CipherAI Report

Raw Model Output:

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 shows an accepted password for root from IP address 10.10.10.10 via SSH. The pcap data indicates a connection to IP 10.0.0.3 on port 22. Memory analysis revealed a running Python process executing a reverse shell script."
}
```"""
),
],
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=123,
prompt_token_count=182,
prompt_tokens_details=[
ModalityTokenCount(
modality=,
token_count=182
),
],
total_token_count=305
) 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-b243c028-e40d-46a3-9d28-734ad3b9fe97' 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 shows an accepted password for root from IP address 10.10.10.10 via SSH. The pcap data indicates a connection to IP 10.0.0.3 on port 22. Memory analysis revealed a running Python process executing a reverse shell script."\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='37fa04c5-2702-4eb5-9a76-8d56aa6530fa' timestamp=1763919249.111852
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": "The log indicates a successful SSH login for 'root' from IP 10.10.10.10 on port 39202. The PCAP data shows network traffic to IP 10.0.0.3 on port 22 (SSH). Additionally, a Python reverse shell script '/usr/bin/python3 reverse_shell.py' was found running in memory. This suggests a potential compromise, where an attacker might have gained access via SSH and is now running a reverse shell."
}
```"""
),
],
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=195,
prompt_token_count=185,
prompt_tokens_details=[
ModalityTokenCount(
modality=,
token_count=185
),
],
total_token_count=380
) 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-b243c028-e40d-46a3-9d28-734ad3b9fe97' 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": "The log indicates a successful SSH login for \'root\' from IP 10.10.10.10 on port 39202. The PCAP data shows network traffic to IP 10.0.0.3 on port 22 (SSH). Additionally, a Python reverse shell script \'/usr/bin/python3 reverse_shell.py\' was found running in memory. This suggests a potential compromise, where an attacker might have gained access via SSH and is now running a reverse shell."\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='8f2be312-c845-49d6-8158-b4154260d3cc' timestamp=1763919250.603627 model_version='gemini-2.5-flash-lite' content=Content(
parts=[
Part(
text="""The user provided a memory dump. I will summarize it and extract any Indicators of Compromise (IOCs) in the form of IP addresses.

The memory dump indicates that a Python script named `reverse_shell.py` was found running.

**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=69,
prompt_token_count=158,
prompt_tokens_details=[
ModalityTokenCount(
modality=,
token_count=158
),
],
total_token_count=227
) 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-b243c028-e40d-46a3-9d28-734ad3b9fe97' author='MemoryAgent' actions=EventActions(skip_summarization=None, state_delta={'memory_result': 'The user provided a memory dump. I will summarize it and extract any Indicators of Compromise (IOCs) in the form of IP addresses.\n\nThe memory dump indicates that a Python script named `reverse_shell.py` was found running.\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='d6c1bd38-b52b-4359-91a5-03dcdf91ee75' timestamp=1763919251.890521 model_version='gemini-2.0-flash' content=Content(
parts=[
Part(
text="""```json
{
"iocs": {
"ips": [
"10.10.10.10",
"10.0.0.3"
],
"ports": {
"39202": 1,
"22": 1
},
"processes": [
"/usr/bin/python3 reverse_shell.py"
]
},
"summary": "A potential security compromise has been detected. The log shows a successful SSH login for 'root' from IP address 10.10.10.10 on port 39202. Network traffic was observed to IP 10.0.0.3 on port 22 (SSH). Critically, a Python reverse shell script ('/usr/bin/python3 reverse_shell.py') was found running in memory. This strongly suggests that an attacker may have gained unauthorized access via SSH and is now operating a reverse shell to maintain persistence or further compromise the system."
