CipherAI Digital Forensics Report

Executive Summary

This report summarizes the findings from system logs, network captures, and memory artefacts. The following sections highlight key indicators, suspicious IP addresses, port activity, and reconstructed DFIR insights.

Parsed Summary

Detected IPs: None

Active Ports: None

Log/Memory Events:
model_version='gemini-2.5-flash-lite' content=Content(parts=[Part(text="""```json { "iocs": { "ips": ["10.10.10.10"] }, "summary": "An accepted password for root from IP 10.10.10.10 via SSH was logged." } ```"""),], role='model') grounding_metadata=None partial=None turn_complete=None finish_reason= error_code=None error_message=None interrupted=None custom_metadata=None usage_metadata=GenerateContentResponseUsageMetadata(candidates_token_count=69, prompt_token_count=81, prompt_tokens_details=[ModalityTokenCount(modality=, token_count=81),], total_token_count=150) live_session_resumption_update=None input_transcription=None output_transcription=None avg_logprobs=None logprobs_result=None cache_metadata=None citation_metadata=None invocation_id='e-30e29dbb-7b90-4a61-93a9-a781723cfa86' author='LogAgent' actions=EventActions(skip_summarization=None, state_delta={'log_result': '```json\n{\n "iocs": {\n "ips": [\n "10.10.10.10"\n]\n },\n "summary": "An accepted password for root from IP 10.10.10.10 via SSH was logged."\n}\n```'}, artifact_delta={}, transfer_to_agent=None, escalate=None, requested_auth_configs={}, requested_tool_confirmations={}, compaction=None, end_of_agent=None, agent_state=None, rewind_before_invocation_id=None) long_running_tool_ids=None branch='ParallelTeam.LogAgent' id='5286c553-31bf-4409-b70a-87203ad7297d' timestamp=1763920525.847457
model_version='gemini-2.5-flash-lite' content=Content(parts=[Part(text="""The log entry indicates a successful password-based SSH login for the 'root' user from the IP address 10.10.10.10. **IOC IPs:** * 10.10.10.10"""),], role='model') grounding_metadata=None partial=None turn_complete=None finish_reason= error_code=None error_message=None interrupted=None custom_metadata=None usage_metadata=GenerateContentResponseUsageMetadata(candidates_token_count=53, prompt_token_count=57, prompt_tokens_details=[ModalityTokenCount(modality=, token_count=57),], total_token_count=110) live_session_resumption_update=None input_transcription=None output_transcription=None avg_logprobs=None logprobs_result=None cache_metadata=None citation_metadata=None invocation_id='e-30e29dbb-7b90-4a61-93a9-a781723cfa86' author='MemoryAgent' actions=EventActions(skip_summarization=None, state_delta={'memory_result': "The log entry indicates a successful password-based SSH login for the 'root' user from the IP address 10.10.10.10.\n\n**IOC IPs:**\n* 10.10.10.10"}, artifact_delta={}, transfer_to_agent=None, escalate=None, requested_auth_configs={}, requested_tool_confirmations={}, compaction=None, end_of_agent=None, agent_state=None, rewind_before_invocation_id=None) long_running_tool_ids=None branch='ParallelTeam.MemoryAgent' id='0b2a4e9d-c3f2-4806-956b-e084371af5b4' timestamp=1763920528.610643
model_version='gemini-2.5-flash-lite' content=Content(parts=[Part(text="""```json { "iocs": { "ips": ["10.10.10.10"], "ports": { "39202": 1 } }, "summary": "Successful SSH login for root from IP 10.10.10.10 on port 39202." } ```"""),], role='model') grounding_metadata=None partial=None turn_complete=None finish_reason= error_code=None error_message=None interrupted=None

