ATHANASIUS J.K GADOSEY

Week 4

Practical Task: The Web Shell Log Analysis

The following answers are for both log files being analyzed below:

1. Firewall Analysis:

    - **Attacker's IP**: 88.198.5.10
    - **Server's IP**: 10.0.0.5
    - The **three ports** the attacker tried to connect to that were blocked are: **22, 3389, and 445**
    - The **one port** that was opened is port **80.**

2. Web Server Analysis:

    - The three files the attackers tried to look for, which didn't exist, were: /**admin.php**, /**config.txt,** and /**backup.zip.**

    - The filename that they found that did exist: **/upload.php,** which returned (200), and then made a **POST** to it.

    - User_agent is **curl/7.68,** and this is not a **normal web browser** but rather indicates scripted probing or uploading.

3. The Breach (Correlation):

    - During the time at 14:30:09, the attacker made a POST request, which was likely the attacker uploading a WebShell script file, such as **shell.php,** under **/uploads/,** which was to be POSTed to **/upload.php.**

    - **Smoking gun (full URI at 14:30:10):** /uploads/shell.php?cmd=whoami

    - **The specific command run**:
      whoami (used to confirm their **privilege level** on the system or displays the current **username**) and
      ifconfig (used to display network interface configuration, such as IP addresses)

4. Trying it on Frameworks (MITRE ATT&CK):

    - The long list of **404 errors** shows the attacker was doing recon, which basically meant checking what files or pages existed on the server.

- The request to shell.php?cmd=whoami is simply a web shell being used to run commands on the server. This fits the **Web Shell (T1505)** and **Command Execution (T1059)** technique.

5. Final Recommendation:

    - This is a **True Positive** because the server, which was scanned by an attacker, found upload.php, which helps to upload files through it, and then ran commands using the uploaded shell.
    - **What to do with the web server:**
      I will take it off the network immediately, keep all logs and the contents of the uploads folder, and start a proper incident investigation and cleanup.

    - **What to do about the attacker's IP:**
      Block 88.198.5.10 on the firewall/IPS, create detection rules for this behaviour, and report the IP to the hosting provider/