}
```"""
),
],
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=238,
candidates_tokens_details=[
ModalityTokenCount(
modality=,
token_count=238
),
],
prompt_token_count=592,
prompt_tokens_details=[
ModalityTokenCount(
modality=,
token_count=592
),
],
total_token_count=830
) live_session_resumption_update=None input_transcription=None output_transcription=None
avg_logprobs=-0.0908941300977178 logprobs_result=None cache_metadata=None
citation_metadata=None invocation_id='e-b243c028-e40d-46a3-9d28-734ad3b9fe97'
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='d1644a86-d0b4-4b2d-9db1-b04a9179395b' timestamp=1763919255.414444
model_version='gemini-2.5-flash-lite' content=Content(
parts=[
Part(
text="""## Digital Forensics Report

Case ID: [Insert Case ID Here]
Report Date: 2023-10-27
Prepared By: ReportAgent

---

1. Executive Summary

This report details findings from a digital forensics examination of system artifacts. Evidence indicates a potential security incident involving unauthorized access and the execution of malicious code. Specifically, a successful SSH login by the 'root' user originating from IP address 10.10.10.10 was recorded. Network traffic analysis reveals a connection to IP address 10.0.0.3 on port 22 (SSH). Furthermore, memory analysis has identified a running process associated with a Python script named `reverse_shell.py`, indicative of a reverse shell being active.

---

2. Data Sources Examined

The following data sources were analyzed:

* **System Logs:** Records of system events, including authentication attempts.
* **Network Packet Capture (PCAP):** Captured network traffic data.
* **Memory Dump:** A snapshot of the system's active memory.

---

3. Findings

3.1. System Logs

* **Event:** Accepted password for root from 10.10.10.10 port 39202 ssh2.
* **Analysis:** This log entry confirms a successful authentication for the highly privileged 'root' account. The connection originated from the internal IP address `10.10.10.10` on port `39202`. The use of SSH is explicitly stated.

3.2. Network Packet Capture (PCAP)

* **Observed Traffic:**
* Destination IP: `10.0.0.3`
* Destination Port: `22` (SSH)
* **Analysis:** The PCAP data indicates network communication directed towards IP address `10.0.0.3` on port `22`. This aligns with the SSH protocol identified in the system logs, suggesting that the SSH connection either terminated at this IP or was proxied through it.

3.3. Memory Analysis

* **Process Found:** `/usr/bin/python3 reverse_shell.py`
* **Analysis:** The memory dump revealed an active process executing the Python interpreter (`/usr/bin/python3`) with the script `reverse_shell.py`. The name of this script strongly suggests it is designed to establish a reverse shell connection, allowing an external attacker to gain command and control over the compromised system.

---

4. Indicators of Compromise (IOCs)

The following Indicators of Compromise were identified:

* **IP Addresses:**
* `10.10.10.10` (Source of SSH login)
* `10.0.0.3` (Destination of SSH traffic)
* **Ports:**
* `39202` (Source port for SSH login)
* `22` (Destination port for SSH traffic)
* **Processes:**
* `/usr/bin/python3 reverse_shell.py` (Identified running process)

---

5. Conclusion

The collected evidence strongly suggests a security breach has occurred. The successful SSH login by 'root' from an external IP, coupled with the presence of a reverse shell script running in memory, indicates that an unauthorized actor may have gained privileged access to the system and is actively maintaining control or attempting further actions.

---

6. Recommendations

* Immediately isolate the affected system from the network to prevent further unauthorized access or data exfiltration.
* Conduct a full system scan for malware and rootkits.

* Review all user accounts, particularly privileged accounts, for any suspicious activity.
* Investigate the origin of the connection from `10.10.10.10` and the network path to `10.0.0.3`.
* Preserve all collected forensic artifacts for potential further investigation or legal proceedings.
* Implement enhanced network monitoring and intrusion detection systems.

