CipherAI Digital Forensics Report

1. Executive Summary

This report presents the results of an automated DFIR (Digital Forensics & Incident Response) analysis conducted using CipherAI. The analysis includes log inspection, PCAP network evaluation, and memory forensic assessment to identify suspicious activity, potential Indicators of Compromise (IOCs), and anomalies in system behavior.

2. Indicators of Compromise (IOCs)

No suspicious IP addresses detected.

No unusual port activity detected.

3. Memory Forensics Findings

• model_version='gemini-2.5-flash-lite' content=Content(parts=[Part(text="""The log indicates a successful SSH login for the `root` user from the IP address `10.10.10.10`. The PCAP data shows a TCP connection to port 22 (SSH) on destination IP `10.0.0.3`. The memory dump reveals a running Python process named `reverse_shell.py`. 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=93, prompt_token_count=158, prompt_tokens_details=[ModalityTokenCount(modality=, token_count=158),], total_token_count=251) 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-13217c18-4e0a-4510-8f37-10431c87ba68' author='MemoryAgent' actions=EventActions(skip_summarization=None, state_delta={'memory_result': 'The log indicates a successful SSH login for the `root` user from the IP address `10.10.10.10`. The PCAP data shows a TCP connection to port 22 (SSH) on destination IP `10.0.0.3`. The memory dump reveals a running Python process named `reverse_shell.py`.\n\nIOC 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='298dd6b4-8b0f-4f31-a7a0-66bb9abdc89e' timestamp=1763920950.642626

• model_version='gemini-2.5-flash-lite' content=Content(parts=[Part(text="""```json { "iocs": { "ips": ["10.10.10.10", "10.0.0.3"], "ports": { "39202": 1, "22": 1 } }, "summary": "A successful SSH login for root from 10.10.10.10:39202 was observed. Network traffic shows a connection to 10.0.0.3:22. A Python reverse shell process was detected, which may be related to the SSH activity." } ```"""),], 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=153, prompt_token_count=185, prompt_tokens_details=[ModalityTokenCount(modality=, token_count=185),], total_token_count=338) 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-13217c18-4e0a-4510-8f37-10431c87ba68' author='NetworkAgent' actions=EventActions(skip_summarization=None, state_delta={'network_result': '```json\n{\n "iocs":

{\n "ips": [\n "10.10.10.10",\n "10.0.0.3"\n],\n "ports": {\n "39202": 1,\n "22": 1\n }\n },\n "summary": "A successful SSH login for root from 10.10.10.10:39202 was observed. Network traffic shows a connection to 10.0.0.3:22. A Python reverse shell process was detected, which may be related to the SSH activity."\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='7d448cbc-e7ca-442a-b7a7-3883c68bab55' timestamp=1763920949.303447

• model_version='gemini-2.5-flash-lite' content=Content(parts=[Part(text="""```json { "iocs": { "ips": ["10.10.10.10", "10.0.0.3"] }, "summary": "The log indicates a successful password login for the 'root' user from IP address 10.10.10.10 via SSH. The PCAP data shows a TCP connection to destination port 22 on IP address 10.0.0.3. The memory analysis reveals a running Python process executing a script named 'reverse_shell.py'." } ```"""),], 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=137, prompt_token_count=182, prompt_tokens_details=[ModalityTokenCount(modality=, token_count=182),], total_token_count=319) 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-13217c18-4e0a-4510-8f37-10431c87ba68' author='LogAgent' actions=EventActions(skip_summarization=None, state_delta={'log_result': '```json\n{\n "iocs": {\n "ips": [\n "10.10.10.10",\n "10.0.0.3"\n]\n },\n "summary": "The log indicates a successful password login for the \'root\' user from IP address 10.10.10.10 via SSH. The PCAP data shows a TCP connection to destination port 22 on IP address 10.0.0.3. The memory analysis reveals a running Python process executing a script named \'reverse_shell.py\'."\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='5db078c8-8586-400e-b542-361b5b1c9b5a' timestamp=1763920947.785514