custom_metadata=None usage_metadata=GenerateContentResponseUsageMetadata(candidates_token_count=93, prompt_token_count=84, prompt_tokens_details=[ModalityTokenCount(modality=, token_count=84),], total_token_count=177) live_session_resumption_update=None input_transcription=None output_transcription=None avg_logprobs=None logprobs_result=None cache_metadata=None citation_metadata=None invocation_id='e-30e29dbb-7b90-4a61-93a9-a781723cfa86' author='NetworkAgent' actions=EventActions(skip_summarization=None, state_delta={'network_result': '```json\n{\n "iocs": {\n "ips": [\n "10.10.10.10"\n],\n "ports": {\n "39202": 1\n }\n },\n "summary": "Successful SSH login for root from IP 10.10.10.10 on port 39202."\n}\n```'}, artifact_delta={}, transfer_to_agent=None, escalate=None, requested_auth_configs={}, requested_tool_confirmations={}, compaction=None, end_of_agent=None, agent_state=None, rewind_before_invocation_id=None) long_running_tool_ids=None branch='ParallelTeam.NetworkAgent' id='c1878872-2e4e-48de-acc0-734d1bab65b7' timestamp=1763920527.329215 model_version='gemini-2.0-flash' content=Content(parts=[Part(text="""## Security Report **Summary:** A successful password-based SSH login for the 'root' user was detected from IP address 10.10.10.10 on port 39202. **Indicators of Compromise (IOCs):** * **IP Address:** 10.10.10.10 * **Port:** 39202 **Analysis:** The log entry indicates a potential security concern due to the successful SSH login for the 'root' user using a password. Password-based authentication for the root user is generally discouraged due to security risks associated with brute-force attacks and password compromise. **Recommendations:** * Disable password-based authentication for the root user and enforce key-based authentication. * Investigate the source of the login from IP address 10.10.10.10 to determine its legitimacy. * Monitor network traffic for any suspicious activity originating from the identified IP address. * Consider implementing multi-factor authentication for SSH access. """),], role='model') grounding_metadata=None partial=None turn_complete=None finish_reason= error_code=None error_message=None interrupted=None custom_metadata=None usage_metadata=GenerateContentResponseUsageMetadata(candidates_token_count=225, candidates_tokens_details=[ModalityTokenCount(modality=, token_count=225),], prompt_token_count=320, prompt_tokens_details=[ModalityTokenCount(modality=, token_count=320),], total_token_count=545) live_session_resumption_update=None input_transcription=None output_transcription=None avg_logprobs=-0.11388190375434028 logprobs_result=None cache_metadata=None citation_metadata=None invocation_id='e-30e29dbb-7b90-4a61-93a9-a781723cfa86' author='CipherAggregator' actions=EventActions(skip_summarization=None, state_delta={}, artifact_delta={}, transfer_to_agent=None, escalate=None, requested_auth_configs={}, requested_tool_confirmations={}, compaction=None, end_of_agent=None, agent_state=None, rewind_before_invocation_id=None) long_running_tool_ids=None branch=None id='a2a5b8bd-bcfb-414d-89ac-989912a08692' timestamp=1763920531.425156 model_version='gemini-2.5-flash-lite' content=Content(parts=[Part(text="""**Digital Forensics Report** **Case ID:** [To be assigned] **Report Date:** 2023-10-27 **Prepared For:** [Recipient Name/Organization] **Prepared By:** ReportAgent (Digital Forensics Unit) **1. Executive Summary** This report details findings from the analysis of log data pertaining to a successful SSH login event. A successful password-based authentication for the 'root' user was identified originating from the IP address 10.10.10.10, connecting via SSH on port 39202. This event represents a potential security incident requiring further investigation and mitigation. **2. Introduction** The objective of this investigation was to analyze provided log data and identify any anomalies or indicators of compromise. The analysis focused on a specific log entry indicating an unauthorized or suspicious login event. **3. Data Sources** The primary data source for this analysis was a log entry with the following content: `Accepted password for root from 10.10.10.10 port 39202 ssh2` Additional contextual information was provided by the LogAgent, MemoryAgent, NetworkAgent, and CipherAggregator, which corroborated and enriched the findings from the initial log entry. **4. Methodology** The analysis involved: * Parsing the provided log entry to extract key details such as username, source IP address, port, and protocol. * Cross-referencing extracted information with contextual data provided by other agents to confirm the event's details and identify potential Indicators of Compromise (IOCs). * Evaluating the security implications of the identified event, particularly regarding the use of password-based authentication for the 'root' user. * Formulating actionable recommendations based on best security practices. **5. Findings** The following key findings were derived from the analysis: * **Event Type:** Successful SSH Login (Password-based