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=903,
prompt_token_count=824,
prompt_tokens_details=[
ModalityTokenCount(
modality=,
token_count=824
),
],
total_token_count=1727
) 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-b243c028-e40d-46a3-9d28-734ad3b9fe97' author='ReportAgent' actions=EventActions(skip_summarization=None, state_delta={'report': "## Digital Forensics Report\n\n**Case ID:** [Insert Case ID Here]\n**Report Date:** 2023-10-27\n**Prepared By:** ReportAgent\n\n---\n\n### 1. Executive Summary\n\nThis report details findings from a digital forensics examination of system artifacts. Evidence indicates a potential security incident involving unauthorized access and the execution of malicious code. Specifically, a successful SSH login by the 'root' user originating from IP address 10.10.10.10 was recorded. Network traffic analysis reveals a connection to IP address 10.0.0.3 on port 22 (SSH). Furthermore, memory analysis has identified a running process associated with a Python script named `reverse_shell.py`, indicative of a reverse shell being active.\n\n---\n\n### 2. Data Sources Examined\n\nThe following data sources were analyzed:\n\n* **System Logs:** Records of system events, including authentication attempts.\n* **Network Packet Capture (PCAP):** Captured network traffic data.\n* **Memory Dump:** A snapshot of the system's active memory.\n\n---\n\n### 3. Findings\n\n#### 3.1. System Logs\n\n* **Event:** Accepted password for root from 10.10.10.10 port 39202 ssh2.\n* **Analysis:** This log entry confirms a successful authentication for the highly privileged 'root' account. The connection originated from the internal IP address `10.10.10.10` on port `39202`. The use of SSH is explicitly stated.\n\n#### 3.2. Network Packet Capture (PCAP)\n\n* **Observed Traffic:**\n * Destination IP: `10.0.0.3`\n * Destination Port: `22` (SSH)\n* **Analysis:** The PCAP data indicates network communication directed towards IP address `10.0.0.3` on port `22`. This aligns with the SSH protocol identified in the system logs, suggesting that the SSH connection either terminated at this IP or was proxied through it.\n\n#### 3.3. Memory Analysis\n\n* **Process Found:** `/usr/bin/python3 reverse_shell.py`\n* **Analysis:** The memory dump revealed an active process executing the Python interpreter (`/usr/bin/python3`) with the script `reverse_shell.py`. The name of this script strongly suggests it is designed to establish a reverse shell connection, allowing an external attacker to gain command and control over the compromised system.\n\n---\n\n### 4. Indicators of Compromise (IOCs)\n\nThe following Indicators of Compromise were identified:\n\n* **IP Addresses:**\n * `10.10.10.10` (Source of SSH login)\n * `10.0.0.3` (Destination of SSH traffic)\n* **Ports:**\n * `39202` (Source port for SSH login)\n * `22` (Destination port for SSH traffic)\n* **Processes:**\n * `/usr/bin/python3 reverse_shell.py` (Identified running process)\n\n---\n\n### 5. Conclusion\n\nThe collected evidence strongly suggests a security breach has occurred. The successful SSH login by 'root' from an external IP, coupled with the presence of a reverse shell script running in memory, indicates that an unauthorized actor may have gained

privileged access to the system and is actively maintaining control or attempting further actions.\n\n---\n\n### 6. Recommendations\n\n* Immediately isolate the affected system from the network to prevent further unauthorized access or data exfiltration.\n* Conduct a full system scan for malware and rootkits.\n* Review all user accounts, particularly privileged accounts, for any suspicious activity.\n* Investigate the origin of the connection from `10.10.10.10` and the network path to `10.0.0.3`.\n* Preserve all collected forensic artifacts for potential further investigation or legal proceedings.\n* Implement enhanced network monitoring and intrusion detection systems.\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='8a369699-1776-4db8-9c76-1da1b53dc03a' timestamp=1763919259.499246

Parsed Summary:


```
{
"parsed_events": [
"model_version='gemini-2.5-flash-lite' content=Content(\n parts=[\n Part(\n
text=\"\"\"```json\n{\n \"iocs\": {\n \"ips\": [\n \"10.10.10.10\",\n \"10.0.0.3\"\n
]\n },\n \"summary\": \"The log shows an accepted password for root from IP address
10.10.10.10 via SSH. The pcap data indicates a connection to IP 10.0.0.3 on port 22.