• model_version='gemini-2.0-flash' content=Content(parts=[Part(text="""```json { "security_report": { "summary": "A potential security breach has been detected. A successful SSH login for the 'root' user was observed from IP address 10.10.10.10 via port 39202. Simultaneously, network traffic indicates a connection to IP address 10.0.0.3 on port 22 (SSH). Critically, a Python process named 'reverse_shell.py' is running, suggesting a possible reverse shell attack originating from the SSH session. This combination of events warrants immediate investigation.", "iocs": { "ips": ["10.10.10.10", "10.0.0.3"], "ports": ["39202", "22"], "processes": ["/usr/bin/python3 reverse_shell.py"] }, "details": { "log_analysis": "Successful password login for root from 10.10.10.10.", "network_analysis": "Network traffic shows connection to 10.0.0.3 on port 22 (SSH).", "memory_analysis": "A python reverse shell process is running." }, "recommendations": ["Immediately investigate the SSH login from 10.10.10.10. Determine if the login was authorized.", "Examine the 'reverse_shell.py' script to understand its functionality and potential impact.", "Monitor network traffic to and from 10.0.0.3 for suspicious activity.", "Consider isolating the affected machine (likely 10.0.0.3) to prevent further compromise.", "Change the root password immediately.", "Implement multi-factor authentication for SSH access to prevent future unauthorized logins."] } } ```"""),], 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=443, candidates_tokens_details=[ModalityTokenCount(modality=, token_count=443),], prompt_token_count=589, prompt_tokens_details=[ModalityTokenCount(modality=, token_count=589),], total_token_count=1032) live_session_resumption_update=None input_transcription=None output_transcription=None avg_logprobs=-0.13862032061505802 logprobs_result=None cache_metadata=None citation_metadata=None invocation_id='e-13217c18-4e0a-4510-8f37-10431c87ba68' 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='792d624d-1ea1-4297-bb7d-e4e6a567e34b' timestamp=1763920953.945177

