Solution Guide: Alert - FTP File Extraction

The goal of this activity was to reinforce concepts related to network security monitoring and the NSM Detection stage processes of Collection and Analysis.

- 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)

1. From the Sguil analyst console, perform a query by IP against the destination IP `130.89.149.129`, and bring up the Event Query window.
2. Using the information presented in the Event Query window, highlight the alert that contains the IP `130.89.149.129`, and answer the following questions:
   - In the Packet Data window, what was the FTP server response and what type of file was downloaded?
     - Response: `RETR`. File type: .exe or executable
   - What Snort rule triggered this alert?
     - `alert tcp $HOME_NET any -> $EXTERNAL_NET 21`
   - What is the Snort message?
     - `ET INFO .exe File requested over FTP`
   - What is the direction of traffic flow indicated by this alert?
     - Outbound from `$HOME_NET`
   - Looking at the DNS resolution information contained in the IP Resolution Window, in what country is the victim located?
     - The Netherlands
3. Switch from Sguil to NetworkMiner, select the **Parameters** tab, and answer the following questions.
   - What username and password did the attacker use to log into the system?
     - Username: `anonymous`
     - Password: `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`
   - What the file transfer successful?
     - No
4. 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)?
     - `00:18:39:F7:3E:D2`
   - What is the vendor of the NIC for the server’s machine?
     - Cisco-Lynksys
   - What is the MAC or hardware address of the victim’s machine?
     - `00:0C:29:9C:AA:25`
   - What is the vendor of the NIC for the victim's machine?
     - VMware

- What operating system is the victim is 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

5. Using the Chromium browser built into Security Onion, visit www.virustotal.com and perform a search against the URL that you discovered.
   - How many virus engine matches come back?
     - Zero
   - Is this URL malicious?
     - No