Cybersecurity

Activity File

Module 12 Day 2: 11 Alert - FTP File Extraction

In this activity, you'll continue in your role as SOC analyst for the California DMV.

- You deployed Security Onion at the DMV headquarters. Immediately afterwards, your organization experienced an attack.
- One of your junior security analysts noticed a red alert on their Security Onion console. Snort identified it as an emerging threat for a file transfer using FTP.
- You must work quickly to examine the alert and determine if any systems were breached or if any data was supplanted or exfiltrated from the network.

Activity Instructions

For the following section, open the Chromium web browser and open the Security Onion Console. Use Security Onion and NetworkMiner to gather information for this investigation.

Log in using the same credentials.

- Username: sysadmin@example.com
- Password: cybersecurity

- Use the following attack profile provided by your junior analyst to complete this exercise.
    - Destination port: 21
    - Destination IP: 130.89.149.129 (server)
    - Source IP: 192.168.10.128 (victim)

Steps

1. From the Security Onion analyst console, Group By Destination IP and filter against the destination IP 130.89.149.129, and select the alert and click Drilldown.
2. Using the information presented in the window, expand the alert, and answer the following questions:
    - In the Event Fields window, what was the FTP server response and what type of file was downloaded? .exe file

- What was the name of the rule that triggered this alert? ET INFO .exe File requested over FTP
- What is the direction of traffic flow indicated by this alert? outbound
- What country is the server located? Netherlands

3. Click on the destination IP address and select VirusTotal from the dropdown.
    - How many virus engine matches come back? 0
    - Is this server malicious? It is clean
4. Change to PCAP view and download the PCAP. Now switch from Security Onion to NetworkMiner, select the Parameters tab, and answer the following questions.
    - What username and password did the attacker use to log in to the system? Anonymous and IEUser@
    - Was the login successful? Yes
    - What is the name of the file the attacker tried to install on the victim's machine? mirc635.exe
    - Was the file transfer successful? No
5. In NetworkMiner, click on the Hosts (2) tab, right-click the IP 130.89.149.129, and select Expand All. Answer the following questions.
    - What is the MAC or hardware address of the server's network interface card (NIC)? 001839F73ED2
    - What is the vendor of the NIC for the server's machine? Cisco-Linksys, LLC
    - What is the MAC or hardware address of the victim's machine? 000C299CAA25
    - What is the vendor of the NIC for the victim's machine? VMware, Inc.
    - What operating system is the victim using? Windows
    - Looking at the Host Details portion of the server window, what URL did the attacker connect to in order to begin the file transfer? ftp.snt.utwente.nl