Memory analysis revealed a running Python process executing a reverse shell
script.\"\n}\n```\"\"\"\n ),\n ],\n role='model'\n) grounding_metadata=None
partial=None turn_complete=None finish_reason= error_code=None error_message=None
interrupted=None custom_metadata=None
usage_metadata=GenerateContentResponseUsageMetadata(\n candidates_token_count=123,\n
prompt_token_count=182,\n prompt_tokens_details=[\n ModalityTokenCount(\n
modality=,\n token_count=182\n ),\n ],\n total_token_count=305\n)
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-b243c028-e40d-46a3-9d28-734ad3b9fe97'
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 shows an
accepted password for root from IP address 10.10.10.10 via SSH. The pcap data
indicates a connection to IP 10.0.0.3 on port 22. Memory analysis revealed a running
Python process executing a reverse shell script.\"\\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='37fa04c5-2702-4eb5-9a76-8d56aa6530fa'
timestamp=1763919249.111852",
"model_version='gemini-2.5-flash-lite' content=Content(\n parts=[\n Part(\n
text=\"\"\"```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\": \"The log
indicates a successful SSH login for 'root' from IP 10.10.10.10 on port 39202. The
PCAP data shows network traffic to IP 10.0.0.3 on port 22 (SSH). Additionally, a
Python reverse shell script '/usr/bin/python3 reverse_shell.py' was found running in
memory. This suggests a potential compromise, where an attacker might have gained
access via SSH and is now running a reverse shell.\"\n}\n```\"\"\"\n ),\n ],\n
role='model'\n) grounding_metadata=None partial=None turn_complete=None
finish_reason= error_code=None error_message=None interrupted=None
custom_metadata=None usage_metadata=GenerateContentResponseUsageMetadata(\n
candidates_token_count=195,\n prompt_token_count=185,\n prompt_tokens_details=[\n
ModalityTokenCount(\n modality=,\n token_count=185\n ),\n ],\n
total_token_count=380\n) 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-b243c028-e40d-46a3-9d28-734ad3b9fe97' 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\": \"The
log indicates a successful SSH login for \\'root\\' from IP 10.10.10.10 on port
39202. The PCAP data shows network traffic to IP 10.0.0.3 on port 22 (SSH).
Additionally, a Python reverse shell script \\'/usr/bin/python3 reverse_shell.py\\'
was found running in memory. This suggests a potential compromise, where an attacker
might have gained access via SSH and is now running a reverse shell.\"\\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='8f2be312-c845-49d6-8158-b4154260d3cc'
```

timestamp=1763919250.603627",
"model_version='gemini-2.5-flash-lite' content=Content(\n parts=[\n Part(\n text=\"\"\"The user provided a memory dump. I will summarize it and extract any Indicators of Compromise (IOCs) in the form of IP addresses.\n\nThe memory dump indicates that a Python script named `reverse_shell.py` was found running.\n\n**IOC IPs:**\n* 10.10.10.10\"\"\"\n),\n],\n role='model'\n) grounding_metadata=None partial=None turn_complete=None finish_reason= error_code=None error_message=None interrupted=None custom_metadata=None usage_metadata=GenerateContentResponseUsageMetadata(\n candidates_token_count=69,\n prompt_token_count=158,\n prompt_tokens_details=[\n ModalityTokenCount(\n modality=,\n token_count=158\n),\n],\n total_token_count=227\n) 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-b243c028-e40d-46a3-9d28-734ad3b9fe97' author='MemoryAgent' actions=EventActions(skip_summarization=None, state_delta={'memory_result': 'The user provided a memory dump. I will summarize it and extract any Indicators of Compromise (IOCs) in the form of IP addresses.\\n\\nThe memory dump indicates that a Python script named `reverse_shell.py` was found running.\\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='d6c1bd38-b52b-4359-91a5-03dcdf91ee75' timestamp=1763919251.890521",
