LOG ANALYSIS OF CYBER SECURITY TRAINING EXERCISES

BY IZZMIER IZZUDDIN

LOGS

Firewall

1. **Log Entry 1 (Threat Log)**:
   - **Date/Time**: 2024/09/09 17:39:51
   - **Type of Log**: Threat (URL)
   - **Source IP**: 10.60.3.123 (NAT'd Source IP: 19.31.169.76)
   - **Destination IP**: 120.44.239.154
   - **Source User**: SE\waynerooney
   - **Destination Port**: 443 (HTTPS)
   - **Protocol**: TCP
   - **Action**: Alert
   - **URL**: settings-win.data.microsoft.com
   - **Severity**: Informational
   - **Direction**: Client-to-Server
   - **Device Name**: SESYDVIR-FW01

2. **Log Entry 2 (Traffic Log)**:
   - **Date/Time**: 2024/05/07 04:04:35
   - **Type of Log**: Traffic (End)
   - **Source IP**: 10.192.104.61 (NAT'd Source IP: 25.145.141.193)
   - **Destination IP**: 20.67.222.222
   - **Application**: DNS
   - **Action**: Allow
   - **Source Port**: 62494
   - **Destination Port**: 53 (DNS)
   - **Protocol**: UDP
   - **Bytes Sent/Received**: 99/155
   - **Session End Reason**: Aged-out
   - **Device Name**: SEWATSV-FW01

3. **Log Entry 3 (Traffic Log)**:
   - **Date/Time**: 2024/06/14 09:39:01
   - **Type of Log**: Traffic (End)
   - **Source IP**: 10.48.33.163 (NAT'd Source IP: 19.31.174.84)
   - **Destination IP**: 124.42.196.205
   - **Source User**: SE\bruno
   - **Destination Port**: 443 (HTTPS)
   - **Protocol**: TCP
   - **Action**: Allow
   - **Bytes Sent/Received**: 4541/8413
   - **Device Name**: SE-FW01

4. **Log Entry 4 (Threat Log)**:
   - **Date/Time**: 2024/06/14 09:39:12
   - **Type of Log**: Threat (URL)
   - **Source IP**: 10.138.40.51 (NAT'd Source IP: 138.117.201.152)
   - **Destination IP**: 17.37.97.229
   - **Source User**: SE\lisandro
   - **Destination Port**: 443 (HTTPS)
   - **Protocol**: TCP
   - **Action**: Alert
   - **URL**: unitedstates.smartscreen.microsoft.com
   - **Severity**: Informational
   - **Direction**: Client-to-Server
   - **Device Name**: SE-FW01

Antivirus

1. **Log Entry 1**:
   - **Date/Time**: 2024-06-14 05:47:32
   - **Local Host IP**: 192.168.0.22
   - **Remote Host IP**: 175.193.13.3
   - **Application**: C:/Program Files (x86)/Dropbox/Client/Dropbox.exe
   - **Action**: Blocked
   - **User Name**: garnacho
   - **SHA-256**: 7462b5db619e77833d7cebcdca98352976154ba72d24080eb20edb01925accb6
   - **MD-5**: 6B532CE4B97BC0F4D6CFA12E9637CBF5

2. **Log Entry 2**:
   - **Date/Time**: 2024-05-04 14:07:50
   - **Local Host IP**: 192.168.99.4
   - **Remote Host IP**: 168.215.65.86
   - **Application**: C:/PROGRAM FILES (X86)/FILEZILLA SERVER/FILEZILLA SERVER.EXE
   - **Attack**: OpenSSL Heartbleed CVE-2014-0160
   - **Action**: Detected but not blocked
   - **User Name**: IZZMIER
   - **SHA-256**: EEBCC1D79679BB23F1D8C8F7FA1DD07FE2A0DE0444FC7985D29803C51B61FF3A

QUESTIONS

These questions can help to better understand and analyse the details and security incidents recorded in the logs.

1. **Firewall Log Questions:**
   - What is the action taken for the URL "settings-win.data.microsoft.com" in the log entry dated 2024/09/09 17:39:51?
   - Which device name is associated with the threat log entry on 2024/06/14 at 09:39:12?
   - What protocol and action are recorded in the traffic log entry on 2024/05/07 04:04:35?
   - Identify the source and destination IPs for the log entry dated 2024/06/14 09:39:01.
   - What is the session end reason mentioned in the traffic log on 2024/05/07 04:04:35?

2. **Antivirus Log Questions:**
   - What application was blocked by the antivirus on 2024-06-14 05:47:32, and what was the action taken?
   - Provide the SHA-256 hash value for the file associated with the log entry on 2024-06-14 05:47:32.
   - Which vulnerability attack was detected in the log entry dated 2024-05-04 14:07:50?
   - What is the remote host IP in the antivirus log entry on 2024-05-04 14:07:50, and what was the action taken?
   - Who is the user associated with the antivirus log entry on 2024-05-04 14:07:50?