• model_version='gemini-2.5-flash-lite' content=Content(parts=[Part(text="""**Digital Forensics Report** **Case Number:** [Assigned Case Number] **Date of Report:** 2023-10-27 **Prepared By:** ReportAgent **Report Version:** 1.0 **1. Executive Summary** This report details findings from a digital forensics investigation, which indicates a potential security breach involving unauthorized access and the execution of malicious code. Evidence suggests a successful SSH login for the `root` user from an external IP address (`10.10.10.10`) followed by the initiation of a reverse shell via a Python script (`reverse_shell.py`) on the target system (`10.0.0.3`). The findings warrant immediate action to contain and remediate the incident. **2. Incident Overview** The investigation was triggered by the observation of the following events: * A successful password-based SSH login for the `root` user originating from IP address `10.10.10.10`, connecting from port `39202`. * Network traffic analysis revealing a TCP connection to destination IP address `10.0.0.3` on port `22` (SSH). * Memory analysis identifying a running process associated with a Python script named `reverse_shell.py`. **3. Evidence Collected and Analysis** The following data sources were analyzed: **3.1. Log Data Analysis** * **Source:** System logs (e.g., `/var/log/auth.log`, `secure`) * **Relevant Entry:** `Accepted password for root from 10.10.10.10 port 39202 ssh2` * **Analysis:** This log entry confirms a successful authenticated login for the `root` user. The source IP address is identified as `10.10.10.10`, and the originating port is `39202`. This indicates the point of entry for the attacker. **3.2. Network Packet Capture (PCAP) Analysis** * **Source:** Network traffic capture. * **Relevant Data:** * Destination IP: `10.0.0.3` * Destination Port: `22` (TCP) * **Analysis:** The PCAP data corroborates network activity directed towards the target system (`10.0.0.3`) on the standard SSH port (22). This aligns with the SSH login observed in the logs. It is important to note that while the initial SSH connection was from `10.10.10.10` to the target, the PCAP analysis provided shows a connection to `10.0.0.3`, implying `10.0.0.3` is the target system where the SSH login occurred. **3.3. Memory Analysis** * **Source:** System memory dump. * **Relevant Finding:** Process entry `/usr/bin/python3 reverse_shell.py` * **Analysis:** The presence of a running Python process executing `reverse_shell.py` is a significant indicator of malicious activity. A "reverse shell" is a common technique used by attackers to establish a command and control channel back to their own system, allowing them to execute commands remotely. This script likely was initiated following the successful SSH login. **4. Indicators of Compromise (IOCs)** * **IP Addresses:** * `10.10.10.10` (Source of SSH connection) * `10.0.0.3` (Target system) * **Ports:** * `39202` (Source port for SSH connection) * `22` (Destination port for SSH connection) * **Processes:** * `/usr/bin/python3 reverse_shell.py` (Suspected reverse shell executable) **5. Correlation and Timeline (Inferred)** Based on the evidence, the following inferred timeline of events can be established: 1. An attacker, originating from IP `10.10.10.10` (port `39202`), established an SSH connection to the target system `10.0.0.3` on port `22`. 2. The attacker successfully authenticated using the `root` user credentials (via password). 3. Shortly after gaining root access, the attacker executed a Python script named `reverse_shell.py` on the target system (`10.0.0.3`). This action likely initiated a reverse shell connection, allowing the attacker persistent remote access and control. **6. Recommendations** Based on the findings of this investigation, the following actions are recommended: * **Immediate Containment:** * Isolate the compromised system (`10.0.0.3`) from the network to prevent further lateral movement or data exfiltration. * Block all inbound and outbound traffic from and to the suspected malicious IP address `10.10.10.10`. * **Investigation and Remediation:** * Perform a full forensic analysis of the compromised system (`10.0.0.3`) to identify the full scope of the compromise, including any other malicious files, processes, or persistent mechanisms. * Analyze the content of the `reverse_shell.py` script to understand its exact functionality and the attacker's objectives. * Change the `root` password on the compromised system immediately. * Review all SSH access logs for the compromised system for any other suspicious login attempts. * Identify how the attacker obtained the `root` credentials. * **Proactive Security Measures:** * Implement strong password policies and enforce regular password changes for all privileged accounts. * Enable and enforce multi-factor authentication (MFA) for all SSH access. * Review and restrict SSH access to only necessary IP addresses. * Deploy and maintain up-to-date intrusion detection and prevention systems (IDPS). * Implement regular security awareness training for users. **7.

