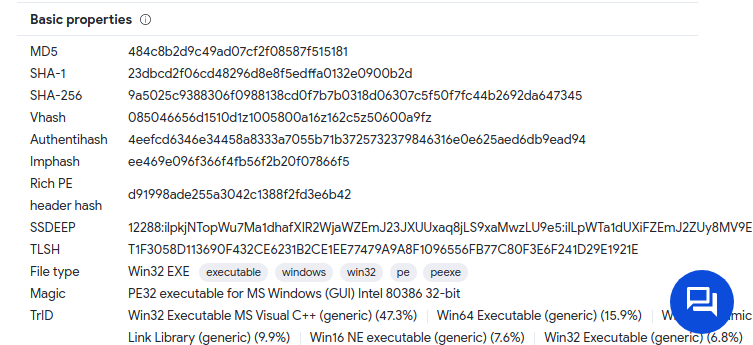
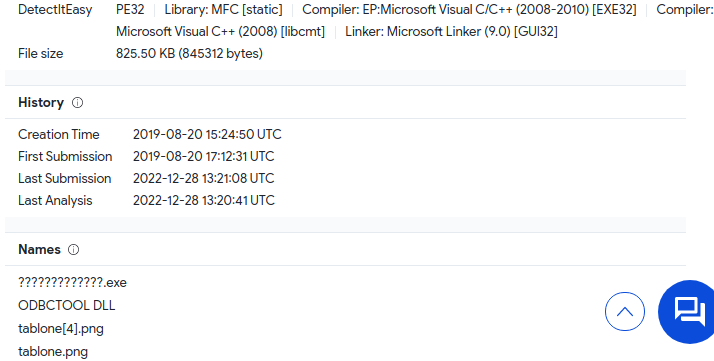
Type your answers here.

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



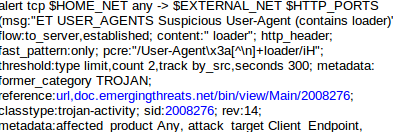
Type your answers here.

* + - 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.

In 2016, the modular trojan known as Trickbot made its debut. On the compromised device, Trickbot is capable of the following actions: For a thorough study, see Win32/Trickbo. Here, the threat was Trojan.trickbot/mint. And the category was Trojan, banker. Banker Trojan redirects traffic from online banking websites to attacker-accessed websites, copying itself, and stealing personal finance cookie files. It collects cookies and passwords, and can remove itself when commanded. Criminals increasingly steal confidential financial information. Here, Trojan banker type malicious has been found. The time, file and the way it effected has been shown.

Csdsafdsfdsgdfg

jmjj

End of document