3. **Firewall Log Analysis**:
   - Analyse the threat log entry on 2024/09/09. What was the URL that triggered the alert and what action was taken?
   - In the traffic log entry on 2024/05/07, what was the source and destination IP address? What application was being used?

4. **User Activity Monitoring**:

- Based on the log entries, identify the users involved in the logged activities. What actions were taken by the user SE\bruno on 2024/06/14?
- What information can be deduced about the user SE\lisandro from the firewall logs?

5. **Antivirus Log Examination**:
    - Review the antivirus log entry on 2024-06-14. What application was blocked and what were the hash values associated with it?
    - Examine the antivirus log entry on 2024-05-04. What attack was detected, and what action was taken?

6. **Security Severity Assessment**:
    - What is the severity level of the threats detected in the firewall logs? Discuss the implications of these severity levels for network security.

7. **Protocol and Port Analysis**:
    - Analyse the different protocols and ports used in the firewall traffic logs. How do these choices impact network security and performance?

ANSWERS

1. **Firewall Answer:**
    - **Action taken for the URL "settings-win.data.microsoft.com" in the log entry dated 2024/09/09 17:39:51:**
        - **Action:** alert
    - **Device name associated with the threat log entry on 2024/06/14 at 09:39:12:**
        - **Device Name:** SE-FW01
    - **Protocol and action recorded in the traffic log entry on 2024/05/07 04:04:35:**
        - **Protocol:** udp
        - **Action:** allow
    - **Source and destination IPs for the log entry dated 2024/06/14 09:39:01:**
        - **Source IP/NAT'd Source IP:** 10.48.33.163/19.31.174.84
        - **Destination IP/NAT'd Destination IP:** 124.42.196.205/124.42.196.205
    - **Session end reason mentioned in the traffic log on 2024/05/07 04:04:35**:
        - **Session end reason:** aged-out

2. **Antivirus Log Answers:**
    - **Application blocked by the antivirus on 2024-06-14 05:47:32, and the action taken**:
        - **Application:** C:/Program Files(x86)/Dropbox/Client/Dropbox.exe
        - **Action:** Blocked
    - **SHA-256 hash value for the file associated with the log entry on 2024-06-14 05:47:32**:
        - **SHA-256:** 7462b5db619e77833d7cebcdca98352976154ba72d24080eb20edb01925accb6
    - **Vulnerability attack detected in the log entry dated 2024-05-04 14:07:50**:
        - **Vulnerability attack:** OpenSSL Heartbleed CVE-2014-0160
    - **Remote host IP in the antivirus log entry on 2024-05-04 14:07:50, and the action taken**:
        - **Remote Host IP:** 168.215.65.86
        - **Action:** detected but not blocked

- **User associated with the antivirus log entry on 2024-05-04 14:07:50**:
    - **User:** IZZMIER

3. **Firewall Log Analysis Answers:**
    - **Analyse the threat log entry on 2024/09/09. What was the URL that triggered the alert and what action was taken?**
        - **URL:** settings-win.data.microsoft.com
        - **Action Taken:** Alert
        - **Details:** The log entry from 2024/09/09 at 17:39:51 shows that an alert was triggered for a URL categorized under credential-phishing. The source IP was 10.60.3.123 and the NAT source IP was 19.31.169.76.
    - **In the traffic log entry on 2024/05/07, what was the source and destination IP address? What application was being used?**
        - **Source IP:** 10.192.104.61
        - **NAT Source IP:** 25.145.141.193
        - **Destination IP:** 20.67.222.222
        - **Application:** DNS
        - **Details:** This log entry is from 2024/05/07 at 04:04:35. The traffic type was end and the action taken was allow. The protocol used was UDP, with source port 62494 and destination port 53

4. **User Activity Monitoring Answer:**
    - **Based on the log entries, identify the users involved in the logged activities. What actions were taken by the user SE\bruno on 2024/06/14?**
        - **Users Involved:** SE\waynerooney, SE\bruno, SE\lisandro, garnacho, IZZMIER
        - **Actions by SE\bruno:**

            a. **Action:** Allow
            b. **Details:** On 2024/06/14 at 09:39:01, user SE\bruno had traffic allowed with the source IP 10.48.33.163 and the NAT source IP 19.31.174.84 to the destination IP 124.42.196.205. The protocol used was TCP, with the destination port 443. Bytes sent were 4541 and bytes received were 8413