"model_version='gemini-2.0-flash' content=Content(\n parts=[\n Part(\n text=\"\"\"```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 \"processes\": [\n \"/usr/bin/python3 reverse_shell.py\"\n]\n },\n \"summary\": \"A potential security compromise has been detected. The log shows a successful SSH login for 'root' from IP address 10.10.10.10 on port 39202. Network traffic was observed to IP 10.0.0.3 on port 22 (SSH). Critically, a Python reverse shell script ('/usr/bin/python3 reverse_shell.py') was found running in memory. This strongly suggests that an attacker may have gained unauthorized access via SSH and is now operating a reverse shell to maintain persistence or further compromise the system.\"\n}\n```\"\"\"\n),\n],\n role='model'\n) grounding_metadata=None partial=None turn_complete=None finish_reason= error_code=None error_message=None interrupted=None custom_metadata=None usage_metadata=GenerateContentResponseUsageMetadata(\n candidates_token_count=238,\n candidates_tokens_details=[\n ModalityTokenCount(\n modality=,\n token_count=238\n),\n],\n prompt_token_count=592,\n prompt_tokens_details=[\n ModalityTokenCount(\n modality=,\n token_count=592\n),\n],\n total_token_count=830\n) live_session_resumption_update=None input_transcription=None output_transcription=None avg_logprobs=-0.0908941300977178 logprobs_result=None cache_metadata=None citation_metadata=None invocation_id='e-b243c028-e40d-46a3-9d28-734ad3b9fe97' 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='d1644a86-d0b4-4b2d-9db1-b04a9179395b' timestamp=1763919255.414444",
"model_version='gemini-2.5-flash-lite' content=Content(\n parts=[\n Part(\n text=\"\"\"## Digital Forensics Report\n\n**Case ID:** [Insert Case ID Here]\n**Report Date:** 2023-10-27\n**Prepared By:** ReportAgent\n\n---\n\n### 1. Executive Summary\n\nThis report details findings from a digital forensics examination of system artifacts. Evidence indicates a potential security incident involving unauthorized access and the execution of malicious code. Specifically, a successful SSH login by the 'root' user originating from IP address 10.10.10.10 was recorded. Network traffic analysis reveals a connection to IP address 10.0.0.3 on port 22 (SSH). Furthermore, memory analysis has identified a running process associated with a Python script named `reverse_shell.py`, indicative of a reverse shell being active.\n\n---\n\n### 2. Data Sources Examined\n\nThe following data sources were analyzed:\n\n* **System Logs:** Records of system events, including authentication attempts.\n* **Network Packet Capture (PCAP):** Captured network traffic data.\n* **Memory Dump:** A snapshot of the system's active memory.\n\n---\n\n### 3. Findings\n\n#### 3.1. System Logs\n\n* **Event:** Accepted password for root from 10.10.10.10 port 39202 ssh2.\n* **Analysis:** This log entry confirms a successful authentication for the highly privileged 'root' account. The connection originated from the internal IP address `10.10.10.10` on port `39202`. The use of SSH is explicitly stated.\n\n#### 3.2. Network Packet Capture (PCAP)\n\n* **Observed Traffic:**\n * Destination IP: `10.0.0.3`\n * Destination Port: `22` (SSH)\n* **Analysis:** The PCAP data indicates network communication directed towards IP address `10.0.0.3` on port `22`. This aligns with the SSH protocol identified in the system logs, suggesting that the SSH connection either terminated at this IP or was proxied through it.\n\n#### 3.3. Memory Analysis\n\n* **Process Found:** `/usr/bin/python3 reverse_shell.py`\n* **Analysis:** The memory dump revealed an active process executing the Python interpreter (`/usr/bin/python3`) with the script `reverse_shell.py`. The name of this script strongly suggests it is designed to establish a reverse shell connection, allowing an external attacker to

gain command and control over the compromised system.\n\n---\n\n### 4. Indicators of Compromise (IOCs)\n\nThe following Indicators of Compromise were identified:\n\n* **IP Addresses:**\n * `10.10.10.10` (Source of SSH login)\n * `10.0.0.3` (Destination of SSH traffic)\n* **Ports:**\n * `39202` (Source port for SSH login)\n * `22` (Destination port for SSH traffic)\n* **Processes:**\n * `/usr/bin/python3 reverse_shell.py` (Identified running process)\n\n---\n\n### 5. Conclusion\n\nThe collected evidence strongly suggests a security breach has occurred. The successful SSH login by 'root' from an external IP, coupled with the presence of a reverse shell script running in memory, indicates that an unauthorized actor may have gained privileged access to the system and is actively maintaining control or attempting further actions.\n\n---\n\n### 6. Recommendations\n\n* Immediately isolate the affected system from the network to prevent further unauthorized access or data exfiltration.\n* Conduct a full system scan for malware and rootkits.\n* Review all user accounts, particularly privileged accounts, for any suspicious activity.\n* Investigate the origin of the connection from `10.10.10.10` and the network path to `10.0.0.3`.\n* Preserve all collected forensic artifacts for potential further investigation or legal proceedings.