Conclusion** The evidence strongly suggests that the system `10.0.0.3` has been compromised via an unauthorized SSH login, followed by the execution of a reverse shell. Prompt and thorough remediation is critical to mitigate the impact of this security incident. --- **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=1395, prompt_token_count=1026, prompt_tokens_details=[ModalityTokenCount(modality=, token_count=1026),], total_token_count=2421) 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-13217c18-4e0a-4510-8f37-10431c87ba68' author='ReportAgent' actions=EventActions(skip_summarization=None, state_delta={'report': '**Digital Forensics Report**\n\n**Case Number:** [Assigned Case Number]\n**Date of Report:** 2023-10-27\n**Prepared By:** ReportAgent\n**Report Version:** 1.0\n\n**1. Executive Summary**\n\nThis report details findings from a digital forensics investigation, which indicates a potential security breach involving unauthorized access and the execution of malicious code. Evidence suggests a successful SSH login for the `root` user from an external IP address (`10.10.10.10`) followed by the initiation of a reverse shell via a Python script (`reverse_shell.py`) on the target system (`10.0.0.3`). The findings warrant immediate action to contain and remediate the incident.\n\n**2. Incident Overview**\n\nThe investigation was triggered by the observation of the following events:\n\n* A successful password-based SSH login for the `root` user originating from IP address `10.10.10.10`, connecting from port `39202`.\n* Network traffic analysis revealing a TCP connection to destination IP address `10.0.0.3` on port `22` (SSH).\n* Memory analysis identifying a running process associated with a Python script named `reverse_shell.py`.\n\n**3. Evidence Collected and Analysis**\n\nThe following data sources were analyzed:\n\n**3.1. Log Data Analysis**\n\n* **Source:** System logs (e.g., `/var/log/auth.log`, `secure`)\n* **Relevant Entry:** `Accepted password for root from 10.10.10.10 port 39202 ssh2`\n* **Analysis:** This log entry confirms a successful authenticated login for the `root` user. The source IP address is identified as `10.10.10.10`, and the originating port is `39202`. This indicates the point of entry for the attacker.\n\n**3.2. Network Packet Capture (PCAP) Analysis**\n\n* **Source:** Network traffic capture.\n* **Relevant Data:**\n * Destination IP: `10.0.0.3`\n * Destination Port: `22` (TCP)\n* **Analysis:** The PCAP data corroborates network activity directed towards the target system (`10.0.0.3`) on the standard SSH port (22). This aligns with the SSH login observed in the logs. It is important to note that while the initial SSH connection was from `10.10.10.10` to the target, the PCAP analysis provided shows a connection to `10.0.0.3`, implying `10.0.0.3` is the target system where the SSH login occurred.\n\n**3.3. Memory Analysis**\n\n* **Source:** System memory dump.\n* **Relevant Finding:** Process entry `/usr/bin/python3 reverse_shell.py`\n* **Analysis:** The presence of a running Python process executing `reverse_shell.py` is a significant indicator of malicious activity. A "reverse shell" is a common technique used by attackers to establish a command and control channel back to their own system, allowing them to execute commands remotely. This script likely was initiated following the successful SSH login.\n\n**4. Indicators of Compromise (IOCs)**\n\n* **IP Addresses:**\n * `10.10.10.10` (Source of SSH connection)\n * `10.0.0.3` (Target system)\n* **Ports:**\n * `39202` (Source port for SSH connection)\n * `22` (Destination port for SSH connection)\n* **Processes:**\n * `/usr/bin/python3 reverse_shell.py` (Suspected reverse shell executable)\n\n**5. Correlation and Timeline (Inferred)**\n\nBased on the evidence, the following inferred timeline of events can be established:\n\n1. An attacker, originating from IP `10.10.10.10` (port `39202`), established an SSH connection to the target system `10.0.0.3` on port `22`.\n2. The attacker successfully authenticated using the `root` user credentials (via password).\n3. Shortly after gaining root access, the attacker executed a Python script named `reverse_shell.py` on the target system (`10.0.0.3`). This action likely initiated a reverse shell connection, allowing the attacker persistent remote access and control.\n\n**6. Recommendations**\n\nBased on the findings of this investigation, the following actions are recommended:\n\n* **Immediate Containment:**\n * Isolate the compromised system (`10.0.0.3`) from the network to prevent further lateral movement or data exfiltration.\n * Block all inbound and outbound traffic from and to the suspected malicious IP address `10.10.10.10`.\n* **Investigation and Remediation:**\n * Perform a full forensic analysis of the compromised system (`10.0.0.3`) to identify the full scope of the compromise, including any other malicious files, processes, or

persistent mechanisms.\n * Analyze the content of the `reverse_shell.py` script to understand its exact functionality and the attacker\'s objectives.\n * Change the `root` password on the compromised system immediately.\n * Review all SSH access logs for the compromised system for any other suspicious login attempts.\n * Identify how the attacker obtained the `root` credentials.\n* **Proactive Security Measures:**\n * Implement strong password policies and enforce regular password changes for all privileged accounts.\n * Enable and enforce multi-factor authentication (MFA) for all SSH access.\n * Review and restrict SSH access to only necessary IP addresses.\n * Deploy and maintain up-to-date intrusion detection and prevention systems (IDPS).\n * Implement regular security awareness training for users.\n\n**7. Conclusion**\n\nThe evidence strongly suggests that the system `10.0.0.3` has been compromised via an unauthorized SSH login, followed by the execution of a reverse shell. Prompt and thorough remediation is critical to mitigate the impact of this security incident.\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='99e984de-9379-4e37-9646-c7d03be1c1b1' timestamp=1763920959.815145

4. Visual Summary