- **What information can be deduced about the user SE\lisandro from the firewall logs?**
  - **User: SE\lisandro**
  - **Activity:**

    a. **Action:** Alert
    b. **Details:** On 2024/06/14 at 09:39:12, an alert was triggered for a URL categorized under credential-phishing for the user SE\lisandro. The source IP was 10.138.40.51 and the NAT source IP was 138.117.201.152. The destination IP was 17.37.97.229 and the destination port was 443

5. **Antivirus Log Examination Answers:**
   - **Review the antivirus log entry on 2024-06-14. What application was blocked and what were the hash values associated with it?**
     - **Application Blocked:** C:/Program Files (x86)/Dropbox/Client/Dropbox.exe
     - **SHA-256:** 7462b5db619e77833d7cebcdca98352976154ba72d24080eb20edb01925accb6
     - **MD-5:** 6B532CE4B97BC0F4D6CFA12E9637CBF5
     - **Details:** On 2024-06-14 at 05:47:32, an antivirus log entry shows that the Dropbox application was blocked. The local host IP was 192.168.0.22 and the remote host IP was 175.193.13.3
   - **Examine the antivirus log entry on 2024-05-04. What attack was detected, and what action was taken?**
     - **Attack Detected:** OpenSSL Heartbleed CVE-2014-0160
     - **Action Taken:** Detected but not blocked
     - **Details:** On 2024-05-04 at 14:07:50, an antivirus log entry shows that the OpenSSL Heartbleed vulnerability was detected in the FileZilla Server application. The local host IP was 192.168.99.4 and the remote host IP was 168.215.65.86

6. **Security Severity Assessment Answers:**
   - **What is the severity level of the threats detected in the firewall logs? Discuss the implications of these severity levels for network security.**
     - **Severity Level:** Informational
     - **Details:** The threats detected in the firewall logs on 2024/09/09 and 2024/06/14 were categorized as informational. This indicates that while these threats were flagged, they were not deemed critical or high risk. However, consistent monitoring and

analysis are essential to ensure that even informational threats do not escalate into significant security incidents

7. **Protocol and Port Analysis Answers:**
   - **Analyse the different protocols and ports used in the firewall traffic logs. How do these choices impact network security and performance?**
     - **Protocols Used:** TCP, UDP
     - **Ports Used:** 443 (HTTPS), 53 (DNS)
     - **Details:**

       a. **TCP over port 443:** Commonly used for secure web traffic. Ensures encryption and security for data in transit but can be a target for encrypted threats

       b. **UDP over port 53:** Used for DNS queries. Lightweight and faster for querying but more susceptible to certain types of attacks like DNS amplification

     - **Impact on Network Security and Performance:**

       a. **Security:** Using secure protocols like HTTPS (TCP/443) is beneficial for data protection, but administrators must ensure proper inspection of encrypted traffic to prevent hidden threats. DNS traffic (UDP/53) should be monitored for unusual patterns to mitigate potential attacks

       b. **Performance:** TCP is reliable but can be slower due to the overhead of connection management. UDP is faster and suitable for quick queries but lacks built-in security, requiring additional measures for protection

EXTRA QUESTION & ANSWERS

These questions and answers provide a comprehensive understanding of the network's security posture, user behaviour, and the effectiveness of existing security measures based on the provided logs.

Correlation Analysis:

1. **Correlate the threat logs with the traffic logs. Identify any instances where a threat alert coincides with a significant traffic event.**
   - **Instance 1**:
     - **Traffic Log (2024/06/14 09:39:01)**: Traffic allowed for user SE\bruno with source IP 10.48.33.163 and destination IP 124.42.196.205.
     - **Threat Log (2024/06/14 09:39:12)**: Alert for credential-phishing for user SE\lisandro with source IP 10.138.40.51 and destination IP 17.37.97.229.
   - **Analysis**: The threat alert does not directly coincide with the significant traffic event involving SE\bruno, but both logs are from the same date, suggesting that multiple activities were happening around the same time, which could be investigated further for any hidden correlations.

Log Detail Interpretation:

2. **What details can you infer about the potential security posture of the network based on the logs provided? Discuss the implications of the observed activities.**
   - **Inference**: The network is actively monitoring both traffic and potential threats, indicating a proactive security posture. The detection of credential-phishing attempts and blocked applications suggests a layered security approach. However, the presence of detected but not blocked threats (e.g., Heartbleed vulnerability) indicates areas for improvement in real-time threat mitigation.
   - **Implications**: The network is somewhat secure but could benefit from enhanced threat prevention measures and real-time blocking capabilities to mitigate potential risks more effectively.

Incident Response:

3. **Propose an incident response plan based on the detected threats in the logs. What steps would you take to mitigate these threats?**
   - **Step 1**: Immediate isolation of affected systems (e.g., machines with detected threats) to prevent further spread.