\n* Implement enhanced network monitoring and intrusion detection systems.\n\n---\n**End of Report**\"\"\"\n),\n],\n role='model'\n) grounding_metadata=None partial=None turn_complete=None finish_reason= error_code=None error_message=None interrupted=None custom_metadata=None usage_metadata=GenerateContentResponseUsageMetadata(\n candidates_token_count=903,\n prompt_token_count=824,\n prompt_tokens_details=[\n ModalityTokenCount(\n modality=,\n token_count=824\n),\n],\n total_token_count=1727\n) 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-b243c028-e40d-46a3-9d28-734ad3b9fe97' author='ReportAgent' actions=EventActions(skip_summarization=None, state_delta={'report': \"## Digital Forensics Report\\n\\n**Case ID:** [Insert Case ID Here]\\n**Report Date:** 2023-10-27\\n**Prepared By:** ReportAgent\\n\\n---\\n\\n### 1. Executive Summary\\n\\nThis report details findings from a digital forensics examination of system artifacts. Evidence indicates a potential security incident involving unauthorized access and the execution of malicious code. Specifically, a successful SSH login by the 'root' user originating from IP address 10.10.10.10 was recorded. Network traffic analysis reveals a connection to IP address 10.0.0.3 on port 22 (SSH). Furthermore, memory analysis has identified a running process associated with a Python script named `reverse_shell.py`, indicative of a reverse shell being active.\\n\\n---\\n\\n### 2. Data Sources Examined\\n\\nThe following data sources were analyzed:\\n\\n* **System Logs:** Records of system events, including authentication attempts.\\n* **Network Packet Capture (PCAP):** Captured network traffic data.\\n* **Memory Dump:** A snapshot of the system's active memory.\\n\\n---\\n\\n### 3. Findings\\n\\n#### 3.1. System Logs\\n\\n* **Event:** Accepted password for root from 10.10.10.10 port 39202 ssh2.\\n* **Analysis:** This log entry confirms a successful authentication for the highly privileged 'root' account. The connection originated from the internal IP address `10.10.10.10` on port `39202`. The use of SSH is explicitly stated.\\n\\n#### 3.2. Network Packet Capture (PCAP)\\n\\n* **Observed Traffic:**\\n * Destination IP: `10.0.0.3`\\n * Destination Port: `22` (SSH)\\n* **Analysis:** The PCAP data indicates network communication directed towards IP address `10.0.0.3` on port `22`. This aligns with the SSH protocol identified in the system logs, suggesting that the SSH connection either terminated at this IP or was proxied through it.\\n\\n#### 3.3. Memory Analysis\\n\\n* **Process Found:** `/usr/bin/python3 reverse_shell.py`\\n* **Analysis:** The memory dump revealed an active process executing the Python interpreter (`/usr/bin/python3`) with the script `reverse_shell.py`. The name of this script strongly suggests it is designed to establish a reverse shell connection, allowing an external attacker to gain command and control over the compromised system.\\n\\n---\\n\\n### 4. Indicators of Compromise (IOCs)\\n\\nThe following Indicators of Compromise were identified:\\n\\n* **IP Addresses:**\\n * `10.10.10.10` (Source of SSH login)\\n * `10.0.0.3` (Destination of SSH traffic)\\n* **Ports:**\\n * `39202` (Source port for SSH login)\\n * `22` (Destination port for SSH traffic)\\n* **Processes:**\\n * `/usr/bin/python3 reverse_shell.py` (Identified running process)\\n\\n---\\n\\n### 5. Conclusion\\n\\nThe collected evidence strongly suggests a security breach has occurred. The successful SSH login by 'root' from an external IP, coupled with the presence of a reverse shell script running in memory, indicates that an unauthorized actor may have gained privileged access to the system and is actively maintaining control or attempting further actions.\\n\\n---\\n\\n### 6. Recommendations\\n\\n* Immediately isolate the affected system from the network to prevent further unauthorized access or data exfiltration.\\n* Conduct a full system scan for malware and rootkits.\\n* Review all user accounts, particularly privileged accounts, for any suspicious activity.\\n* Investigate the origin of the connection from `10.10.10.10` and the network path to `10.0.0.3`.\\n* Preserve all collected forensic artifacts for potential further investigation or legal proceedings.\\n* Implement enhanced network monitoring and intrusion detection systems.\\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='8a369699-1776-4db8-9c76-1da1b53dc03a' timestamp=1763919259.499246"
],
"ips": [],
"ports": {}
}
```