authentication). * **Username:** `root` * **Source IP Address:** `10.10.10.10` * **Source Port:** `39202` * **Protocol:** `ssh2` **6. Indicators of Compromise (IOCs)** The following IOCs have been identified: * **IP Address:** `10.10.10.10` * **Port:** `39202` **7. Analysis and Discussion** The log entry `Accepted password for root from 10.10.10.10 port 39202 ssh2` clearly indicates a successful authentication to the system using the 'root' user account via SSH. The use of password-based authentication for the highly privileged 'root' account is a significant security concern. This method is vulnerable to various attacks, including brute-force, dictionary attacks, and credential stuffing, especially if weak or reused passwords are employed. The source IP address `10.10.10.10` and port `39202` are identified as points of origin for this login attempt. The legitimacy of this login must be immediately scrutinized. Without further context on the expected activity from this IP address, it is treated as potentially malicious or unauthorized. **8. Recommendations** Based on the findings, the following recommendations are made: * **Disable Root SSH Login:** It is strongly recommended to disable direct SSH login for the 'root' user entirely. Users should log in with their own accounts and then use `sudo` to escalate privileges when necessary. * **Enforce Key-Based Authentication:** If SSH access for privileged accounts is unavoidable, implement SSH key-based authentication instead of password-based authentication. This significantly enhances security by eliminating the risk of password-related compromises. * **Investigate Source IP:** Conduct an investigation into the activity originating from `10.10.10.10`. Determine if this IP address belongs to a trusted internal network, a known external partner, or if it is an unknown or suspicious entity. * **Review Access Logs:** Perform a comprehensive review of SSH and system access logs to identify any other suspicious login attempts, successful or failed, from `10.10.10.10` or other unusual IP addresses. * **Implement Firewall Rules:** Consider implementing strict firewall rules to limit SSH access to only trusted IP addresses or subnets. * **Monitor for Brute-Force Attempts:** Implement or enhance intrusion detection/prevention systems (IDS/IPS) to monitor for and alert on brute-force SSH login attempts. * **Consider Multi-Factor Authentication (MFA):** For critical systems, implementing MFA for SSH access provides an additional layer of security beyond passwords or keys. **9. Conclusion** The successful password-based SSH login for the 'root' user from `10.10.10.10` is a critical security event that warrants immediate attention. Implementing the recommended security measures will help to mitigate the risk of unauthorized access and protect the integrity of the system. Further investigation into the source of this login is essential. **10. Appendices** [No appendices attached at this time.] --- **End of Report**"""),], role='model') grounding_metadata=None partial=None turn_complete=None finish_reason= error_code=None error_message=None interrupted=None custom_metadata=None usage_metadata=GenerateContentResponseUsageMetadata(candidates_token_count=1117, prompt_token_count=539, prompt_tokens_details=[ModalityTokenCount(modality=, token_count=539),], total_token_count=1656) live_session_resumption_update=None input_transcription=None output_transcription=None avg_logprobs=None logprobs_result=None cache_metadata=None citation_metadata=None invocation_id='e-30e29dbb-7b90-4a61-93a9-a781723cfa86' author='ReportAgent' actions=EventActions(skip_summarization=None, state_delta={'report': "**Digital Forensics Report**\n\n**Case ID:** [To be assigned]\n**Report Date:** 2023-10-27\n**Prepared For:** [Recipient Name/Organization]\n**Prepared By:** ReportAgent (Digital Forensics Unit)\n\n**1. Executive Summary**\n\nThis report details findings from the analysis of log data pertaining to a successful SSH login event. A successful password-based authentication for the 'root' user was identified originating from the IP address 10.10.10.10, connecting via SSH on port 39202. This event represents a potential security incident requiring further investigation and mitigation.\n\n**2. Introduction**\n\nThe objective of this investigation was to analyze provided log data and identify any anomalies or indicators of compromise. The analysis focused on a specific log entry indicating an unauthorized or suspicious login event.\n\n**3. Data Sources**\n\nThe primary data source for this analysis was a log entry with the following content:\n`Accepted password for root from 10.10.10.10 port 39202 ssh2`\n\nAdditional contextual information was provided by the LogAgent, MemoryAgent, NetworkAgent, and CipherAggregator, which corroborated and enriched the findings from the initial log entry.\n\n**4. Methodology**\n\nThe analysis involved:\n* Parsing the provided log entry to extract key details such as username, source IP address, port, and protocol.\n* Cross-referencing extracted information with contextual data provided by other agents to confirm the event's details and identify potential Indicators of Compromise (IOCs).\n* Evaluating the security implications of the identified event, particularly regarding the use of password-based