- **Step 2**: Detailed analysis of the detected threats (e.g., credential-phishing URLs) to understand the attack vectors and scope.
- **Step 3**: Apply necessary patches and updates to address vulnerabilities (e.g., Heartbleed).
- **Step 4**: Strengthen real-time detection and blocking capabilities, especially for critical threats.
- **Step 5**: Educate users on security best practices and phishing awareness to reduce the likelihood of successful attacks.
- **Step 6**: Conduct a post-incident review to identify gaps in the response process and improve future incident handling.

Comparative Analysis:

4. **Compare the actions taken in the threat logs versus the antivirus logs. How do the responses differ and what does this indicate about the different security measures in place?**
    - **Threat Logs**: Actions mainly involved alerts without blocking (e.g., credential-phishing).
    - **Antivirus Logs**: Actions included both blocking (e.g., Dropbox.exe) and detection without blocking (e.g., Heartbleed vulnerability).
    - **Indication**: The antivirus system seems more aggressive in blocking identified threats, while the firewall relies more on alerting. This suggests a need for better integration and coordination between different security systems to ensure comprehensive threat mitigation.

Network Traffic Patterns:

5. **Examine the traffic patterns indicated in the logs. Are there any unusual or unexpected patterns that might indicate a security issue?**
    - **Pattern**: Regular use of TCP and UDP protocols with common ports (443 for HTTPS and 53 for DNS).
    - **Unusual Patterns**: None explicitly unusual from the provided logs, but the presence of high traffic volume to external IPs (e.g., 124.42.196.205) should be monitored for potential data exfiltration.
    - **Security Issue Indication**: No immediate red flags, but continuous monitoring for abnormal spikes in traffic or unusual destination IPs is recommended.

User Behavior Analysis:

6. **Based on the user activities recorded in the logs, what can you deduce about the users' behavior and their potential security awareness?**
    - **Users Involved**: SE\waynerooney, SE\bruno, SE\lisandro, garnacho, IZZMIER.

- **Behavior Deduction**: Users SE\bruno and SE\lisandro were involved in activities around the same time a credential-phishing attempt was detected, suggesting potential phishing targets. User garnacho's involvement with a blocked Dropbox application might indicate risky behavior (downloading suspicious files).
- **Security Awareness**: Mixed levels of security awareness. Users might need further training on identifying phishing attempts and safe application usage.

Protocol Usage:

7. **Discuss the significance of the protocols used (TCP and UDP) in the context of the network's security. How do these protocols affect the security strategy?**
   - **TCP**: Reliable, ensures data integrity and connection security, suitable for sensitive transactions (e.g., HTTPS). However, encrypted traffic can hide threats.
   - **UDP**: Faster, suitable for quick queries (e.g., DNS), but less secure due to lack of connection establishment. Susceptible to spoofing and amplification attacks.
   - **Security Strategy Impact**: The security strategy must include robust inspection of encrypted TCP traffic and additional safeguards for UDP to prevent abuse.

Detection and Prevention:

8. **Evaluate the effectiveness of the detection and prevention mechanisms as evidenced by the logs. How well do they appear to be working?**
   - **Effectiveness**: The detection mechanisms are effective in identifying threats (e.g., credential-phishing, Heartbleed). However, the prevention mechanisms are partially effective; some threats are detected but not blocked.
   - **Working Well**: The blocking of suspicious applications shows proactive prevention.
   - **Improvements Needed**: Enhanced real-time blocking for high-severity threats and better coordination between detection systems.

Log Management:

9. **Suggest improvements to the log management process based on the provided logs. How can the logging system be enhanced to provide better security insights?**
   - **Improvement 1**: Implement centralized log management for easier correlation and analysis.

- **Improvement 2**: Enhance log detail with context-rich data (e.g., user roles, device context).
- **Improvement 3**: Regular review and tuning of log rules to minimize false positives and ensure critical events are not missed.
- **Improvement 4**: Incorporate automated threat intelligence to enrich log data with external threat information.
- **Improvement 5**: Enable real-time alerting and automated response based on log analysis.

Security Policy Review:

10. **Based on the logs, review and suggest potential updates to the network security policy. What additional rules or measures would you recommend?**
    - **Update 1**: Mandatory real-time blocking of high-severity threats.
    - **Update 2**: Regular security training for users on identifying phishing and safe application usage.
    - **Update 3**: Implementation of strict access controls and least privilege principle for sensitive applications.
    - **Update 4**: Periodic vulnerability assessments and patch management to address known vulnerabilities (e.g., Heartbleed).
    - **Update 5**: Enhanced monitoring and anomaly detection for unusual traffic patterns or high-volume data transfers.