Activity File: Wireshark Strikes Back

Overview

You are working as a Security Engineer for X-CORP, supporting the SOC infrastructure. The SOC analysts have noticed some discrepancies with alerting in the Kibana system and the manager has asked the Security Engineering team to investigate.

Yesterday, your team confirmed that newly created alerts are working. Today, you will monitor live traffic on the wire to detect any abnormalities that aren't reflected in the alerting system.

You are to report back all your findings to both the SOC manager and the Engineering Manager with appropriate analysis.

Fill out the Network Report Template as you progress through this activity.

Setup

You will use the Kali VM to analyze live traffic on the wire.

In order to get started, you will need to: - Connect to the Kali VM. - Open a terminal window and run the command `systemctl start sniff`. - This command uses `tcpreplay` to replay PCAPs in `/opt/pcaps` onto Kali's `eth0` interface. - Launch Wireshark and capture traffic on the `eth0` interface. - After 15 minutes have passed, run the command `systemctl stop sniff` to stop the `tcpreplay`. - Please note that replaying the PCAPs will use up the CPU memory. You will need to stop this service in order to avoid performance issues with your virtual machine. - Save the capture to file. (**This is an important step**.) - Profile users' behavior from their packet data.

If you are unable to find some of the solutions, it is possible you did not allow Wireshark to capture traffic for long enough. To save time, feel free to use the following PCAP file below to answer the questions:

- PCAP
- If copy and paste is not available on the VM, use `curl` to download the file with this alternate URL: http://tinyurl.com/yaajh8o8.

- For example: `curl -L -o pcap.pcap http://tinyurl.com/yaajh8o8`

Note: You will be dealing with live malware in this activity. Please make sure all work is done on Azure machines.

Instructions

Connect to your Kali VM, launch Wireshark, and begin capturing on the `eth0` interface using the steps above. Let the capture run for at least fifteen minutes and then stop it. As your capture runs, read the following overview:

- The Security team requested this analysis because they have evidence that people are misusing the network. Specifically, they've received tips about:
  - "Time thieves" spotted watching YouTube during work hours.
  - At least one Windows host infected with a virus.
  - Illegal downloads.
- A number of machines from foreign subnets are sending traffic to this network. Therefore, you will see many IP ranges in your capture.
- Your task is to collect evidence confirming the Security team's intelligence.
- Be sure to use display filters. In addition, be sure to record your work by adding comments to packets as you go.
  - For example, if you find a packet containing a username of interest, comment on the packet: `Illegal Downloads: Contains Windows username`.

Record your answers in the following Google Doc. This file will be submitted as a deliverable at the end of the project. You must make a copy of this file in order to edit it.

- Network Analysis Report Template

Time Thieves

At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to this behavior, but it seems these people have created their own web server on the corporate network. So far, Security knows the following about these time thieves:

- They have set up an Active Directory network.
- They are constantly watching videos on YouTube.

- Their IP addresses are somewhere in the range `10.6.12.0/24`.

You must inspect your traffic capture to answer the following questions in your Network Report: 1. What is the domain name of the users' custom site? 2. What is the IP address of the Domain Controller (DC) of the AD network? 3. What is the name of the malware downloaded to the 10.6.12.203 machine? - Once you have found the file, export it to your Kali machine's desktop.

1. Upload the file to VirusTotal.com.
2. What kind of malware is this classified as?

Vulnerable Windows Machines

The Security team received reports of an infected Windows host on the network. They know the following: - Machines in the network live in the range `172.16.4.0/24`. - The domain mind-hammer.net is associated with the infected computer. - The DC for this network lives at `172.16.4.4` and is named Mind-Hammer-DC. - The network has standard gateway and broadcast addresses.

Inspect your traffic to answer the following questions in your network report:

1. Find the following information about the infected Windows machine:
    - Host name
    - IP address
    - MAC address
2. What is the username of the Windows user whose computer is infected?
3. What are the IP addresses used in the actual infection traffic?
4. As a bonus, retrieve the desktop background of the Windows host.

Illegal Downloads

IT was informed that some users are torrenting on the network. The Security team does not forbid the use of torrents for legitimate purposes, such as downloading operating systems. However, they have a strict policy against copyright infringement.

IT shared the following about the torrent activity:

- The machines using torrents live in the range `10.0.0.0/24` and are clients of an AD domain.
- The DC of this domain lives at `10.0.0.2` and is named DogOfTheYear-DC.

- The DC is associated with the domain dogoftheyear.net.

Your task is to isolate torrent traffic and answer the following questions in your Network Report:

1. Find the following information about the machine with IP address `10.0.0.201`:
    - MAC address
    - Windows username
    - OS version
2. Which torrent file did the user download?