authentication for the 'root' user.\n* Formulating actionable recommendations based on best security practices.\n\n**5. Findings**\n\nThe following key findings were derived from the analysis:\n\n* **Event Type:** Successful SSH Login (Password-based authentication).\n* **Username:** `root`\n* **Source IP Address:** `10.10.10.10`\n* **Source Port:** `39202`\n* **Protocol:** `ssh2`\n\n**6. Indicators of Compromise (IOCs)**\n\nThe following IOCs have been identified:\n\n* **IP Address:** `10.10.10.10`\n* **Port:** `39202`\n\n**7. Analysis and Discussion**\n\nThe log entry `Accepted password for root from 10.10.10.10 port 39202 ssh2` clearly indicates a successful authentication to the system using the 'root' user account via SSH. The use of password-based authentication for the highly privileged 'root' account is a significant security concern. This method is vulnerable to various attacks, including brute-force, dictionary attacks, and credential stuffing, especially if weak or reused passwords are employed.\n\nThe source IP address `10.10.10.10` and port `39202` are identified as points of origin for this login attempt. The legitimacy of this login must be immediately scrutinized. Without further context on the expected activity from this IP address, it is treated as potentially malicious or unauthorized.\n\n**8. Recommendations**\n\nBased on the findings, the following recommendations are made:\n\n* **Disable Root SSH Login:** It is strongly recommended to disable direct SSH login for the 'root' user entirely. Users should log in with their own accounts and then use `sudo` to escalate privileges when necessary.\n* **Enforce Key-Based Authentication:** If SSH access for privileged accounts is unavoidable, implement SSH key-based authentication instead of password-based authentication. This significantly enhances security by eliminating the risk of password-related compromises.\n* **Investigate Source IP:** Conduct an investigation into the activity originating from `10.10.10.10`. Determine if this IP address belongs to a trusted internal network, a known external partner, or if it is an unknown or suspicious entity.\n* **Review Access Logs:** Perform a comprehensive review of SSH and system access logs to identify any other suspicious login attempts, successful or failed, from `10.10.10.10` or other unusual IP addresses.\n* **Implement Firewall Rules:** Consider implementing strict firewall rules to limit SSH access to only trusted IP addresses or subnets.\n* **Monitor for Brute-Force Attempts:** Implement or enhance intrusion detection/prevention systems (IDS/IPS) to monitor for and alert on brute-force SSH login attempts.\n* **Consider Multi-Factor Authentication (MFA):** For critical systems, implementing MFA for SSH access provides an additional layer of security beyond passwords or keys.\n\n**9. Conclusion**\n\nThe successful password-based SSH login for the 'root' user from `10.10.10.10` is a critical security event that warrants immediate attention. Implementing the recommended security measures will help to mitigate the risk of unauthorized access and protect the integrity of the system. Further investigation into the source of this login is essential.\n\n**10. Appendices**\n\n[No appendices attached at this time.]\n\n---\n**End of Report**"}, artifact_delta={}, transfer_to_agent=None, escalate=None, requested_auth_configs={}, requested_tool_confirmations={}, compaction=None, end_of_agent=None, agent_state=None, rewind_before_invocation_id=None) long_running_tool_ids=None branch=None id='6d0b0f75-2699-4072-a9b7-86d52bcdf0b5' timestamp=1763920535.400784

Visual Analysis